HALKLARIN EŞİTLİK VE DEMOKRASİ PARTİSİ
GRUP BAŞKANLIĞI
Sayı : 17361
Tarih : 08.04.2026

43270

Ömer Faruk Gergerlioğlu
Kocaeli Milletvekili

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

Aşağıdaki sorularımın **Milli Eğitim Bakanı Sayın Yusuf Tekin** tarafından Anayasanın 98 'inci ve TBMM İçtüzüğünün 96 'ncı ve 99 'uncu maddeleri gereğince yazılı olarak cevaplandırılmasını saygılarımla arz ederim.

Ömer Faruk GERGERLİOĞLU

Kocaeli Milletvekili

Munzur Üniversitesi'nin resmî internet sitesi ve dijital altyapısının uzun süredir ciddi siber güvenlik sorunları yaşadığı, üniversiteye ait internet alanlarında yer yer "lele" ve "toto868" gibi ifadelerle kaçak bahis sitelerine ait reklam ve içeriklerin göründüğü, bu durumun arama motoru sonuçlarına da yansıdığı kamuoyuna yansımıştır. Bir devlet üniversitesinin resmî internet alan adının uzun süredir yasa dışı bahis içerikleriyle ilişkilendirilmesi, yalnızca kurumsal itibar açısından değil; kamu bilişim altyapısının korunması, resmî bilgiye erişim güvenliği ve vatandaşın devlete duyduğu güven açısından da son derece vahimdir.

Öte yandan, Munzur Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dekanı tarafından fakülte personeline gönderildiği belirtilen bir WhatsApp mesajında, "üniversite veritabanı yine hacklenmiştir", "nitelikli imza şifrelerine saldırılar olmaktadır", "lütfen bugünlerde üniversite dışından UBYS'ye çok fazla girmeyiniz", "imzalarınızı üniversite içinde atınız", "dışardan imza atarsanız ve imza şifreniz çalınırsa siz sorumlu olursunuz" ifadelerine yer verildiği belirtilmektedir. Bu içerik doğru ise mesele yalnızca internet sitesinin görünürlüğüyle sınırlı olmayıp, doğrudan üniversitenin veritabanına, kurumsal otomasyon sistemine, elektronik imza süreçlerine ve personel güvenliğine uzanan ciddi bir siber güvenlik krizine işaret etmektedir.

Bir kamu üniversitesinin veritabanının "yine hacklendiği" yönünde kurum içi uyarı yapılması; personelin üniversite dışından sisteme giriş yapmaması konusunda uyarılması; nitelikli elektronik imza şifrelerine saldırı olduğunun ifade edilmesi ve buna rağmen doğabilecek sonuçların personele yüklenmesi, kamu kurumlarında dijital güvenlik yönetimi ve sorumluluk rejimi bakımından ciddi soru işaretleri doğurmaktadır. Bu durum; öğrencilerin, akademik ve idari personelin kişisel verileri, not bilgileri, özlük dosyaları, resmî yazışmalar, idarî kararlar ve elektronik imzayla yürütülen işlemler bakımından telafisi güç zararlar doğurabilecek niteliktedir.

TBMM Halkla İlişkiler Binası
2. Kat, 2 Nolu Banko Oda: F214 Bakanlıklar/Ankara
Tel.: +90 (312) 420 63 86 - 87 Faks: +90 (312) 420 24 82

Bu bağlamda;

