Analiz · 26 Mayıs 2026

← Önceki·Sonraki →

Gerçek vs görünürdeki gizlilik: kendinize sormanız gereken sorular

2. döngünün operasyonel sentezi: mimari gizliliğe sahip bir hizmeti beyana dayalı gizliliğe sahip bir hizmetten ayıran sorular. Hassas veriler için herhangi bir dijital araç benimsemeden önce Avrupalı profesyonel için bir soru listesi.

Anlaşmak için: Aynı yasal bildirime sahip iki hizmet çok farklı davranabilir. Biri teknik tasarımla korur. Diğeri sözleşmesel bir vaatle korur. Fark bildirimde okunmaz — somut sorular sorularak keşfedilir. Cevapların kalitesi, ürün hakkında kendi içerikleri kadar çok şey söyler.

Mimari gizlilik ile beyana dayalı gizlilik arasındaki fark

Bu döngünün önceki yedi yazısı boyunca aynı konunun farklı katmanlarından geçtik. Schrems II ile uluslararası aktarımların hukuku. Her Cuaderno'yu mühürleyen kriptografik hash'in matematiksel fikri. Kill switch'in mimari seçimi ve neredeyse her zaman ona eşlik eden kurumsal ele geçirme. Uçtan uca şifrelemenin mekanizması ve anahtarların nerede bulunduğuna dair operasyonel soru. İş modeline göre teşviklerin hizalanması. Öz egemen kriptografik kimlik. Orantılı bir strateji olarak self-hosting. Her yazı bir açıyı ele aldı. Döngünün sonuncusu olan bu yazı, onları bir soru listesinde bir araya getiriyor.

Akılda tutulması gereken ayrım basittir: gizliliği *mimari* olan hizmetler vardır ve gizliliği *beyana dayalı* olan hizmetler vardır. Birincisi teknik tasarıma gömülüdür: gizlilik taahhüdünün belirli ihlalleri teknik olarak zordur veya imkânsızdır çünkü mimari bunlara izin vermez. İkincisi yasal bildirimin metnine yatırılmıştır: belirli ihlaller gerçekleşirse sözleşmesel olarak yaptırıma tabi olur, ama teknik olarak hiçbir şey onları engellemez. İki model de GDPR'ye uyabilir; ama biri tasarım yoluyla korur, diğeri vaat yoluyla korur ve fark operasyonel olarak devasadır.

Aşağıdaki sorular, bir durumu diğerinden ayırmak için tasarlanmıştır. Bunlar ileri düzey teknik sorular değildir. Bunlar, dürüst herhangi bir sağlayıcının kamuya açık belgelerinde cevaplayabileceği sorulardır. Cevabın kalitesi ve hassasiyeti, ürün hakkında cevabın kendisi kadar çok şey söyler. Sorular altı katmanda gruplandırılmıştır; hassas veriler için hizmeti benimsemeden önce, yalnızca ilk içgüdünün belirlediklerini değil, hepsini sormak yerinde olur.

Katman 1: mimari

Devam etmeden önce bir terimi netleştirelim. *Operatör* derken hizmeti sunan şirketi kastediyoruz: sunucuları ve yazılımı denetleyen kuruluşu, belirli bir kişiyi değil. Bu açıklığa kavuştuktan sonra temel mimari soru şudur: operatör, gönderici ile alıcı arasındaki içerikle ne yapıyor? Üç olası yanıt vardır ve bunları ayırt edebilmek gerekir, çünkü üçü de zaman zaman benzer sözcüklerle tanıtılır.

- Birincisi: içerik, operatörün bir sunucusundan açık metin olarak geçer; burada operatör, yapmamayı vaat etse bile onu okuyabilir.

- İkincisi: içerik, operatörün bir sunucusundan şifrelenmiş olarak geçer; burada anahtarlar yalnızca kullanıcıların cihazlarında bulunuyorsa operatör onu okuyamaz.
- Üçüncüsü: içerik, operatörün hiçbir sunucusundan geçmez, çünkü o belirli akışta operatörün bir sunucusu yoktur.

Bu üçü arasındaki fark derece farkı değil: tür farkıdır.

Tamamlayıcı soru — şifrelemeye dair Cuaderno'da zaten formüle edilmişti — şudur: içeriği okumaya izin veren kriptografik anahtarlara kim sahip? Bunlara kullanıcı ve yalnızca kullanıcı sahipse, şifreleme gerçektir. Bunlara ayrıca operatör de herhangi bir biçimde sahipse — „hesap kurtarma“ veya „cihazlar arası senkronizasyon“ adı altında bile — şifreleme nominaldir. Soru, dürüst bir ara cevabı kabul etmez.

