Access Control

Cyber Club

Agenda

1. Attack surface review
2. Access control
3. Zero trust
4. RMF
5. Demo

Attack Surface

What is an attack surface?

Attack Surface

Everything outside of the network perimeter can be classified as dangerous while everything trusting everything inside of the network

This is the old model and allows attackers, once inside, full permissions to exfiltrate any critical information

Access Control

Access control ensures only authorized users access sensitive systems and data, reducing the risk of breaches

Zero Trust Architecture (ZTA)

A security framework that operates on the principle of “never trust, always verify”

Assumes all devices and users are not safe even if inside of network

Zero Trust Architecture (ZTA)

Core Principles:

- Never trust, always verify
- Least privilege
- Assume breach
- Continuous verification

How is access control seen in ZTA

Replaces traditional safety perimeter -> protect resources and not the network segments

A combination of network segmentation, strict firewall policies, and integration with Identity Providers (IdP) and IPS to enforce security at every layer.

Also reduces attack surface by limiting access to everything, making it harder for threats to spread within a network

Why should I know this

Frameworks are published documentation which act as guidelines which all public and many private organisations use on a daily basis

NIST SP 800-207

A U.S. government publication that defines the Zero Trust Architecture, emphasizing continuous verification of users and devices to enhance cybersecurity.

ISO/IEC 27000/1

An international standard that provides an overview (27000) and the requirements (27001) for establishing, implementing, maintaining, and continually improving an information security management system.

NIST SP 800-207

A cybersecurity framework published by the National Institute of Standards and Technology that outlines the principles and components of Zero Trust Architecture (ZTA)

https://nvlpubs.nist.gov/nistpubs/specialpublications/NIST.SP.800-207.pdf

Section 2.1 - ZTA tenets

Defines ZTA tenets to allow for greater understanding when adhering to the guideline

- All data sources and computing services are considered resources
- All communication is secured regardless of network location
- Access to individual enterprise resources is granted on a per-session basis
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed

Section 2.2 - ZTA assumptions

Uses tenets from section 2.1 with the following assumptions

- The entire enterprise private network is not considered an implicit trust zone
- Devices on the network may not be owned or configurable by the enterprise
- No resource is inherently trusted
- Remote enterprise subjects and assets cannot fully trust their local network
- connection

Section 4.5 – Enterprise with Public Facing Services

“The enterprise cannot strictly control the state of requesting assets, and anonymous public resources (e.g., a public web page) do not require credentials in order to be accessed.”

“If the users are required to produce or are issued credentials, the enterprise may institute policies regarding password length, life cycle, and other details and may provide MFA as an option or requirement.”

Risk Management Framework [SP800-37]

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

“The RMF provides a disciplined, structured, and flexible process for managing security and privacy risk that includes information security categorization; control selection, implementation, and assessment; system and common control authorizations; and continuous monitoring.”

All frameworks work together to be able to create security - all of them do not need to be memorized or completely known

Identifying Risk and Reducing access based on risk

Risk is defined as the potential for an unwanted outcome resulting from an event

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

It prioritizes security efforts based on the potential impact to the organization and informed decision-making around cybersecurity and system operations.

RMF Steps

Step 1: Prepare – Understand organizational risk tolerance and set priorities

Step 2: Categorize – Classify systems based on the potential impact of a breach

Step 3: Select – Choose security controls based on the system's risk profile

Step 4: Implement – Put selected controls in place to reduce risk

Step 5: Assess – Evaluate the effectiveness of controls in mitigating risk

Step 6: Authorize – Decide if residual risk is acceptable before operation

Step 7: Monitor – Continuously track risks and adjust controls as needed

RMF and Access Control

Access to sensitive systems and data introduces potential attack vectors.

Managing who has access, when, and under what conditions directly impacts risk exposure.

RMF encourages least privilege and need-to-know principles to reduce insider and external threats.

Situation

Look on github for all required information

Currently in doc inside of personal discord - double check

https://github.com/Utica-Cybersecurity-Club/General-Meeting