National Cyber Security Centre
Ministry of Justice and Security

Prepare for Zero Trust

Apply Zero Trust effectively when undertaking replacement and expansion investments

Factsheet FS-2021-02 | version 1.0 | 17 August 2021

More and more organizations are applying Zero Trust principles, and the need for the implementation of these principles is increasing. Technological developments have rendered many organizations' traditional views of security and security policies obsolete. Organizations that have embraced Zero Trust principles are less susceptible to external attacks and threats from within. NCSC-NL recommends that you draw up an action plan so as to ensure that you will be able to apply Zero Trust principles to future investments in your system. Such a plan will show the measures that must be taken to ensure that Zero Trust principles can be implemented effectively.

Background

More and more organizations are choosing to apply Zero Trust principles when protecting their IT infrastructure. They seek to implement a security model that can be effectively adjusted to today's complex environments. In such environments, devices and data must be protected, regardless of where they are located or what types of devices are used within the organizations.

Zero Trust environments allow organizations to minimize the risks posed to them in this new situation. The measures implemented as part of a Zero Trust environment allow you to address shortcomings in the traditional security model. For instance, the measures will make it harder for others to move laterally (i.e. move between the systems to try and find data that can be exfiltrated) within the network.

Senior managers at various organizations are currently discussing the implementation of Zero Trust at their organizations. For instance, many CIOs, CISOs and architects have begun to incorporate the design principles into their organizations' future IT systems.

In addition to the organizational attention paid to Zero Trust, the security model is becoming increasingly necessary. This is because of various types of technological changes (e.g. people working location-, time- and device-independently; adoption of SaaS and other cloud-based technologies) and because threats are becoming more frequent and more serious. The landscape is growing increasingly diverse. The days when one single data center held all the data are gone. Malware attacks are becoming more common, and what is most notable is a significant increase in the use of ransomware. Increased digitalization within organizations and new ways of working are making it easier for hackers to infiltrate networks. As a result, we need to take a different approach to security.

Organizations' users and clients have a greater need for security, and higher expectations, as well. They want their personal data and sensitive information to be protected effectively, both now and in the future. Organizations can ensure that this is the case by applying the Zero Trust principles.

Target audience

CISOs and security managers

The following parties have contributed to this factsheet:

- DICTU
- KPN
- Netherlands National Communications Security Agency
- Schuberg Philis

What is Zero Trust?[1]

Zero is a security model featuring a set of design principles that helps prevent attacks and data leakage. It involves removing the concept of a trusted network position from the system architecture. It is based on a recognition of the fact that traditional security models operate on the outdated premise that the inside of an organization's network can be entrusted with anything.

Zero Trust, based on the principle of never trust, always verify, is designed to protect today's digital environments. They use intricate network segmentation and prevent attacks on the boundaries of the various segments. In addition, Zero Trust simplifies detailed conditional user access control.

A network architecture is Zero Trust-compliant if it complies with the following set of design principles:[2]

- Identify all the components of the IT infrastructure that must be protected and protect all the paths that give access to it.
- Only grant access to data through protected connections, regardless of where the data is located.
- Enforce strict access control on a need-to-know basis.
- Determine who is to be granted access on the basis of the degree of trust that can be gleaned from the various properties of the request for access: account, device, IP address and location.
- Make sure you implement extensive monitoring and logging.

The traditional approach to security impedes cloud adoption. After all, cloud-based environments are by definition located outside an organization's on-premise network. As a result, you cannot necessarily apply the same type of network management to them. However, applying Zero trust principles may promote innovation. The easier it is to use cloud services, the easier it is for people to adopt new applications. The application of Zero Trust principles makes the journey and access to the cloud easier.

What is the situation?

The traditional security model, also known as the castle-and-moat security model, has structural weaknesses and has become untenable due to modern malware and ransomware attacks. The model does not work well when changing technology is used and when the threats come from within. Unlike other aspects of security, which operate on the premise of a defense in depth, organizations here tend to put their trust in the perimeter – the boundary with the outside world. A network designed in this manner does not come with any security and control mechanisms that will stop lateral movements once an attacker has breached the network. This is because the inside of the network is considered a safe and trusted zone in such security models.

The network remains vulnerable from these sorts of threats until the organization switches to a so-called pomegranate security model, which is characterized by a more extensive application of network segmentation. As with a real-life pomegranate, this results in a set of smaller segments. These are combined with strict and conditional identity verification and access management. Some organizations that

[1] See also https://www.ncsc.nl/actueel/weblog/weblog/2020/what-about-zero-trust (only in Dutch).

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

implement Zero Trust choose to reduce their security perimeter to the endpoint, which is to say that they consider their entire network to be untrustworthy.

