T.B.M.M.
YENİ PARTİ
Grup Başkanlığı
Tarih: 4 Kasım 2026
Sayı: 1618

- 52609

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın Ulaştırma ve Altyapı Bakanı Abdulkadir URALOĞLU tarafından yazılı olarak cevaplandırılmasını arz ederim.

Ulaş KARASU
Sivas Milletvekili

Siber güvenlik, özellikle ulaştırma, haberleşme, havacılık ve kritik altyapılar bakımından yalnızca teknik bir hizmet alanı değil, doğrudan doğruya ulusal güvenlik ve kamu güvenliği meselesidir. Kamu kurumlarının bilişim sistemlerini izleyen, güvenlik açıklarını tespit eden, sızma testleri gerçekleştiren, olaylara müdahale eden ve güvenlik operasyonlarını yöneten şirketlerin eriştiği veriler ve sistemler büyük önem taşımaktadır.

2008 yılında Ankara'da kurulan Barikat Siber Güvenlik A.Ş., Türkiye'nin en büyük siber güvenlik sağlayıcılarından biridir. Barikat, kendi internet sitesinde kamu kurum ve kuruluşlarına hizmet verdiğini açıkça belirtmekte; kamu, savunma sanayii, finans ve enerji sektörlerini başlıca faaliyet alanları arasında saymaktadır. Borsa ve Fon vurgunu soruşturmasında tutuklanan Emre Tezmen'in Yönetim Kurulu Başkanlığını yaptığı ve Holdingin %63 oranında pay sahibi olduğu ve "Bağlı Ortaklık" statüsünde yönettiği Barikat, Türkiye siber güvenlik pazarı nda önemli bir oyuncudur.

Barikat'ın bir parçası olarak; Dağıtık Hizmet Reddi (DDoS) test süreçlerinde uzmanlaşan LoDDoS, Barikat'ın %100 bağlı ortaklığı olarak ayrı bir tüzel kişilik yapısında faaliyetlerini sürdürmektedir. Halihazırda 23 ülkede kullanılan LoDDoS'un yanı sıra; siber istihbarat platformu SİPER ve siber güvenlik eğitim simülasyonu CYBERIEN, grubun küresel pazara ihraç ettiği stratejik ürünler arasında yer almaktadır.

Öte yandan Tera Yatırım Teknoloji Holding tarafından Kamuyu Aydınlatma Platformu'na yapılan açıklamada, Barikat'ın Aralık 2025 içerisinde 650 milyon TL tutarında yeni sipariş aldığı, söz konusu siparişlerin stratejik kamu kurumları, finansal kuruluşlar, ulaştırma ve perakende sektörlerini kapsadığı açıklanmıştır.

Kamuya açık ihale kayıtlarında da Barikat'ın 2026 yılında Devlet Hava Meydanları İşletmesi (DHMİ) Genel Müdürlüğü, Borsa İstanbul, Türk Telekom ve Türk Hava Yolları, Diyanet İşleri Başkanlığı, Orman Genel Müdürlüğü, İller Bankası, Türk Standardları Enstitüsü, Enerji Piyasası Düzenleme Kurumu ve Kültür ve Turizm Bakanlığı gibi çeşitli kamu kurumların olduğu görülmektedir. DHMİ'nin Temmuz 2026 tarihli "Bilişim Güvenliği Ürünleri Temin, Tesis ve Modernizasyon İşi" bunlar arasındadır.

Son derece kritik kamu kuruluşlarına siber güvenlik hizmeti veren bir şirkete yönelik soruşturmalar ve ortaya saçılan iddialar; hassas verilerin korunması, güvenlik operasyonlarının sürekliliği ve kritik altyapılara yönelik siber güvenlik hizmetlerinin güvenliği bakımından açıklığa kavuşturması gereken önemli sorular doğurmaktadır. Bu çerçevede;

1. Önergeye konu Barikat İnternet Güvenliği Bilişim Ticaret A.Ş. tarafından Bakanlığınıza, Bakanlığınızın bağlı, ilgili ve ilişkili kuruluşlarına ve bu kuruluşların iştiraklerine siber güvenlik hizmeti verildiği tespit edilmiş midir? Tespit edilmişse hangi kurumlara, hangi tarihler arasında, hangi sözleşmeler kapsamında ve hangi hizmetler verilmiştir?

2. Barikat'ın Ulaştırma ve Altyapı Bakanlığı, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Devlet Hava Meydanları İşletmesi (DHMİ), Karayolları Genel Müdürlüğü, Devlet Demiryolları İşletmesi Genel Müdürlüğü (TCDD), TCDD Taşımacılık A.Ş., PTT A.Ş. ve diğer bağlı/ilgili kuruluşlarla halen devam eden veya son beş yıl içerisinde tamamlanmış herhangi bir sözleşmesi bulunmakta mıdır?

