Analiz · 16 Mayıs 2026

← Önceki·Sonraki →

Arada kimse olmadığında

Bir sunucudan geçenleri şifrelemek içeriği korur. Arada sunucu olmaması soruyu ortadan kaldırır. İkisi aynı şey değildir.

İki kişi, bir konuşma

Bir odada iki kişi yüz yüze konuştuğunda, kimse bir şey duymadığına dair söz vermek zorunda değildir. Duymadı çünkü orada değildi. İki kişi elden ele bir kağıt verdiğinde, aradaki hiç kimse onu okumadığına dair yemin etmek zorunda değildir. Arada kimse yoktur.

Günlük hayattaki çoğu şey bu şekilde işler. Sesimizi ileten havayla veya tuttuğumuz kağıtla gizlilik sözleşmeleri imzalamayız. Konuşmanın gizliliği bir aracının vaadine dayanmaz, çünkü aracı yoktur. Bu, gizli olmanın en güçlü yollarından biridir: bir şeyin veya birinin iyi davranması nedeniyle değil, o şeyin veya o birinin olmaması nedeniyle.

Konuşma dijital bir kanala taşındığında bu varsayılan olarak değişir. Alışılmış model şöyledir: iki kişi bir sunucuya bağlanır, sunucu mesajı alır, şifreler veya şifreli olarak saklar ve alıcıya teslim eder. Sunucu aradadır. Sunucu dürüst olabilir. Denetlenmiş olabilir. Elverişli bir yargı alanında ve katı bir gizlilik politikası altında çalışıyor olabilir. Bunların hepsi doğru olabilir. Ama sunucu aradadır.

Şifrelemek ile toplamamak arasındaki fark (ikinci bölüm)

Bu serinin önceki bir makalesinde, içeriği şifrelemek ile meta verileri toplamamanın aynı şey olmadığını savunmuştuk. Açıklığa kavuşturulması gereken bir adım daha var: sunucudan geçeni şifrelemek ile hiç sunucuya sahip olmamak da aynı şey değildir.

İlk model —arada sunucu, şifreli içerik— içeriği sunucu operatöründen, bakım personelinden ve sistemi tehlikeye atan harici bir saldırgandan korur. Ve bu önemlidir. Ancak sunucuyu ortadan kaldırmaz. Sunucu oradadır. Meta verileri işlemeye devam eder. Bir mahkeme kararı, yasal bir müdahale, siyasi baskı veya bir güvenlik ihlali alabilecek bir nokta olmaya devam eder. Hala birine güven duymayı gerektiren bir nokta olmaya devam eder.

İkinci model —iki uç arasında sunucu bulunmaması— şifreli içeriği daha iyi korumaz: kriptografi sağlamsa, içerik her iki durumda da korunur. Değişen içerik değildir. Değişen şey, *«sunucuya ne oluyor?»* sorusunun anlamsızlaşmasıdır, çünkü hakkında soru sorulacak bir sunucu yoktur.

Güven, yokluk ve ikisi arasındaki fark

Güven doğru yere konulmuş olabilir. Dürüst şirketler vardır. Titiz denetçiler vardır. Kullanıcı lehine yasalar vardır. Yukarıdakilerin tümüne titizlikle uyan ciddi hizmetler vardır. Güven, hak eden bir operatöre verildiğinde kötü bir düzenleme değildir.

Ancak güven, ne kadar sağlam olursa olsun, yine de güvendir. Sosyal bir çözümdür, teknik bir çözüm değil. Bir şirket el değiştirebilir. Bir yargı alanı hükümet değiştirebilir. Yarın bir mahkeme kararı gelebilir. Gelecek ay yeni bir güvenlik açığı keşfedilebilir. Bunların hiçbiri kötü niyetle olmaz. Operatör var olduğu için olur ve var olan her şey dünyanın beklenmedik olaylarına tabidir.

Bir operatörün yokluğu bu aynı beklenmedik olaylara tabi değildir. Bir mahkeme kararı var olmayan bir sunucudan veri isteyemez. Bir saldırgan var olmayan bir sunucuyu tehlikeye atamaz. Bir şirket politikasındaki değişiklik o şirketin hiç sahip olmadığı verileri etkileyemez. Anahtar cümle basittir: Var olmayan veriler kaybedilemez.

Sunucu tarafının meşru argümanı üzerine

Arada sunucu bulunan profesyonel bir mesajlaşma hizmeti sunanlar genellikle üç mükemmel geçerli argüman sunar. Birincisi, alıcı çevrimdışıyken teslimatı garanti etmek için sunucunun gerekli olduğu. İkincisi, içerik şifrelemesinin sağlam olduğu ve bu nedenle operatörün onu okuyamayacağı. Üçüncüsü, hizmetin Avrupa mevzuatına uygun olduğu ve verilerin yasalarla korunduğu.

