Zero Trust model

The *Zero Trust* model is increasingly appealing as it is promoted as a guarantee of secure access to IT resources in mixed usage contexts (remote working, BYOD) and is generating enthusiasm from technological and security solution providers who see the prospect of new gains.

However, as of today, the use of these solutions is challenging due to a lack of maturity: deployment can lead to installation or configuration errors, increase the vulnerability of information systems, and give companies a false sense of security.

If the *Zero Trust* model aligns with the "defense in depth" logic historically promoted by ANSSI, it constitutes a modification of the strict perimeter logic that has long prevailed. Therefore, if implementation of the model is considered, it can only be gradual: it requires the use of new security solutions that must integrate into an overall defense system without replacing it. Implementing such solutions is challenging: deployment can lead to installation or configuration errors, increase the vulnerability of information systems, and give companies a false sense of security.

1. Principles of *Zero Trust*: challenging the "implicit trust" in the perimeter model

Recent technological advances and usage developments challenge the traditional perimeter defense model. Increased use of cloud computing, the rise of homeworking, and the use of personal devices (BYOD) to access professional data reduce the control that entities have over their information systems and data. Meanwhile, the level of threat is rising. In this context, traditional information system (IS) security measures such as firewalls, segmentation (physical or logical), or VPNs encounter limitations.

The *Zero Trust* model aims to address these security issues by an evolution of the notion of a perimeter. *Zero Trust* is primarily an architectural concept dedicated to strengthening secure access to resources and services, not a technology itself, and certainly not an all-in-one commercial software solution.

In a traditional perimeter defense logic, users connected from the entity's network are granted access to extensive resources without applying basic partitioning measures or subsequent controls after their authentication and session access: users are assumed to be "trusted" by default. **The *Zero Trust* approach, on the contrary, aims to reduce the "implicit trust" given to users and activities conducted through the entity's equipment.** The "perimeter protections" do not disappear entirely: there are still, for example, firewalls, proxies, and trusted directories.

To reduce "implicit trust," controls must become regular, dynamic, and granular (reference 1):

- Access to resources should be granted based on the need-to-know.
- Access should be given based on the least privilege necessary to perform the task.
- Access requests should be controlled regardless of their origins (the "internal" or "external" perimeter of the entity).
- The resource access policy should be dynamic and take into account a wide range of attributes (identities of the accessors and the accessed resource, sensitivity of the requested resources, behavioral analysis of the user, access hours, etc.).
- The entity must ensure the security of all its assets during access requests and recurrently during usage.
- Authentications and access authorizations to resources should undergo regular re-evaluations.

2. *Zero Trust*: several operational implementations

A complete transition to a *Zero Trust* model seems unlikely for entities with an inherited and entrenched IT heritage as it would require a complete overhaul of the information system. **Proponents of *Zero Trust* logically advocate for a gradual implementation**. One proposed strategy turns the adoption of the *Zero Trust* model into a two-step process, with the first step involving the integration of encryption solutions, tools to prevent data leakage, and access controls (e.g., NAC) into the "traditional" IS. NIST anticipates an incremental transformation of information systems: entities will first operate a hybrid information system implementing a model halfway between the *Zero Trust* and perimeter models.

An update of the information system's **risk analysis is necessary before any deployment:** the mapping of the information system is revised, clearly distinguishing the perimeters that can be integrated into the *Zero Trust* deployment (e.g., Web applications, cloud applications) from those that cannot.

Several efforts can be considered to integrate *Zero Trust* principles into a "traditional" information system:

- **Improved governance of identity** (access to resources is based on user and device identification, asset status, and environmental factors such as time and geolocation of the connection request). As key elements of the *Zero Trust* model, the identity repositories must be cleansed with a strict policy of updating upon arrivals, departures, and mobility. They must accurately reflect the current situation of the users.
- **More granular and dynamic resource partitioning**. This "micro-segmentation" groups resources into meaningful business groups, and filtering flows between these groups becomes independent of the IP addresses of the resources. This additional layer of abstraction (e.g., tags and VXLAN) allows for adapting resource protection to the exact need for protection, as all resources are partitioned based on their role, sensitivity, and exposure to threats.
- **Use of state-of-the-art authentication means:** since two-factor authentication is generally a prerequisite for implementing the *Zero Trust* model, careful consideration should be given to the choice of authentication factors, for example, favoring certificates generated by a trusted public key infrastructure (PKI) or FIDO tokens.

- **Strengthening detection means**, generated security logs must be correctly configured and centralized in a SIEM. Security teams (SOC) must be sufficiently trained, experienced, and sized to respond to security alarms.
- **State-of-the-art configuration** regarding service security. For example, for stream encryption, TLS should be configured following the ANSSI TLS guide[1].
- **Change management** should not be overlooked. If the *Zero Trust* model is seen as a driver to simplify the user experience, it should not be forgotten that users are the first concerned about the digital security of their entity. New access, authentication, or alert modes must be communicated clearly, emphasizing the importance of being vigilant in the use of digital means.

This transformation must be progressive and controlled to ensure the protection of the data and assets processed and not weaken the historical information system. There is no standardized product or component to implement it.

Finally, the exclusion of administration stations from the *Zero Trust* model is imperative. The doctrine, described in the ANSSI Recommendations[2] to secure administration of IT systems, should be favored. In particular, it is advisable to dedicate administration stations to connect to the administration IS with a non-bypassable IPsec VPN tunnel.

3. ANSSI's view on *Zero Trust*: risks that should be taken into account

***Zero Trust*, if interpreted to break with the traditional perimeter model, is likely to increase vulnerabilities.** In particular, the use of new and numerous software solutions multiplies the risk of losing control compared to physical solutions (e.g., due to bad installation, configuration errors, or the presence of vulnerabilities exploited by third-party attackers), thus giving a false sense of security.

The "all-in-one" approach of commercial *Zero Trust* solution providers may seem attractive on paper; however, it does not exempt from independent reflection on the state-of-the-art of all possible variations of the approach: flow encryption, authentication tokens, logging, and user awareness. **It is also important to keep in mind that adopting a *Zero Trust* model and the associated architecture does not replace the inventory and control of client terminals used to access resources and services.**

If an entity wishes to gradually transition to a *Zero Trust* model, the principles of risk management and control must continue to be applied to ensure the protection of informational and application assets: these principles guarantee the smooth continuity of missions and the sustainability of the entity.

References

1.*Zero Trust Architecture*, NIST Special Publication 800-207, August 2020

[1] https://www.ssi.gouv.fr/en/guide/security-recommendations-for-tls/

[2] https://www.ssi.gouv.fr/en/guide/secure-admin-is/