3. Söz konusu sözleşmelerin toplam bedeli ne kadardır? Hangi işler doğrudan ihale, hangileri doğrudan temin, pazarlık veya diğer usullerle gerçekleştirilmiştir?

4. Barikat'ın kamu kurumlarına sunduğu hizmetler kapsamında kurumların ağlarına, sunucularına, güvenlik operasyon merkezlerine, log kayıtlarına, trafik verilerine, güvenlik olaylarına veya diğer hassas bilgi ve sistemlerine uzaktan ya da yerinde erişim yetkisi bulunmakta mıdır?

5. Barikat'ın Tera Grubu'na yönelik soruşturma kapsamında TMSF yönetimine geçmesinin ardından, Bakanlığınız ve bağlı kuruluşlarınız tarafından şirketin sahip olduğu erişim yetkileri, kullanıcı hesapları, sertifikaları, VPN bağlantıları, yönetici yetkileri ve diğer ayrıcalıklı erişim mekanizmaları hakkında herhangi bir güvenlik incelemesi yapılmış mıdır?

6. Barikat tarafından Bakanlığınız veya bağlı kuruluşlarınıza ait sistemlerde tutulan ya da işlenen kişisel veri, ticari sır, kritik altyapı bilgisi, güvenlik açığı bilgisi, sistem logları ve siber olay kayıtlarının güvenliği açısından yeni bir risk değerlendirmesi yapılmış mıdır?

7. TMSF'nin Barikat'ın yönetimine geçmesinin ardından, Bakanlığınız ve bağlı kuruluşlarınızın şirketle mevcut sözleşmelerinin devamına ilişkin hukuki, teknik ve siber güvenlik değerlendirmesi yapılmış mıdır? Yapılmışsa sonuçları nelerdir?

8. Barikat'ın Bakanlığınıza veya bağlı kuruluşlarınıza sunduğu hizmetlerde görev yapan personelin kritik sistemlere erişim yetkileri yeniden değerlendirilmiş midir? Bu personelin erişim yetkilerinde değişiklik yapılmış mıdır?

9. Barikat'ın kamu kurumlarına verdiği hizmetler kapsamında elde ettiği kamuya ait bilgi, veri ve siber güvenlik kayıtlarının nerede ve hangi altyapılarda saklandığı Bakanlığınız tarafından denetlenmekte midir? Bu verilerin Türkiye sınırları dışına aktarılmasına veya Türkiye dışındaki altyapılarda işlenmesine izin verilmiş midir? Denetim yapılmış ise denetimlerin sonuçları nelerdir?

11. Barikat'ın kamu kurum ve kuruluşlarıyla yaptığı sözleşmelerde, şirketin ortaklık veya yönetim yapısında meydana gelen değişiklikler sonrasında uygulanacak fesih, yeniden değerlendirme, erişimlerin sonlandırılması ve veri iadesi hükümleri bulunmakta mıdır?

12. Bakanlığınızın ve bağlı kuruluşlarınızın kritik bilişim altyapılarında hizmet veren özel şirketlerin ortaklık ve yönetim yapılarındaki değişikliklerin ulusal güvenlik ve siber güvenlik açısından Bakanlık tarafından önceden bildirilmesini veya risk değerlendirmesine tabi tutulmasını sağlayan bir mekanizma bulunmakta mıdır?

13. 2025 yılı Aralık ayında Barikat tarafından alındığı açıklanan 650 milyon TL tutarındaki yeni siparişlerin ulaştırma sektöründeki hangi kamu kurumlarını kapsadığı Bakanlığınız tarafından bilinmekte midir? Biliniyorsa bu kurumlar hangileridir ve siparişlerin toplam bedelinin ne kadarı kamu kaynaklarından karşılanmaktadır?

14. Bakanlığınız ve bağlı kuruluşlarınızın, Barikat'ın TMSF yönetimine geçmesinden sonra kritik siber güvenlik hizmetlerinin kesintisiz sürdürülebilmesi amacıyla alternatif bir tedarikçi veya kurum içi kapasite planı bulunmakta mıdır?

15. Bakanlığınız bünyesinde ve bağlı kuruluşlarınızda, kritik bilişim ve siber güvenlik hizmetlerinin özel şirketlerden temin edilmesi konusunda kurumsal bağımlılık, veri güvenliği ve kamu güvenliği risklerine ilişkin kapsamlı bir denetim veya inceleme yapılması planlanmakta mıdır?