



BULUT GÜVENLİK MİMARİSİ VE ALTYAPI RAPORU

TürkHukuk Production Güvenlik Mimarisi Raporu

CloudMetrik tarafından hazırlanmıştır

İçindekiler

1. Güvenlik Yaklaşımı ve Temel Mimari Prensipler	3
2. Veri Güvenliği ve Anahtar / Secret Yönetimi	3
2.1 Veri Konumu	3
2.2 Veri Disklerinin Şifrelenmesi	3
2.3 Anahtar Rotasyonu ve Secret Yönetimi	4
2.4 OBS Üzerinde Saklanan Veriler	4
2.5 Veri Gizliliği ve Zero Data Retention (ZDR) Yaklaşımı	4
2.6 Veri Yaşam Döngüsü ve Saklama Yaklaşımı	4
3. Şifreli İç Ağ İletişimi	5
4. Ağ İçi Erişim Sınırları ve İzolasyon	5
4.1 Erişim ve Kimlik Yönetimi	5
5. Yüksek Erişilebilirlik ve Süreklilik	5
6. Güvenli Operasyon ve Değişiklik Yönetimi	6
7. Güvenlik Mimarisi Özet Tablosu	6

1. Güvenlik Yaklaşımı ve Temel Mimari Prensipler

TürkHukuk, kullanıcı ve müşteri verilerinin gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı hedefleyen çok katmanlı bir Production altyapısı kullanmaktadır. Sistem altyapısı; müşteri verilerinin Türkiye bölgesinde barındırılması, veritabanı ve depolama kaynaklarının doğrudan internet erişimine kapalı private ağ sınırları içinde tutulması ve tüm katmanlarda savunma derinliği (defense-in-depth) prensiplerinin işletilmesi esasına dayanır.

Güvenlik yaklaşımı, operasyonel dayanıklılık ve veri koruma odağında aşağıdaki temel sütunlar üzerine inşa edilmiştir:

Yerel Veri Barındırma: Tüm uygulama veritabanları, doküman depoları ve yedekleme Huawei Cloud Türkiye bölgesinde (tr-west-1) ve doğrudan internete kapalı private ağ sınırları içinde barındırılacak şekilde tasarlanmıştır.

Depolama ve İletişim Şifrelemesi: Depolanan sistem ve veri disklerinde XTS-AES-256 algoritması, nesne depolamada (OBS) SSE-KMS kullanılır. Kritik veri katmanı servisleri arasındaki uygun bağlantılarda TLS, karşılıklı kimlik doğrulama gerektiren bağlantılarda ise Mutual TLS (mTLS) kullanılır.

Anahtar ve Secret Yönetimi: Disk şifreleme anahtarları Key Management Service (KMS) bünyesindeki müşteri yönetimli anahtarlarla (CMK) idare edilir. Veritabanı parolaları ve servis kimlikleri Secret Management Service (CSMS) içinde saklanır; kalıcı secret veya statik erişim anahtarları iş yüklerinde tutulmaz.

Zero Data Retention (ZDR): Müşteri içeriklerinin yalnızca ilgili hizmet fonksiyonunun yürütülmesi amacıyla işlenmesi, yapay zeka modellerinin eğitimi amacıyla kullanılmaması ve gereksiz kalıcı içerik kopyalarının önlenmesi esas alınır.

Yüksek Erişilebilirlik ve Güvenli Operasyon: Aynı bölgede farklı Availability Zone'lara dağıtılmış yedekli veritabanı kümesi (Patroni / etcd), akıllı bağlantı havuzlama (PgBouncer / HAProxy), merkezi izleme ve hata anında güvenli duruş (fail-closed) kontrolleriyle operasyonel süreklilik desteklenir.

2. Veri Güvenliği ve Anahtar / Secret Yönetimi

2.1 Veri Konumu

TürkHukuk Production altyapısı Huawei Cloud Türkiye bölgesinde (tr-west-1) konumlandırılmıştır. Uygulama verileri, veritabanı verileri, dokümanlar ve kalıcı depolama kaynakları Türkiye bölgesindeki altyapı üzerinde tutulacak şekilde tasarlanmıştır.

