Tomorrow, Together

KDDI

Has perimeter-based security reached its limits? Steps globally expanding companies should take to deploy "Zero Trust"

Steps in Deploying "Zero Trust"

INTRODUCTION

Overseas Locations of Japanese Companies – The Targets of Cyber Attacks –

Vicious cyber attacks continue to wreak havoc. In an effort to protect themselves from these threats, many companies have fortified their defenses, but there are still several blind spots. And one of them is their overseas locations. According to a survey by Teikoku Databank*1, as of 2023, 28.1% of Japanese companies have expanded overseas. As companies expand abroad, they must not forget the increase in the scope of security that needs to be covered. It is very dangerous to underestimate the risk and think that "It is ok, they don't have as important information as the headquarters". Malicious attackers infiltrate from the most vulnerable points and launch critical attacks on important locations through the internal network. Any security incident would be considered a company-wide issue, risking significant damage such as loss of opportunities, stock price decline, and loss of trust from customers. It is crucial to properly consider beforehand security measures not just for the domestic headquarters but also for overseas locations.

CONTENTS

1. What is the popular "Zero Trust Security"?.....02
2. Zero Trust deployment in Japanese companies is still ahead....03
3. Misconceptions about Zero Trust Security: "Ask the Experts" 04
4. Points to note in security for overseas locations.....05
5. How companies can achieve Zero Trust Security.....06
6. If overseas locations take the first step themselves.....07

S&J Co., Ltd.
President and
Representative Director
Mr. Nobuo Miwa

1. What is the popular “Zero Trust Security”?

As new security threats continue to emerge, the concept of “Zero trust security” is gaining a lot of traction. This was prompted by the increased use of cloud in corporate networks and the rise of telework due to the COVID-19 pandemic.

In the traditional "perimeter defense-based security" model, based on the basic principle of "safety on the inside, dangerous on the outside”, various defense measures were taken to prevent attackers from entering from the outside to the inside of the company (Figure 1).

However, as the use of external clouds and connections to the internal network from the outside, like from home, grew more and more common, it becomes difficult to completely prevent breaches at the boundary. Once an intrusion occurs, the perimeter defense model, which lacks internal defense measures, risks allowing free access to company resources.

Suspect and investigate every access before allowing

On the other hand, Zero Trust is based on a “trust-nothing“ model. The principle is to always assumes that every access could potentially be from an attacker. Regardless of whether it's from inside or outside the company, it investigates each access based on information such as the employee's ID or the computer's MAC address to determine whether to allow use (authentication) and how much access to grant to the internal system (authorization). Even for legitimate use by regular employees, only the minimum necessary permissions are granted.

Information related to the security of employees and terminals is constantly collected and updated. For example, even if it's a legitimate employee or terminal, detecting suspicious behavior like attempting to access a database unrelated to work in the middle of the night can trigger temporary control, such as limiting the range of access within the company.

Even if an employee's computer is infected with malware, it cannot freely access the internal network. By dynamically controlling the use of employees or terminals that behave differently than usual, suspecting infection, the risk of malware spread can be mitigated.

Most importantly, with Zero Trust Security, both domestic and overseas locations can be managed under the same security policy without distinction.

Therefore, it is suitable for managing security in environments where it is difficult to grasp the exact situation, such as when employees are not in the office.

However, Zero Trust Security is not without its challenges. It is important to note that effectively utilizing it requires more complex operations than the perimeter defense measures.

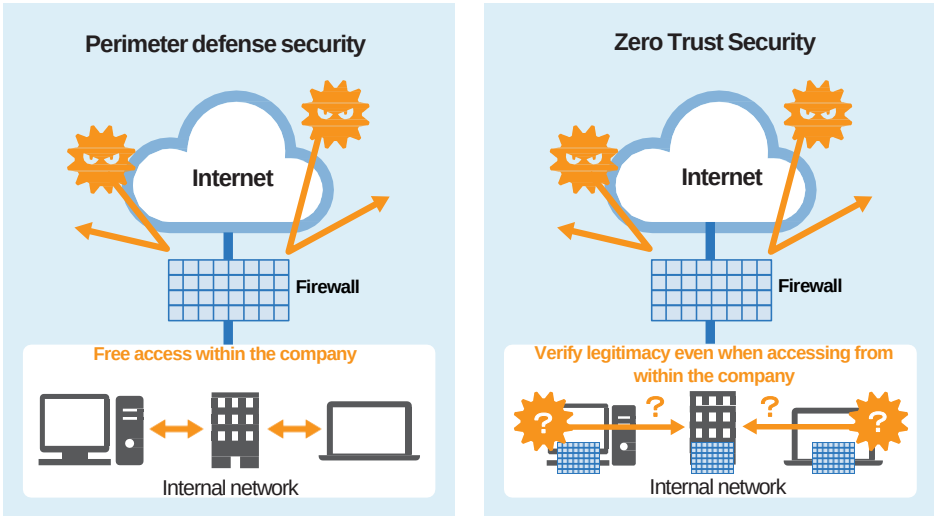


Figure 1: Unlike perimeter defense that protects between internal and external network, Zero Trust security does not trust any access, whether internal or external, and only allows use after verifying the validity.