The traditional model becomes hard to manage after a while due to the large number of client devices outside the organization's premises and the many connections to chain partners' networks. This causes the boundary between 'inside' and 'outside' to be blurred, which means the network is hard to protect. It often involves the protection of various interconnected networks, which can make it hard to keep an eye on what is happening. Furthermore, such connected networks always have more than one access port. For instance, there are entrances and exits through which web servers are reached, and often multiple VPN connections, as well. The situation becomes even more challenging when there are cloud services involved, because these generally have more application programming interfaces (APIs). The problem here is not the number of client devices, but rather the large number of services, which means that there are many places where the network can be accessed. After all, an unsafe external API provides hackers with an opportunity for unauthorized access.

The wish to manage one's hardware oneself is increasingly infeasible from a financial point of view. As a result, the idea that all data must be stored on the organization's own premises is slowly becoming obsolete. It is being replaced by a transition to cloud-based services. This transition presents organizations with certain opportunities. After all, when they have made the decision to invest in cloud adoption, they might as well embrace Zero Trust. Cloud-based services make it easier to implement a Zero Trust environment.

Many organizations do not know where to begin implementing Zero Trust principles. As a result, many of them will assume that their application will take a lot of time and cost a lot of money, and so decide against it. If an organization is granted the opportunity to incorporate Zero Trust into its IT infrastructure in an affordable manner, it is a good idea to have a plan ready at hand that will allow the organization the opportunity to actually do it. For instance, a transition to cloud-based services would be a great time to start implementing Zero Trust principles. At present, many organizations seem to count on their IT suppliers to suggest cheap and efficient ways to implement Zero Trust.

What could happen?

Should you choose to implement Zero Trust, you will make your organization more resilient to external attacks and threats, and your IT infrastructure will be protected in a more future-proof manner. Once a hacker has gained access to your network, he will generally have an easy time moving from one of your systems to the next, which means he will have access to a large part of your network and data. In addition, you may face insider risk, which means that one of your own employees unwittingly or deliberately causes a data breach or grants hackers access to your network.

Once hackers have gained access to your network, they can install malware, which can then be used as a backdoor to your network through which they can exfiltrate sensitive information. Hackers can also use their privileges to gain access to various data systems that are part of your network.

If your organization has a Zero Trust implementation plan ready at hand, you will be able to jump on the opportunity to implement it when it presents itself. Having a plan in place will also give you more certainty with regard to a general implementation, and will allow you to implement Zero Trust professionally. You will be able to implement Zero trust more efficiently if you do it while undertaking a replacement or expansion investment. If you decide to implement Zero Trust later, after the fact, you will incur higher costs. On top of that, it may be a while before the next opportunity presents itself. Until that time, your network will be protected less effectively, and a potential incident may have a more significant impact.

If you embrace a new security model, you will be able to protect your organization's IT infrastructure efficiently while other organizations may not yet have availed themselves of this technology. This means they are probably more likely to fall prey to an attack than your own organization, given that they have fallen behind in the technological race.

What does NCSC-NL recommend?

NCSC-NL recommends that you draw up an action plan so as to ensure that you will be able to apply Zero Trust when your system is replaced or expanded in future. The action plan will show you what changes can be made by which deadline and how much work this will require.

If you properly implement Zero Trust, your organization's susceptibility to attacks will be minimized, critical processes will have improved continuity, you will comply with applicable standards to a higher standard and in a more cost-effective way, and your network architecture will be future-proof.

If you are planning to transition to a cloud environment soon, you may wish to incorporate Zero Trust into this transition. After all, incorporating Zero Trust into it after the fact will cost you extra time and money, since it will require your organization to revise the recently built infrastructure.

Be sure to include the following thoughts when you draw up your action plan:

- Base your action plan on your organization's strategic objectives and the outcomes of a risk analysis.
- Draw up vision statements that paint a clear picture of the objectives, results and type of network architecture.
- Use the action plan to get your organization's senior managers on board, by focusing on the goals of your organization. This is how to receive support for your own objectives, budget allocations and feedback from other parties within the organization.
- Allow end users the opportunity to provide input on the implementation of Zero Trust. This will allow you to protect your system in a way that is not detrimental to their user experience and productivity. If the measures make things less convenient for the end users, they will try to find a way around them, meaning you will be unable to realize the advantages Zero Trust is supposed to give you.
- If necessary, consult IT and cybersecurity suppliers who have an excellent track record in cloud-based security services.

If you wish to implement Zero Trust, start small and seek to realize attainable goals. Do not start work on your main assets ('crown jewels') at once. In this way, you will learn more about the impact the transition will have on your organization, which will show you whether Zero Trust is suited to your organization and can be further implemented.

