nccgroup

Shutterstock: Royalty-free stock photo ID: 260225438

Feb 17, 2020 17:21 GMT

The Zero Trust Model: Security Inside and Out (Part 1)

Could trusting no one be the key to data security? With what seems like a breach every day, taking implicit trust out of the equation could be

beneficial, but at what cost? Before explaining Zero Trust, it's best to understand what is currently being used across organizations.

In the Beginning:The Castle-and-Moat Concept

Even to this day many companies rely on the old school "Castle-and-Moat" concepts to protect their "kingdom". This concept revolving around a single point of entry and exit in the network and in most cases utilizing a single point of entry via a firewall (drawbridge). The firewall is of course in place to determine whether to grant or deny access, however there are still a plethora of organizations who have a draw bridge without guards. I am still finding during assessments that organizations have any-any rules, large port ranges, and complex objects that do little to restrict access. While the Castle-and-Moat model may sound like an easy, yet logical approach, specific and discrete access controls are easier said than done. It only takes one malicious actor getting inside the network, then there is little in the way of stopping them from moving to others.

With the Castle-and-Moat model, we would traditionally see data stored in a single location within the network. Without additional controls, the firewall creates a single point of failure, as a malicious actor would then have a better shot a stealing the crown jewels. So how does one secure the network, and ensure a hacker doesn't gain access to the crown jewels? You add multiple layers of controls, such as additional walls, gates, guards, towers, upgraded weapons and domesticate a dragon to segment the data ensuring that if one control fails, all is not lost.

The Zero Trust Model

As security has adapted and changed over time, so have the methods for securing networks. The OSI 7-layer model became very popular and organizations logically segmented their network , putting extra attention towards segregating sensitive information. The concept of Defense in Depth was hammered into our heads, to the point where we have Defense in Depth meme's and "the fan" graphic was used to overlay controls for each layer. This multi-layered, defense in depth, "everyone at the battle stations" approach will typically make it harder for the adversary, but not for all adversaries. The problem is that we have been so focused on external entities, that little consideration was taken for those behind all of the layers.

Headlines and statistics have consistently shown over the last few years that a large number of breaches occur from those we trust. This can include third parties or vendors, however there is an increasing trend that points directly to the implicit trust we give to internal employees:

- Verizon 2019 Data Breach Investigations Report: 34% of all breaches in 2018 were caused by insiders.

- Ponemon Institute: “it took an average of 73 days to contain the (insider) incident. Only 16 percent of incidents were contained in less than 30 days.”
    - The average cost of an Insider breach is roughly 8.76 million, and 23% of the breaches were related to criminal insiders.

These facts are astounding, and seem to be on an upward trend line from recent years, even though a heavier focus has been put on security. The problem lies in that organizations focus on securing one thing, yet leave another open; which is what I commonly see today. At first, we fortified the front door of the castle to prevent untrusted access; then, over time we began adding layers of security with such things as security guards, additional gates, and hidden doors. While this sounds like good practice, did anyone stop to think about what could potentially happen inside? In many cases, the answer is “No”, and is supported by phrases such as “They have been here 10 years, they would never do that”. It is that mentality that has created the problem we see today, implicit trust of employees.

Benefits of the Zero Trust Model

Though the Zero Trust model has been around roughly 10 years already, it is just now making its way into the mainstream in part due to a huge push by several key players in the cyber world, such as Google and their push to Zero Trust connections with BeyondCorp. But if Zero Trust has been around for almost 10 years, why is it slow to adopt? A major decision factor for most companies is cost and Zero Trust isn’t exactly a cheap endeavour. But is it worth it?

While it is initially time and labor intensive implementing Zero Trust, can provide significant benefits.

Access to resources in the environment becomes significantly limited to only what is explicitly granted to a specific user, or groups of users. Additionally, it provides for more granularity in both the controlling, and monitoring of your internal network. Compounded together, this places employees at a heightened level of awareness, thus reducing the overall chances of internal compromise.

During preparation, critical flows and diagrams should have been created, as well as documented standards for network configurations and interconnections. This documentation is an integral part of an organizations secure growth and provides employees with not only a standardized reference, but a starting point to begin better understanding and securing the network.

Lastly, is the long cost savings potential. When you know everything that comes in or out of your network, and remove implicit trust it becomes relatively easy to identify threats or malicious behaviour. Building upon

that, if you already know what is needed to maintain and grow your environment securely, you can begin to streamline processes, or in some cases, completely automate them. An example being Amazons Web Services (detailed above), which over time has reduced the number of employees required to maintain the cloud in favor of automation and scripting, thus reducing the likelihood of human error. With the annual cost of an insider breach averaged at [JS1] , even with hiccups along the way, Zero Trust is how you keep your companies dollars in their pocket.