Production kapsamındaki birincil veriler, sistem logları ve operasyonel yedeklemeler Huawei Cloud Türkiye bölgesinde (tr-west-1) konumlandırılacak şekilde tasarlanmıştır. Sistem yedekleri ve anlık görüntüler (snapshot) da aynı bölgedeki depolama servislerinde muhafaza edilir.

Veri katmanında kullanılan veritabanı, disk ve nesne depolama kaynakları private ağ sınırları içinde konumlanır. Müşteri verileri, doğrudan internet erişimine kapalı private ağ sınırları içindeki veritabanı servislerinde barındırılır.

2.2 Veri Disklerinin Şifrelenmesi

Production sistem ve veri diskleri Elastic Volume Service (EVS) üzerinde şifreli olarak kullanılır. EVS disk şifrelemesinde XTS-AES-256 algoritmasından yararlanılır. Bu yöntem, disk üzerinde bulunan verinin fiziksel depolama katmanında yetkisiz erişime karşı korunmasını sağlar.

Disk şifreleme anahtarları, Key Management Service (KMS) bünyesinde TürkHukuk platformuna özel tanımlanmış anahtarlarla (Customer Managed Key - CMK) yönetilir. Anahtar materyali, HSM destekli KMS altyapısında korunur; uygulama koduna, sunucu yapılandırmalarına veya çalışma ortamı değişkenlerine yazılmaz.

KMS, disk verisini şifreleyen veri şifreleme anahtarlarını (DEK) korumak için CMK kullanır. Bu katmanlı anahtar yönetimi sayesinde disk şifreleme anahtarları uygulama süreçlerinden ve operasyonel ekiplerin günlük yönetiminden ayrıştırılır.

2.3 Anahtar Rotasyonu ve Secret Yönetimi

KMS müşteri yönetimli anahtarları için periyodik otomatik anahtar rotasyonu kullanılır. Rotasyon sonrasında anahtarın kimliği ve bağlı kaynakları korunur; KMS yeni anahtar materyaliyle çalışmaya devam eder. Önceki anahtar sürümleri, daha önce şifrelenmiş verinin güvenli biçimde çözülebilmesi için KMS içinde muhafaza edilir.

Veritabanı erişim parolaları, veri katmanı servis kimlik bilgileri ve sertifika bileşenleri Secret Management Service (CSMS) içinde saklanır. Secret değerleri kaynak koda, container imajlarına veya sunucu başlangıç yapılandırmalarına eklenmez.

Sunucular yalnız ihtiyaç duydukları bilgilere platform kimlik doğrulama mekanizmaları ve geçici yetkilendirme ile erişir; kalıcı erişim anahtarları iş yükleri üzerinde tutulmaz.

2.4 OBS Üzerinde Saklanan Veriler

Doküman, corpus, yedek ve snapshot gibi nesne verileri Object Storage Service (OBS) üzerinde barındırılır. Bu depolama alanlarında TürkHukuk platformuna özel tanımlanmış anahtarlar ile SSE-KMS sunucu tarafı şifreleme kullanılır. Nesne OBS'ye yazıldığı anda depolama katmanında şifrelenir; şifre çözme işlemi ise yetkili erişim sırasında KMS denetimindeki anahtarlarla gerçekleştirilir.

Müşteri verilerini, dokümanları ve sistem yedeklerini barındıran depolama alanlarında private erişim modeli uygulanır. Erişimler, kimlik ve erişim yönetimi üzerinden tanımlanan en az ayrıcalıklı yetki politikalarıyla sınırlandırılır. Bu depolarda genele açık erişim, anonim okuma veya anonim yazma kullanılmaz; saklanan nesnelerin içeriği ve erişim yolları kontrollü şekilde yönetilir.

