Üniversiteler için Zero Trust Özellikli Ayrıcalıklı Erişim Yönetimi Sistemi

Giriş

Üniversiteler, öğrenci verileri, araştırma çalışmaları ve finansal bilgiler gibi hassas verileri barındırır. Bu verileri korumak, üniversitenin itibarını ve yasal yükümlülüklerini yerine getirmesini sağlamak için kritik öneme sahiptir. Ayrıcalıklı erişim yönetimi sistemleri, hassas verilere ve sistemlere erişimi kontrol ederek ve izleyerek güvenlik risklerini azaltmada önemli bir rol oynar. Bu yayın, Zero Trust güvenlik modelini benimseyen bir PAM sisteminin üniversiteler için nasıl tasarlanabileceğini ve uygulanabileceğini incelemektedir.

Zero Trust Güvenlik Modeli

Zero Trust, "asla güvenme, her zaman doğrula" ilkesine dayanan bir güvenlik modelidir. Bu model, ağın içindeki veya dışındaki hiçbir kullanıcıya veya cihaza otomatik olarak güvenilmediğini varsayar. Her erişim isteği, kimlik doğrulama ve yetkilendirme mekanizmalarından geçmelidir.

Üniversiteler için Zero Trust PAM Sistemi Mimarisi

Üniversiteler için Zero Trust özellikli bir PAM sistemi, aşağıdaki bileşenleri içermelidir:

- **Çok Faktörlü Kimlik Doğrulama:** MFA, kullanıcıların birden fazla kimlik doğrulama faktörü kullanmasını gerektirir (örneğin, parola, biyometrik doğrulama, güvenlik sorusu). Bu, yetkisiz erişim riskini önemli ölçüde azaltır.
- **En Az Ayrıcalık İlkesi:** Kullanıcılara yalnızca görevlerini yerine getirmek için ihtiyaç duydukları minimum erişim izni verilir. Bu, bir güvenlik ihlali durumunda etkilenen alanı sınırlar.
- **Oturum İzleme ve Kaydı:** Tüm ayrıcalıklı oturumlar izlenir ve kaydedilir. Bu, güvenlik olaylarını incelemek ve adli analiz yapmak için önemlidir.
- **Parola Yönetimi:** Güçlü parola politikaları uygulanır ve parolaların güvenli bir şekilde saklanması ve yönetilmesi sağlanır. Parola rotasyonu ve otomatik parola oluşturma gibi özellikler, güvenliği artırır.
- **Merkezi Yetkilendirme:** Erişim kontrolü, merkezi bir yetkilendirme sistemi üzerinden yönetilir. Bu, tutarlı bir güvenlik politikası uygulanmasını sağlar.
- **Mikro Segmentasyon:** Ağın bölümlere ayrılmasıyla, bir güvenlik ihlali durumunda etkilenen alan sınırlandırılır.
- **Güvenlik Bilgi ve Olay Yönetimi Entegrasyonu:** SIEM çözümleriyle entegrasyon, güvenlik olaylarının merkezi olarak izlenmesini ve analiz edilmesini sağlar.
- **Davranış Analitiği:** Kullanıcı davranışları analiz edilerek anormallikler tespit edilir ve potansiyel tehditler belirlenir.

Teknoloji Seçimi

PAM sistemi için güvenli, kararlı ve ölçeklenebilir teknolojiler seçilmelidir. Bu, Linux tabanlı bir işletim sistemi, güvenli bir veritabanı, MFA çözümleri ve güçlü şifreleme yöntemlerini içerebilir.

Uygulama ve Sürekli İyileştirme

Sistem, üniversitenin mevcut altyapısıyla entegre edilmeli ve aşamalı olarak devreye alınmalıdır. Sistemin performansı ve güvenlik etkinliği sürekli olarak izlenmeli ve iyileştirmeler yapılmalıdır. Kullanıcıların ZT-PAM sistemi ve güvenlik politikaları konusunda eğitilmesi sağlanmalıdır.

