CyberEd.io Presentation

JUNE 2023

Gregory J. Touhill CISSP, CISM
Brigadier General, USAF (ret)
Director, CERT Division

Carnegie Mellon University
Software Engineering Institute

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM23-0560

Today's Reality

- The traditional security perimeter has been overcome by mobility, cloud computing, outsourcing, etc.
- The price of offense is ridiculously low while defense is ridiculously high
- Insider threats continue to appear
- Tool complexity continues to frustrate users and operators yielding seams in defenses
- We continue to rely on "ancient" technology that costs too much and delivers too little
- There is no "inside or outside" anymore

Greg's Simple Definition of Zero Trust

"Zero Trust is a security strategy focused on ensuring that people and systems can only see and access data and systems they are authorized to see and access…and nothing else."

Note:

- I said "security strategy"…not "cybersecurity strategy"
- I did not say architecture
- I did not say it is something you buy
- I focus on the data and the systems where they reside

How to Adopt the Zero Trust Security Strategy, part one

Carnegie Mellon University Software Engineering Institute

- Assume you've been breached
- Focus on the outcomes you need (a.k.a. "The Mission")
- Start with the assets or data that need protection
  - Not all data are equal!
- Determine who or what needs access and under what conditions and entitlements
- *Ruthlessly* Implement "Need-to-Know/Least-Privilege"
- Inspect and log all traffic
- Implement everywhere your data are (e.g., IT, OT, ICS, IoT, and Cloud)

How to Adopt the Zero Trust Security Strategy, part two

- Think Like A Hacker
- Understand Your Data and Ensure It is Properly Protected
- Structured, Semi-Structured, Unstructured, and Metadata
- Establish, monitor, and enforce access rules
- Adopt the Zero Trust security strategy everywhere
  - People, Processes, Technology
  - Think Beyond Digital!
- Audit Continuously
- Don’t Be Afraid to Benchmark and Ask for Help

Key Takeaways

- Data is a center of gravity for today's warfighters
- Your data comes from numerous sources, is in many forms, and is in many places
- "Know Your Enemy and Know Your Data"
- Data Integrity is essential to make timely and informed decisions
- Data Integrity often is presumed yet misplaced; remain vigilant!
- Technology can help yet human focus remains essential
- Learn how things work on your Enterprise
- Have a data incident response plan and practice!