2. Zero Trust deployment in Japanese companies is still ahead

Zero Trust Security and its security model able to address the limitations of perimeter defense is gaining high traction among many Japanese companies.

According to the “Network Equipment Usage Survey 2022” published in December 2022 by “Nikkei NETWORK”, more than 80% of respondents have heard the term “Zero Trust” *2. Furthermore, over half of the respondents stated that they have heard of it and understand its meaning *3 (Figure 2).

Companies are continuously considering its deployment

However, when it comes to actual deployment, it seems there is still a long way to go. According to the same Nikkei NETWORK survey, only about 19% of respondents have deployed tools and services related to Zero Trust, and only a mere 4.3% have completely switched to this model *4.

In fact, the adoption of Zero Trust Security by Japanese companies lags behind globally. According to the "Cyber Risk Index" international awareness survey published in May 2023 by Trend Micro Corporation (for the second half of 2022), the proportion of companies that have "launched proactive Zero Trust projects" is below the global average, ranking 27th out of the 28 countries surveyed ※5

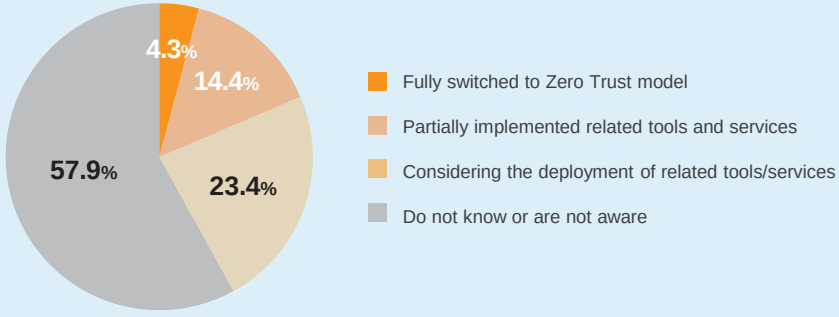
However, this does not mean there is no intention to implement it at all. According to the "2023 Corporate IT Trends Survey Report" released by the Japan Information Systems Users' Association, among 31 new technologies listed including AI (Artificial Intelligence), Public Cloud, AR (Augmented Reality), and VR (Virtual Reality), "Zero Trust" ranked first with 35.0% of respondents considering its deployment ※6.

.

Have you heard of the term "Zero Trust"? (Number of respondents: 923)

Source: Nikkei BP “Nikkei Network” December 2022 Special Collection
“Network Equipment Usage Survey 2022” p.39

Are tools and services related to Zero Trust being implemented or considered at your workplace? (Number of respondents: 764)



Source: Nikkei BP “Nikkei Network” December 2022 Special Collection
“Network Equipment Usage Survey 2022” p.39

Figure 2: Awareness and Deployment Status of Zero Trust Security in Japanese Companies

Interview

3. Ask the experts Misconceptions about Zero Trust Security

How does the current situation of Japanese companies, interested in Zero Trust but hesitant to deploy it, appear in the eyes of an information security expert? Nobuo Miwa, President and Representative Director of S&J Co., Ltd., a leader in Japan's information security business, raises an alarm about the recent perception of Zero Trust Security.

It seems that the term "Zero Trust Security" has taken on a life of its own in Japan. Many companies think that just by adopting the concept of Zero Trust Security, their security will be foolproof and benefits will be gained, as if it was a cure-all magic. This is a major misconception and is just a fantasy.

More effort should be spent comparing to perimeter based models

Zero Trust, and the “trust-nothing“ model, require more effort than perimeter-based models. It involves implementing stricter access controls, micro-segmentation to finely divide internal networks in order to achieve better security limitations, and constant (24/7) log monitoring. If you're serious about deploying it, Zero Trust Security demands significant effort. It's not as simple as just installing one tool.