Sonuç

Zero Trust özellikli bir PAM sistemi, üniversitelerin hassas verilerini ve sistemlerini modern siber tehditlere karşı korumak için kapsamlı bir çözüm sunar. Bu sistem, güvenlik duruşunu güçlendirir, yasal düzenlemelere uyumu sağlar, operasyonel verimliliği artırır ve güvenlik risklerini azaltır. Üniversiteler, Zero Trust ilkelerini benim

1. Kimlik ve Erişim Yönetimi Katmanı:

- **Teknolojiler:** Çok Faktörlü Kimlik Doğrulama, Biyometrik Kimlik Doğrulama, Tek Kullanımlık Parolalar, Kimlik Sağlayıcılar (IdP - Okta, Azure AD, Auth0 gibi).
- **Nasıl Kullanılır:** Bu katman, kullanıcıların kimliklerini doğrulamak ve yetkilendirmek için kullanılır. MFA, birden fazla kimlik doğrulama faktörü gerektirir (örneğin, bir şey bildiğiniz - parola, bir şeyiniz olan - güvenlik anahtarı, bir şey olduğunuz - biyometrik veri). IdP'ler, merkezi kimlik yönetimi sağlar ve kullanıcıların farklı sistemlere tek bir oturum açma ile erişmelerini sağlar.

2. Erişim Kontrol Katmanı:

- **Teknolojiler:** Rol Tabanlı Erişim Kontrolü, Nitelik Tabanlı Erişim Kontrolü, Yazılım Tanımlı Çevre.
- **Nasıl Kullanılır:** Bu katman, kullanıcıların hangi kaynaklara erişebileceğini belirler. RBAC, kullanıcılara roller atayarak ve rollere izinler vererek erişimi kontrol eder. ABAC, kullanıcıların ve kaynakların özelliklerine dayalı olarak daha dinamik ve esnek bir erişim kontrolü sağlar. SDP, uygulamalara güvenli bir şekilde erişim sağlamak için ağ segmentasyonu ve erişim kontrolü kullanır.

3. Oturum Yönetimi Katmanı:

- **Teknolojiler:** Ayrıcalıklı Oturum Yönetimi araçları, Oturum Kaydı ve İzleme.
- **Nasıl Kullanılır:** Bu katman, ayrıcalıklı kullanıcı oturumlarını yönetir, izler ve kaydeder. PSM araçları, ayrıcalıklı hesapların güvenli bir şekilde saklanmasını ve yönetilmesini sağlar. Oturum kaydı ve izleme, güvenlik olaylarını incelemek ve adli analiz yapmak için önemlidir.

4. Tehdit Algılama ve Müdahale Katmanı:

- **Teknolojiler:** Güvenlik Bilgi ve Olay Yönetimi sistemleri, Kullanıcı ve Varlık Davranış Analitiği, Saldırı Tespit ve Önleme Sistemleri (IDS/IPS).

- **Nasıl Kullanılır:** Bu katman, şüpheli aktiviteleri tespit etmek ve güvenlik olaylarına müdahale etmek için kullanılır. SIEM sistemleri, farklı kaynaklardan güvenlik günlüklerini toplar ve analiz eder. UEBA, kullanıcı ve cihaz davranışlarındaki anormallikleri tespit eder. IDS/IPS, ağ trafiğini izler ve kötü amaçlı aktiviteleri engeller.

5. Veri Güvenliği Katmanı:

- **Teknolojiler:** Şifreleme (veri hareket halindeyken ve beklerken), Veri Kaybı Önleme, Veri Maskeleme.
- **Nasıl Kullanılır:** Bu katman, hassas verilerin korunmasını sağlar. Şifreleme, verilerin yetkisiz erişime karşı korunmasını sağlar. DLP, hassas verilerin kuruluş dışına çıkmasını önler. Veri maskeleme, hassas verilerin belirli kısımlarını gizleyerek güvenliği artırır.

ZT-PAM Projesinin Aşamaları:

1. **Planlama:** Gereksinimlerin belirlenmesi, kapsamın tanımlanması, bütçenin oluşturulması.
2. **Tasarım:** Sistem mimarisinin tasarlanması, teknoloji seçiminin yapılması.
3. **Uygulama:** Sistemin kurulumu ve yapılandırması.
4. **Test:** Sistemin test edilmesi ve güvenlik açıklarının giderilmesi.
5. **Dağıtım:** Sistemin canlı ortama taşınması.
6. **İzleme ve Bakım:** Sistemin