Azure Identity and Security Workshop Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Azure Identity and Security Workshop, Microsoft Azure ortamlarında kimlik, erişim ve güvenlik yönetiminin temel bileşenlerini uygulamalı olarak öğrenmek isteyen katılımcılar için hazırlanmış **bir günlük yoğun bir atölye çalışmasıdır**.

Eğitim, yalnızca Azure güvenlik özelliklerinin ne işe yaradığını açıklamakla kalmaz; katılımcıların bu özelliklerin nasıl yapılandırıldığını ve bir Azure ortamında nasıl kullanılabileceğini uygulamalar üzerinden görmesini sağlar.

Atölye boyunca kullanıcı kimliklerinin oluşturulmasından ayrıcalıklı erişimlerin yönetilmesine, Multi-Factor Authentication kullanımından Role-Based Access Control yapılandırmasına kadar Azure kimlik ve güvenlik yönetiminin önemli alanları ele alınır. Azure Policies ve Conditional Access gibi kontroller sayesinde kurumların kullanıcı ve kaynak erişimlerini daha kontrollü şekilde yönetmesine yardımcı olan özellikler de incelenir.

Prerequisites

Katılımcıların eğitim öncesinde **Azure temelleri konusunda temel bilgiye sahip olması** beklenmektedir. Bu bilgi, Azure Fundamentals eğitimi veya eşdeğer deneyim yoluyla edinilebilir.

MFA Gereksinimi

Bu eğitimde **Multi-Factor Authentication (MFA)** kullanımı gerekmektedir. Bu nedenle katılımcıların eğitim başlamadan önce gerekli MFA uygulamasını mobil cihazlarına kurmuş ve kullanıma hazır hale getirmiş olmaları gerekir.

Who Should Attend

Bu eğitim:

- Microsoft Azure'un sunduğu kimlik ve güvenlik özelliklerini tanımak isteyen,
- Azure ortamlarında erişim yönetiminin nasıl gerçekleştirildiğini öğrenmek isteyen,
- Azure güvenlik kontrollerini uygulamalı olarak deneyimlemek isteyen,
- Cloud ve IT operasyonlarında kimlik güvenliği konusunda temel bilgi edinmek isteyen

katılımcılar için uygundur.

Azure Identity and Security Workshop Eğitimi

Süre: **1 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Eğitimin sonunda katılımcılar:

- Azure ortamında kullanıcı kimliklerinin ve hesapların nasıl oluşturulduğunu anlayabilecek,
- Privileged Identity Management ile ayrıcalıklı erişimlerin yönetilme yaklaşımını tanıyabilecek,
- Multi-Factor Authentication kullanarak hesap güvenliğinin nasıl güçlendirildiğini anlayabilecek,
- Self-Service Password Reset özelliğinin kullanım amacını ve işleyişini açıklayabilecek,
- RBAC ile Azure kaynaklarına erişimin rol bazlı olarak nasıl kontrol edildiğini kavrayabilecek,
- Azure Policies kullanarak kaynaklar üzerinde kurumsal kuralların nasıl uygulanabileceğini anlayabilecek,
- Conditional Access ile erişim kararlarının belirli koşullara göre nasıl yönetildiğini görebilecek,
- Azure kimlik ve güvenlik özelliklerini birlikte kullanarak daha kontrollü bir erişim modeli oluşturmanın temel yaklaşımını kavrayabilecektir.

Outline

1. User Identity ve Account Creation

Azure ortamındaki kimlik yönetiminin başlangıç noktası olan kullanıcı ve hesap oluşturma süreçleri ele alınır.

- Kullanıcı kimliklerinin oluşturulması
- Kullanıcı hesaplarının yönetilmesi
- Kimliklerin Azure kaynaklarına erişimdeki rolü
- Temel hesap yönetimi yaklaşımı

2. Privileged Identity Management (PIM)

Yüksek yetkili erişimlerin daha kontrollü şekilde yönetilmesine yardımcı olan PIM özellikleri incelenir.

- Privileged access kavramı
- Ayrıcalıklı rollerin yönetilmesi
- Yüksek yetkili erişimlerin kontrol altında tutulması
- PIM'in Azure güvenlik yaklaşımındaki yeri

3. Multi-Factor Authentication (MFA)

Kullanıcı hesaplarını yalnızca parola kullanımına bağlı bırakmayan ek doğrulama yaklaşımı ele alınır.

- MFA kavramı
- Çok faktörlü doğrulamanın amacı
- Kullanıcı hesaplarında MFA kullanımı
- Kimlik güvenliğinin güçlendirilmesi

4. Self-Service Password Reset

Kullanıcıların parola işlemlerini daha bağımsız şekilde gerçekleştirmesine yardımcı olan Self-Service Password Reset özelliği incelenir.

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Self-Service Password Reset yaklaşımı
- Kullanıcı parola sıfırlama süreçleri
- Kimlik yönetimindeki kullanım alanları

5. Role-Based Access Control (RBAC)

Azure kaynaklarına kimin, hangi yetkilerle erişebileceğinin rol bazlı olarak yönetilmesi ele alınır.

- RBAC'ın temel çalışma mantığı
- Roller üzerinden erişim yönetimi
- Kullanıcı ve kaynak yetkilendirmesi
- Azure ortamında kontrollü erişim oluşturma

6. Azure Policies

Azure kaynaklarının belirlenen kurallara uygun şekilde yönetilmesini destekleyen Azure Policies incelenir.

- Policy yaklaşımının amacı
- Kaynaklar üzerinde kuralların uygulanması
- Azure ortamında standartların desteklenmesi
- Kaynak yönetiminin kontrol altında tutulması

7. Conditional Access

Erişim kararlarının belirli koşullara göre yönetilmesini sağlayan Conditional Access yaklaşımı ele alınır.

- Conditional Access kavramı
- Koşullara dayalı erişim yönetimi
- Kimlik ve erişim kontrollerinin birlikte kullanılması
- Azure ortamlarında erişim güvenliğinin güçlendirilmesi

Uygulamalı Öğrenme

Bu program klasik bir teorik eğitimden ziyade**uygulamalı workshop formatında** tasarlanmıştır. Katılımcılar bir günlük eğitim boyunca Azure'un kimlik ve güvenlik özelliklerini inceleyerek bunların uygulanmasına yönelik pratik deneyim kazanır.

Program özellikle Azure ortamlarında kullanıcı erişiminin daha güvenli, kontrollü ve yönetilebilir hale getirilmesi için kullanılabilecek temel araçların anlaşılmasına odaklanır.