Cybersecurity at Scale

Remote work, the shift to cloud environments, expansion of digital services and other trends have altered the threat terrain. ***Chris Radosh,*** *vice president and general manager for U.S. public sector at Trend Micro, discusses emerging tools and practical strategies for advanced threat protection.*

Considering Trend Micro's recent cybersecurity report, what threats should be top of mind for state and local governments?

Ransomware tops the list. Organizations need to consider both the cost of the actual ransom and the cost to recover compromised machines or endpoints. But the greater cost is service disruption. Peoples' lives and well-being depend on government services. We're also seeing more advanced persistent threats against cloud services and the automation and orchestration layers of cloud services. Many employees working from home lack security controls you would find in an office setting. Adversaries are exploiting those vulnerabilities to target cloud applications.

What high-level strategies are critical for a strong defense?

It boils down to three areas. First, define the capabilities you need to secure your environment. That depends on the maturity of your technical infrastructure, your risk appetite and your organization's mission, which dictates who you serve and the types of data you collect. Next, decide what you want to cover and how you want to tune that coverage to the type of infrastructure you're using. Last, examine your culture. Are you establishing a culture where security is front of mind and pervasive throughout the organization — not just IT?

What should organizations consider as they develop a security strategy for workloads and other functionality that they move to the cloud?

The first thing to understand is whether you're going to lift and shift on-premises workloads or have everything cloud native moving forward. Understanding your cloud strategy will inform your security approach. For example, if you're going to lift and shift a data center where applications are hosted on servers, your workload protection needs to be tuned toward server vulnerabilities, which are very different from vulnerabilities on laptops and desktops. Also, it's not just endpoints that are vulnerable. The automation or orchestration layer can also be an attack vector. Finally, it's important to have tools that monitor conformance to your cloud governance standards so you can avoid misconfigurations that expose your environment to attack.

What identity and access management (IAM) approaches help keep malicious actors at bay?

Multifactor authentication is an essential component of managing identity and access. Beyond that, organizations should review their approach to privileged access management. There have been a number of attacks where a compromised administrative password is used to escalate privileges and get access to sensitive data. Most IAM solutions haven't changed significantly in the last 15 years. They rely on legacy technology and things like passwords and vaulting. We encourage organizations to consider IAM solutions that leverage the security built into cloud architecture by design. Instead of vaults and passwords, cloud-native IAM solutions use temporal keys, which are used once and then expire. This event-based approach is much more powerful as organizations transition to the cloud.

How can organizations best use AI to sustain their security strategy over time?

AI can be very effective, but it's not a silver bullet. Because it's based on algorithms that are designed by humans with inherent biases, a human has to vet either the input or the output. That vetting can cause bottlenecks, so even if you have the best AI, you may be unable to scale human resources to manage everything AI can do. Organizations should use AI where it makes sense and within the constraints of the resources in their environment.

What do you anticipate in the next generation of threats and how can organizations prepare?

We're on the cusp of a broad rollout of 5G technology. With 5G you get roughly 10 times the bandwidth you have now. That's going to fuel edge computing and provide more bandwidth to transmit data. Very complex software is going to proliferate on these edge devices, because a lot more data can move between these endpoints and a centralized cloud repository. That in turn will compound the threat landscape dramatically. We can answer this scalability problem via a security abstraction layer. This next-generation technology abstracts and consolidates all the pertinent telemetry and value from security tools and makes analysis and response much more efficient. It's just around the corner and organizations should start planning for it now.

Learn more at **Carah.io/GT-Dec-TrendMicro**

CYBERSECURITY CAN BE BEAUTIFUL.

Cyber threats are malicious, dark, and intrusive.

As the world becomes increasingly complex, you need connected solutions and visibility across your entire IT infrastructure.

Trend Micro enables you to protect, detect, and respond to threats faster—so you can be more resilient. Because when you can see the big picture, cybersecurity can be beautiful.

That's The Art of Cybersecurity.
TheArtofCybersecurity.com

TREND MICRO™

This artwork illustrates the global shift of Trend Micro customers from on-premises to SaaS—where we deliver faster updates, less operational impact, and better security. Created with real data by artist Brendan Dawes.