ON2IT ZERO TRUST INNOVATORS

A hands-on approach to Zero Trust implementation

The Zero Trust approach to cybersecurity has gained tremendous traction in the past two years. The strategy, developed by analyst John Kindervag when he was working at Forrester, was first mentioned in 2010, but did not take off immediately. At that time, strategic frameworks for cybersecurity were not a high-priority item on CIO and CISO agendas. Times have changed and Zero Trust is widely accepted as a sound strategy. But where do you start?

The widespread acceptance of the Zero Trust ideas has inevitably led to different opinions about the best way to implement the principles in an existing cybersecurity infrastructure. And even to a heated discussion about what Zero Trust is really about. “You have to remember that Zero Trust is a strategy”, says Rob Maas, a senior consultant at ON2IT who has been implementing Zero Trust at very diverse organizations for several years. “The Zero Trust strategy can accommodate different frameworks, technologies and operations”, Maas says. “There is no literal interpretation or definitive checklist.”

It’s OK to start small

Starting with Zero Trust is by the same token not an all-or-nothing operation, according to Maas. But customers are looking for guidance, architectures and best practices to start their journey. For Maas, the starting point is always drawing up the Zero Trust Risk Map. This is the step that John Kindervag now describes as ‘defining the protect surface’.

Define your protect surface: find and classify

Maas: “In the original version of the five-step methodology Kindervag started with defining sensitive data that needs to be protected, the so called-crown jewels. Over time, Zero Trust protections expanded beyond data to include other elements of the network. Apart from critical data it now covers custom applications, assets such as medical or manufacturing equipment and services, such as DNS or Active Directory.”

The basic idea, however, remains the same: all elements that need protection must be identified and classified. The approach that Maas and his colleagues at ON2IT follow to classify data is agnostic to specific security standards. “With some customers, a practical classification could be public, internal and confidential. Other customers are used to CIA-ratings or industry-specific classifications of sensitive data and processes. At this stage, the classification system helps to make a first broad sweep.”

In most cases, the analysis of data starts to reveal patterns of which assets, applications and services form natural segments. These

become even more transparent in the second step of the move to Zero Trust security: mapping all transaction flows.

Map the transaction flows: look for logical clusters

Maas agrees with Kindervag that to properly design a network, it's critical to understand how systems should work. "What are the traffic patterns to the data, particularly the data with a high-risk score, what are the interactions between the applications and the services." In this stage of the process, Maas also sees big differences between organizations. "Sometimes existing process descriptions are so complete that a top-down approach can map a substantial part of all relevant network flows. In other cases, we need more elaborate scanning and mapping to get a complete view of the various ways in which sensitive resources are accessed." It can take more or less effort to understand how the systems were designed to work. The flow analysis does not need to be perfect, but it should be detailed enough to tell you the most logical places to insert controls. Just like any good security process, this is an iterative, continuous cycle.

The result of the first two stages is an inventory and a classification of all protect surfaces, and a logical flow-based clustering of the relevant data, applications and services in logical groups, called micro-segments in Zero Trust parlance. The analysis in these first steps can in principle be performed without referencing users, roles or policies in detail, Maas says. The classification of data and applications and all relevant traffic flows often naturally leads to intuitive segments which should have their own protected perimeter. Frequently used and highly-sensitive services, such as those for identity management, might have a private micro-segment.

The attributes and locations of the micro-segments are always accessible as an integral part of ON2IT's Automation and Orchestration platform. They enable the SOC specialists to contextualize alerts and anomalies with relevant Zero Trust information specific to a customer's organization.

Architect a Zero Trust network: enforce and inspect

Based on this analysis, the infrastructure can now be architectured. By implementing security controls such as next-generation firewalls, which will act as a segmentation gateway, a micro-perimeter around the protect surfaces or micro-segments can be implemented. With this architecture, each packet that accesses a resource inside the protect surface will pass through a next-generation firewall so policies can be enforced. Another essential part of Zero Trust is the inspection and logging of every single packet, all the way through Layer 7, to determine if packets are clean. This is done by inspecting all network traffic for malicious content with multiple integrated security services, including intrusion prevention systems (IPS), sandboxing, URL filtering, DNS security, and data loss prevention (DLP) capabilities.

With the rapid adoption of SaaS, IaaS and PaaS, micro-segments are no longer limited to the on-premises environment, Maas says. In many use cases, virtual instances of next-generation firewalls can still be implemented in cloud environments. In some instances, other mechanisms to enforce policies might be required. When it comes to this cloud transformation, Maas points out that the Zero Trust strategic principles remain unchanged. The five steps still work, but you may need new tooling and technology to implement them.

Create the Zero Trust Policy

The endgame for the Zero Trust policymakers is that only known allowed traffic or legitimate application communication is allowed in the network or cloud. Similar to the data classification system, there is no best policy framework for Zero Trust, Maas says. Most best practices employ some form of a User, Role, Permission matrix. Kindervag propagates the so-called Kipling Method, answering the who, what, when, where, why, and how of your network and policies.

- Who should be accessing a resource? This defines the "asserted identity."
- What application is the asserted identity of the packet using to access a resource inside the protect surface?
- When is the asserted identity trying to access the resource?
- Where is the packet destination? A packet's destination is often automatically pulled from other systems that manage assets in an environment, such as a load-balanced server via a virtual IP.
- Why is this packet trying to access this resource within the protect surface? This relates to data classification, where metadata automatically ingested from data classification tools helps make your policy more granular.
- How is the asserted identity of a packet accessing the protect surface via a specific application?

In all cases, for one resource to talk to another, a specific rule must whitelist that traffic. In Zero Trust, there is no "unknown traffic", Maas stresses. If you don't know what the traffic is, it shouldn't be allowed.

Monitor and maintain the network
The iterative process of monitoring and maintaining the network and device configurations is, in the case of ON2IT customers, usually combined with detection and remediation delivered through the SOC-as-a-Service. By using data science, AI and behavioral baselining, all internal and external logs are stitched together and continuously monitored, raising an alert when a malicious or suspicious occurrence should be investigated. Enriching the log data with Zero Trust and microsegment data is key to giving context and relevance to these logs

Get started!
Although many customers are attracted to the Zero Trust approach offered by ON2IT, it is not always easy to find a good starting point for this prevention strategy, Maas says. He found that getting key people in an organization on the same page is a must. "A workshop with engineers and architects to get everyone to understand the basic concepts of Zero Trust and build a prototype segmentation is usually our starting point for these engagements", Maas says.
His final word of advice: it's OK to start Zero Trust on a small scale, such as the development of a new online service or app. "Hands-on working with these concepts gives customers the confidence to implement Zero Trust in highly mission-critical or sensitive environments."

The five steps to a Zero Trust network
- Define your protect surface
- Map the transaction flows
- Architect a Zero Trust network
- Create the Zero Trust policy
- Monitor and maintain the network

ON2IT
ZERO TRUST INNOVATORS

7300 Lone Star Drive / Suite C200 Plano / TX 75024
E-mail: sales@on2it.net / Phone: (214) 206-8446