2.5 Veri Gizliliği ve Zero Data Retention (ZDR) Yaklaşımı

TürkHukuk, müşteri içeriğinin yalnızca talep edilen hizmet fonksiyonunun yerine getirilmesi amacıyla ve gerekli kapsamla sınırlı tutulması prensibini benimser. İlgili analiz ve sorgulama bileşenleri, kullanıcı girdilerini yalnızca anlık işlemin yürütülmesi doğrultusunda ele alır. Müşteri verilerinin herhangi bir yapay zeka modelinin eğitimi veya hizmet kapsamı dışındaki amaçlar için kullanılmaması esas alınır.

Zero Data Retention (ZDR) yaklaşımı, işlem döngüsü sırasında sistem üzerinde gereksiz kalıcı içerik kopyalarının oluşmasını önlemeyi hedefler. Hizmetin güvenli biçimde sunulması için gerekli olan operasyonel yönetim, denetim kaydı ve yedekleme süreçleri ise tanımlı veri güvenliği kontrolleri çerçevesinde yürütülür.

2.6 Veri Yaşam Döngüsü ve Saklama Yaklaşımı

Veriler; işleme, depolama, yedekleme ve erişim aşamalarını içeren yaşam döngüsü boyunca kontrollü biçimde yönetilir. Uygulama verilerinin güncelliği ve tutarlılığı ön planda tutulurken, sistem yedekleri ve operasyonel kayıt saklama ihtiyaçları ilgili kurumsal politikalar ve yasal yükümlülükler çerçevesinde ayrı ayrı ele alınır. Geçici verilerin yönetimi, tanımlı veri güvenliği prensipleri doğrultusunda ele alınır.

3. Şifreli İç Ağ İletişimi

Kullanıcıya açık web uç noktalarında güncel TLS protokolleri üzerinden HTTPS kullanılır. Production veri katmanındaki kritik servisler arası iletişim de TLS ve gerektiğinde Mutual TLS (mTLS) ile korunur. İç sertifika otoritesi tarafından oluşturulan güven zinciri, servis kimliklerinin doğrulanmasına ve şifreli iletişime destek olur.

İç sertifika otoritesinin (Internal CA) imzalama özel anahtarı iş yükü sunucularına veya uygulama container'larına dağıtılmaz. İstemcilerin güvenli bağlantı kurduğu senaryolarda istemci, tanımlı güven zincirini kabul eder ve hedef servis adını doğrular. Bu mimari model, yetkisiz dinleme ve Man-in-the-Middle (MitM) risklerini önemli ölçüde azaltır.

4. Ağ İçi Erişim Sınırları ve İzolasyon

Production ortamında uygulama, veri ve yönetim bileşenleri farklı özel ağ segmentlerinde (private subnets) çalışır. Veritabanı node'larının internete açık IP adresi yoktur; bu node'lara erişim yalnız tanımlı ağ yolları ve gerekli portlarla sınırlandırılır.

Uygulama veritabanı erişimi, özel DNS adı ve Private Load Balancer üzerinden bağımsız erişim node'larına dağıtılır. Bu erişim noktası internetten erişilemez. Güvenlik grubu kuralları, yalnız yetkili uygulama ağlarından gelen gerekli trafiğe izin verecek şekilde uygulanır.

TLS kullanılan veritabanı bağlantılarında Private Load Balancer şifreli trafiği TCP seviyesinde (Layer 4) iletir; TLS oturumunu sonlandırmaz veya içeriğini açmaz.

Yönetim erişimi ayrılmış bir bastion host üzerinden sağlanır. Doğrudan yönetim erişimi sınırlı kaynak adresleri ve güvenli anahtar doğrulamasıyla korunur.

4.1 Erişim ve Kimlik Yönetimi

Sistem bileşenlerine ve yönetim katmanına erişimler en az ayrıcalık (least privilege) ilkesiyle sınırlandırılmıştır. Sunucular ve servisler yalnızca görev tanımları gereği zorunlu olan kaynaklara erişebilir. Yönetim erişimleri kontrollü erişim noktaları ve güçlü kimlik doğrulama mekanizmaları kullanılarak yürütülür. Sistem üzerinde kalıcı erişim anahtarları barındırmak yerine, kontrollü ve sınırlı yetkilendirme yaklaşımı benimsenmektedir.

