the cyberwire

Identity management and zero-trust: ISMG Virtual Summit

By Tim Nodar

Zero-days and vulnerabilities introduced post-compromise are particularly difficult to deal with. Electrosoft Services and the not-for-profit association ITPA-NCC hosted a summit on April 22nd that offered perspectives on how they might be better addressed through effective identity management and a zero-trust approach to security.

Identity management and a zero-trust approach to security not only help the defender. They complicate the attacker's task as well.

The importance of making the adversary work harder.

Dr. Ron Ross, a Fellow at the National Instute for Standards and Technology (NIST), opened the summit by pointing to the vast complexity of modern computers and networks. He noted that two classes of vulnerabilities—zero-days and vulnerabilities that a threat actor introduces after they've compromised your system—are particularly difficult to defend against. "Even our best scanning tools – they pick up a lot of these things – but there's a certain percentage of these types of things that are not picked up at all, these vulnerabilities that are never going to be seen by even the best scanning tools and all the threat hunting in the world," Ross said. "So, this is what's driving us to take more of an engineering focus."

Ross explained that much of the risk is shared and in the hands of other organizations, as seen in the SolarWinds campaign.

"I like to use a metaphor – above the waterline, below the waterline," he added. "You can think of it like in the ocean, most of the bad stuff that happens with icebergs and sharks is below the waterline. Above the waterline is where our consumers, our customers – that's where you work. You put in firewalls, you put in two-factor authentication, encryption technologies, all the controls and frameworks, you do your contingency plans. All these things are things you have control over as consumers."

"But below the waterline there's a whole other world down there that we call the system stack," he continued. "The applications, the middleware, the operating system, the firmware, the integrated circuits, all the network connectivity. All of that is the complexity that I was referring to earlier – the trillions of lines of code, the billions of devices, all of these ubiquitous connections around the globe bringing us together in this shared risk environment. So, we have to really pay more attention to what's going on below the waterline."

Ross advocated for a "multidimensional protection strategy" that can disrupt the adversary in space and time.

"You want to increase their work factor once they're inside," he said. "You want to limit their lateral movement. And you want to reduce the time they have on target to do damage. And then that second dimension of damage limitation will then lead us to a third dimension that we call 'cyber and system resiliency.' That's the ability to take a punch and not have the system go down for the count."

Specifically, Ross pointed to a zero-trust strategy with micro-segmentation to hamper the adversary's movement, and micro-virtualization with the ability to revert to a known-safe state to limit the adversary's time.

Zero-trust is about recognizing trust extensions.

Matthew Scholl, Chief of the Computer Security Division in the Information Technology Laboratory at NIST, explained that zero-trust is largely about identifying "trust extensions," and tracing them back to the foundational technologies that our trust assumptions are based upon.

"What it is, is we are going to leverage and double down on some of our trust roots, and really use them to assure the security in places where we don't have as much assurance," Scholl said. "And identity is a strong trust root that we are going to be leveraging not just now, as we've seen in our telework operations, but for zero-trust operations for the future."

Scholl added that most of our security measures are based in trust: we assume that the technology is working correctly.

"When we look at zero-trust architecture, a lot of the concept is to minimize those trust assumptions to just the very core, essential ones that we need to operate our businesses correctly," he said.

Issuing ID cards: a new approach to an old school way of managing identity.

Darlene Gore, Director of the Identity Management Solutions Division at the General Services Administration (GSA), discussed the US Postal Service's Point Pilot, a partnership with the GSA to allow Federal employees to obtain new or updated PIV cards (Personal Identity Verification cards) from nearby post offices. The pilot began with seven DC-area post offices, and Gore says the project has been a success.

"The progress of that point pilot has really exceeded our expectations, beyond expectation, and allowed us to rethink the way that we deliver the card-issuing services," she said. "So, there's some good stuff that's come out of the pandemic – it forced us to think differently and pivot on how do we continue to deliver these services?"

Gore added that the success of the pilot led them to look for other areas that they could streamline, and they're now in the early stages of looking at how to improve the Federal enrollment processes for GSA's customers.

Continuous Vetting Analytical Services: identifying authoritative sources.

Reid Baldwin, Director of the Enterprise Security Division at the DHS's Office of the Chief Security Officer, said that one of the things his office has been working on "access to personal information and identifying an authoritative source for that information."

"We're calling it 'Continuous Vetting Analytical Services,'" Baldwin said. "We're putting that in place so personnel security, when they vet these folks, they can make that proper risk decision on whether or not the person can have access to any of the DHS' resources, information, or facilities. So, to date, so far we've – through a SQL staging database and an XML web service interface that we developed – we've so far transferred one million identity records and one million credential records. And we will soon have a data sync between those two systems, because one is a legacy system, and we're also coming out this Fall with a new – hopefully getting a contract in place to stand up...a brand new system to help manage identities across DHS." ■

Please visit The CyberWire to view the original article: https://thecyberwire.com/stories/6d0f1cbe0d984f25889c034a8fd4ea68/identity-management-and-zero-trust-ismg-virtual-summit

---

About Elecrosoft Services, Inc.

Electrosoft

An award-winning government IT and professional services firm, Electrosoft delivers comprehensive technology-based solutions and services to federal civilian and DoD organizations, with a strong focus on cybersecurity. Founded on deep technical expertise, customer service excellence and quality that propels mission success, the company is celebrating its 20th anniversary in 2021! www.electrosoft-inc.com