CPR101-Activity 5

Luca Novello (gnovello)

# Part A: Security Policy Analysis (50%)

## Select an organization (10%):

* TD Bank

## Identify Assets and Risks (20%):

* **Assets:**
  + Customer data
  + Employee data
  + Financial records
  + Money
* **Risks:**
  + Database breaches
  + Employee hacking
  + Physical robbery
  + Fraud

## Security Policy Proposal (20%):

* **Data Breaches:**
  + Make sure all data traveling over a unsecure network is encrypted so that no information can be read by hackers.
  + Make sure that all code is protected from SQL or command injections to avoid anyone trying to compromise the database or internal systems.
  + Make sure the backend is separate from the database to avoid anyone having direct access to it.
* **Employee Hacking:**
  + Use a Zero Trust Architecture and only trust applications and users that have been properly authorized.
  + Regularly review authentication practices and remove obsolete practices to avoid new threats.
  + Make sure passwords meet high security protocols (min character length, mandatory use of certain characters, no repeat/sequential characters or keyboard walking.
  + Force employees to change passwords on a regular basis.
  + Check and reject compromised passwords from known databases.
* **Physical robbery:**
  + Make sure that all doors are locked when the bank is closed.
  + Any passcodes used to access a physical location should be screened for repeat/sequential passcodes, and checked on a database of known/common passcodes.
  + Don’t open doors outside of working hours.
* **Fraud:**
  + Make sure that password protocols are in place for customer accounts (min length, repeat/sequential characters, use of certain known/common passwords.
  + Offer MFA options for online systems.
  + Make sure all customer data is encrypted and stored on a separate database, isolated from the client.
  + Create alerts/flags for high risk transactions and have them reviewed by a person.

# Part B: Authentication and Authorization (50%)

## Authentication and Access Control (25%):

* Authentication is the process of verifying the identity of the user and implies valid association. Having a mechanism for Access Control, helps define roles and privileges, and restrict system access to authorized users.
* A potential authentication policy for the organization could be:
  + Create a Role-based access control system to give users of the system specific roles and access to certain parts of the system.
  + Mandatory sign in for all users.
  + Usernames are different from email addresses and determined by internal protocols.
  + Passwords must comply with all current security procedures, such as minimum character length, mandatory use of certain characters and cases, no repeating/sequential terms, no common phrases, and use databases of known compromised passwords to filter out any additional passwords that don’t meet security requirements.
  + Use of a salt and hash format to encrypt all data to and from the database.
  + Make sure that websites are properly programmed and sanitized from potential hacks (sql injections, buffer overloads…)
  + Use a spam filter to remove any external emails that might pose a threat.
  + Limit the type of files that can be downloaded/opened by the user based on their role.
  + Enterprise SSO with IdP and MFA via SAML
  + Single Sign On, Identity Provider, Security Assertion Markup Language for authentication and authorization

## Authorization Framework (25%):

* Authorization is the function of specifying access rights/privileges to resources and/or users. Access Control is an approach to restricting system access to authorized users, and to implementing mandatory access control (MAC) or discretionary access control (DAC).
* Roles are created for various job functions. The permissions to perform certain operations are assigned to specific roles. Since users are not assigned permissions directly, but only acquire them through their role (or roles), management of individual user rights becomes a matter of simply assigning appropriate roles to the user's account.
* The organization can determine what access each role requires and then give each employee their appropriate role.
* Use “principle of least privilege” to grant only the minimum authority needed.
* Use Role Based Access/Auth. Control (RBAC) for job functions, not individual users.