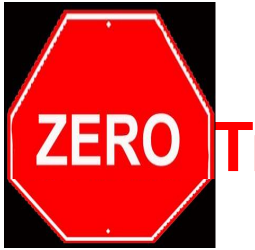

Trust - devices are not to be trusted by default

Major Concepts of Zero Trust :

- Every device and network flow needs to be proven as to why it is configured the way it is.
- Users should have least privilege access to resources and services
- All units are hostile and should be carefully examined
- All traffic must be logged and inspected
- The risk to systems increases over time

Data breaches cost money - use Zero trust

Statistics:

- In 2020, 98% of point of sale data breaches in the accommodation and food services industry were financially motivated.
- An average of 4,800 websites a month are compromised with form-jacking code.
- 71% of breaches are financially motivated.
- By stealing only 10 credit cards per website, cyber criminals earn up to $2.2 million through form-jacking attacks.
- The number of data breaches in the U.S. has significantly skyrocketed within the past decade from a mere 662 in 2010 to over a thousand by 2020.

IAM capabilities to secure data from password compromises

- Use multi-factor authentication (MFA) where authentication is primarily a two step process as follows :
  - the user enters something they know such as a password or pin.
  - the user enters information from something that they have such as a SMS text message with a code or a software token.

- Use attribute-based access control (ABAC) to define which combination of user and/or environmental attributes, such as username and location, are needed to perform an action (i.e. read,write,view) with a resource.
  - For example,a teller at a bank in the US West region should only be able to view and not update a customer’s personal identifiable information (PII) on the west coast.
    - If the teller attempt to access a customer’s PII on the east coast it will be flagged as suspicious.

Use password less authentication

Examples:

- Yubikey is a hardware device used for password less authentication. It allow for storing static passwords for use at sites that do not support one-time passwords.

- Biometrics is an authentication mechanism based on a person’s physical characteristics.
  - ❏ Biometric identifiers are physiological characteristics such as fingerprint and face recognition.
  - ❏ Biometrics classified as behavioral characteristics such as gait, keystroke and voice are related to the behavior of a person.

Zero Trust can improve compliance

Examples:

- All authentication is continuously validated and recorded in real time.
- It uses the risk management approach to “trust nothing and record everything.
- It uses NIST 800-207 to focus on protecting resources instead of network segments. Users and assets shouldn’t be trusted just because they are on the network.