Information Security Thought Paper – Zero Trust

Introduction

The average size of data breaches continues to increase today. This is despite increased spending on information security products and services. With the corporate IT environment shifting away from traditional corporate data centres, and corporate applications being accessed from a range of devices and locations, the Zero Trust model is thought to deliver the best results in securing corporate data.

The purpose of this paper is to provide an overview of the Zero Trust model. It provides the benefits and challenges of implementing Zero Trust. Some best practices in implementing Zero Trust Network Access (ZTNA) are also provided.

What is Zero Trust?

Zero Trust is a security model that acknowledges there are threats behind the corporate firewall. This model requires all access requests to corporate applications and data to be verified before access is granted.

To achieve Zero Trust, a coordinated cybersecurity and system strategy needs to be a part of an organization's digital transformation strategy. It also calls for a set of system design principles, and the adoption of governance policies, such as only giving users the least amount of access permissions needed to perform a specific task. In a Zero Trust environment, networks, applications and services are designed to:

- Provide access privileges that are just enough to perform the task on hand; and,
- Enforce verification of access requests via mutual authentication[1] before access is granted.

A Zero Trust environment is built by design, not by retrofit. Nor is it achieved by simply installing a 'Zero Trust' product/technology. Several security technologies need to be used in concert to enforce the idea that no one and nothing has access until they've proven they can be trusted. Therefore, Zero Trust efforts need to be planned out as a continually maturing roadmap. Planning for Zero Trust begins from initial preparation to basic, intermediate, and advanced stages. As a result, cybersecurity protection, response, and operations are improved over time.

Yet, Zero Trust is not the panacea for all security ills. Why? It doesn't protect against inappropriate access or use of sensitive data by authorized users, or phishing threats. Also, a complete Zero Trust security structure may never be reached for the following reasons:

- Organization resistance to the Zero Trust model; and,
- Limitations in legacy applications, and capabilities of an organization's security.

The Zero Trust Environment

To build a Zero Trust environment, the technologies such as the following are in used in concert:

- Multi-Factor Authentication (MFA);
- Identity and Access Management (IAM);
- Privileged Access Management (PAM);

[1] Mutual authentication is a process or technology in which both entities in a communications link authenticate each other. It is a default mode of authentication in some protocols, e.g. SSH, and is optional in others, e.g. TLS.

- Orchestration;
- Analytics;
- Encryption;
- Scoring;
- Labelling; and,
- File system permissions.

Thus, the Zero Trust environment can be built with security technologies that are already in use. However, it can't be implemented successfully without a mindset and organizational cultural change[2]. Full executive support is needed to foster this mindset and organizational cultural change.

Benefits:

The benefits of Zero Trust environment are:

- Reduction of a business-impacting event like ransomware or data compromise. How? In a Zero Trust environment, the network is designed to operate in the presence of an attacker, and to contain and manage an incident. The implicit trust that exists within a traditional network is removed. Thus, the attack surface is reduced, and the resilience of an organization's IT infrastructure is increased.
- Corporate data security is increased with the enforced verification of identities of all users (and machines) and minimized access.
- Flexibility and adaptability in a hybrid work environment[3] is enabled. In a Zero Trust environment, context[4] and identity are used as a control pane to control access from any device and location to data and corporate applications. Control in the cloud computing environment is also increased.
- Simple and modular IT environments can be achieved with proper design and engineering of zero trust architectures. User access control and management also becomes more straightforward.
- Corporate IT environment security is increased when carefully designed zero trust architectures that embed automation and orchestration can amplify and work in concert with automated IT practices such as DevSecOps[5] and NoOps[6].

Challenges:

The challenges to implementing a Zero Trust environment:

[2] The organizational cultural change is about getting people to understand that bad actors are already in the environment and to act accordingly.

[3] The hybrid environment today involves a mix of remote working, a traditional corporate IT data centre, and cloud computing.

[4] The context of access can be also based on the information security classification labels for the data and applications. For example, access to data with a Protected C label can be restricted to a source IP address within the internal corporate network in addition to the type of device used for the access, user authorization and time of access.

[5] DevSecOps involves embedding security, privacy, policy and controls into the DevOps culture, processes and tools. Threat modelling, risk assessment, and security-task automation are foundational components of product development initiatives, from ideation to iteration to launch to operations in the development of an application.

[6] NoOps occurs when the provisioning of software and software-defined hardware is fully automated, freeing operations talent from mundane server management responsibilities for more creative responsibilities e.g. computing farm engineers.

