Pega Güvenlik Mimarisi: Erişim Kontrolü ve Veri Koruma Stratejileri

Yönetici Özeti

Bu brifing belgesi, Pega platformundaki temel güvenlik ve erişim kontrolü mekanizmalarını incelemektedir. Analiz, üç temel erişim kontrol modeline odaklanmaktadır: Rol Tabanlı Erişim Kontrolü (RBAC), Nitelik Tabanlı Erişim Kontrolü (ABAC) ve İstemci Tabanlı Erişim Kontrolü (CBAC). RBAC, Pega'daki güvenlik uygulamalarının yaklaşık %90'ını oluşturan, kullanıcı rollerine (örneğin, yönetici, geliştirici, kullanıcı) dayalı standart yaklaşımdır. ABAC, rollerin ötesinde daha ayrıntılı bir kontrol sağlayarak, kullanıcıların departman veya konum gibi belirli niteliklerine (özelliklerine) dayalı olarak erişimi yönetir. CBAC ise özellikle Kişisel Tanımlayıcı Bilgilerin (PII) korunmasına odaklanır ve GDPR gibi düzenlemelerden kaynaklanan gereksinimleri karşılamak üzere tasarlanmıştır. Bu temel modellerin yanı sıra, belge ek güvenliği, veri şifreleme (hem blob hem de özellik düzeyinde) ve alan düzeyinde denetim gibi tamamlayıcı güvenlik mekanizmalarını da ayrıntılı olarak ele almaktadır.

Erişim Kontrol Modelleri

Pega, farklı güvenlik senaryolarını ele almak için katmanlı bir erişim kontrolü yaklaşımı sunar. Bu modeller, tek başlarına veya birlikte kullanılarak esnek ve sağlam bir güvenlik yapısı oluşturur.

Rol Tabanlı Erişim Kontrolü (RBAC)

RBAC, Pega'daki güvenliğin temel taşıdır ve erişim haklarını bir kullanıcının organizasyon içindeki rolüne göre tanımlar. Pega, kutudan çıktığı haliyle Kullanıcı (User), Yönetici (Manager), Geliştirici (Developer) ve Sistem Yöneticisi (Administrator) gibi temel rollerle gelir.

RBAC'nin Temel Bileşenleri:

- **Operatör ID (Operator ID):** Sisteme giriş yapan bireysel kullanıcıyı temsil eder.
- **Erişim Grubu (Access Group):** RBAC'nin merkezinde yer alır ve üç temel işlevi vardır:
    - Kullanıcının hangi **uygulama kuralına (application rule)** erişebileceğini belirler (Erişim Grubu ile Uygulama Kuralı arasında bire bir ilişki vardır).
    - Kullanıcının göreceği **kullanıcı arayüzünü (portal)** tanımlar (örneğin, geliştirici portalı vs. kullanıcı portalı).
    - Kullanıcıya atanmış **rolleri (roles)** listeler (Erişim Grubu ile Roller arasında bire çok ilişki vardır).
- **Roller (Roles):** Bir kullanıcının sahip olduğu tüm potansiyel **yetkinlikleri (capabilities)** tanımlar. Bu, kullanıcının teorik olarak neler yapabileceğinin bir listesidir.
- **Rolün Nesneye Erişimi (Access of Role to Object - ARO):** Bir kullanıcının belirli nesneler (sınıflar) üzerinde **gerçekte ne yapmaya yetkili (authorized)** olduğunu tanımlar. Roller tarafından sağlanan geniş yetkinlikleri kısıtlayarak veya özelleştirerek çalışır. Bir rol bir kullanıcıya 10 yetkinlik verebilirken, ARO belirli bir nesne için bu yetkinliklerden yalnızca 5'ini kullanmasına izin verebilir.
    - **Analoji:** Bir eve gelen çocukların teorik olarak her şeyi yapma potansiyeli (Roller) vardır, ancak ebeveynlerinin onlarla nasıl konuşacaklarına dair sınırlar koyması (ARO) gibi, ARO da kullanıcının potansiyelini belirli nesneler üzerinde sınırlar.
- **Üretim Seviyeleri (Production Levels):** ARO kuralları, 0'dan 5'e kadar olan seviyelerle bir ortamdaki yetkileri tanımlar. Bir kullanıcının bir eylemi gerçekleştirebilmesi için yetki seviyesinin, içinde bulunduğu ortamın seviyesine eşit veya ondan yüksek olması gerekir.
    - **5:** Üretim (Production)
    - **4:** Üretim Öncesi (Pre-production)
    - **3:** Test
    - **2:** Geliştirme (Development)
    - **1:** Deneysel (Experimental)