In your design and budget allocations, keep in mind the concept of *people-centered security*[3]. This will stop users from seeking to find a way around the security measures, which may render them useless. A Zero Trust

[3] See also https://www.ncsc.gov.uk/collection/10-steps/engagement-and-training.

environment may make things unnecessarily inconvenient and complicated for users. It is crucial that you strike the right balance between continuous protection from threats on the one hand and a convenient system that allows users to be productive on the other.

An effective implementation of Zero Trust will require certain investments:

Network segmentation

Do not build your entire infrastructure in one single network, but rather invest in extensive, separate environments that each have their own perimeter. Keep the network segments as small as possible, as larger segments do not allow for much access control. Make sure you strike the right balance between very small functional segments and a manageable control mechanism governing access to the segments.

Authentication and authorization

Ensure proper identity verification[4] by implementing an access strategy based on multifactor authentication, conditional access and detection of risks posed when running sessions. Access to the various applications within your network must be authorized, and authorization must be granted based on the principle of least privilege. This means that users are only granted access to those tools, data and segments that they actually need to perform their duties. This will be more manageable if you assign users to predetermined roles and groups. The risk of identity fraud can be minimized by means of a central identity provider that supports open standards (such as SAML).

Access and security policy

Define an acceptable access policy for your segments and data. Enforce this by means of a security policy that provides both an understanding of and a course of action with regard to abnormalities.

Monitoring and automation

Make sure that your SOC/SIEM officers are aware of the network segmentation. This will allow them to use all the information garnered by your Zero Trust environment. The procedure used to assess potential incidents depends on various data sources, which in turn relate to various segments of the network. With Zero Trust, the emphasis lies on monitoring the segments and the individual devices used within your network. Automate the monitoring of these data flows in such a way that the most important hits are reported first. In this way, your SOC officers will be up to date on what is happening, which will allow them to detect and identify misuse sooner and so fight off threats.

Perspective for action

1. Perform a risk analysis and use the results and your organization's strategic objectives to draw up a business case for a Zero Trust environment.[5]
2. Convene a meeting with the parties involved. Together, determine in which segment of your network you wish to begin implementing Zero Trust and which requirements must be met. Make sure that your organization’s senior management supports your decisions. Inform senior management of what will happen if they do not implement Zero Trust. People who may be able to help you finetune your action plan are the IT team, the Chief Information

[4] See also https://www.ncsc.nl/onderwerpen/authenticatie (only in Dutch).

[5] See https://english.ncsc.nl/publications/factsheets/2020/september/15/factsheet-risk-management-the-value-of-information-as-point-of-departure.

Officer (CIO), the Data Protection Officer (DPO) and the end users. If you have any IT and security suppliers, be sure to involve them in the drafting of the action plan, as well. Which people should be involved in the drafting differs in each organization.

3. Draw up a separate action plan with timeline for each component of your network that needs replacing or expanding. Find out when the next investment takes place. Identify what must be done to realize the investments outlined in the previous chapter. Determine how much time the supplier will need to deliver and implement these facilities.
4. Initially, implement the changes to small components of the system only, in accordance with the step-by-step plan for the implementation of Zero Trust as presented below.
5. Guard and maintain the entire system by analyzing the data flows associated with the network, systems, applications and cloud service. Make sure that the collected logs and data flows are all gathered in your SIEM. These relate to user behavior, identity and access management (IAM) logs, network behavior and external threats. They will help your security team or SOC to distinguish between normal and abnormal behavior. You can revise the classification of your data accordingly.

How do I begin with the technical implementation of Zero Trust?[6]

1. Determine with which component of your infrastructure you wish to begin, and identify the segment within that component that needs protection. Identify which critical data, assets, applications and/or services (DAAS) you wish to incorporate into the compartment to be protected.
2. Map the transaction flows based on the interactions between the DAAS components identified in Step 1. This will allow you to identify and learn to understand interdependencies between sensitive data, applications (e.g. web/application/database servers), network services and users.
3. First design a Zero Trust environment on paper, and be sure to apply network segmentation, only allow specific users access to sensitive data and provide policy enforcement for the various segments, to prevent threats to the system. Then work on getting a proof of concept.
4. Develop the access policy for your Zero Trust environment by asking six questions based on the Kipling method: 'who, what, when, where, why and how' can users be granted access?
5. Guard and maintain the entire system by analyzing the data flows associated with the network, systems, applications and cloud service. Make sure that the collected logs and data flows are all gathered in your SIEM. These relate to user behavior, identity and access management (IAM) logs, network behavior and external threats. They will help your security team or SOC to distinguish between normal and abnormal behavior. You can revise the classification of your data accordingly.

[6] See https://www.paloaltonetworks.com/resources/guides/zero-trust-maturity-model.

Publication
National Cyber Security Centre (NCSC)
Postbox 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

More information
https://english.ncsc.nl
info@ncsc.nl
@ncsc_nl

August 2021