



TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın Ulaştırma ve Altyapı Bakanı Abdulkadir Uraloğlu tarafından Anayasanın 98. ve TBMM içtüzüğü'nün 96. Maddelerine göre yazılı olarak yanıtlandırılmasını saygılarımla arz ederim. 11.12.2024

Barış BEKTAŞ

Konya Milletvekili

10 Aralık tarihinde milyonlarca Hızlı Geçiş Sistemi (HGS) kullanıcısının telefonlarına gelen bildirimler ve medya organlarında yer alan haberler, HGS sisteminin hacklenerek güvenlik açığına maruz kaldığını ve bu durum sonucunda hackerların 25 bin dolar fidye talebinde bulunduğunu ortaya koymuştur. Bu olay, Türkiye'nin dijitalleşme sürecindeki güvenlik zaaflarını bir kez daha gözler önüne sermiştir. Daha önce de devlete ait birçok dijital platformun hacklenmesi, yurttaşların kişisel bilgilerinin çalınarak internet ortamında satılması gibi vakalar yaşanmış, ancak bu olaylara karşı alınan tedbirler yetersiz kalmıştır. Bu durum, sadece bireysel mağduriyetlere yol açmamakta, aynı zamanda yurttaşların kamu hizmetlerine olan güvenini zedelemekte ve ulusal güvenlik açısından ciddi tehditler oluşturmaktadır.

HGS gibi milyonlarca yurttaş doğrudan etkileyen bir sistemin hacklenmesi, hem yurttaşların ödeme bilgilerinin ve kişisel verilerinin korunması konusunda büyük bir ihmali ortaya koymuş hem de devletin dijital altyapılarındaki güvenlik açıklarını gözler önüne sermiştir. Türkiye'nin bu alandaki yetersizlikleri, kamu kurumlarının itibarını sarsmakta ve yurttaşları sürekli bir tehdit altında bırakmaktadır.

Siber güvenlik, yalnızca bireysel verilerin korunmasını değil, aynı zamanda kamu hizmetlerinin güvenilir bir şekilde sürdürülmesini ve ulusal güvenliği de kapsayan geniş bir

sorumluluk alanıdır. Dünyada birçok ülke, dijital altyapılarının güvenliği için uluslararası standartlara uygun adımlar atarken, Türkiye'nin bu alandaki ihmali, daha büyük çaplı siber saldırılara açık hale gelmesine neden olmaktadır.

Bu bağlamda;

1. Hızlı Geçiş Sistemi'ne (HGS) yönelik gerçekleşen siber saldırı hakkında bakanlığınız tarafından inceleme veya soruşturma başlatılmış mıdır? Başlatılmış ise bu incelemenin kapsamı ve aşamaları nelerdir?
2. Söz konusu saldırıda yurttaşların kişisel bilgilerinin (ad, soyad, T.C. kimlik numarası, araç bilgileri vb.) ve ödeme bilgilerinin güvenliği hangi ölçüde tehlikeye girmiştir? Çalındığı iddia edilen verilerin internet ortamında paylaşılması veya satılmasına ilişkin bir bulgu bulunmakta mıdır?
3. HGS sisteminin mevcut güvenlik altyapısı en son ne zaman denetlenmiştir? Bu denetimlerde tespit edilen eksiklikler nelerdir ve bu eksikliklerin giderilmesi için hangi somut adımlar atılmıştır?
4. Siber saldırıyı gerçekleştiren hackerların fidye talebi yerine getirilmiş midir?
5. Yurttaşların mağduriyetlerini gidermek ve benzer saldırıların tekrarını önlemek amacıyla hangi kısa ve uzun vadeli tedbirler alınmıştır?
6. Daha önce devlete ait diğer dijital platformlara yapılan siber saldırılar sonucunda yurttaşların verilerinin çalındığı ve satıldığı iddialarına yönelik hangi çalışmalar yürütülmüştür? Bu olaylardan alınan dersler ışığında HGS gibi kritik altyapılarda ne gibi güvenlik önlemleri alınmıştır?
7. Türkiye'nin dijital altyapılarının siber güvenliğini sağlamak adına uluslararası standartlara uygun politikalar geliştirmek ve uygulamak için bir strateji planınız bulunmakta mıdır? Bu plan çerçevesinde hangi somut adımlar atılmıştır?
8. Türkiye'de kamuya ait dijital sistemlerin siber saldırılara karşı dayanıklılığını artırmak için gerekli bütçe ve kaynaklar sağlanmış mıdır? Bu bütçenin ne kadarı siber güvenlik altyapısının iyileştirilmesine ayrılmıştır?
9. HGS gibi dijital kamu hizmetlerinde kullanılan sistemlerin güvenlik protokolleri ve şifreleme yöntemleri hangi uluslararası standartlara uygun olarak belirlenmektedir? Bu protokoller son olarak hangi kurum veya bağımsız otorite tarafından denetlenmiştir?
10. HGS kullanıcılarının verilerini korumak ve sistemin modernizasyonunu sağlamak için bakanlığınız ne gibi projeler yürütmektedir? Bu projelerin takvimi ve bütçe planlaması nedir?