CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for Critical Infrastructure Security and Resilience, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

IDENTITY AND ACCESS MANAGEMENT (IAM): A ZERO TRUST JOURNEY

Agenda

- **Introduction to Identity & Access Management (IAM)**
- **Core Concepts**
- **Key Technologies**
- **IAM Best Practices**
- **Common Threats and Challenges**
- **Trends and Future of IAM**
- **Questions & Answer Session**

Introduction To Identity and Access Management

Definition: Identity and Access and management is the framework of policies, processes, and technologies that ensure the right individuals have the appropriate access to technology resources.

Why it matters:

- Protect Sensitive Data
- Ensure Compliance (HIPPA, GDPR, FISMA, CMMC)
- Reduce the risk of security breaches
- Support Zero Trust Model (User and Devices should not be trusted by default)

Core Concepts

Identification:

- How users assert who they are (username, ID badges)
- How the System Recognizes the user (login ID's)

Authentication:

- How the user verifies identity (password, biometrics, multifactor authentication)
- How the System Prove the user is who they claim to be

Authorization:

- How users are granted access to resources based on identity and permissions
- How the systems authorizes what users are allowed to do once access is granted

Accountability:

- How users' activities are tracked and audited
- How the systems tracks and Audits users activities

Identity and Access Management Principles

Least Privilege: If they don't need access, they shouldn't have it

Separation of Duties: Reduces fraud risk (No single person approves and pays invoices)

Need to Know: Access decisions should be role based, and task based, not relationship –based " I know them, so I trust them"

Key Technology

Directory Services: Store user credential and group information (Active Directory, Lightweight Directory Access Protocol).

Single Sign-On (SSO): Enables users to log in once and gain access to multiple system.

Multifactor Authentication (MFA): Requires more than one form of verification, such as something you know, have, are.

Privileged Access Management (PAM): Control and monitor administrative level accounts access.

Identity Governance and Administration (IGA): Managing the identity lifecycle of on and off-boarding, access reviews and de-provisioning.

Cloud Identity and Access Management (Cloud IAM): Manages identity in cloud services (Amazon webservices, Microsoft Azure) API, roles, service identities.

Common Threats & Challenges

Credential Theft: Phishing, keylogging, credential stuffing

Insider Threat: User who could abuse access

Orphaned Account: Accounts no one knows about or not associated with a current active user.

Overprivileged Users: Accounts with too much access without a real need

Poor Password Hygiene: Low standard for password enforcement

Shadow IT: Use of unauthorized devices and apps

Future of IAM

Password less Authentication: Using biometrics or trusted devices instead of passwords

Decentralized Identity: Blockchain based solutions that put users in control of their credentials.

Artificial Intelligence and Machine Learning: Analyze behavior and detect anomalous access.

Zero Trust Architecture: Trust nothing, verify everything at every request.

Cross-Enterprise Identity Federal: Single Authentication across multiple enterprises or services.

Key Takeaways

Identity and Access Management is fundamental for Cyber Security

Automation and Continuous improvements are necessary for scalability and resilience.

Identity has become the new Perimeter in modern network security models

For The Next Session

Non-Technical

1. How often are users access rights formally reviewed?
2. Is privileged access request and approval formally reviewed?
3. Are there clear policies mandating the use of MFA?
4. Are onboarding and offboarding processes standardized and enforced?
5. How is identity and access management integrated with compliance audits?

Technical

1. Are privileged and regular user accounts separated with different levels of monitoring?
2. Are single sign on and Multifactor authentication implemented across cloud and on-premise systems?
3. Are orphaned accounts regularly detected and deactivated?
4. Is role-based access control or attribute-based access control systematically used?
5. Are abnormal user behaviors detected and alerted on automatically?

For more information:
www.cisa.gov

Questions?

Email: William.Hicks@mail.cisa.dhs.gov
Phone: 202-809-4179
giovanni.williams@cisa.gov
Phone:202-503-5614

Visit **CISA.gov** to learn more and see our mission in action at **cisa.gov/about/2023YIR**
or contact us at **central@cisa.dhs.gov**