İSTANBUL
ESNAF VE SANATKARLAR ODALARI BİRLİĞİ

KURULUŞ: 1951

Sayı : 4273

23 Haziran 2026

Konu: Nato Zirvesi Kapsamında Kritik Altyapıların Siber Saldırılara Karşı Dayanıklılığının Güçlendirilmesi hk.

ODASI BAŞKANLIĞINA

İlgi: İstanbul Valiliği İl Yazı İşleri Müdürlüğü'nün 19.06.2026 tarih ve E.1172694 sayılı yazısı,

Cumhurbaşkanlığı Siber Güvenlik Başkanlığı tarafından Valiliğimize gönderilen; Nato Zirvesi Kapsamında Kritik Altyapıların Siber Saldırılara Karşı Dayanıklılığının Güçlendirilmesi hakkındaki yazısı ilişiktir.

Bilgilerinizi rica ederiz.

Lütfi DEMİR
Genel Sekreter

Zeki ATEŞ
Kurul Üyesi

EKİ:
1- Cumhurbaşkanlığı Siber Güvenlik Başkanlığı'nın yazısı (3 sayfa)

Kartaltepe Mah. Alpay İzer Sok. No: 12 İncirli Pk. 34145 - Bakırköy / İSTANBUL
Telefon: 0850 279 70 70 Fax : (0212) 660 29 97
Web Site: www.istesob.org.tr E-mail: info@istesob.org.tr Kep: istesob@hs03.kep.tr

T.C.
CUMHURBAŞKANLIĞI
Siber Güvenlik Başkanlığı

Sayı : E-17394444-951.01.09-7520
Konu : NATO Zirvesi Kapsamında Kritik Altyapıların Siber Saldırılara Karşı Dayanıklılığının Güçlendirilmesi

DAĞITIM YERLERİNE

Bilindiği üzere 7-8 Temmuz 2026 tarihlerinde ülkemiz NATO Zirvesine ev sahipliği yapacaktır. NATO Zirvesi süresince; ulusal siber güvenlik ve dayanıklılık kapasitesinin güçlendirilmesi, siber tehditlere karşı operasyonel hazırlık seviyesinin en üst düzeye çıkarılması ve kritik altyapı hizmetlerinin kesintisiz sürdürülebilmesi büyük önem arz etmektedir. Bu doğrultuda, kritik kamu hizmetleri başta olmak üzere, kritik altyapılarda meydana gelebilecek siber güvenlik zafiyetlerinin tespit edilmesi ve bunlara yönelik siber tehditlerin bertaraf edilmesi için gerekli çalışmalar başkanlığımız uhdesinde yürütülmektedir.

Uluslararası düzeyde geniş katılımla gerçekleştirilecek olan söz konusu organizasyonun ülkemiz açısından güvenli, kesintisiz ve etkin şekilde icra edilmesini teminen; kamu kurum ve kuruluşları, kritik altyapıya sahip kuruluşlarile ilgili özel sektör paydaşlarınca, sorumluluk alanları dahilindeki bilişim sistemleri, dijital hizmetler ve haberleşme altyapılarına yönelik siber güvenlik tedbirlerinin en üst seviyede uygulanması önem arz etmektedir.

Bu kapsamda;

a) Kurum ve kuruluşların sorumluluğunda bulunan kritik bilgi sistemleri, dijital altyapı ve hizmetler, internet erişim altyapıları, haberleşme sistemleri, veri merkezleri, bulut bilişim hizmetleri ve organizasyonla doğrudan veya dolaylı ilişkili tüm bilişim varlıklarının güvenlik seviyelerinin gözden geçirilmesi,
b) Kamuya açık internet siteleri, çevrim içi başvuru ve işlem platformları, mobil uygulamalar, API servisleri, uzaktan erişim sistemleri, e-posta altyapıları ve dış dünyaya açık tüm servislerde zafiyet taraması ve yapılandırma kontrolünün ivedilikle yapılması,
c) Tespit edilen kritik ve yüksek seviyeli zafiyetler başta olmak üzere, istismar edilebilir güvenlik açıklarına yönelik gerekli yamaların uygulanması, güvenli yapılandırmaların tesis edilmesi ve telafi edici kontrollerin gecikmeksizin devreye alınması,
ç) Kritik sistemlerin sürekliliğini teminen iş sürekliliği planları, felaket kurtarma senaryoları, yedeklilik mekanizmaları, yedeklerden geri dönüş süreçleri ve kriz yönetimi prosedürlerinin gözden geçirilmesi; eksikliklerin giderilmesi,
d) Kurumsal Siber Olaylara Müdahale Ekipleri (SOME), bilgi işlem, ağ yönetimi, sistem yönetimi, uygulama geliştirme, veri tabanı yönetimi, güvenlik operasyon merkezi ve ilgili idari birimler arasında kesintisiz koordinasyon sağlanması; olay müdahale ve eskalasyon prosedürlerinin güncellenmesi,

