T.B.M.M.
CUMHURİYET HALK PARTİSİ
Grup Başkanlığı
CHP
Tarih: 04 Ekim 2024
Sayı : 7246

18200

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın Türkiye Cumhuriyeti Anayasası'nın 98 inci ve Türkiye Büyük Millet Meclisi İçtüzüğü'nün 96 ıncı maddesine uygun olarak, T.C. Sağlık Bakanlığı'na iletilmesi ve Sayın Bakan Kemal Memişoğlu tarafından yazılı olarak yanıtlanması için gereğinin yapılmasını arz ederim. 03/10/2024

Prof.Dr. Kayıhan PALA
Bursa Milletvekili

Sağlık Bakanlığına ait veri sisteminden verilerin çalındığına dair bugüne kadar birçok iddia ortaya atılmış, iddialar hakkında kamuyu bilgilendirmek amacı ile Bakanlığınızdan herhangi bir açıklama yapılmamıştır.

Sağlık veri standardizasyonunun sağlanması amacıyla, 2003 yılında duyurulan 'Sağlıkta Dönüşüm' programının bir parçası olarak kurulan; Sağlık Net1, Sağlık Net2 ve e-nabız sisteminde toplanan ve muhafaza edilen verilerin güvenliğinin sağlanamaması iddiaları başta olmak üzere; 2021 yılında e-nabız uygulamasına ait olduğu öne sürülen 7 milyon satırlık veri tabanının da yasadışı internet ortamlarında satışa çıkarıldığı iddia edilmektedir. Benzer şekilde, 26 Eylül ve 21 Kasım 2022 tarihlerinde Halk Sağlığı Yönetim Sisteminde oluşan bir açık nedeniyle ele geçirildiği iddia edilen 101 milyon (yaşayan ve hayatını kaybetmiş) kişinin verisi internet ortamında satışa çıkarılmıştır. Son olarak, 9 Eylül 2024 tarihinde ifade ve internet özgürlüğü alanında yayın yapan Free Web Turkey sitesi, Türkiye'deki resmî kurumlarda kaydı olan 108 milyon yurttaşın kişisel verilerinin çalındığını iddia etmiştir.

Bakanlığınız tarafından toplanan ve muhafaza edilen verilerin güvenliğinin ihlal edildiği ve kamuya açık bir şekilde satışa sunulduğu iddiaları hakkında Bakanlığınızın sessiz kalmasına karşın; 12 Eylül 2024 tarihinde Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu pandemi döneminde Sağlık Bakanlığı sisteminden kaynaklı bir sızıntı yaşandığını "*Bu pandemi sürecindeki hatırlarsınız, sağlık sisteminden bir sızıntıdır. Onun haricinde yok. İnsanların güncel verilerinin çalındığıyla ilgili bir veri yok. Pandemi sürecinde bazı bilgilerin maalesef belli şekliyle elde edilmiş olduğu doğru. O süreçte o maalesef önlenemedi.*" açıklaması ile kabul etmiştir. Bu bağlamda;

1. Bakanlığınızın veri gizliliği politikası ne kadar kapsamlıdır? Bu politika çalışanlar, veriyi işleyenler ve veri sağlayan hastalar tarafından bilinmekte midir?
2. Bu verilerin toplanması ve işlenmesi için hangi yasal dayanağınız bulunmaktadır? Verilerin toplanması ve saklanması süreçlerinde Kişisel Verilerin Korunması Kanununa uygunluk sağlanmakta mıdır?
3. Veriler üçüncü kişilerle paylaşılmakta mıdır? Paylaşılıyor ise hangi kurum veya kişilerle ve hangi amaçla paylaşılmaktadır?