Cyber attacks have increasingly become more and more sophisticated even before the COVID-19 pandemic. The essence of security lies in properly understanding the information assets that need protection and implementing appropriate measures. The reality is that Japanese companies are just beginning to realize that the emergence of Zero Trust Security means they need to strengthen their security measures even more.

Mr. Nobuo Miwa President and Representative Director of S&J Co., Ltd.

Leading the information security industry, including founding LAC, a company providing security solution services. He has served as a Ministry of Internal Affairs and Communications CIO Advisor since 2009, and also under many other government-related committee roles. Currently, he is the President and Representative Director of S&J, an independent security company he founded.

Understand the unique characteristics of overseas locations

When thinking about strengthening the security at overseas locations, which tend to be a blind spot, the first thing to consider is the organizational characteristics unique to overseas locations. Unlike domestic locations, where most of the workers are Japanese and therefore easy to control, local employees working at overseas locations come from a variety of backgrounds, and in many cases, have fundamentally different ways of thinking and working.

Interview

3. Ask the experts Misconceptions about Zero Trust Security

Unless the employees' evaluations or salaries reflect this, it's hard to effectively implement governance.

It may be hard to believe, but it's not uncommon to arrive one morning and find out that all the computers in the factory have been stolen. Therefore, instead of thinking "this person is fine" and making exceptions, it's necessary to finely limit access in the system, thinking that "Mr. A only needs this information for his job, so let's only give him these permissions". Simply spreading awareness through guidelines is often ineffective.

Additionally, attention must be paid to maintenance contractors and anyone who physically access overseas locations.

In fact, there have been instances where maintenance contractors breached the network. They managed all company resource information through Windows Active Directory (AD) * domain controllers, and maintained them using Windows Remote Desktop, logging in remotely from a distance with just ID/password authentication. And those IDs/passwords were compromised.

Once ID/password information is leaked externally, there's always a risk of it being misused.

When dealing with important information, multi-factor authentication should ideally be used. Care should also be taken when hiring maintenance contractors. While local procurement is unavoidable, measures such as seeking maintenance contractors who operate globally from Japan, or selecting local contractors who can provide security services at Japanese standards, are essential to prevent such incidents.

*Windows servers come standard with this feature, which provides directory services that centrally manage IT asset information within a company, such as users, computers, PCs, printers, and applications

4. Points to note in security for overseas locations

How should security be enhanced at overseas locations? Instead of uniformly adopting solutions like a complete set of ID management or EDR (Endpoint Detection and Response) tools, it's crucial to accurately identify what information assets each overseas location needs to protect and what are the appropriate security measures.

From a security perspective, locations can be broadly classified into two types: those with factories and those without.

In office environments without factories, the main focus is on email-based work, phishing emails and attachments are the primary surveillance targets. In countries or regions with high awareness of personal data, such as the EU or North America, measures such as implementing systems to manage personal data may be necessary, as leaks of employee or customer information could lead to lawsuits.

Locations with factories handle even more critical information. For example, they deal with confidential data like CAD drawings, or transmit sensor data over IoT (Internet of Things). Strict management, such as systems for confidential information management and encryption of communication channels is required to prevent leaks of this information.

Focus on protecting areas with critical information

When considering security measures, it's crucial to set priorities based on where the highest risks are,, focusing and applying decisive measures to locations with greater security risks.

When considering measures, there are two points to be mindful of: one is to "form a solid internal consensus on what is considered a risk", and the other is "relying too much on hearings may not reveal the truth".

For example, in manufacturing, many onsite employees might think the risk lies in the theft of CAD drawings. However, management may think differently. If they believe that "while drawings can be redesigned, if the wholesale prices to Company A are known to Company B, it could lead to bankruptcy", then the real critical information to protect is not the drawing database but the Excel file on a salesperson's computer containing the wholesale prices. As the measures change depending on what needs to be protected, it's vital to reach an internal consensus on what is the company's most significant information asset.

The latter point emphasizes the importance of understanding the actual situation through the use of tools, rather than relying solely on hearings. Conducting hearings with employees is a standard method to understand the information assets and potential risks that need protection. However, employees rarely admit to using unauthorized tools when asked. It's crucial not to take the answers from hearings at face value but to combine interviews with other employees and the use of IT asset tools to accurately grasp the situation.

5. How companies can achieve Zero Trust Security

Zero Trust Security is no simple equation of just combining and implementing tools. The most important thing is to understand what assets need to be protected. However, Mr. Miwa also has an advice for companies that want to achieve Zero Trust as soon as possible: “For SMEs with smaller IT systems compared to large corporations, one method could be to switch to a full cloud environment, including overseas locations. This way, everything can be controlled from the headquarters. For example, computers in Tokyo and Indonesia can be managed in the same way”.