  - **0:** Yetki Verme (Do Not Grant)
- **Ayrıcalıklar (Privileges):** Bir rol içinde daha da ayrıntılı kontrol sağlar. Genellikle bir When kuralına dayanır ve "kullanıcı bir yönetici ise" gibi koşullara bağlı olarak ek yetenekler sunar. Bu, belirli bir aktiviteyi çalıştırma, bir bölümü gösterme veya bir yazışma gönderme gibi eylemlere uygulanabilir.
- **Erişim Yöneticisi (Access Manager):** Bir erişim grubunun farklı vaka türleri (case types) üzerindeki yetkilerini kuş bakışı bir görünümle sunan bir araçtır. ARO ilişkilerini görselleştirir ve yönetimi kolaylaştırır.
- **Kalıtım (Inheritance):** Pega'nın nesne yönelimli doğası gereği, alt vakalar (child cases) varsayılan olarak üst vakaların (parent case) güvenlik ayarlarını miras alır. Ancak, bu kalıtım, alt vaka için özel bir ARO veya ABAC kuralı tanımlanarak geçersiz kılınabilir.

Nitelik Tabanlı Erişim Kontrolü (ABAC)

ABAC, yalnızca kullanıcı rolüne dayalı erişimin yetersiz kaldığı durumlarda, daha ayrıntılı ve bağlama duyarlı bir güvenlik katmanı sağlar. Erişim kararları, kullanıcının veya verinin belirli niteliklerine (özelliklerine) göre verilir.

- **Kullanım Senaryosu:** Bir kullanıcı grubundaki belirli bireylere özel erişim hakları tanımak gerektiğinde kullanılır. Örneğin, bir devlet kurumundaki tüm kullanıcılar aynı role sahip olabilir, ancak "adli tıp departmanında" çalışan bir kullanıcının, diğerlerinin erişemediği hassas verilere erişmesi gerekebilir.
- **Uygulama:** Access Control Policy (Erişim Kontrol Politikası) kuralları aracılığıyla uygulanır. Bu politikalar, belirli bir özelliğin (property) değeri belirli bir koşulu sağladığında erişime izin verir veya erişimi kısıtlar.
- **İşleyiş:** ABAC, RBAC'nin yerine geçmez; onunla birlikte çalışır. Kullanıcı önce RBAC aracılığıyla yetkilendirilir, ardından ABAC ek bir kontrol katmanı olarak devreye girer.
- **Politika Türleri:** Oku (Read), Güncelle (Update), Keşfet (Discover), Sil (Delete) ve Özellik Oku (Property Read) gibi çeşitli eylemler için politikalar oluşturulabilir.
- **İpucu:** Kaynakta belirtildiği üzere, FBI veya CIA gibi kurumlardan bahseden senaryolar genellikle ABAC kullanımına işaret eder.

İstemci Tabanlı Erişim Kontrolü (CBAC)

CBAC, özellikle Kişisel Tanımlayıcı Bilgilerin (PII - Personally Identifiable Information) korunması amacıyla geliştirilmiş bir güvenlik modelidir.