Her üç argüman da doğrudur. Hiçbiri meselenin doğasını değiştirmez. Bir sunucunun mesajları gecikmeli teslimat için saklamaya izin verdiği doğrudur; gecikmeli teslimatın, onlarca yıldır geliştirilen ve bugün operasyonel olan cihazlar arası doğrudan iletişim protokolleri aracılığıyla başka bir şekilde çözülebileceği de doğrudur. Ciddi hizmetlerde iletim halindeki içeriğin şifrelenmesinin sağlam olduğu doğrudur. Ve Avrupa mevzuatının kullanıcıları diğer pek çok yerdekine göre daha fazla koruduğu doğrudur.

Mesele arada sunucu bulunan hizmetlerin yasal olup olmadığı, güvenli olup olmadığı veya içeriği koruyup korumadığı değildir. Olabilirler, yasaldırlar ve genellikle güvenlidirler. Mesele, arada bir sunucuya sahip olmanın teknik bir zorunluluk değil, mimari bir seçim olmasıdır. Ve her seçimin sonuçları vardır. Arada sunucu bulunan bir mimari, mutlaka güvenilmesi gereken bir aktör yaratır. Arada sunucu bulunmayan bir mimari ise yaratmaz.

Yasanın söylediği ve mimarinin yaptığı

GDPR (KVKK benzeri Avrupa düzenlemesi) belirli bir mimari model talep etmez. Sonuçlar talep eder: veri minimizasyonu, sınırlı amaç, tasarım gereği ve varsayılan olarak koruma, uyumluluğu kanıtlama yeteneği. Arada sunucu bulunan bir hizmet tüm bu gereksinimleri karşılayabilir. Arada sunucu bulunmayan bir hizmet bunların birçoğunu beyanla değil, yapı gereği karşılar. Mutlak minimizasyon —mesajı teslim etmek için kesinlikle gerekli olmayan hiçbir şeyi toplamamak— bir şey toplayabilecek bir sunucu olmadığında çok basittir.

Hassas olmayan günlük kullanımlar için sunuculu bir mimari tamamen makuldür ve ciddi bir operatöre güvenmek geçerli bir düzenlemedir. Diğer kullanımlar için —düzenlenmiş mesleki sır taşıyanlar, etik sorumluluk getirenler, özellikle hassas bilgilere dokunanlar— bir güven noktasının yokluğu bir lüks değil, yapısal bir avantajdır.

Profesyonel okuyucu için

Bu serinin önceki makalelerinden zaten tanıdık olan profesyonel bir iletişim hizmeti karşısında sorulması gereken sorulara bir mimari soru daha eklenir:

1. İletim halindeki içeriği şifreliyor mu? (Muhtemelen evet.)
2. Kiminle ve ne zaman konuştuğuma dair meta veriler oluşturup saklıyor mu? (Muhtemelen evet.)
3. Cihazım ile alıcının cihazı arasındaki yolda bir sunucu var mı?
4. Varsa: Kim işletiyor, hangi yargı alanında ve hakkımda veri teslim etmesi için ne olması gerekir?
5. Yoksa: Önceki soruların bir anlamı yoktur.

İki kategori arasındaki fark derece farkı değil, tür farkıdır. Bunu bir müşteriye, bir hastaya veya bir meslektaşa açıklama zamanı geldiğinde, en dürüst ifade aynı zamanda en basitidir: Birinde arada birisi vardır; diğerinde ise yoktur.

Bu makale Cuadernos Lacre'nin ilk döngüsünü kapatıyor. Şifreleme, meta veriler ve mesleki sırdan bahsettikten sonra mimari tabloyu tamamlıyoruz: İçeriği şifrelemek ile arada sunucu olmaması farklı şeylerdir. Her ikisi de yasal olabilir; sadece biri güven noktasını ortadan kaldırır.

Kaynaklar ve ek okumalar

- Saltzer, J. H.; Reed, D. P.; Clark, D. D. — *End-to-end arguments in system design*, ACM TOCS, 1984. Bir sistemin garantilerinin aradaki kanalda değil, uçlarda uygulanması gerektiği ilkesinin temel metni.
- Düzenleme (AB) 2016/679, md. 25 — tasarım gereği ve varsayılan olarak veri koruması.
- Düzenleme (AB) 2016/679, md. 5.1.c — veri minimizasyonu ilkesi.
- Schneier, B. — *Data and Goliath: the hidden battles to collect your data and control your world* (2015), W. W. Norton. Veri toplamayı yapı gereği en aza indiren mimariler üzerine bölümler.

← ÖncekiGDPR ve profesyonel mesajlaşma: çoğu kişi neden bilmeden kuralları ihlal ediyor?Sonraki →CUADERNOS_LIST_SCHREMS_TITLE

Son okumalar

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

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 0916a550fac14283bbeec428c37429661729b3b5ff4e514d4ffb69f484a3b961

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