Even if security are only necessary for overseas locations, transitioning to a full cloud environment is a strong option when implementing zero-trust.

This is because it is always a lot of work to maintain firewalls, servers, and in-house security, especially for overseas locations with limited resources.

"If full cloud is not feasible and there's no time to identify risks", Mr. Miwa advises to apply the latest patches to VPN (Virtual Private Network) devices, which are vulnerable to external attacks, and then introducing EDR tools and conducting email training for employees.

He also emphasizes on the need to strengthen threat monitoring, as introducing the tools is not enough. Ideally, directory services that centrally manage internal information and computers should be monitored 24/7, and even if there are no resources in-house, securing a budget for outsourced monitoring is desirable.

To ensure effective prevention, system measures are important, not human measures

When it comes to security measures, in Japan, there might be a tendency to focus on "human measures" such as raising awareness and spreading knowledge. However, Mr. Miwa points out that to ensure security, it's desirable to adopt "technical measures" that prevent breaches through systems, as it is the case in Western countries.

In a survey conducted by NRI Secure Technologies Ltd. from July to September 2022, companies that raised employee awareness and knowledge as measures triggered by cyber alerts were about 30% in the U.S. and Australia, while in Japan, it was more than double at about 70% (Table 1). Conversely, Japanese companies that implemented system-based measures such as "revising cloud service settings" and "enabling multi-factor authentication" were less than half of those in the U.S. and Australia.

Mr. Miwa says, “For overseas countries, it’s common to enforce governance through the system. Trying to implement human measures as mere requests without penalties is often ineffective in reality”.

Table 1: Measures taken to reduce risks in response to cyber alerts that occurred after February 2022	Japan (1772 responses)	America (540 responses)	Australia (528 response)
	67.10%	35.20%	29.70%
Alert and raise employee awareness	30.30%	33.00%	34.50%
Understand vulnerabilities & apply patches	28.60%	30.60%	29.70%
Achieve account and review password	18.00%	39.80%	44.90%
Enable multi-factor authentication	15.20%	41.90%	45.80%
Review cloud service settings	9.40%	25.40%	19.50%

Source: NRI Secure Technologies Co., Ltd.
“NRI Secure Insight 2022 Survey on Information Security in Companies”

6. If overseas locations take the first step themselves

Some readers may have been assigned to overseas locations where information systems are managed by local employees, and may not have a detailed understanding of their operations. In such situations, how should one quickly implement security measures at the overseas locations without relying too much on the head office in Japan? Mr. Miwa advises as follows.

"You should thoroughly investigate what could damage the company's brand and take individual effective measures to avoid such scenarios. It's crucial to localize the points that need protection. Before considering how security should be implemented, it is important to understand the roles of each employee, identify what is most important for their work in an honest manner, and then ensure proper protection for overseas locations".

"The Internet is fundamentally a world of Westerners where one must protect oneself", says Mr. Miwa. You should always assume that you are a target if you go out unarmed. In aiming to achieve "Zero Trust Security", it seems we must always cultivate the habit of thinking how to protect ourselves from threats.

Contact Us

Tomorrow, Together KDDI

KDDI Corporation https://www.kddi.com/

〒**102-0072** Garden Air Tower, 3-10-10 Iidabashi, Chiyoda-ku, Tokyo

03-3347-0077 (Head Office Representative)

Sources

***1 Teikoku Databank**

"Survey on the Actual Production and Sales Situation at Overseas Locations of Expanding Companies (2023)"
https://www.tdb.co.jp/report/watching/press/p230716.html

***5 Trend Micro Co., Ltd.**

Cyber Risk International Awareness Survey "Cyber Risk Index" (2nd half of 2022 edition)

https://www.trendmicro.com/ja_jp/about/press-release/2023/pr-20230508-01.html

***2, 3, 4 Nikkei BP "Nikkei Network" December 2022 Special Collection**

"Network Equipment Usage Survey 2022" p.39

***6 Japan Institute Users Association of Information Systems**

"Corporate IT Trend Survey Report 2023"
https://juas.or.jp/cms/media/2023/07/JUAS_IT2023.pdf

***7 NRI Secure Technologies Co., Ltd.**

"NRI Secure Insight 2022 Survey on Information Security in Companies"

https://www.nri-secure.co.jp/hubfs/NRIS/download/ebook/NRISecure_Insight2022_230201_Report.pdf