Potential Pitfalls

While Zero Trust may seem like a logical solution to today's security threats, it does come with its fair share of possible headaches. It's very common for permissions to be requested and granted without a thorough understanding of whether it's truly needed or not. When permissions begin to creep, it can be daunting trying to review each account and assigned permission periodically. On a larger scale, misconfigured permissions across the enterprise could result in disruptions and a loss in overall productivity. It's imperative to include Subject Matter Experts (SME's), System Owners, Management, and external third party experts. Attempting to rush and/or "bolt on" something like Zero Trust without ensuring proper preparation is only going to cause issues and result in failure.

Configuring the network for Zero Trust requires a significant amount of time and resources. Misconfigurations are a leading cause of downtime in a Zero Trust environment, as permissions are mapped to specific tasks to ensure access creep does not occur. Additionally, it is extremely common during an on-site assessment for an organization to struggle with such things as firewall settings, most commonly having the infamous "any-any" line.

Some companies, however, have chosen a different approach to handling internal threats while simultaneously catapulting towards a zero trust environment. Such companies as AWS have removed the human element from most equations; accomplished through the use of automation scripts. By automating most processes and relying less and less on human intervention, AWS is simultaneously reducing the risk of an insider threat while also reducing their financial burden.

Though Amazon is taking a different approach, I generally would not recommend smaller companies to jump right in towards automation, as most do not have the budget required to implement it throughout the network. Additionally, bringing everything full circle, companies are still not doing the basic blocking and tackling to support core security controls, such as change management and access control. Compounding the desire for automation with a lack of defined controls and processes in place can lead to confusion and crucial steps being overlooked during implementation.

So who can benefit from Zero Trust? In my opinion there is something for everyone; be it a full scale implementation at places such as Google,

automation within AWS, or learning from some of the underlying principles if you are a start-up. In fact, beginning the journey at an early stage could save countless migration hours in the future. Zero Trust is not necessarily a “rip out and start over” type of implementation. Zero Trust is the addition of granular policies and segmentation at a gradual rate into the network. It would be asinine to replace an entire network at one time.

Being that this is a gradual implementation over a period of time, there are a few tools on the market that are advertised to speed up the process such as Illumio’s Zero Trust eXtended (ZTX) framework, and Okta’s Integration Network. These tools cover such tasks as violation alerts, granular policy design, infrastructure-agnostic enforcement, device security and management and many more. See links below for more information on the tools listed.

Shifting the Mindset to "Trust No One"

This begs the question, if I don’t trust my employees, then what do I do? Surely the answer isn’t to spend an outrageous amount of money on monitoring, nor is it to ignore the situation either. The ideal situation is to implement safeguards commensurate with the data or information you are trying to protect.

Here is an example to better understand. “Employee A accesses a folder that he/she should not be allowed to view according to the company policy for Access Management. The folder has sensitive Non-Public financial information in it.” While initially this sounds like an issue that should be corrected with a quick permissions change, you have to begin to view it in a “Trust No One?” mindset. In all actuality, most employees would notify a supervisor and have the issue corrected, however, depending on the employees situation, access to that folder could have quickly manifested into a threat actor; such as the internal employee having malicious intentions.

Every day people are put into undesirable or less than beneficial situations due to unforeseen changes both in, and out of their control. Be it blackmail, threats of harm, or financial loss. These types of situations are driving factors for committing internal crimes, and until action is taken to remove inherit employee trust, malicious threats and insiders alike can continue to be a growing threat.

Stay tuned next week as we release Part 2 of "The Zero Trust Model: Security Inside and Out", which will provide guidance around how to gain stakeholder support to adopt the Zero Trust model, as well as how to obtain stakeholder support prior to doing so.

About NCC Group

NCC Group exists to make the world safer and more secure.

As global experts in cyber security and risk mitigation, NCC Group is trusted by over 15,000 clients worldwide to protect their most critical assets from the ever-changing threat landscape.

With the company's knowledge, experience and global footprint, it is best placed to help businesses identify, assess, mitigate and respond to the evolving cyber risks they face.

To support its mission, NCC Group continually invests in research and innovation, and is passionate about developing the next generation of cyber scientists.

With over 1,800 colleagues in 12 countries, NCC Group has a significant market presence in North America, continental Europe and the UK, and a rapidly growing footprint in Asia Pacific with offices in Australia and Singapore.

Contacts

Regional Press Office - North America
Press Contact
NCCGroup@cdc.agency
+1 408 776 1400
+1 408 893 8750