Katman 2: iş modeli

İş modeline ilişkin soru, mimari soru kadar önemlidir ve aynı esaslı nedenle: teşvikler, zaman içinde, beyan edilen amaçlar özdeş olsa bile sistematik olarak farklı ürünler üretir. Operatör bugün nasıl para kazanıyor? Tek bir kaynak mı, iki mi, karışım mı? Finansman reklam veya veri ticarileştirmesi içeriyorsa, hangi veriler ticarileştiriliyor ve bu hangi GDPR yasal dayanağıyla yapılıyor? Yasal bildirimde beyan edilen amaç, profesyonelin hizmete emanet etmeyi düşündüğü üçüncü taraf verilerini kapsıyor mu?

Ve her zaman formüle edilmeyen ikinci derece soru: operatörün üç ya da beş yıllık perspektifte finansal durumu nedir? Risk sermayesi aşamasındaki bir şirket, istikrarlı kârlılığa sahip bir şirketten farklı baskılar altında çalışır. Finansman modelinin değişmesi, defalarca, kullanıcılarla yapılan örtük sözleşmenin müzakere olmaksızın yeniden yazıldığı andır.

Katman 3: yargı yetkisi

Avrupalı profesyonel için yargı yetkisi sorusu retorik değildir. Operatör hangi yargı yetkisinde kurulu? Verileri işleyen sunucular fiziksel olarak hangi ülkede? Önceki iki sorunun cevabı aynı mı yoksa farklı mı ve farklıysa hangi mevzuat uygulanır? Bir ABD şirketi tarafından işletilen bir Avrupa bölgesi, Schrems II açısından Avrupalı bir cevap değildir: şirket, sunucuların nerede olduğundan bağımsız olarak FISA 702'ye tabidir.

Tamamlayıcı operasyonel soru şudur: yarın operatörün yargı yetkisinde geçerli bir istihbarat emri gelip benim veya müşterilerimin verilerini teslim etmeyi istese ne olurdu? Dürüst cevap „şirket bunları teslim etmekle yükümlü olurdu“ ile başlıyorsa, reklam aksini ne kadar ima ederse etsin, hizmet bu emre karşı korumaz. Dürüst cevap „şirket bunları teslim edemezdi çünkü açık metin olarak elinde tutmuyor“ ile başlıyorsa, hizmet korur; ve fark, gizlilik politikasının kalitesine değil, neredeyse tamamen ilk iki katmana bağlıdır.

Katman 4: operatör ve kill switch

Operatör hizmeti uzaktan askıya almak, engellemek, silmek veya bozmak için hangi teknik kapasiteyi elinde tutuyor? Soru paranoyakça değil: operasyonel. Dijital platformlar son yıllarda bu kapasiteyi defalarca kullandı — kimi zaman kendi inisiyatifiyle, kimi zaman Hükümetlerin emriyle, kimi zaman mülkiyet veya politika değişikliklerinin ardından. Kapasite mevcutsa, hangi sözleşmesel olarak beyan edilen varsayımlar altında kullanıldığını bilmek ve son yılların pratiğinin en az o kadar önemli olduğunu gösterdiği beyan edilmemiş varsayımlar için bir pay ayırmak yerinde olur: beklenmedik mahkeme emri, uluslararası yaptırım, kurumsal yönetim değişikliği, başka bir politikaya sahip bir kuruluş tarafından satın alınma.

Kardeş soru süreklilik planına ilişkin olandır: operatör bu kapasiteyi profesyonele karşı kullanırsa — haklı olsun ya da olmasın, herhangi bir nedenle — ne kadar etkinlik süresi kullanılabilir kalır, hangi veri aktarım prosedürü mevcuttur ve hangi alternatif sağlayıcıya geçilebilir? Cevap „bu olmamalı“ ile başlıyorsa, bu operasyonel bir cevap değildir; bir vaattir.

Katman 5: kimlik ve erişim

Hizmete erişim kimlik bilgilerini kim kontrol ediyor? Operatör kullanıcının erişimini kullanıcının katılımı olmadan sıfırlayabiliyorsa — genellikle „hesap kurtarma“ denen prosedür — operatör teknik olarak hesabın koruyucusudur ve uygun prosedürle talep eden kişiye de devredebilir. Operatör erişimi sıfırlayamıyorsa, çünkü kimlik kriptografik olarak kullanıcının cihazında bulunuyorsa, operatör bir emir altında bile onu devredemez. İki yöntem de bağlama göre meşrudur; ama yine, bunlar farklıdır ve hangisinin benimsendiğini bilmek yerinde olur.

Profesyonel erişimi kaybederse profesyonelin verilerine ne olur? Operatöre bağlı kurtarma mekanizmaları — hesap, dosya, oturum — var mı? Operatör bunları kullanmaya zorlanırsa, bu mekanizmalar sektörün mesleki deontolojisiyle bağdaşır mı?