Cumhurbaşkanlığı Çankaya Yerleşkesi Ziaur Rahman Cad. 06550 Çankaya/ Ankara/
Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : siberguvenlikbaskanligi@hs01.kep.tr

e) Organizasyon öncesinde ve organizasyon süresince kritik sistemler için artırılmış izleme seviyesine geçilmesi; güvenlik izleme, loglama, alarm üretimi, olay korelasyonu, tehdit istihbaratı takibi ve anomali tespiti süreçlerinin etkin şekilde işletilmesi,

f) Dağıtık hizmet engelleme saldırıları (DDoS), oltalama faaliyetleri, zararlı yazılım yayılımı, kimlik bilgisi ele geçirme teşebbüsleri, web uygulama saldırıları, tedarik zinciri kaynaklı riskler ve sosyal mühendislik faaliyetlerine karşı gerekli teknik ve idari tedbirlerin alınması,

g) Kurum ve kuruluşların uzaktan erişim amacıyla kullandığı SSL VPN, IPsec VPN ve benzeri dış erişim servislerinin risk değerlendirmesine tabi tutulması; organizasyonun icra edileceği 05/07/2026 - 10/07/2026 tarihleri arasında, hizmet sürekliliği bakımından zorunlu olmayan uzaktan erişimlerin mümkün olduğunca kapatılması veya kısıtlanması; açık tutulması zorunlu olan erişimlerde çok faktörlü kimlik doğrulama, kaynak IP kısıtlaması, kullanıcı/yetki gözden geçirmesi, oturum kayıtlarının izlenmesi ve anomali kontrollerinin sıkılaştırılması,

ğ) Hizmet alınan internet servis sağlayıcıları, veri merkezi işletmecileri, bulut hizmeti sağlayıcıları ve DDoS koruma hizmeti sunan taraflarla koordinasyon sağlanması; dağıtık hizmet engelleme saldırılarına karşı mevcut koruma profilleri, trafik eşikleri, kara liste/beyaz liste kuralları, yönlendirme ve filtreleme mekanizmaları ile alarm ve eskalasyon süreçlerinin gözden geçirilmesi; organizasyon süresince mümkün olan en yüksek koruma seviyesinin uygulanması,

h) Kimlik doğrulama ve yetkilendirme prosedürlerinin gözden geçirilerek, uzaktan erişim, yönetici hesapları, ayrıcalıklı kullanıcı yetkileri, servis hesapları ve üçüncü taraf erişimlerinde mümkün olan sıkılaştırmaların yapılması; çok faktörlü kimlik doğrulama, güçlü parola politikaları, erişim kısıtlamaları ve kayıt altına alma mekanizmalarının etkin biçimde uygulanması,

ı) Üçüncü taraf hizmet sağlayıcıları, yükleniciler, bakım-destek firmaları, bulut hizmeti sağlayıcıları ve teknoloji tedarikçilerinden kaynaklanabilecek tedarik zinciri risklerinin değerlendirilmesi; bu tarafların erişim yetkileri, güvenlik yükümlülükleri ve olay bildirim sorumluluklarının kontrol edilmesi,

i) Sistemlerde planlı bakım, sürüm güncellemesi, konfigürasyon değişikliği, servis taşıma, altyapı dönüşümü ve benzeri değişikliklerin risk değerlendirmesi yapılmaksızın gerçekleştirilmemesi; zorunlu değişiklikler dahil olmak üzere değişiklik yönetimi süreçlerinin eksiksiz işletilmesi,

j) Kritik sistemlere ilişkin güncel varlık envanteri, ağ diyagramları, servis bağımlılıkları, irtibat listeleri ve olay müdahale dokümantasyonunun hazır bulundurulması,

k) SOME ekiplerinin iletişim bilgilerinin güncelliğinin SOME iletişim platformu üzerinden kontrol edilerek organizasyonun icra edileceği 05/07/2026 - 10/07/2026 tarihleri süresince 7/24 esaslı ulaşılabilir olmasını sağlayacak tedbirlerin alınması,

l) Olası siber güvenlik olaylarında görev alacak teknik ve idari irtibat personelinin önceden belirlenmesi, iletişim bilgilerinin güncel tutulması ve organizasyon süresince erişilebilir olacak şekilde gerekli nöbet/icap düzenlemelerinin yapılması,

m) Olası siber olayların erken tespiti, hızlı müdahalesi, etkilerinin sınırlandırılması ve hizmet sürekliliğinin sağlanması amacıyla kurum içi bildirim, karar alma, teknik müdahale ve üst makamlara raporlama süreçlerinin önceden netleştirilmesi,

n) Siber güvenlik vakalarının ve yetkisiz erişim girişimlerinin tespit edilebilmesi amacıyla; tüm bilişim sistemlerinin merkezi bir "Güvenlik İzleme ve Olay Yönetimi" sistemi (SIEM – Security Information and Event Management) üzerinden takip edilecek şekilde yapılandırılması,

Cumhurbaşkanlığı Çankaya Yerleşkesi Ziaur Rahman Cad. 06550 Çankaya/ Ankara/
Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : siberguvenlikbaskanligi@hs01.kep.tr

o) SIEM aracılığıyla şüpheli durumları otomatik bir şekilde tespit ederek bildirim oluşturacak alarm mekanizmalarının kurulması,

ö) Tüm uygulamalarda, her kullanıcının ne kadar sıklıkla işlem yapabileceğini sınırlayan (rate-limiting) bir sistemin aktif hale getirilmesine, söz konusu sınırlamaların SIEM sistemi üzerinden kullanıcı bazlı takip edilmesi,

p) Organizasyon süresince meydana gelebilecek kritik siber güvenlik olayları, şüpheli aktiviteler, kesinti girişimleri, veri sızıntısı emareleri ve hizmet sürekliliğini etkileyebilecek gelişmeler hakkında Siber Güvenlik Başkanlığı ile gecikmeksizin bilgi paylaşılması

hususlarında

Gereğini arz/rica ederim.

Ümüt ÖNAL
Siber Güvenlik Başkanı

Dağıtım:
Dağıtım Listesi (406 Muhatap)

Cumhurbaşkanlığı Çankaya Yerleşkesi Ziaur Rahman Cad. 06550 Çankaya/ Ankara/
Türkiye
Tel: 0 312 969 3900 0 312 969 3901
KEP Adresi : siberguvenlikbaskanligi@hs01.kep.tr