Don't Trust: Verify

Implementing Zero Trust involves both implementation of technology, but also a shift in culture and attitude toward cybersecurity.

Don Maclean
Chief Cybersecurity Technologist
DLT

If you haven't suffered a cybersecurity breach, you soon will: That's one of the underlying tenets behind the Zero Trust approach to cybersecurity.

The "moat-and-castle" approach to security does not work. For confirmation, look no further than the recent intrusions affecting our nation's critical infrastructure: Kaseya, the Colonial Pipeline hack, the venerable the Office of Personnel Management (OPM) hack of 2015 and the biggest and most sophisticated of all, the Sunburst intrusion.

John Kindervag coined the term "Zero Trust" while working at Gartner, to describe the phenomena of the disintegrating network perimeter – accelerated by the pandemic – and the associated failure of traditional network-perimeter defenses.

Today, the term arises constantly, but what exactly is Zero Trust? It is a philosophy and set of security principles based on the acknowledgment that we need to re-think security from the ground up. Obviously, this is a tall order, but the advent of cloud computing offers a rare chance to deploy completely new models of information technology as well as security. There are many approaches to Zero Trust; let's look at some of the more common facets of this concept.

Visibility: Data, Traffic and Devices

If you can't see it, you cannot protect it. Data-flow diagrams, Secure Sockets Layer (SSL) decryption, and device management and discovery are all critical aspects of visibility, which underpins all other aspects of security, especially in a Zero Trust environment.

Network Architecture

Kindervag states, "The actual design of a Zero Trust network should be based on how transactions flow across a network and how users and applications access toxic data." This approach applies equally to on-premise network design and cloud architecture. It's a relatively new and different approach to network architecture, and it may take time for technical professionals to learn and implement. Micro-segmentation is a key element here.

Automated Incident Response

If you assume your organization will be breached, automate response to intrusions. Micro-segmentation is essential to this component of the Zero Trust approach.

Zero Trust is a philosophy and set of security principles based on the acknowledgment that we need to re-think security from the ground up. Zero Trust is not a product or specific technology and the advent of cloud computing offers a rare chance to deploy completely new models of information technology as well as security.

Threat Intelligence

Often overlooked, threat intelligence is a key part of a Zero Trust implementation. Threat intelligence lets you anticipate breaches and protect against them in advance. You may not stop every breach, but you will stop some if you stay ahead of the game.

Data Protection

In real estate, the mantra is "location, location, location." In data protection, it is "encryption, encryption, encryption." Data is most organizations' most valuable asset, so encrypt it in place, encrypt it over the wire (even on the "internal" network) and use file integrity monitoring and remote deletion and encryption.

Identity and Access Management (IAM)

A one-time login with user ID (Identity) and password is only the beginning. Multi-factor authentication (MFA) is an important step up, and continuous identification and authorization are really the essential elements of IAM in a Zero Trust context.

Application Security

Application security includes use of secure code, knowing and validating your application inventory, and a solid approach to developing secure applications: DevSecOps. DLT's Secure Software Factory is an excellent comprehensive approach to creation and maintenance of secure software in any organization.

Zero Trust is a concept and strategy, not a product or specific technology. Implementing Zero Trust involves both implementation of technology, but also a shift in culture and attitude toward cybersecurity. Keep both elements in mind as you pursue your journey into Zero Trust.

DLT has recently launched the Zero Trust Hub to guide public sector agencies through Zero Trust implementation. Access our free resources and tools to better understand Zero Trust from multiple perspectives, and to identify common themes that emerge from the major frameworks and initiatives. Get insights on common challenges and sought-after solutions addressed by the Zero Trust framework.

Learn more at Cybersecurity-Solutions@dlt.com. ■

About The Author

Mr. Maclean, Chief Cybersecurity Technologist with DLT, has extensive experience working with U.S. Federal agencies, having managed security programs for U.S. Department of Justice, U.S. Department of Labor, Federal Aviation Administration, Federal Bureau of Investigation, and U.S. Department of the Treasury. He contributed to the Cybersecurity Solarium Report, whose recommendations appeared in the National Defense Authorization Act (NDAA). He is certified as a Forrester ZTX (Zero Trust eXtended) Strategist and Cybersecurity Maturity Model Certification (CMMC) Registered Practitioner.