Şifrelemek gizli olmak demek değildir: meta veriler hakkınızda ne söyler?

Şifrelenmiş içerik ve görünür meta veriler iki farklı şeydir. Bir servis "uçtan uca şifreleme"den bahsettiğinde, hikayenin sadece yarısını anlatıyor demektir.

Her şeyi korumayan kilit

Günümüzdeki mesajlaşma servislerinin büyük bir kısmı uçtan uca şifreleme reklamı yapıyor. Ve bu doğru: mesajların içeriği şifreli olarak seyahat eder, böylece yol üzerindeki hiç kimse – servis sağlayıcı bile – aktarım halindeyken metni okuyamaz. Buraya kadar ifade doğrudur.

Sorun şu ki, içerik hikayenin sadece bir kısmıdır. Kimse ne dediğinizi okuyamasa da, servis başka şeyleri çok yüksek bir hassasiyetle bilir: kiminle, ne zaman, ne sıklıkta, yaklaşık hangi konumdan, hangi cihazda konuştuğunuz, kaç mesaj gönderdiğiniz ve kaç mesaj aldığınız, kaç dosya paylaştığınız. Tüm bunlara meta veri denir. Ve meta veriler, birçok durumda neredeyse mesajın kendisi kadar çok şey söyler.

Meta verilerin ifşa ettikleri

Pek çok şeyi bilmek için bir mesajı okumaya gerek yoktur. Eğer bir kişi altı ay boyunca her Salı sabahı saat dokuzda bir onkoloğu arıyor veya ona yazıyorsa, neler olup bittiğini tahmin etmek için konuşmayı dinlemek gerekmez. Eğer iki kişi günde yüz mesaj alıp veriyor ve aniden bunu kesiyorlarsa, ne olduğunu anlamak için tek bir tanesini bile okumanıza gerek yoktur. Eğer bir mali müşavir, dönem kapanışından önceki gece aynı müşteriden arka arkaya yirmi mesaj alıyorsa, bu kalıp kendi adına konuşur.

Meta veriler davranış kalıplarını ifşa eder: kimin kiminle ilişkisi olduğu, her kişinin programının ne olduğu, ne zaman ayakta olduğu, ne zaman uyuduğu, ne zaman seyahat ettiği, hangi müşterilerin en aktif olduğu, hangi mesleki ilişkilerin en yoğun olduğu. Meta veri toplayan bir sunucu, kullanıcının ne yazdığından tek bir kelime bile okumadan, herhangi bir kullanıcının kişisel ve mesleki yaşamının ayrıntılı bir profilini oluşturabilir.

Bunu sert bir şekilde örnekleyen tarihi bir örnek vardır. Eski NSA direktörü Michael Hayden bunu 2014'te açıkça ifade etmiştir: *"We kill people based on metadata"*. Bu ifade, münhasıran iletişim kalıplarına göre tanımlanan hedeflere yönelik ABD askeri operasyonlarına atıfta bulunuyordu. Tek bir okunmuş mesaj yok. Sadece iletişim grafiği ve zaman çizelgeleri.

Bir servisin meta veri toplaması, bunları mutlaka kullanıcılarına karşı kullanacağı anlamına gelmez. Bunu yapma kapasitesine sahip olduğu ve bu verilere erişimi olan bir üçüncü tarafın – mahkeme kararı, bir güvenlik açığı veya servis şartları izin veriyorsa üçüncü taraflara satış yoluyla – da buna sahip olduğu anlamına gelir.

Rehbere erişim

Neredeyse hiç fark edilmeyen bir başka vektör: rehber listesi. Mesajlaşma servislerinin büyük bir kısmı kayıt sırasında telefon rehberine erişim ister. Başka kimlerin servisi kullandığını göstermek için tüm numaraları sunucularına yüklerler. O andan itibaren, kullanıcı hiç kimseye tek bir mesaj yazmamış olsa bile, şirket kullanıcının ilişkilerinin tam bir haritasına sahip olur.