1. Munzur Üniversitesi'nin resmî internet sitesi ve bağlı alt alan adlarında kaçak bahis, spam veya yetkisiz içerik görüntülendiği iddiaları doğru mudur?
2. Arama motoru sonuçlarında Munzur Üniversitesi ile bağlantılı sayfalarda "lele", "toto868" ve benzeri yasa dışı bahis içeriklerinin görünmesine neden olan teknik zafiyet nedir?
3. Munzur Üniversitesi'nin resmî internet sitesine ve dijital altyapısına son iki yıl içinde kaç kez siber saldırı, yetkisiz erişim, zararlı kod yerleştirme, SEO spam, yönlendirme manipülasyonu veya veri tabanı ihlali gerçekleştirilmiştir?
4. Bu saldırıların tarihleri, kapsamı ve etkilediği sistemler nelerdir?
5. Munzur Üniversitesi veritabanının hacklendiği iddiası doğru mudur?
6. İktisadi ve İdari Bilimler Fakültesi Dekanı tarafından personele gönderildiği belirtilen ve "üniversite veritabanı yine hacklenmiştir" ifadesini içeren WhatsApp mesajı Bakanlığınızın bilgisi dahilinde midir?
7. Söz konusu WhatsApp mesajında yer alan "nitelikli imza şifrelerine saldırılar olmaktadır" ifadesi hangi teknik tespit, rapor veya güvenlik analizine dayanmaktadır?
8. UBYS sistemi, personel otomasyonu, e-imza altyapısı ve diğer üniversite bilgi sistemleri bu saldırılardan etkilenmiş midir?
9. Üniversite personeline "üniversite dışından UBYS'ye çok fazla girmeyiniz" şeklinde uyarı yapılmasını gerektiren güvenlik açığı tam olarak nedir?
10. Akademik ve idari personele "imzalarınızı üniversite içinde atınız" ve "dışardan imza atarsanız ve imza şifreniz çalınırsa siz sorumlu olursunuz" denilmesinin hukuki ve idari dayanağı nedir?
11. Kurumsal bir siber güvenlik açığının doğuracağı sonuçların personele yüklenmesi, kamu kurumlarında güvenlik yönetimi ve idari sorumluluk ilkeleriyle bağdaşmakta mıdır?
12. Bu saldırılar sonucunda öğrencilerin, akademik personelin, idari personelin veya diğer kullanıcıların kişisel verileri, kullanıcı bilgileri, işlem kayıtları, resmî belgeleri ya da elektronik imza süreçleri etkilenmiş midir?
13. Kişisel Verilerin Korunması Kanunu kapsamında herhangi bir veri ihlali bildirimi yapılmış mıdır? Yapıldıysa hangi kurumlara, hangi tarihte bildirimde bulunulmuştur?
14. Üniversite yönetimi, bilgi işlem birimi veya ilgili kamu görevlileri hakkında bu olaylar nedeniyle herhangi bir idari inceleme ya da soruşturma başlatılmış mıdır?
15. Olayla ilgili BTK, USOM, YÖK, adli makamlar veya diğer ilgili kurumlarla herhangi bir koordinasyon sağlanmış mıdır?
16. Munzur Üniversitesi'nin bilgi işlem altyapısında çok aşamalı doğrulama, IP kısıtlaması, oturum güvenliği, log takibi, saldırı tespit sistemleri ve acil müdahale protokolleri mevcut mudur?
17. Munzur Üniversitesi'nin internet altyapısı en son ne zaman bağımsız bir sızma testinden, güvenlik taramasından veya teknik denetimden geçirilmiştir?
18. Üniversitenin resmî internet sitelerinde görülen kaçak bahis içerikleri ile veritabanına ve UBYS sistemine yönelik saldırılar arasında bir bağlantı tespit edilmiş midir?

43270

Ömer Faruk Gergerlioğlu
Kocaeli Milletvekili

19. Bu olaylar sonucunda herhangi bir elektronik imza yetkisiz kullanılmış, sahte işlem yapılmış veya resmî belge güvenliği zedelenmiş midir?
20. Son beş yıl içinde Türkiye'de kaç devlet üniversitesinde benzer şekilde site ele geçirilmesi, spam içerik yerleştirilmesi, veritabanı ihlali, otomasyon sistemi saldırısı veya e-imza güvenliği zafiyeti yaşanmıştır?
21. Devlet üniversitelerinin internet siteleri, veritabanları, öğrenci bilgi sistemleri, personel otomasyonları ve e-imza süreçleri için merkezi ve bağlayıcı asgari siber güvenlik standartları bulunmakta mıdır?
22. Yükseköğretim kurumlarının dijital altyapılarının düzenli biçimde denetlenmesi için Bakanlığınız ile YÖK arasında işleyen bir mekanizma var mıdır?
23. Munzur Üniversitesi'nde yaşanan bu olayların tekrar etmemesi için hangi acil ve kalıcı tedbirler alınmıştır?
24. Üniversite personeli, öğrencileri ve vatandaşların resmî bilgiye güvenli biçimde erişebilmesi için Bakanlığınız tarafından hangi somut adımlar atılacaktır?
25. Kamu üniversitelerinde benzer siber güvenlik zafiyetlerinin önlenmesi amacıyla merkezi bir siber güvenlik eylem planı, teknik destek programı veya özel bütçe desteği hazırlanmakta mıdır?

TBMM Halkla İlişkiler Binası
2. Kat, 2 Nolu Banko Oda: F214 Bakanlıklar/Ankara
Tel.: +90 (312) 420 63 86 - 87 Faks: +90 (312) 420 24 82