Identity and Access Management (IAM)

Control physical and logical access to assets

Access is controled by setting up rules and procedures for access. If you are going to use the object, there should only be one/two ways to get to it. You must confirm someones identitiy by having them prove: Something they know, something they have, or something they are.

- Information
- Systems
- Devices
- Facilities

Manage identification and authentication of people, devices, and services

- Identity management implementation
- Single/multi-factor authentication - in multi-factor authentication, you must provide two of three different forms of identity
- Accountability - beng able to audit a system and demonstrate the actions of subjects
- Session management - providing the user some type of token that they use to acquire resources and identity them with. They don't need to re-authenticate everytime they want to access something
- Registration and proofing of identity - when signing up for a service you may be asked for PII, personal questions about your pas that would be difficult for other to figure out, and information that is unique to you like your email.
- Federated Identity Management (FIM) - setup a trust relationship between two companies so they can share authentication information
- Credential management systems - keeps passwords encrypted and safe from unauthorized access. allows passwords services read permissions to the hashes that need to authenticate someones password

Integrate identity as a third-party service

- On-premise - generally most identifications with information systems are on premise
- Cloud - Identity as a service (IDaaS)
- Federated - doing SSO at a much larger scale. doing it across organizations

Implement and manage authorization mechanisms

- Role Based Access Control (RBAC) - define roles in your organization(nurse, janitor, IT, manager) and give them default permissions
- Rule-based access control - series of rules, restrictions, and filters for accessing objects
- Mandatory Access Control (MAC) - system-enforced based on a subject's clearance and object's labels
- Discretionary Access Control (DAC) - give full control of objects they created or given access to
- Attribute Based Access Control (ABAC) - "IF" "then" access control. lots of policies combined together

Manage the identity and access provisioning lifecycle

- User access review - users can slowly keep gaining privileges over time. need to review them and take away when they are longer need those roles/permissions/resources. This is authorization creep
- System account access review - samething?
- Provisioning and deprovisioning - need to have policies and guides in place to review people, give them permissions, and take them away after certain key events

Definition of Existing Services

what is it used for? what does it provide?

- Directory services - allows an admin to configure and manage how identification, authentication, authorization, and access control take place within the network and on individual systems.
- Active Directory - A database that is a directory service. allows user access control functionality and network resources. like some users can only view certain files, use printer, etc
- LDAP - a protocol used to query the directory services database. this is how subjects and applications find out if they can AAA a user, because LDAP queries their database information.
- Domain Controller - hosts Active Directory
- CA - users don't trust each other, but they do trust certificate authority. CA vouches for individuals identities by using digital certificates.
- Samba - directory services for linux. Domain controller for linux
- SSO - subject may authenticate once, then access multiple systems. Authenication, authorization, and accountabilitiy.
- SAML - an XML standard that allows the exchange of authentication and authorization to be shared between security domains. Ex, your business uses Gmail and SAML. when a user goes to login, they are directed to your SSO server, which has access and password rules. SAML is the request and response to/from SSO server. REST requests will exlicit an HTML, XML, or JSON response. Example operations are GET,POST,PUT,DELETE
- REST - Representation State Transfer. an approach that uses HTTP protocol to access and manipulate text without keeping track of any data(or state)
- SOAP - like REST but has security in mind. Outlines how web service information is exchanged. When requesting access, a SOAP body contains a SAML request or response inside of it
- JSON - JavaScript Object Notation is a lightweight data format
- OAUTH - open standard for authorization(not authentication) to third parties. Like when you authenticate with facebook, you can then authorize it to go off and manage your photos. Facebook could access your photos until you tell it not to anymore
- Kerberos - Authentication protocol. works in client/server model. SSO for distributed environment. symmetric key encryption that doesn't send any passwords over the network. has a session key. has a key distribution center that holds all users keys. a challenge packet is sent to user for their user name, and if they enter password right, the challenge is decrypted. session keys are created for each session greated.
- One time pad - can't be cracked. requireds a preshared key that is same size or longer than message being sent
- RADIUS - provides client/server authentication and audits remote users.
- TACACS - basically same as RADIUS but uses TCP. Seems more secure than RADIUS.
- Biometrics - a way to authenticate a user. won't match perfectly all the time, so if more restrict will have more false positives.

Home Page
To next domain! - D6 - Security Assessment and Testing