Cybersecurity News

NEWS AND INFORMATION TO HELP PROTECT COMPANIES AND EMPLOYEES

OCTOBER 2021

Zero trust pushes past the enterprise to maintain security

The modern security environment includes remote users (many of whom are using their own devices) and cloud-based assets located outside of the enterprise-owned network boundaries. Organizations are increasingly turning to a zero trust security strategy because the network location is no longer seen as the prime component to the security posture. Zero trust goes beyond network perimeters to focus on users, assets, and resources to protecting resources (e.g., assets, services, workflows, network accounts), instead of just focusing on network segments.

- It assumes no implicit trust is granted to assets or user accounts based solely on their physical and/or network location or asset ownership (enterprise or personally owned).
- Authentication and authorization (both subject and device) are discrete functions to be performed before a session is established.[1]

How it works

To meet security demands, zero trust:

- Mitigates security vulnerabilities through learned trust by monitoring user access and authorizations.
- Addresses identity management based on real-time variables—not just who the user claims to be, but verifies permissions, what the user is accessing, and from what devices and networks.
- Enables conditional access that can be tightened or relaxed based on unique needs. Access can be challenged based on abnormal authentication attempts and denied when attempted through untrusted devices or networks. Multi-factor authentication (e.g., biometrics or keys) can also be required for sensitive access points.
- Moves toward provision authoritative identities and credentials and away from password usage that simply presents the correct combination of credentials. User identification includes the user, device, and network that are aligned with permissions granted for any resource the user is trying to access. The requirement of various forms of multi-factor authentication may be used to support this approach.[2]

The zero trust concept addresses the reality of both the current and future work distributed, remote-work environments.

[1] National Institute of Standards and Technology (NIST). *SP 800-207 Zero Trust Architecture*. NIST. August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final.

[2] Bhargava, Rajat. *Why The "New Normal" Requires Zero Trust*. Forbes. February 9, 2021. https://www.forbes.com/sites/forbestechcouncil/2021/02/09/why-the-new-normal-requires-zero-trust/.

(continued)

What is zero trust?

In 2010, John Kindervag (who worked at Forrester at the time) introduced the concept of zero trust: trust nothing, verify everything. This strategy assumes that every device, user, system and location—inside or outside of the organization—cannot be trusted and needs to be verified.

Today, this strategy is a touchstone for how organizations approach security.

1. Always authenticate and authorize
2. Apply the least-privilege principle
3. Continuously monitor and adapt

Source: Ram, Sree. *Why implementing Zero Trust is more important than ever*. Security Boulevard. July 23, 2021. https://securityboulevard.com/2021/07/why-implementing-zero-trust-is-more-important-than-ever-before/.

Identity and access management (IAM): one digital identity for each item and user

To administer user access across an enterprise and ensure compliance with corporate policies and government regulations, organizations use IAM tools and technologies to track each user's role and activities and generate reports on those activities.

IAM defines and manages the roles and access privileges of network entities—both users and devices—with the objective of establishing one digital identity per individual or item.

- Users: customers, partners, and employees
- Devices: computers, smartphones, routers, servers, controllers, and sensors

The goal is to grant access to users and devices in a given context (e.g., onboarding and offboarding users and systems, permissions authorizations).

Learn more about IAM by visiting our Insights page at: https://www.mufgamericas.com/insights-and-experience/trending-topics/what-iam-identity-and-access-management-explained.

Source: Strom, David. *What is IAM? Identity and access management explained.* Originally published by CSO Magazine. April 8, 2021. https://www.mufgamericas.com/insights-and-experience/trending-topics/what-iam-identity-and-access-management-explained

Cyber insurance as part of the ransomware crime cycle

According to the U.S. Government Accountability Office, as the risk of ransomware attacks increases, more organizations are opting for cyber insurance (from 26% in 2016, to 47% in 2020); meanwhile, breach insurance premiums are also increasing.

Successful breaches mean more ransomware attacks. Despite the urges of U.S. law enforcement to not pay ransoms, many organizations facing costly downtime and the implications of sensitive data going public choose to comply with attacker demands. However, paying ransoms equates to greater incentives for more attacks, perpetuating the crime cycle. Another layer adding to the ransomware situation: criminals also may target cyber insurance companies. The goal is to obtain insured client information to then target the insured organizations, knowing there is a higher likelihood they will pay ransoms.

To help handle a ransomware attack, organizations can get expert help from reputable consultants. These experts may be able to help avoid the need to pay a ransom by finding flaws in the ransomware or recovering the keys to decrypt data without paying the ransom.

Gnanaprakasam, Pandian. *Ransomware and cyber insurance: What are the risks?* Help Net Security. August 12, 2021. https://www.helpnetsecurity.com/2021/08/12/ransomware-cyber-insurance/.

Cybersecurity first: do your part. #becybersmart October is national Cybersecurity Awareness Month

Every October in the U.S., the Department of Homeland Security's Cybersecurity and Infrastructure Agency (CISA) and National Cyber Security Alliance (NCSA) lead observance of National Cybersecurity Awareness Month (NCAM). The 2021 theme focuses on empowering organizations and individuals to own their roles in protecting cyberspace. Highlights of this month's promotions and outreach:

- Use security practices and cyber hygiene to keep information safe (e.g., strong passwords, multi-factor authentication, data backups, updating software).
- Fight phishing with a wary view of emails, texts, and chat boxes from strangers and other unexpected contacts. Think before clicking on emails, links, and attachments.
- Develop a cybersecurity-first mindset by training during employee onboarding and providing tools to keep staff safe. With new devices and apps, consider security and privacy settings and update default passwords.

For more information about how to promote Cybersecurity Awareness month, visit the National Cybersecurity Alliance Stay Safe Online site: https://staysafeonline.org/.

Source: National Cyber Security Alliance. Stay Safe Online. https://staysafeonline.org/cybersecurity-awareness-month/theme/.

The information above is provided as a convenience, without warranties of any kind and MUFG Union Bank, N.A. disclaims all warranties, express and implied, with respect to the information. You are solely responsible for securing your systems, networks, and data. You should engage a qualified security expert to advise on your specific needs and requirements.

This *Cybersecurity News* contains news and information designed to help protect your company and employees.