- **Kullanım Senaryosu:** GDPR (Genel Veri Koruma Tüzüğü) gibi düzenlemelerden kaynaklanan, kişisel verilerin korunması ve yönetilmesi gerekliliklerini karşılamak için kullanılır.
- **Kökeni:** Avrupa Birliği'ndeki veri gizliliği düzenlemeleri ve Facebook gibi şirketlerin kişisel verileri kullanmasıyla ilgili endişelerden doğmuştur.
- **Uygulama:** Pega'da CBAC'yi kullanmak için ana uygulamaya özel bir çerçeve (framework) veya uygulama eklenmesi gerekir. Bu, Client-Based Access Control (İstemci Tabanlı Erişim Kontrolü) kuralını etkinleştirir.
- **Temel İşlevler:** Bu model kapsamında üç ana seçenek sunulur: Eriş (Access), Düzelt (Rectify) ve Sil (Erase).
- **İpucu:** Bir senaryoda PII veya GDPR'den bahsediliyorsa, çözüm büyük olasılıkla CBAC ile ilgilidir.

Ek Güvenlik Mekanizmaları

Erişim kontrol modellerine ek olarak Pega, veri koruma ve izlenebilirlik için çeşitli araçlar sunar.

Ek Güvenliği (Attachment Security)

Bu mekanizma, vakalara eklenen dosyalar üzerindeki erişimi ve eylemleri kontrol eder.

- **Amaç:** Kimlerin bir eki görüntüleyebileceğini, oluşturabileceğini, düzenleyebileceğini veya silebileceğini yönetmek.
- **Uygulama:** Attachment Category (Ek Kategorisi) kuralları ile yapılandırılır.
- **Kontrol Yöntemleri:**
    - **Ayrıcalıklar (Privileges):** Eylemler, kullanıcı ayrıcalıklarına bağlanabilir. Örneğin, bir When kuralı kullanılarak "sadece yönetici ise" gibi koşullara bağlı yetkiler verilebilir. Silme seçenekleri arasında "sadece sahibi silebilirse (delete if owner)" veya "herkes silebilir (delete anything)" gibi seçenekler bulunur.
    - **Ek Düzeyinde Güvenlik (Attachment Level Security):** Bu onay kutusu etkinleştirildiğinde, eklere erişim belirli bir çalışma grubundaki (workgroup) kişilerle sınırlandırılarak daha da ayrıntılı bir kontrol sağlanır.

Veri Şifreleme (Data Encryption)

Pega, hassas verileri korumak için iki düzeyde şifreleme sunar.

- **Blob Şifrelemesi:**
    - **Amaç:** Bir vaka örneğine ait tüm verileri içeren veritabanı bloğunu (blob) şifrelemek.
    - **Yapılandırma:** İlgili sınıf (class) kuralının tanım (definition) sekmesindeki bir onay kutusu ile etkinleştirilir.
    - **Dezavantaj:** Yüksek güvenlik sağlarken, şifreleme ve şifre çözme işlemleri nedeniyle sistem performansını olumsuz etkileyebilir. FBI/CIA gibi yüksek güvenlik gerektiren senaryolar için performans düşüşü kabul edilebilir bir ödündür.
- **Özellik Düzeyinde Şifreleme (Property-Level Encryption):**
    - **Amaç:** Raporlama için optimize edilmiş (optimized for reporting) tekil özellikleri şifrelemek. Bu, tüm bloğu şifrelemek yerine yalnızca belirli hassas veri alanlarını korumak için kullanılır.

Veri Denetimi (Auditing Data)

Bu özellik, bir vaka içindeki belirli alanlarda yapılan değişikliklerin izlenmesini ve kaydedilmesini sağlar.

- **Amaç:** Hangi alanın, kim tarafından, ne zaman ve nasıl değiştirildiğini takip etmek.
- **Uygulama:** Vaka türü (case type) ayarlarındaki "Auditing" sekmesinden etkinleştirilir. İzlenmesi istenen alanlar bu ekrandan seçilir.
- **İşleyiş:** Denetim etkinleştirildikten sonra, vaka çalıştırıldığında "Geçmişi Görüntüle (View History)" sekmesi belirir. Bu sekme, izlenen alanlardaki tüm değişiklikleri, eski ve yeni değerleriyle birlikte gösterir.