**Understanding the zero trust model**

In the age of digitization where massive data is stored online and business processes are automated, one of the looming threats is data breaching. According to a report published by IBM and Ponemon institute, in the last few years, the cost taken as an average for data breaching has risen exponentially up to 11 %. It is becoming evident each day that the castle and the moat security model is longer appropriate for protecting data infrastructure. Companies are now prioritizing cyber security by integrating security systems and implementing security policies to safeguard public sensitive data. This is one of the fundamental reasons why the world of corporate is quickly adopting stiffer security models such as the zero trust model.

**What is this model all about?**

The zero trust model is an IT security model in which users and devices are granted access only when they have proper authentication and only to the number of resources they need to operate different actions. One of the primary features of this model is that it mandates strict identification verification for every user and device that are present inside or outside the network organization parameter. This model was invented by John Kinderbag, one of the leading cyber security expect back in 2010. The former Forrester Research principal analyst had developed this model after concluding that all forms of traditional security models which are based on the assumption that all entities within an organization’s network can be trusted and relayed Upton is an outdated approach to data security and data management. The core principle of this approach is that one must never trust but always verify.

As opposed to the castle and moat approach where every device, network identity, and resource are trusted as a default phenomenon, no user or device or any kind of source is trusted within the organization and also outside the organization. Identities that are both inside and outside the network parameter are seen as possible threats. Thus every access request is only accepted after verifying the authentication of the source of the request, the sender, etc, and encryption. Since its inception, the Zero trust model has become one of the very popular concepts in cyber security. The implementation of the zero trust model requires the implementation of advanced technologies, such as Identity and Access Management (IAM), Multiple Factor Authentication, Next -Generation Endpoint Security Technology, etc. These technologies help in verifying the identity of the user, thereby defending the system's security.

**What are its principles?**

There are mainly three principles that the model sticks to and executes by fair means. The below-enlisted ones are the following.

**1. Explicit Verification**

One of the primary principles of the zero trust model is to verify each user requesting data access with the available resources like the user’s device information, location, user identity, any kind of anomaly, if any, etc.

**2. Limited Access grant**

Each user upon clearing the verification process is given minimum access to data. This is to ensure that only the data required for a particular action is permitted for accessing, thereby minimizing the risk of data breaching.

**3. Defense improvement**

Minimization of segment access is incorporated and end-to-end verification is implemented to improve defense management, threat detection, etc.

**Why is this model so important?**

The zero trust model is an important concept in the cyber security domain. It has various importance. Belo enlisted are some of them.

1)Zero trust model prevents data breaching and curb damage if the system is ever compromised.

2) Multi-factor authentication ensures that all the users that are granted access have authenticated verification and are trusted sources. Users are not trusted by default as they can sometimes also be the source of data breaching.

3)Only legitimate applications are granted access to protected services to avoid mismanagement of data security.

4)The main objective of the zero trust model not only helps in preventing data breaching but also efficiently manages data security.

**References**

1)<https://www.microsoft.com/en-in/security/business/zero-trust>

2)<https://www.techtarget.com/searchunifiedcommunications/securityandcompliance/Why-Zero-Trust-Why-Now>

3)<https://www.ibm.com/in-en/topics/zero-trust>

4)<https://www.printerlogic.com/blog/zero-trust-what-is-it-how-does-it-work-why-should-i-use-it/?campaignid=18209799586&adgroupid=&adid=&gclid=Cj0KCQjwyOuYBhCGARIsAIdGQRMiIYiOj3aL8B6JMIoOEQ8l_ShyhAqF2UshWM5EY0T98nDHZM-z294aAkAoEALw_wcB>

5)<https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/>

6)<https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust>

7)<https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html>