EQST insight

Seven access privilege control strategies to respond to cyber security threats in the WFA era

■ Outline

Many changes in daily life have occurred due to COVID-19. In particular, the office working environment in the IT field that has been maintained as a tradition for a long time has changed, causing inconvenience. Remote work has gradually accelerated and expanded, and is now taking its place as a sustainable hybrid environment.

A hybrid environment is realized when IT technology is actively used. Various remote meetings and chatting programs are used as tools for non-face-to-face work, and collaboration using cloud technology is also taking place.

That is, a complex hybrid environment with many access channels means that a New Normal is required. It is high time that a new endpoint security strategy should be needed, e.g., how users access the network, familiarization with security policies corresponding to various user-equipment configurations, and appropriate control methods in changing environments.

■ New Normal era due to WFA

The hybrid work environment refers to WFA (Work-From-Anywhere); people can work anywhere, and security in the WFA era must be able to protect moving data. As POLR, which attackers mainly target to steal corporate data and assets, is also changing, the security team's IT risk management priorities must also change.

For the security of the existing IT industry, the security environment was configured with top priority given to virus vaccines and firewall. However, virus vaccines cannot detect about 60% of all cyber attacks, and it is difficult to install vaccine software in the IoT and OT (Operation Technology) environment. Also, the firewall policy is also often incapacitated or not fulfilling its role due to the increasing cloud and distributed computing environment.

In addition, the most difficult issue in building a WFA environment is endpoint security. In a typical corporate network system, a firewall is used to block access from the outside to the inside. However, if a user connects to a VPN in a situation where endpoints are infected with malware due to leakage of stored data and accounts, the malware may bypass the firewall, enter the internal system and infect the network.

Therefore, in the WFA environment, it is becoming difficult to prevent external attacks with existing security policies, and policies and solutions are required to prepare for various security threats.

Seven security strategies based on access privilege control

Organizations that have built a digital environment must address security gaps and actively manage threat elements. Recently, IT security proposes a core security solution model called 'Zero Trust' based on identity as a network security strategy to respond to newly emerging cyber threats.

Zero Trust is a cyber security model based on the premise that 'nothing is trusted'. It performs thorough verification when a user or device requests access, and grants only minimum privileges during the verification process before allowing access

In order for a company to build core architecture configuration elements of Zero Trust, Privileged Access Management ' (PAM) is essential. As the privileged access management solution is designed to protect the most critical systems and assets at the core of an enterprise, it can optimize the access policy.

The 2022 Cybersecurity Survival Guide[1] presents seven security strategies based on privilege control to more effectively respond to the latest security threats, e.g., the rapidly changing office/work paradigm, increasing threat situations, and sophisticated cyber crime tactics.

1. Protection of privileged accounts
Automate search and protection of all privileged accounts
Store and manage all privileged credentials
Enforce adaptive access controls
Continuous monitor all sessions related to privileged accounts and privileged activities
Apply multi-factor authentication (MFA)
Remove shared accounts
Remove/delete built-in passwords

2. Secure remote access
Broker all connections through a single access path
Proxy access for all access paths and other important software
Network zoning and segmentation
Minimum privilege access control
Automatically control management credentials
Implement BYOD management
Application-level micro-segmentation
Monitor, manage and audit all sessions started from remote

3. Apply endpoint privilege management
Apply minimum privilege in all environments
Control specific Unix and Linux commands
Separate duties and privileges
Apply advanced application control and minimum privilege application management
Strengthen security by blocking S/W execution and installation

[1] https://www.paloaltonetworks.com/resources/techbriefs/cybersecurity-survival-guide

4. Vulnerability management and hardening

Strengthen the IT environment
Strengthen and protect BIOS
Implement continuous vulnerability management

5. Tamper-proofing mobile and remote endpoints

Implement disk encryption
Use built-in hard disks
Seal devices
Require distribution and use of computer security cables
Tamper-proof BIOS

6. Strengthen service desk security and privilege management

Powerful privileged access control for all remote support sessions
Client segmentation
Implement credential security best practices
Enable independent support for platforms
Simplify workflows and integrated them with other service desk tools
Distribute endpoint privilege management together with the remote support tool

7. Remote user penetration (mock hacking) test

Private and home-based network
Devices owned by other companies
Individuals and IoT devices
Personal e-mail addresses that may exist in the same BYOD asset
Cell phone numbers
Non-business social media accounts

The biggest causes of security incidents that require the above seven security strategies are internal users' reckless abuse of privileges and work PCs infected with ransomware. To cope with this, it is necessary to strengthen security by controlling the user environment and endpoint privileges.

Establishment of the minimum privilege environment of the endpoint, which is the user environment, aims to define detailed items such as 'when', 'where', 'who', and 'what', and based on this, control the execution of commands and applications appropriate for business purposes and privileges, e.g., removing the administrator's privilege with regard to the user environment. Application of endpoint privilege management is an essential security tool to achieve this goal, and it should be the top priority for security because it is effective in blocking an arbitrary execution environment, especially a ransomware execution environment.