Mesleki sır saklama yükümlülüğü olan bir profesyonel için – avukat, doktor, psikolog, danışman – o rehber müşterileri içerir. Rehber üçüncü taraf bir sunucuya yüklendiyse, müşterilerin isimleri, profesyonelin yargı yetkisini ve politikalarını kontrol etmediği bir altyapıda bulunur. Mesleki sır, birinin bir konuşmayı sızdırdığı gün bozulmaz: çok daha önce, yükleme onaylandığı anda bozulmuştur.

Şifrelemek ile toplamamak arasındaki fark

Şifrelemek içeriği korumaktır. Gizli olmak, ihtiyaç duyulmayanı toplamamaktır. Bunlar farklı şeylerdir ve fark operatif olarak belirleyicidir. Bir servis tüm mesajları mükemmel bir şekilde şifreleyebilir ve aynı zamanda meta veriler aracılığıyla kullanıcıları hakkında neredeyse her şeyi bilebilir. İkisi tamamen uyumludur. Aslında sektördeki baskın iş modelidir.

Bir servisin gerçek gizliliğini değerlendirmek için sorulması gereken doğru soru *"içeriği şifreliyor mu?"* değildir. Bu soru yıllardır cevaplanmış kabul ediliyor. Doğru soru şudur: *"hangi meta verileri üretiyor ve bunlar nerede saklanıyor?"*. Ve her şeyden önce: *"hangi meta verileri üretmesine gerek yok?"*.

Meta verileri vaatlerle değil, dahili politikalarla değil, tasarımla (privacy by design) en aza indiren bir mimari, bunları toplayan ve şifreleyen bir mimariden yapısal olarak daha gizlidir. Çünkü var olmayan veriler sızdırılamaz, satılamaz, mahkeme kararına teslim edilemez veya bir güvenlik açığında kaybolamaz.

Profesyonel okuyucu için

Mesleki faaliyetiniz sır, gizlilik veya sadece üçüncü şahısların bilgilerine saygı içeriyorsa, soruları şu sırayla sormaya değer:

1. İletişim kurmak için kullandığım uygulama içeriği şifreliyor mu? (Muhtemelen evet.)
2. Meta verileri şifreliyor mu? (Muhtemelen hayır.)
3. Çalışmak için *ihtiyaç duymadığı* meta verileri üretiyor mu? (Neredeyse kesinlikle evet.)
4. Bu meta veriler nerede ve hangi yargı yetkisi altında saklanıyor? (Muhtemelen Avrupa Ekonomik Alanı dışında.)
5. Müşterim veya hastam verilerinin orada olduğunu biliyor mu?

Son soru rahatsız edici olanıdır. Çünkü dürüst cevap çoğu durumda hayırdır.

Bu makale, profesyonel iletişim araçlarının gerçek işleyişi üzerine bir serinin ilkidir. Gelecek sayılar mesajlaşmada GDPR uyumluluğunu ve dijital çağda mesleki sır kavramını ele alacaktır.

Kaynaklar ve ek okumalar

- Hayden, M. – Johns Hopkins Üniversitesi'ndeki beyan, 2014 ("We kill people based on metadata"). Kamuya açık transkriptler mevcuttur.
- GDPR (AB 2016/679 Yönetmeliği), madde 4 ve 5 – Kişisel verilerin tanımı ve işleme ilkeleri (meta veriler kişisel veridir).
- EDPS ve EDPB – Elektronik iletişimde trafik verilerinin ve meta verilerin işlenmesine ilişkin görüşler (e-Gizlilik direktifi).

← ÖncekiMühür mumunun kısa bir tarihiSonraki →Dijital çağda mesleki sır saklama yükümlülüğü

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 6bdaa03b832842d15549a2133879912d84a9025a07683edb6e1dbce0c2ed1610

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