Katman 6: gelecek

Bu son katman genellikle ihmal edilir çünkü öngörü gerektirir. Hizmet başka bir şirket tarafından satın alınsaydı ne olurdu? Neredeyse tüm satın almalar, sonraki aylarda hizmet şartlarının gözden geçirilmesini beraberinde getirir. Düzenleyici gereklilikler değişseydi ne olurdu? Avrupa hukuku 2022'den bu yana kaldırma ve engelleme yükümlülüklerini azaltmadı, artırdı. Operatör ortadan kaybolsaydı ne olurdu? Bulut hizmetlerinin önemli bir kısmının operatörün kapanması senaryosu için belgelenmiş bir çıkış planı yoktur; profesyonel sorunu, onu hazırlamaya artık vakit kalmadığında keşfeder.

Bu katman için akılda tutulması gereken bir formülasyon var: operatöre daha az bağımlı mimariler, operatör değişikliklerine karşı daha dayanıklıdır. Self-hosting'in herhangi bir biçimi, öz egemen kriptografik kimlik, araya sunucu girmeyen iletişimler — bunların hepsi, mevcut bağımlılık yüzeyini azaltma yöntemiyle gelecekteki risk yüzeyini azaltır. Onu ortadan kaldırmaz; azaltır.

Yapı ile vaat arasındaki fark

Bu döngüyü tek bir cümleye damıtmamız gerekseydi, şu olurdu: yapısal cevaplar, operatör, idare veya mevzuat değişse de varlığını sürdürür; vaade dayalı cevaplar, vaat eden kişi bunları sürdürebildiği ve sürdürmek istediği sürece varlığını sürdürür. İkisi de benimsendikleri anda doğru olabilir. Ama yalnızca biri, zamanın geçişinden ve koşulların değişiminden bağımsız olarak ayakta kalır.

Bu, her profesyonelin benimsediği tüm hizmetlerden yapısal cevaplar talep etmesi gerektiği anlamına gelmez. Orantılılık meşru olmayı sürdürür: dâhili muhasebe için bir hesap tablosu, bir hastanın klinik dosyasıyla aynı cevaba ihtiyaç duymaz. Ancak şu anlama gelir: profesyonellik, her durumda ne tür bir cevabın kabul edildiğini bilmek ve bu tür bir cevabın somut veriyle orantılı olduğuna bilinçli olarak karar vermiş olmaktır.

Soru listesi, düzenli hâliyle

Döngüyü sentezleyen, her birinin cevabının bir sonrakini bilgilendirecek şekilde düzenlenmiş on iki somut soru:

1. İçerik operatörün bir sunucusundan geçiyor mu? Geçiyorsa: açık metin olarak mı, operatörün anahtarlarıyla şifrelenmiş olarak mı, yoksa yalnızca kullanıcıya ait anahtarlarla şifrelenmiş olarak mı?
2. Uçtan uca şifreleme öne sürülüyorsa, kriptografik anahtarlar nerede bulunuyor? Operatör, „kurtarma“ dâhil herhangi bir biçimde bunların herhangi bir kısmını biliyor veya saklıyor mu?
3. Hizmet hangi meta verileri üretiyor ve saklıyor? Ne kadar süreyle? Kimlere görünür?
4. Operatör nasıl finanse ediliyor? Finansman reklam veya veri ticarileştirmesi içeriyorsa, beyan edilen amaç profesyonelin emanet ettiği üçüncü taraf verilerini kapsıyor mu?
5. Operatörün üç ya da beş yıllık perspektifte finansal durumu nedir? Model değişikliğinin yakın olduğunu düşündüren faktörler var mı (bekleyen halka arz, tükenmekte olan finansman turu, olası satın alma)?

6. Operatör hangi yargı yetkisinde kurulu? Sunucular fiziksel olarak hangi ülkede? Farklıysa, işlemeye hangi ulusal mevzuat uygulanır?
7. Operatörün yargı yetkisinde geçerli bir istihbarat emri verilerimi teslim etmeyi istese ne olurdu? Şirket bunu teknik olarak yerine getirebilir miydi?
8. Operatör hizmeti askıya almak, engellemek veya silmek için hangi teknik kapasiteyi elinde tutuyor? Hangi sözleşmesel varsayımlar altında? Tarihsel olarak belgelenmiş hangi sözleşme dışı varsayımlar altında?
9. Operatör bu kapasiteyi haklı ya da haksız bir şekilde bana karşı kullanırsa hangi çıkış planı var? Alternatif bir sağlayıcıya veri aktarımı için belgelenmiş bir prosedür var mı?
10. Erişim kimlik bilgilerini kim kontrol ediyor? Operatör bunları benim katılımım olmadan sıfırlayabiliyor mu? Bu beni korur mu yoksa açığa mı çıkarır?
11. Bu belirli işlev için Avrupalı, kendi kendine barındırılan veya araya sunucu girmeyen bir alternatif var mı? Değerlendirilen riskle kıyaslandığında gerçek maliyeti nedir?
12. Bugünün kararı beş yıl içinde bir müfettiş, bir denetçi veya bir ihlalden etkilenen bir müşteri tarafından incelenseydi, mevcut seçim bugün elde bulunan argümanlarla savunulabilir olur muydu, yoksa makul sorular sorulmadığı için özür dilemek mi gerekirdi?

