ÜÇLÜ İZ MODELİ

Sürüm 1.0 - Ağustos 2026

Denetci.org

İçindekiler Tablosu

AMAÇ 3
YETKİ İZİ 3
İŞLEM İZİ 4
KARAR İZİ 4
İZLERİN İLİŞKİLENDİRİLMESİ 5
İZLERİN NİTELİKLERİ 6
YENİDEN OLUŞTURULABİLİRLİK 6
İSTİSNA İŞLEMLERİ 7
KARAR VE UYGULAMA AYRIMI 7
UYGULAMA ESASLARI 7
MODELİN SINIRLARI 8

AMAÇ

Üçlü İz Modeli, kritik işlem ve kararların sonradan anlaşılabilir, doğrulanabilir ve denetlenebilir olmasını sağlamak üzere geliştirilmiş bir izlenebilirlik modelidir.

Model, bir işlemin gerçekleştiğine ilişkin kaydın tek başına yeterli bir denetim izi oluşturmayabileceği kabulüne dayanır. Kritik bir işlem veya kararın bütüncül biçimde değerlendirilebilmesi için işlemi gerçekleştiren aktörün ve kullandığı yetkinin, gerçekleşen işlemin ve işlemin dayandığı gerekçe, kural veya tetikleyicinin birbirleriyle ilişkilendirilebilir olması gerekir.

Üçlü İz Modeli bu yapıyı üç bileşen üzerinden ele alır:

Yetki İzi: Kim veya ne yaptı ve hangi yetkiyle yaptı?

İşlem İzi: Ne, nerede, ne zaman ve nasıl yapıldı?

Karar İzi: Neden yapıldı?

Yetki İzi işlemin meşruiyetini, İşlem İzi gerçekleşmesini, Karar İzi ise gerekçelendirilmesini ortaya koyar.

Model; insan tarafından gerçekleştirilen işlemler, kurumsal kararlar, bilgi sistemleri, otomatik süreçler, algoritmik mekanizmalar ve yapay zekâ sistemleri dâhil olmak üzere kritik işlem ve kararların izlenebilirliğinin önem taşıdığı alanlarda kullanılabilir.

Üçlü İz Modeli belirli bir sektör, teknoloji veya denetim türüyle sınırlı değildir.

YETKİ İZİ

Yetki İzi, bir işlem veya kararın kim ya da ne tarafından gerçekleştirildiğinin ve söz konusu aktörün işlemi hangi yetkiye dayanarak gerçekleştirdiğinin belirlenebilmesini ifade eder.

Model kapsamında aktör yalnızca gerçek kişiyi ifade etmez. Kullanıcı hesabı, servis hesabı, uygulama, otomatik görev, robotik süreç, algoritma, yapay zekâ sistemi veya yapay zekâ ajanı da işlemin aktörü olabilir.

Aktörün belirlenmesi ile kullanılan yetkinin belirlenmesi birbirinden farklı hususlardır. Bir işlemin hangi aktör tarafından gerçekleştirildiğinin bilinmesi, söz konusu aktörün o işlemi gerçekleştirmeye yetkili olduğunu tek başına göstermez.

Bu nedenle Yetki İzinin, işlemin niteliğine göre, aktör kimliğinin yanı sıra yetkinin kaynağı ve kapsamının da belirlenebilmesine imkân vermesi gerekir.

Yetki İzi kapsamında;

- aktör veya hesap kimliği,
- rol ve yetki profili,
- yetkinin kaynağı,

- yetkinin kapsamı,
- yetkinin geçerlilik dönemi,
- yetki devri veya vekâlet,
- ilgili onay ilişkileri

gibi unsurlar dikkate alınabilir.

Kritik bir işlemin doğrulanabilir bir aktöre ve işlemin gerçekleştirilmesine imkân veren belirlenebilir bir yetkiye bağlanabilmesi esastır.

İŞLEM İZİ

İşlem İzi, meydana gelen olayın veya gerçekleştirilen faaliyetin ne olduğunu ve hangi koşullarda gerçekleştiğini ortaya koyar.

İşlem İzinin, işlemin niteliğine göre;

- ne yapıldığını,
- işlemin nerede gerçekleştirildiğini,
- ne zaman gerçekleştirildiğini,
- hangi yöntem veya mekanizmayla gerçekleştirildiğini

belirlemeye imkân vermesi gerekir.

Bu kapsamda işlem türü, işlem konusu kayıt veya varlık, kullanılan sistem veya süreç, tarih ve zaman bilgisi, kullanılan kanal veya yöntem, işlemin manuel ya da otomatik gerçekleştirilme durumu, işlem sonucu ile hata veya istisna bilgileri İşlem İzinin parçasını oluşturabilir.

Kritik işlemlerde yalnızca işlemin gerçekleştirildiğinin değil, işlemin meydana getirdiği değişikliğin de belirlenebilmesi önem taşır.

