Professional Labs: Identity Management

Traditionally, network security has been the primary strategy for maintaining an organization's network perimeter. But with the rise of BYOD policies and cloud applications, network perimeters are becoming increasingly porous and less effective at defending against cyber-attack. For this reason, many consider identity management to constitute the new data security perimeter.

For those on the Azure cloud, Active Directory (Azure AD) is the Microsoft solution for identity and access management. Azure AD is a multi-tenant, cloud-based directory and identity management service from Microsoft. It combines core directory services, application access management, and identity protection into a single solution.

The following are three ways you can leverage Azure AD and identity management to ensure your network perimeter remains secure.

Centralize identity management

While many organizations aspire to exist 100% in the cloud, the reality is that nearly all cloud deployments are a hybrid of on-premises and public cloud infrastructure. To enable your IT team to manage accounts from a single location, on-premises and cloud directories need to be integrated. This also provides a common identity for users accessing cloud and on-premises resources, which allows them to be more productive.

If you don't integrate your on-premises identity with the cloud, managing accounts becomes far more challenging. This extra overhead increases the likelihood of mistakes and security breaches.

To centralize identity management, organizations can use Azure AD Connect for on-premises and cloud directories. You can also use Azure AD Connect to enable password hash synchronization. Hash synchronization is a feature used to synchronize user password hashes from on-premises Active Directory instances to a cloud-based Azure AD instance.

Leverage role-based access control (RBAC)

Due to the shift from network to people as a perimeter, it's imperative that organizations restrict access to privileged information where possible. RBAC can be used to assign permissions to users, groups, and applications at various scopes. The scope can be a subscription, a resource group, or a single resource.

Azure makes it easy to assign roles to users using built-in RBAC features. If you don't enforce data access control by using tools such as RBAC, you're likely giving more privileges than necessary to your users. This can lead to data compromise by allowing user access to certain types of data (for example, high business impact) that they don't strictly need.

Restrict access to privileged data where possible

Securing privileged access is a critical first step in protecting data assets. Minimizing the number of people who have access to secure information or resources decreases the odds of a data breach occurring, as the more users who have access to data, the more potential points of attack are created. This also decreases the chances of an authorized user inadvertently affecting a sensitive resource.

So what is a privileged account? Privileged accounts administer and manage IT systems. For this reason, they're a prime target for cyber attackers who want to gain access to your data and systems.

Organizations that fail to secure access to privileged accounts and data may find that they have too many users in highly privileged roles and are more vulnerable to attack. Cyber attackers and malicious actors use credential theft to target admin accounts and other elements of privileged access to gain access to sensitive data.

To begin restricting privileged access, isolate systems and accounts from the risk of being exposed to malicious users. You should also work to create and follow a roadmap to secure identities and access to privileged data. To accomplish this in the Hybrid Azure Cloud with Azure AD, begin by following these best practices:

- Enable Azure AD Privileged Identity Management. You will begin receiving emails when new users are given access to highly privileged roles.

- Implement “just in time” access to further lower the exposure time of privileges and increase your visibility into the use of privileged accounts.
- Turn on and require Azure Multi-Factor Authentication at sign-in for anyone who is permanently assigned to an Azure AD admin role.

Have more questions about security in the cloud? Contact http://prolabs.co.in/contact