MeriTalk
Improving the Outcomes of Government IT

ciena

Encryption's Vital Role in Protecting Data in Transit

For now—and perhaps enduringly—the work of the federal government is no longer happening primarily in large office buildings in the Washington, D.C. area. Rather, it is taking place in many hundreds of thousands of homes across the region as government employees continue to work remotely during the coronavirus pandemic.

And crucial to the federal government's cybersecurity mission, that work is being done via myriad government and personal devices, and across a wide variety of network connections that all represent a sharp ramp-up in possible attack vectors.

So, while the workplace has changed, the cybersecurity threat has only grown larger—not only because of home-based connections and devices, but also as a result of the growing capability and audacity of adversaries who sense profit potential in the midst of the public health crisis.

"We know that our adversaries see opportunities in these tumultuous times," said Kevin Cox, program manager of the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation program, in an interview with MeriTalk.[1]

Government agencies are not the only ones who have had to shore up their cyber defenses to meet growing attack threats. Large corporations that hold Personally Identifiable Information (PII) about their customers have also been ripe targets for attack.

Shifting attack trends

For government and the private sector, however, the nature of cyber intrusions has been changing over the last few years. While malware attacks spiked in recent years, the trend appears to have leveled off recently. In 2019, over half (51 percent) of attacks used malware-free techniques, compared to only 40 percent of attacks using malware-free techniques in 2018, according to a report from the cybersecurity firm CrowdStrike released earlier this year.

As governments and businesses expand their use of Virtual Private Network (VPN) capabilities to support telework, attackers have followed the same path. "In 2020, we are seeing targeting of VPN vulnerabilities," declared CISA's Bryan Ware, assistant director for Cybersecurity, in an interview.[2]

The agility of adversaries in targeting the next perceived weakness in the security landscape is causing the cybersecurity industry to adapt and put in place new tools to meet the new horizon of threats—one of which is as old as networking itself, but can get lost in the more familiar lineup of phishing and malware threats.

Less visible than many cyber threats in the news these days is mayhem that can happen within the physical layers of the network—in particular, the optical cables that transport data. Cyber adversaries can steal data transiting these cables without the sending or receiving parties ever becoming aware of the theft.

[1] https://www.meritalk.com/articles/cio-crossroads-federal-it-in-the-covid-crisis-cdm-edition/
[2] https://www.meritalk.com/articles/cio-crossroads-federal-it-in-the-covid-crisis-cisa-cyber-edition/

Optical encryption

Ciena offers WaveLogic™ Encryption, designed to protect up to 800Gbps of bandwidth in transit through optical cables. WaveLogic Encryption is the industry's first programmable 100G-800G optical encryption solution. It builds on years of experience in coherent optics and transport-layer encryption, delivering a simple-to-implement, always-on encryption solution over distances from metro to submarine.

Now it is easier than ever for customers to deploy 10G, 100G, 200G, 400G and even up to 800G encrypted services across their entire infrastructure, eliminating costly separate encryption boxes per application.

WaveLogic Encryption provides a cost-effective, simple-to-implement bulk-encryption solution that protects all in-flight traffic on the network as it spans the globe. It offers MyCryptoTool—a simple-to-use, dedicated encryption management portal designed for distributed management of the network. This enables the owner of the critical data, the end-user, to independently manage the encryption security parameters and alarms of their encrypted services remotely.

Optical encryption—engineered by Ciena's WaveLogic modem and demonstrated in this video presentation—protects against any cyber breaches that may occur. That is because the high speed encryptor masks all the optical data and overhead that is in transit and renders ineffective any attempts to steal it.

Learn more about Ciena's WaveLogic Encryption:
https://www.ciena.com/insights/what-is/What-Is-Optical-Encryption.html