Bu nedenle gerekli olduğu durumlarda aşağıdaki ilişkinin izlenebilmesi gerekir:

Önceki durum → İşlem → Sonraki durum

Bir yetki değişikliğinde önceki ve sonraki yetkilerin, bir limit değişikliğinde önceki ve sonraki limitlerin veya bir kayıt değişikliğinde değiştirilen değerlerin belirlenebilmesi bu kapsamda değerlendirilir.

KARAR İZİ

Karar İzi, bir işlem veya kararın neden ortaya çıktığının belirlenebilmesini ifade eder.

Bir işlemin kim tarafından, nerede, ne zaman ve nasıl gerçekleştirildiğinin bilinmesi, işlemin neden gerçekleştirildiğini her durumda açıklamaz. Karar İzi, işlemin arkasındaki gerekçe veya mekanizmanın izlenebilirliğini sağlar.

Karar İzinin dayanağı işlemin niteliğine göre;

- iş gerekçesi,
- karar kriteri,
- değerlendirme sonucu,
- risk değerlendirmesi,
- yönetici veya kurul kararı,
- politika veya prosedür,
- iş kuralı,
- kullanılan bilgi veya veri,
- algoritmik koşul,
- model çıktısı,
- sistem olayı,
- otomatik tetikleyici

olabilir.

Karar İzi yalnızca insan tarafından verilen kararlarla sınırlı değildir.

Önceden tanımlanmış bir iş kuralının uygulanması veya belirli bir olayın otomatik bir işlemi başlatması da Karar İzi kapsamında değerlendirilir.

Örneğin bir hesabın belirli sayıda başarısız oturum açma girişimi sonrasında otomatik olarak kilitlenmesi durumunda hesabın kilitlenmesi İşlem İzini, işlemi gerçekleştiren sistem ve yetkisi Yetki İzini, kilitlemeyi başlatan güvenlik kuralı ve gerçekleşen başarısız girişimler ise Karar İzini oluşturur.

Karar İzinin, her kararın bütün düşünsel sürecinin kayıt altına alınması şeklinde yorumlanmaması gerekir. Kritik işlem veya kararın neden ortaya çıktığının denetim bakımından gerekli ölçüde anlaşılabilir ve doğrulanabilir olması yeterlidir.

İZLERİN İLİŞKİLENDİRİLMESİ

Yetki, İşlem ve Karar İzlerinin aynı sistem veya kayıt içerisinde tutulması zorunlu değildir.

Yetki bilgileri bir kimlik ve erişim yönetimi sisteminde, işlem kayıtları uygulama sisteminde, kararın dayanağı ise iş akışı, talep veya karar yönetimi sisteminde bulunabilir.

Bununla birlikte üç izin gerektiğinde aynı işlem veya karar etrafında ilişkilendirilebilmesi gerekir.

İlişkilendirme;

- işlem veya olay kimliği,
- aktör kimliği,
- talep numarası,

- karar numarası,
- süreç numarası,
- korelasyon kimliği,
- güvenilir zaman bilgisi

gibi yöntemlerle sağlanabilir.

Kullanılan yöntem model açısından belirleyici değildir. Esas olan, bir işlem bakımından Yetki, İşlem ve Karar İzlerinin birbirlerinden kopuk kayıtlar olarak kalmamasıdır.

İzlerin ayrı ayrı mevcut olması, aralarındaki ilişkinin kurulamaması durumunda işlemin bütüncül biçimde değerlendirilmesi için yeterli olmayabilir.

İZLERİN NİTELİKLERİ

Üçlü İz Modelinde bir izin yalnızca mevcut olması yeterli kabul edilmez. İzin denetim amacıyla kullanılabilmesi için kaynağının belirlenebilir, bütünlüğünün korunmuş, diğer ilgili izlerle ilişkilendirilebilir ve gerektiğinde erişilebilir olması gerekir.

Kaynağın Belirlenebilirliği: İzin hangi kişi, sistem, uygulama veya süreç tarafından üretildiği belirlenebilmelidir.

Bütünlük: İzler yetkisiz değiştirme, silme, ekleme veya diğer manipülasyonlara karşı uygun şekilde korunmalıdır.

İlişkilendirilebilirlik: Farklı kaynaklarda bulunan Yetki, İşlem ve Karar İzleri aynı olay veya karar çevresinde bir araya getirilebilmelidir.

Erişilebilirlik: İzler, yetkili inceleme veya denetim faaliyetleri sırasında makul süre ve yöntemlerle erişilebilir olmalıdır.

Bu nitelikler model kapsamında ayrı birer iz oluşturmaz; Yetki, İşlem ve Karar İzlerinin kullanılabilirliğine ilişkin ortak gereklilikleri ifade eder.

YENİDEN OLUŞTURULABİLİRLİK

Üçlü İz Modelinin uygulanmasında, kritik bir olayın sonradan makul ölçüde yeniden oluşturulabilmesi gözetilir.