5. Yüksek Erişilebilirlik ve Süreklilik

Production PostgreSQL katmanı, aynı Türkiye bölgesindeki farklı Availability Zone'lara (AZ) dağıtılmış bir primary ve bir standby node'dan oluşur. Standby node, primary node'daki veriyi streaming replication ile güncel tutar.

Patroni, PostgreSQL node'larının rolünü ve güvenli failover sürecini yönetir. Üç üyeli etcd quorum yapısı; iki PostgreSQL node'u ile ayrı bir witness node'undan oluşur. Primary node erişilemez olduğunda, etcd quorum ve Patroni sağlık kontrolleri üzerinden sağlıklı standby node kontrollü failover sürecinde primary rolünü devralabilir. Arızadan sonra geri dönen node, güncel primary'den verisini eşitleyerek yeniden standby rolünde kümeye katılır.

Uygulama bağlantıları bağımsız erişim node'larında çalışan HAProxy ve PgBouncer katmanından geçer. HAProxy yalnız Patroni tarafından primary olduğu doğrulanan PostgreSQL node'una yönlendirme yapar. PgBouncer, bağlantı havuzlama ile veritabanı bağlantılarının kontrollü ve verimli kullanılmasına yardımcı olur. Private Load Balancer ise sağlıklı erişim node'ları arasında TCP bağlantı dağıtımı yapar.

Sağlık kontrolleri, erişim katmanındaki node'ların ve veritabanı servislerinin çalışır durumda olmasını izler. Böylece erişilemeyen bir node'a yeni bağlantı yönlendirilmez; sağlıklı node'lar hizmet vermeye devam eder.

Bu katmanlı mimari yaklaşım, tekil altyapı ve sunucu arızalarının sistem üzerindeki etkisini sınırlandırmak ve operasyonel sürekliliği desteklemek üzere tasarlanmıştır. Sistem bileşenlerinin yedekli ve kontrollü dağılımı, plansız kesinti olasılıklarını minimize etmeye yardımcı olur.

6. Güvenli Operasyon ve Değişiklik Yönetimi

Altyapı kaynakları ile veri katmanı kurulum ve işletim akışları, tanımlı güvenlik ve operasyon prosedürleri kapsamında yönetilir. Kritik veri katmanı değişiklikleri, dar kapsamlı uygulanabilir planlar ve servis sağlık kontrolleriyle ele alınır. Kurulum ve bakım akışları, beklenmeyen bir durumda işlemi güvenli biçimde durduracak fail-closed kontroller içerir.

Sistem sağlığı, erişilebilirlik ve güvenlik açısından anlamlı olaylar merkezi izleme ve kayıt mekanizmalarıyla takip edilir. Bu kayıtlar; hizmet sürekliliğini desteklemek, olay incelemelerini kolaylaştırmak ve operasyonel iyileştirmeleri yönlendirmek amacıyla ilgili erişim ve saklama politikaları çerçevesinde yönetilir.

TürkHukuk, güvenlik mimarisini altyapı ve uygulama gereksinimleri doğrultusunda güncel tutar.

7. Güvenlik Mimarisi Özet Tablosu

Aşağıdaki tablo, TürkHukuk Production altyapısında uygulanan temel güvenlik mekanizmalarını, ilgili bileşenleri ve teknik kapsamlarını özetlemektedir:

Katman / Alan	Bileşen	Güvenlik Mekanizması & Yöntem	Teknik Kapsam
Veri Konumu	Huawei Cloud (tr-west-1)	Türkiye Bölgesi Yerel Barındırma, Private Ağ İzolasyonu	Veriler ve depolama kaynakları Türkiye bölgesindeki altyapı üzerinde tutulacak şekilde tasarlanmıştır. Veritabanı node'larına doğrudan internet erişimi verilmez; erişim private ağ yolları ve tanımlı güvenlik kurallarıyla sınırlandırılır.
Depolama	Elastic Volume Service (EVS)	XTS-AES-256 Şifreleme, KMS / HSM Destekli CMK	Disk düzeyinde verinin fiziksel depolama katmanında yetkisiz erişime karşı korunmasını sağlar. Anahtar materyali sunucu ortamına yazılmaz.
Secret & Anahtar Yönetimi	KMS & CSMS	Periyodik Otomatik Anahtar Rotasyonu, Rol Tabanlı Erişim	Veritabanı parolaları, veri katmanı servis kimlikleri ve sertifikalar CSMS'te saklanır. Kalıcı erişim anahtarları yerine kontrollü geçici yetkilendirme kullanılır.
Nesne Depolama	Object Storage Service (OBS)	SSE-KMS Sunucu Tarafli Şifreleme, Müşteri Verisi İçin Private Bucket Modeli	Müşteri yönetimli anahtarlarla şifreleme ve en az ayrıcalıklı yetkilendirme uygulanır. Müşteri verisi içeren bucket'larda genele açık erişim, anonim okuma veya anonim yazma kullanılmaz.
Veri Gizliliği	Uygulama ve Yapay Zeka İşleme Bileşenleri	Zero Data Retention (ZDR) Yaklaşımı	Müşteri içeriğinin model eğitimi amacıyla kullanılmaması hedeflenir. Hizmetin işletilmesi için gerekli veri yönetimi, güvenlik kaydı ve yedekleme süreçleri ilgili kontroller çerçevesinde yönetilir.

Katman / Alan	Bileşen	Güvenlik Mekanizması & Yöntem	Teknik Kapsam
İç Ağ İletişimi	Kritik Veri Katmanı Servisleri	mTLS / TLS, Dahili Güven Zinciri (Internal CA)	Doğrulanmış iç servis katmanlarında şifreli iletişim sağlanır. Yetkisiz dinleme ve Man-in-the-Middle (MitM) risklerini önemli ölçüde azaltır.
Ağ İçi Erişim Sınırları	Private Subnet'ler, Private Load Balancer (L4), Bastion Host	Güvenlik Grupları, IP Sınırlandırması ve Güvenli Anahtar Doğrulaması	Veritabanı node'larının genel internete açık IP adresi yoktur. TLS kullanılan veritabanı bağlantılarında Private Load Balancer şifreli trafiği TCP seviyesinde iletir; TLS oturumunu sonlandırmaz veya içeriğini açmaz.
Erişim ve Kimlik Yönetimi	Yönetim Erişimi ve Servis Kimlikleri	En Az Ayrıcalık ve Kontrollü Yetkilendirme	Erişimler görev gereksinimine göre sınırlandırılır; yönetim erişimi kontrollü erişim noktaları ve güçlü kimlik doğrulama yaklaşımıyla korunur.
Yüksek Erişilebilirlik	PostgreSQL Kümesi, Patroni, etcd, HAProxy, PgBouncer	Aynı Bölgede Çoklu Erişilebilirlik Alanı (Multi-AZ), Quorum ve Sağlık Kontrolleri	Primary node erişilemez olduğunda etcd quorum ve Patroni sağlık kontrolleri üzerinden sağlıklı standby node kontrollü failover sürecinde primary rolünü devralabilir.
Operasyon Güvenliği	Güvenli Kurulum ve İşletim Süreçleri	Kontrollü Değişiklik Yönetimi, Fail-Closed Prosedürleri	Kritik altyapı ve veri katmanı değişiklikleri, planlı kontroller ve servis sağlık doğrulamalarıyla ele alınır. Beklenmeyen durumlarda fail-closed kontroller devreye girer.
İzleme ve Denetim	Merkezi İzleme ve Kayıt Mekanizmaları	Erişilebilirlik ve Güvenlik Olay Takibi	Sistem sağlığı ve güvenlik açısından anlamlı olaylar, hizmet sürekliliği ve inceleme ihtiyaçlarını desteklemek üzere izlenir.