■ Practical implementation of the Zero Trust principle

To implement the seven security strategies presented above, the Zero Trust principle defined in NIST SP 800-207 must be pursued in a smart and practical way, and the ability to restore and respond to changes must be maintained. Also, a perfect Privileged Access Management Platform must be provided to implement the security environment required for remote work and digital transformation.

〈Table 1〉 The Zero Trust principle defined in NIST SP 800-207

The Zero Trust architecture is a corporate cyber security plan using the concept of Zero Trust, and includes relationships between components, workflow design, and access policy. In addition, Zero Trust enterprise means the network infrastructure (physical and virtual) and policy that exist in the enterprise by implementing this Zero Trust architecture.

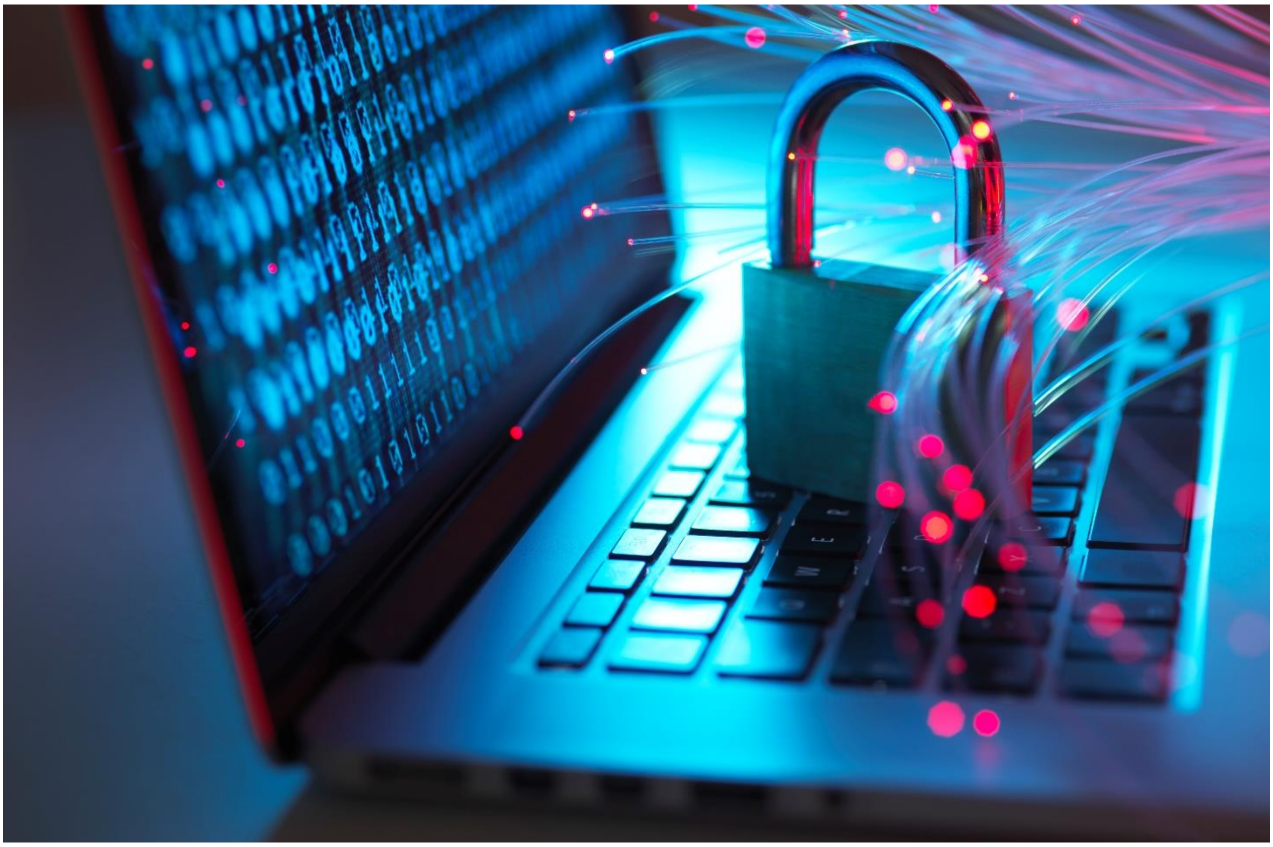
* Source: US NIST, "Zero Trust Architecture", 2020[2]

[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

Closing remarks

Platforms that can be built individually or integrated must support on–premise, cloud, and hybrid environments. They must be built for each solution or built together as part of an integrated platform to enjoy the effect of security synergy and strengthen security to a higher level.

In fact, Company A has introduced and is operating the endpoint solution PAM (Privileged Access Management), and in particular, it is controlling the access privileges of remote users and strengthening the security of the user's work PC environment. Through this, it is possible to perform governance and compliance that satisfies the Zero Trust principle, and more effective IT security can be implemented.



> We have definitely entered the era of "Zero Trust", and it is necessary to build an improved security environment according to the changes in technology that are happening around us.

■ Reference site

url: https://ponemonsullivanreport.com/2020/05/the-state-of-endpoint-security-risk-its-skyrocketing/