What kind of zero trust do you need?

An important technical measure in the Zero Trust security is "Least Privilege", "Continuous Verification, Dynamic Authorization". Seeing that a large provider introduced that the detection rate of express threat perception in its zero-trust security solution has increased from 60% based on the characteristic database to 96%, this is actually a very ridiculous indicator. If there are still 4% of confidential documents probably leaked, and 4 out of 100 intruders can get the confidential documents. Is this still a secure system? Does zero trust like this work?

That's what I'm going to talk about today: what kind of zero trust do you really need? How should you start small and move towards zero trust? How to properly evaluate a zero-trust security solution? The author puts forward some evaluation ideas here for reference.

1. If a zero-trust authentication solution is still based on username and password, especially if the webpage where the user enters username and password does not have https, it is definitely an unusable solution, no matter how famous the manufacturer is.

Not only the login authentication system requires HTTPS encryption, but all business systems and all data collection systems, whether on the intranet or extranet, must deploy SSL certificates to encrypt web traffic with HTTPS to ensure that confidential information will not be illegally stolen and illegal

tampering during transmission. HTTPS encryption of cleartext http traffic is the first requirement of zero trust security.

There may be a hidden security risk here, that is, some authentication systems are no longer based on the direct input of usernames and passwords on web pages, but based on mobile App authentication, support fingerprint and face authentication, and it seems that there is no need to remember cumbersome password that it is very convenient, but if the communication between the App and the authentication server does not use an SSL certificate to implement https encrypted transmission, it is still insecure. Even if https encrypted communication is used, but this App does not check the correct use of https, there may still be security problems.

2. If the threat detection rate of a zero-trust solution is not 100%, it is still doubtful whether it is usable, unless the business system can tolerate a 4% missed detection rate. So, how can we achieve 100% detection rate? There must be some security experts who say: 96% is already very high, it's amazing, it's impossible to achieve 100%! Indeed, 96% is really good, but there are still problems with zero-tolerance systems, so how to achieve 100%? Then we need to jump out from the traditional "Holmes-style" thinking of security protection to find the answer!

Just imagine traveling by airplane, can an airline accept that 4 out of 100 passengers are terrorists? The problem with the "Holmes-style" traditional security protection idea is that you don't know who the user is, and you can only rely on guessing (judging its characteristics and behavior), which is unreliable, and the so-called "security brain" may not be able to guess out! What to do then? Only real-name authentication for air travel can ensure flight safety.

The zero-trust solution based on cryptographic technology is to give each individual a trusted digital identity. Users must present their trusted identity to obtain the corresponding data access rights after passing verification and obtain the required data in an encrypted way. At the same time, through timestamp signature to record data access time. This is a 100% reliable solution. We call it the "Native Trust" mechanism. The user is first of all have a trusted identity, and the certificate presented is a

trusted certificate. The authenticity of the identity can be verified through the digital signature algorithm, then the user can successfully pass the security check and board the plane, which is faster and more accurate than the "Holmes-style" continuous screening and verification. This is the magic of cryptography!

3. If a zero-trust solution is just an authentication system, it is not enough. Identity authentication is not the purpose, the purpose is to protect the data behind! Therefore, a zero-trust security solution must be a systematic project, which must integrate the five key elements: identity, device, network, application, and data into the zero-trust security architecture and provide a complete solution.

ZoTrus' zero trust security solution is a solution based on cryptographic technology, which can perfectly apply PKI digital certificates to the security protection of the five key elements, so that every individual (person and device) in the network can have trusted digital identity, never trust individuals without trusted digital identities, individuals must present their trusted identity certificates to communicate with other elements in order to obtain the required data through authentication. The largest traffic on the Internet, http traffic, must be fully https encrypted, the second largest traffic, email, must also be encrypted end-to-end using S/MIME technology, and the most critical DNS traffic must also use SSL certificates to achieve DoH or DoT encryption. Never trust the non-encrypted traffic on the Internet and intranet.

And all application software must have digital signature, never trust software code without digital signature, never trust OTA upgrade software without trusted digital signature, so that the system security can be effectively guaranteed. The data security is achieved through certificate encryption. The data is encrypted with the public key of the user who has the right to obtain the data, only this user can decrypt using his private key. This is the only feasible data security solution.

Of course, data encryption is inseparable from the key management system. It is not only necessary to realize that users can use any device anytime, anywhere to obtain the key to decrypt their data, but also

to realize that users can use any device to obtain the public key of the recipient at anytime, anywhere to achieve fully automatic encryption of confidential data. Of course, it is also inseparable from the timestamp service to ensure that the data generation time is trusted, and the data usage time is trusted, non-repudiation and non-tamperable.

In short, zero trust is definitely not something that can be done by an identity authentication product, nor can it be done by deploying a system in one day. It is a journey, not a destination. It must start with a very simple https encryption, gradually transform the existing system and business process, and gradually realize the security and trusted of all elements based on the principle of zero trust, such as individual identity trusted, traffic encryption, application trusted and data encryption.

Richard Wang

Dec. 23, 2021
In Shenzhen, China