Sorular mükemmel cevaplar beklemez. Dürüst cevaplar bekler; dürüst operatörün vermeyi bildiği, daha az dürüst operatörün ise hassasiyetle formüle etmekten kaçındığı cevaplar. İki operatör sınıfı arasındaki operasyonel fark, bunu dramatize etmeden söylüyoruz, genellikle daha fazlasını istemek zorunda kalmadan önce bile, onların gönüllü olarak sundukları cevapları yavaşça okuyarak fark edilir.

Bu yazıyla Cuadernos Lacre'nin ikinci döngüsünü kapatıyoruz. Schrems II'den miras kalan editoryal yükümlülükle başladık ve operasyonel bir soru listesiyle bitiriyoruz. Yol boyunca kavramlardan — hash, şifreleme, kimlik — ve uygulamalı analizlerden — kill switch, iş modeli, self-hosting — geçtik. Yayının beyan edilen editoryal niyeti, okuyucuyu kapsamlı bir sorunlar listesiyle bunaltmak değil, ona herhangi bir yeni hizmet karşısında ne tür bir cevabı kabul ettiğini ayırt edebilmesi için araçlar vermekti. Bu ayrım — mimari ile vaat arasındaki — araçtır. Geri kalanı her profesyonel, kendi pratiğinde bu soruya layık gördüğü verilerin hizmetine sunacaktır.

Kaynaklar ve ek okumalar

- Bu yayın, 2. döngü (Mayıs 2026) — *Schrems II, beş yıl sonra*, *SHA-256 Gerçekte Nedir?*, *Kill switch ve kurumsal ele geçirme*, *Uçtan uca şifreleme, gerçek anlamıyla açıklama*, *Güven Sinyali Olarak İş Modeli*, *24 Kelime: Kriptografik Kimlik Nedir?*, *Profesyonel bir uygulama olarak Self-hosting*. Bu soru listesinin dayandığı yedi yazı.
- Yönetmelik (AB) 2016/679 — Genel Veri Koruma Yönetmeliği. Soru listesinin ortaya koyduğu tüm sorular için, özellikle 5, 6, 25, 28, 32, 33. maddeler ve V. bölüm için referans hukuki çerçeve.
- Avrupa Veri Koruma Kurulu — Schrems II, uluslararası aktarımlar, etki değerlendirmeleri ve proaktif sorumluluk üzerine operasyonel kılavuzlar ve görüşler (2020-2024 yayınları).
- İspanya Veri Koruma Ajansı — 2022-2024 yıllarında uygunsuz aktarım araçları veya esaslı içerikten yoksun biçimsel etki değerlendirmeleri nedeniyle veri sorumlularına yayınlanan yaptırımlar.
- noyb.eu — Maximilian Schrems'in yönettiği Avrupa Dijital Haklar Merkezi. Avrupa veri koruma kurallarına gerçek, görünürdeki değil, gerçek uyum konusunda şikâyetler, başvurular ve analizler içeren kamuya açık bir depo.

← ÖncekiProfesyonel bir uygulama olarak self-hostingSonraki →Bir imzanın düzeltemeyeceği şeyler

Son okumalar

- Düşünce · 29 Haziran 2026 Anonim değilsin
- Düşünce · 27 Mayıs 2026 Bir imzanın düzeltemeyeceği şeyler
- Analiz · 25 Mayıs 2026 Profesyonel bir uygulama olarak self-hosting

Bu makaleyi ihtiyacınız olan her yere yanınızda götürün.

↓ Markdown ↓ Düz metin ↓ PDF

Dosya cihazınıza indirilecektir. Oradan kaydedebilir, Solo2'ye aktarabilir veya istediğiniz yerde paylaşabilirsiniz. Cuadernos hedef noktaya sizin yerinize karar vermez.

Mühür mumu · SHA-256 c2f9c35d39960d35d0a9d6ab69daf7781b54a577268b1b015646992c654bfecc

Cuadernos Lacre · Menzuri Gestión S.L. yayını ·
R.Eugenio tarafından yazıldı · Solo2 ekibi tarafından düzenlendi.