7 key tenets of Zero Trust

@Chidambaram-narayanan

1 All data sources and computing services are resources

- ✓Devices
- ✓Aggregators
- ✓Storage systems
- ✓Saas systems
- ✓Enterprise resources

in @Chidambaram-narayanan

2 | All communication is to be secured regardless of location

✓On the enterprise network or remote

✓End-to-end encryption and mutual TLS,

✓Source authentication is crucial to validate the legitimacy of the communicating entities.

3 | Access given to resources on a session by session basis

- ✓Principle of Lease Privilege, but to its rock bottom level.
- ✓This minimizes the potential attack surface and exposure.

4 | Dynamic access policy for resources

- ✓Access decisions cannot be binary;
- ✓Attributes that can determine policy include:
  - ✓Client identity
  - ✓App/ service
  - ✓Asset state
  - ✓Behavioural factors
  - ✓Environmental factors

5 | Monitor & measure integrity and security posture of all assets

✓Continuous monitoring is critical;

✓Enterprise needs to have a comprehensive inventory and understanding of all its assets;

✓Assets with higher vulnerabilities need to be treated separately

@Chidambaram-narayanan

6 | Dynamic auth’n and authZ

✓Trust nothing, verify everything is the dictum;

✓Every access request goes through the verification process.

Yes this will get messy and costly, but in the long run, its worth it!

@Chidambaram-narayanan

7 | Collect & use information on each asset to improve its security posture

✓Data helps to make decisions

Gather as much as you can. There’s never enough!

@Chidambaram-narayanan

Thank you!

Like, subscribe, follow (why not all 3?)

- ✓ Auditing of financial and systems
- ✓ Cloud awareness
- ✓ Certified Information Systems Audits

in @Chidambaram-narayanan