- Zero Trust is a relatively new process in network security. Many end user organizations lack the experience in implementing Zero Trust. This often leads to a poorly designed Zero Trust environment that may cause users to feel their privacy is in jeopardy, or to become frustrated from being challenged every time to justify their need to access resources. Such users will often resort to using their own unsecured personal devices and services. This use of shadow IT results in increased security risks instead of reducing them.
- The lack of full support throughout the enterprise. The mindset required for a Zero Trust environment must be fully embraced by leadership, administrators, and users for any solution to be successful. Leaders need to be willing to spend the necessary resources to build and sustain it. Administrators and network defenders must have the requisite expertise to implement it. Users must follow, and not circumvent the governance policies. The benefits of Zero Trust will not be realized otherwise.

Zero Trust Environment Implementation Best Practices:

1. Assume compromise. Don't implement Zero Trust Network Access (ZTNA) like it's a traditional virtual private network (VPN). Identify the use cases where ZTNA matters, e.g. controlling access to sensitive applications, or granting access to contractors. Apply specific governance policies to appropriate user groups.
2. Document application usage before starting your ZTNA implementation. Map which applications users (and machines) access early to inform the design of your ZTNA. Discovering and identifying sensitive data, i.e. crown jewels, and the data flows are necessary to:
    a) define and architect micro-perimeters or data enclaves, and,
    b) apply the security policy and control framework.
3. Remove access privileges and entitlements to applications and services that are no longer relevant or needed. They create unnecessary weaknesses in your ZTNA design.
4. Put in place strong measures for user and device authentication. Use contextual identity[7] as the foundation for access decisions.
5. Log everything and monitor for unusual activities.
6. Encrypt data at rest and in motion.
7. Always fine-tune zero trust policies to meet changing business needs. Otherwise, they will impede business operations and frustrate users[8].
8. Start small to gain experience and user acceptance.
9. Prepare the organization for the change. Communicate on the changes being made. Explain unfamiliar concepts and terminology, e.g. what context-based multi-factor authentication[9] (MFA) means. Negotiate with business leaders to overcome objections and to address concerns.

[7] Contextual identity is a notion that entities reveal different aspects of themselves depending on context. With Zero Trust, this means trust in an entity will be based on the identity of the entity and the context of the access before access is granted.
[8] Access policies should allow for good user experience and enable business needs without being too 'open'. Track the access policies for effectiveness. Remediate access issues quickly. Manage change to promote positive user experience and acceptance.
[9] With context-based MFA, users will need to provide extra authentication when they try to access a corporate application from a personally owned device. They may not need to do so when accessing the application from a corporate device that's on the corporate network.

Conclusion:

Capital investments in new security products and technologies aren't always needed to implement a Zero Trust environment. It does need a mindset change, though.

Planning, change management and leadership support is needed to implement a Zero Trust environment. A well-designed Zero Trust environment is also key to promoting user acceptance. To sustain a Zero Trust environment, the security products and processes must be kept tuned in-step with changing business needs and security risks.

Getting to a Zero Trust environment is a worthwhile journey. Implementing it brings many business benefits along the way even if there's no end to the journey.

Resources:

CSO: https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html
NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
Wikipedia: https://en.wikipedia.org/wiki/Zero_trust_networks
https://www.oreilly.com/library/view/zero-trust-networks/9781491962183/ch01.html
https://searchsecurity.techtarget.com/definition/zero-trust-model-zero-trust-network
https://www.techrepublic.com/article/zero-trust-security-a-cheat-sheet/
https://www2.deloitte.com/content/dam/insights/articles/6730_TT-Landing-page/DI_2021-Tech-Trends.pdf

- https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/embedding-security-devops-pipelines-devsecops.html
- https://www2.deloitte.com/us/en/insights/focus/tech-trends/2019/noops-serverless-computing-transforming-it-operations.html

https://www.pwc.ch/en/publications/2020/ch-zero-trust-whitepaper-final.pdf
https://www.helpnetsecurity.com/2020/03/02/building-zero-trust/
Govt. of Canada - https://www.canada.ca/en/shared-services/corporate/publications/network-security-strategy.html
https://blog.isc2.org/isc2_blog/2020/12/absolute-zero-.html
NSA paper on zero trust - https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF

Gartner articles:

1. Quick Answer: How to Explain Zero Trust to Technology Executives (Sept 2021) – Article G00758250
2. Best Practices for Implementing Zero Trust Network Access (June 2021) – Article G00744105
3. What are Practice Projects for Implementing Zero Trust? (Mar 2021) – Article G00744839