AKAMAI

Achieving a global perspective on cyberthreats

Insights into worldwide security trends and incidents are a game-changer for securing government networks

Rob San Martin | Akamai

New cyberthreats are always arising. One development that is particularly concerning for all agencies is the discovery that adversaries are working together to target government systems and critical infrastructure. Countries like Iran and Russia used to operate in an independent fashion, but they are now sharing expertise and resources and joining forces to maximize the depth and breadth of attacks, which is complicating the challenge for network defenders.

Such alliances dramatically expand the size and intensity of attacks and make it increasingly difficult to identify who is behind them. Fortunately, industry leaders are working closely with government to bring technology and strategies into play that will enable agencies to protect against even the most sophisticated threats.

Bringing tailored solutions to agencies

Akamai has been providing cybersecurity technology and services to the government for over 25 years, particularly excelling in the area of cyberthreat identification and mitigation. Akamai's Connected Cloud has worldwide visibility and identifies cyberattacks at an unmatched level, filtering by size, scope and scale.

Our insights give us the ability to help government agencies take appropriate action. We bring tailored solutions to agencies before they're attacked and recommend the best way to respond because we've seen the signatures and we've seen countless attacks play out elsewhere.

Akamai processes over 11 trillion Domain Name System requests a day, and that vast amount of activity helps us identify prevailing trends in security. According to our internal threat intelligence, 60% of distributed denial-of-service attacks in 2023 had a DNS component. Akamai's DDoS protection is built on dedicated infrastructure to protect agencies' internet-facing applications and systems while maintaining fast, highly secure and always available DNS.

A solid foundation for a zero trust strategy

The executive branch of the U.S. government has maintained that moving to zero trust is essential to operating securely in today's threat landscape. Independent of an agency's use of legacy systems or software as a service and regardless of whether employees are on-site or remote, Akamai's zero trust solutions are built to complement the specifics of any IT environment. Our visibility into assets, access and network flows provides a solid foundation for a successful zero trust strategy, and in the event of a breach, our expertise can help agencies hunt down the most evasive threats and limit lateral movement.

We believe we are uniquely positioned to handle large-scale attacks and keep adversaries away from agencies' infrastructure without affecting daily operations or the delivery of public services. Our experts help agencies modernize and harden key assets to ensure that the government's mission-critical capabilities are secure regardless of what adversaries throw at them. ■

Rob San Martin is vice president of the public sector at Akamai.