Extending zero trust down to the file level

Agencies should assume users, devices and even files are malicious until proven otherwise

Michael Hylton
Senior Director of Government Sales, OPSWAT

WITH THE RISE IN REMOTE WORK and the changing nature of cyberthreats, agencies must adopt a new mentality and approach to cybersecurity. That begins with understanding that devices are connecting to government data and systems from outside a traditional firewall, and users are likely interacting with multiple cloud-based platforms and services. Securing the cloud infrastructure may not be an agency's responsibility, but securing government data is.

Agencies can achieve their security goals by combining zero trust with a software-defined perimeter. A zero trust mindset involves authenticating users and also authenticating and validating any devices that connect to an agency's network. Before a desktop or laptop is allowed access to a government system, the agency must ensure that the device meets its requirements for IT security, such as having an encrypted password, and contains nothing malicious, such as keystroke loggers.

Refining security protocols

A software-defined perimeter integrates proven, standards-based security tools to create the ideal foundation for zero trust. When used together, those two approaches give agencies the granularity to customize their security protocols. For example, the IT team could allow USB mice but not USB thumb drives that can store data, and they could block potentially unwanted applications that anti-malware engines might not identify as malicious, such as bitcoin-mining or file-sharing apps.

Zero trust is a mindset rather than a specific group of tools. The National Institute of Standards and Technology's Special Publication 800-207 on zero trust architecture advocates taking a holistic approach to authenticating devices and users and extending that attitude to agency assets, services and workflows.

Ultimately, IT administrators need to be able to say they know the user and trust his or her device enough to allow access to a resource such as email or a database that's behind a firewall or in the cloud. When a device fails to meet security requirements, agencies should help the user update the device and any applications that could be vulnerable to attack.

Shutterstock/FCW Staff

The risks embedded in files

It's a sobering truth that a single file can bring down a network, halting its operations and risking the loss or exposure of sensitive data. Malware and viruses can be embedded in documents that agency employees exchange daily, such as PDF and Word files.

Agencies should apply a zero trust mentality to every file and assume that

> **Malware and viruses can be embedded in documents** that agency employees exchange daily, such as PDF and Word files.

it's malicious until proven otherwise. At OPSWAT, we recommend sanitizing files by breaking them down and rebuilding them from the ground up, leaving nothing behind that could potentially be used for malicious purposes. For example, a PDF file of a résumé doesn't need to have active Java content. Instead, agencies should filter that out before allowing the human resources team to review the résumé.

OPSWAT applies deep data sanitation, or content disarm and reconstruction (CDR), to decompose files into their discrete components for analysis to ensure their integrity and supports over 100 file types. Additionally, our proactive DLP CDR can scan for sensitive data, such as personally identifiable information.

Our motto has always been trust no file, trust no device. By assuming that a user, device or file is not safe until proven otherwise, agencies can reduce the risk of cyberthreats and prevent the loss of valuable data. ■

Michael Hylton is senior director of government sales at OPSWAT.