4. Kurumunuzun elektronik ağ altyapısı nasıl korunmaktadır?
5. Bakanlığınızda tutulan veriler şifrelenmekte midir? Eğer şifrelenmişse hangi şifreleme algoritması kullanılmaktadır?
6. Kurumunuzda sızma tespit sistemleri kullanılmakta mıdır? Bu sistemlerin ne sıklıkla güncellendiği ve test edildiği konusunda raporlar bulunmakta mıdır?
7. Sisteme erişimde ağ trafiği düzenli olarak izlenmekte midir? Şüpheli aktiviteler için uyarı sistemleri mevcut mudur?
8. Veri saklama ve işleme sisteminize erişimi olan kullanıcılar kimlerdir? Bu kullanıcıların erişim yetkileri nasıl belirlenmektedir? Veri tabanlarına erişim nasıl kontrol edilmektedir? Yetkilendirme ve kimlik doğrulama mekanizmaları nelerdir?
9. Veri tabanına sızma işlemleri hangi aşamalarından geçerek gerçekleşmiş ve hangi güvenlik açıkları kullanılmıştır?
10. Veri güvenliği ihlallerinin nasıl gerçekleştiği konusunda yapılan teknik inceleme sonucunda ne gibi sonuçlara varılmıştır? Her bir olay için tek tek açıklanmak üzere;
    a. Verilerin ne kadar süre boyunca yetkisiz erişime açık olduğu tahmin edilmektedir?
    b. İddia edilen tüm veri güvenliği ihlallerinde sızdırılan verilerin tam listesi nedir? Sızdırılan veriler arasında hangi kategorilerdeki bilgiler yer almaktadır (örneğin, T.C. kimlik numarası, adres, telefon numarası, sağlık bilgileri vb.)?
    c. Sızdırılan verilerin boyutları nedir?
    d. Veriler nasıl sızdırılmıştır (örneğin, brute force saldırısı, SQL injection, phishing vb.)?
    e. Sızmaların gerçekleştiği nokta tam olarak neresidir? Sistemin hangi kısmında bir güvenlik zafiyeti oluşmuştur?
    f. Sızma anında sistemde hangi güvenlik önlemleri aktifti? Bu önlemler neden sızıntıyı engelleyemedi?
    g. Sızıntılar ne zaman fark edildi? İlk belirtiler neydi?
    h. Sızıntıların fark edilmesinde gecikme yaşanmasının nedenleri nelerdir?
    i. Sistemde tespit edilen güvenlik açıkları nelerdir? Bu açıkların varlığı ne kadar süredir biliniyordu?
    j. Nüfus Vatandaşlık İşleri (NVİ) üzerinden alınan veriler yaşayan siber saldırılarda kaybedilmiş midir?
11. Sızıntıların sorumluluğu kimdedir? Sorumlular hakkında ne gibi disiplin işlemleri başlatılmıştır? Olaylarla ilgili iç soruşturma başlatılmış mıdır? Soruşturma kapsamında kimler sorguya çekilmiştir? Soruşturmaların sonuçları açıklanmış mıdır/ ne zaman açıklanacaktır?
12. Olaylarla ilgili yasal süreç başlatılmış mıdır? Başlatılmışsa, her olay için ayrı ayrı bilgi verilmek üzere süreç hangi aşamadadır?
13. Kurumunuzun veri güvenliği sistemleri denetlenmekte midir? Denetleniyor ise, hangi sıklıkta ve ne zamandan denetlenmektedir?
14. Suç teşkil eden bu tür ihlallerin tekrarlanmaması için kurumunuzda ne gibi yapısal değişiklikler yapılmıştır?
15. Bu olayların yaşanması nedeniyle veri sahipleri nasıl bilgilendirilmiştir? Mağdurların mağduriyetlerinin giderilmesi için ne gibi önlemler alınmaktadır?

18200

16. Bakanlığınız, sağlık hizmeti veren kamu özel ve vakıf üniversiteleri kuruluşları için kişilere ait verileri nüfus vatandaşlık işleri (nvi) sisteminden sorgularken, sağlık kuruluşlarında kullanılan sağlık yazılımları veri tabanlarına kişisel verileri kaydetmekte midir? Kaydediliyor ise bu verilerin güvenliğini nasıl sağlanmaktadır?
17. Kişisel sağlık verileri özel sigorta şirketlerinin eline nasıl geçmiştir?