Robert Casteel

11/3/2022

Lab 3

Introduction

The following document is designed to create an Identity Policy to set the standards for developing an online profile. The Identity Policy will go in depth in three different sections regarding the overall Enrollment and Identity Proofing methods based on the NIST 800-63 publication. Other sections will also go into authentication and LifeCycle Management. The final section of this document will cover the overall reset policy for authentication devices.

Section A: Enrollment and Identity Proofing

One of the biggest challenges that organizations face when having customers, employees, etc., sign up for accounts on their websites, networks, etc., is the overall verification of individual identity who are enrolling in their programs. The NIST 800-63 Publication details four primary outcomes of identity proofing.

1. Resolve a claimed identity to a single, unique identity within the context of the population of users the CSP serves
2. Validate that all supplied evidence is correct and genuine
3. Validate that the claimed identity exists in the real world
4. Verify that the claimed identity is associated with the actual person supplying the identity evidence.

This Policy will follow many standards NIST describes, such as their three methods of processing identities and enrollment.

The three methods include **Resolution, Validation, and Verification.**

Resolution

In this section the organization will collect Personal Identifiable information (PII) from an applicant such as name, address, date of birth, phone number, email ,etc. Not only will we collect this information but we will also attempt to collect two forms of identity evidence such as a driver's license and a passport. This way the enrollment process will have a very specific sign up process requiring information that is very specific and should only be known and accessible to the individual.

Validation

After the organization has collected the PII, The organization using this policy will be required to validate the information by checking authoritative sources to determine if the data matches authoritative source records. The organization will also be responsible for cross-examining the images of licenses and passports to determine whether no alterations are made and that pictures of the individual match. Queues will also be a significant part of the validation process for issuing the sources for licenses so that everything is validated and examined in a fair, first come, first serve, timely manner.

Verification

To Verify Enrollment information is legitimate, we will ask the applicants for recent photos of themselves to help match their license and passport together. After that, the organization must ensure they are a match. Another verification method that could be used to verify Enrollment is Multi-Factor Authentication (MFA). This could be done through validated enrollment codes sent to the enrolled phone number. This will allow the organization to verify that the user has the phone with the enrolled number.

Section B: Authentication and LifeCycle Management

This portion of the policy will discuss the widespread practice of how users authenticate their information to a specified system such as (Username/ Password, SSO, etc.)

In addition, it will also go into detail about the password rotation policy.

One of the main methods this policy will handle account authentication is by using Multi-Factor Authentication to verify the user's login. This will be done by ascertaining through two main methods. The first method would be using the phone number to authenticate by sending a verification code to the phone number to allow the user to verify their identity. The following approach to authenticating information would enable users to verify their account login by entering a code sent to them via email upon login attempt. Lifecycle management for user accounts will be done via a password rotation that will be required to participate every three months to help protect the overall confidentiality of passwords.

Authentication Device Reset:

If a user loses the device used to authenticate their login or wishes to change their authentication device, a method for swapping the authentication device will indeed be needed for the policy. During the sign-up process for the account, the company will ask for some specific PII information that could be used during the reset authentication device process to help ensure that the person trying to reset the device in question is the current owner of the device. It will do this by asking questions only the account owner can answer, such as security questions, birthdate, email verification, and possible further measures to help ensure the uniqueness of answers for the overall reset process.