Yeniden oluşturulabilirlik; yetkili bir inceleyicinin mevcut izlerden hareketle işlemi gerçekleştiren aktörü ve yetkisini, gerçekleşen işlemi, işlemin zamanını ve yöntemini, meydana gelen değişikliği ve işlemin dayandığı gerekçe veya tetikleyiciyi bir araya getirerek olayın gelişimini anlayabilmesini ifade eder.

Yeniden oluşturulabilirlik, olayın bütün teknik ayrıntılarıyla tekrar edilmesi anlamına gelmez. Amaç, işlem veya kararın denetim açısından önemli unsurlarının sonradan güvenilir biçimde ortaya konulabilmesidir.

İSTİSNA İŞLEMLERİ

Normal süreç dışında gerçekleştirilen işlemler Üçlü İz Modeli bakımından ayrıca önem taşır.

Manuel müdahaleler, olağan süreç dışı onaylar, kontrol veya kuralın devre dışı bırakılması, yetki aşımı, otomatik işlemin insan tarafından değiştirilmesi ve benzeri istisnaların niteliğine uygun izlerin oluşturulması gerekir.

Bu tür işlemlerde özellikle;

- müdahaleyi gerçekleştiren aktörün,
- kullanılan yetkinin,
- yapılan değişikliğin,
- istisnanın gerekçesinin

belirlenebilir olması önemlidir.

İstisna işlemlerinin taşıdığı risk, olağan işlemlere göre daha ayrıntılı iz oluşturulmasını gerektirebilir.

KARAR VE UYGULAMA AYRIMI

Bir işlemin yapılmasına karar veren aktör ile işlemi fiilen gerçekleştiren aktör aynı olmak zorunda değildir.

Bir yönetici işlemi onaylayabilir, bir çalışan talebi oluşturabilir ve bir bilgi sistemi işlemi otomatik olarak gerçekleştirebilir.

Bu durumda Yetki, İşlem ve Karar İzlerinin karar ve uygulama arasındaki ilişkiyi ortaya koyacak şekilde ilişkilendirilebilmesi gerekir.

Otomasyon kullanılması, yetki ve hesap verebilirlik zincirini ortadan kaldırmaz. İşlemi gerçekleştiren makine aktörünün kimliği ile kendisine tanımlanan yetkinin ve işlemi başlatan karar veya tetikleyicinin belirlenebilir olması gerekir.

UYGULAMA ESASLARI

Üçlü İz Modeli, bir puanlama veya olgunluk modeli değildir. Modelin uygulanmasında esas olan, kritik işlem veya karar bakımından Yetki, İşlem ve Karar İzlerinin mevcut olup olmadığının, gerekli unsurları içerip içermediğinin ve aynı olay çevresinde ilişkilendirilebilir durumda bulunup bulunmadığının değerlendirilmesidir.

Tespit edilen eksiklikler ilgili iz üzerinden ifade edilir.

Yetki İzi Eksikliği: İşlemi gerçekleştiren aktörün veya kullanılan yetkinin dayanağının belirlenemediği durumları;

İşlem İzi Eksikliği: İşlemin ne olduğunun veya gerçekleşme koşullarının yeterli biçimde ortaya konulamadığı durumları;

Karar İzi Eksikliği: İşlemin dayandığı gerekçe, kural, değerlendirme veya tetikleyicinin belirlenemediği durumları;

izler arası ilişki eksikliği ise izlerin ayrı ayrı mevcut olmasına rağmen aynı işlem veya karar etrafında ilişkilendirilemediği durumları ifade eder.

Modelin uygulanacağı işlem ve kararlar ile oluşturulacak izlerin kapsamı, her durumda aynı olmak zorunda değildir. Gerekli ayrıntı düzeyi belirlenirken işlemin kritikliği, taşıdığı risk, finansal veya hukuki etkisi, geri döndürülebilirliği, otomasyon düzeyi ve ilgili yükümlülükler dikkate alınır.

Üçlü İz Modelinin uygulanmasında amaç, mümkün olan en fazla kaydın oluşturulması değil; kritik bir işlem veya kararın meşruiyetini, gerçekleşmesini ve gerekçesini sonradan ortaya koymaya yetecek izlerin oluşturulması ve korunmasıdır.

MODELİN SINIRLARI

Üçlü İz Modeli, belirli bir loglama, kayıt tutma veya veri saklama standardı değildir. Model herhangi bir teknoloji, ürün, veri formatı veya teknik mimarinin kullanılmasını zorunlu tutmaz.

Modelin uygulanması, bütün işlemlerin aynı kapsam ve ayrıntı düzeyinde kayıt altına alınmasını gerektirmez. İzlerin kapsamı ve niteliği, ilgili işlem veya kararın özelliklerine ve uygulanabilir yükümlülüklere göre belirlenir.

Üçlü İz Modelinin uygulanmış olması, tek başına bir işlemin hukuka uygun, güvenli, doğru veya etkin olduğunu göstermez. Benzer şekilde model, mevcut mevzuat, denetim standartları, iç kontrol çerçeveleri, bilgi güvenliği gereksinimleri veya diğer mesleki düzenlemelerin yerine geçmez.