CYSE 445 – Project 1 James Cogswell
Microsoft Identity Platform

Problem Solved

Passwords are constantly needing to be changed due to data breaches, reuse of passwords, simplicity, etc. People don't like having to remember a different 15-character password for all their online accounts or devices. The issue this inevitably presents is very easily-guessed passwords that barely pass the complexity requirements, little to no variety in a user's passwords – get one of them and you may very well have all of them.

NIST 800-63B provides guidelines for technical requirements regarding the implementation of digital identity services. One of these digital identity services is provided by Microsoft, which can be configured to meet the standards defined in NIST 800-63B. Microsoft Identity Platform supersedes Azure Active Directory and is a collection of several components that work together to allow application developers to enable passwordless authentication using technology such as Fast Identity Online (FIDO2) keys, biometric login via Windows Hello, and more. Additionally, Microsoft Identity Platform improves confidentiality, integrity, and availability since compromised passwords are a powerful attack vector.

Technology

Microsoft Identity Platform works differently for different types of applications. In general, if you login to an application for the first time on a device, you will be prompted to enter your username and password. After that, any time you login to that application on that same device you will be asked to use your phone to match a number in the Microsoft Authenticator. Organizations should require that their users configure the application to work in Microsoft Authenticator during user creation or upon the adoption of the platform.

The application will make an API call to your organization's Azure Active Directory to authenticate the user, check permissions, etc. and allow legitimate users to login. The idea here is that the users will have a mobile device on them to authenticate themselves into the network and bad actors would have a lot of trouble gaining unauthorized access. The password is *something you know*, the authenticator on your phone acts as *something you have*, and if the application allows Windows Hello for facial scans, fingerprint sensors like TouchID on iPhones, or something of that nature, then that would be *something you are*. With that said, Microsoft Identity Platform provides both 2-factor authentication (2FA) or multi-factor authentication (MFA).

Microsoft works as the control plane for the process, using what they call *Conditional Access*. Conditional Access uses machine learning, policies, and a real-time evaluation engine to evaluate risk, based on certain conditions, which it then uses to implement controls. Conditions include employee & partner users and roles, trusted & compliant devices, physical & virtual location, and more. Examples of controls are allowing/blocking access, granting limited access, require MFA, forcing a password reset, among others. Controls are implemented based both on policy restrictions, and on a risk evaluation by the machine learning algorithm which considers the user's conditions alongside the organization's policies. The type of control that will be implemented is based on the policy or the risk evaluation score.

Requirements

Microsoft Identity Platform is deployed directly into the code. The program should include API calls using Microsoft's myMSAL JavaScript library – which supports all methods of authentication – to do the following: request a login and then acquire a login token without interrupting the user for more information unless the login request had issues, in which case it would acquire a token by interacting with the user. Implementation is designed to be simple and flexible with various applications. An organization should have policies and controls in place, a directory of users, and anything else that would be necessary for an organization to securely authenticate users.

The primary benefit of Microsoft Identity Platform is that it improves the organization's ability to authenticate by more accurately identifying potential risks and policy issues. There isn't really anything additional that the organization would need to implement this tool since they would likely already have users, policies, and controls ironed out so that the platform could be configured appropriately.

Cost Estimate

There is no up-front cost for Microsoft Identity Platform since it's billed monthly. Depending on several variables including the number of internal users, number of external users, which tier you choose, and the location of the Microsoft servers which will be used for authentication purposes. As an example, a US East server with users internal to the organization will cost $6 per user in the P1 tier, and $9 per user in the P2 tier. A US East server with users external to the organization will be free for 50,000 user authentications per month. The price for more than 50,000 external users is $0.00325 per Monthly Active User in the P1 tier and $0.01625 per Monthly Active user in the P2 tier.

Costs for training users is minimal or zero, updates to the platform come for free, and the cost for developers to implement the tool vary widely. If your organization has employees that understand Azure AD and JavaScript, then there would be no additional cost. Otherwise, developers or contractors would need to be hired for implementation.

Competition

Other tools like Microsoft Identity Platform are Callsign, Google Authentication, Cisco Duo, Gemalto, and others. Microsoft has the advantage of being the developer of the world's most common personal computer operating system, Windows, which means that many users already have Microsoft accounts and are familiar with Microsoft products. Microsoft has an established cloud platform in Azure which is well-known and trusted by organizations globally. Users want a fast and pleasant user experience that they know they can trust. Additionally, Microsoft verifies application publishers so the user can feel comfortable working with them.

Recommendation

My recommendation is that you acquire Microsoft Identity Platform for secure authentication. Passwords are one of the biggest weak points in any organization's infrastructure and a data breach can cost millions of dollars in reparations, degradation of trust, and time lost working to recover from the breach that your employees could spend on other projects. 2FA and MFA has been used to overcome these issues, and Microsoft not only implements the option for either additional authentication method, but they also provide machine learning algorithms to prevent bad actors from circumventing your efforts.