Siber Güvenlik Kanunu

SGK · No: 7545

Madde 3 Tanım ve kısaltmalar

Bu Kanunda geçen;

a) Barındırma: Bilişim sistemlerinin harici bir veri merkezinde bulundurulmasını,

b) Başkan: Siber Güvenlik Başkanını,

c) Başkanlık: Siber Güvenlik Başkanlığını,

ç) Bilişim sistemleri: Bilgi ve iletişim teknolojileri vasıtasıyla sağlanan her türlü hizmetin, işlemin ve verinin sunumunda kullanılan donanım, yazılım, sistem ve aktif veya pasif durumda bulunan tüm diğer bileşenleri,

d) Kritik altyapı: İşlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara ve güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları,

e) Kritik kamu hizmeti: Ulusal, toplumsal veya ekonomik faaliyetlerin sürdürülmesi için gerekli olan ve kesintiye uğraması veya zarar görmesi halinde ulusal güvenlik, ülkenin sosyal veya ekonomik refahı, kamu düzeni veya sağlığı ya da diğer hizmetlerin sunumu üzerinde önemli bir etki oluşturabilecek ülke genelinde tekel veya sınırlı ikame ile sunulan hizmeti,

f) Siber güvenlik: Siber uzayı oluşturan bilişim sistemlerinin saldırılardan korunmasını, bu ortamda işlenen verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber olayların tespit edilmesini, bu tespitlere karşı tepki ve alarm mekanizmalarının devreye alınmasını ve sonrasında yaşanan siber olay öncesi duruma geri döndürülmesini kapsayan faaliyetler bütününü,

g) Siber olay: Bilişim sistemlerinin veya verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini,

ğ) Siber saldırı: Siber uzaydaki bilişim sistemlerinin ve bu sistemler tarafından işlenen verinin gizliliği, bütünlüğü veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın herhangi bir yerindeki kişi veya bilişim sistemlerine yönelik olarak kasıtlı yapılan işlemleri,

h) Siber tehdit: Bilişim sistemlerinin, bu sistemlerde bulunan veya bu sistemler tarafından işlenen verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesine neden olabilecek potansiyel tehlikeleri,

ı) Siber tehdit istihbaratı: Siber uzaydaki varlıklara yönelik mevcut veya potansiyel siber tehdit unsurları ile siber saldırılar hakkında bir araya getirilmiş, dönüştürülmüş, analiz edilmiş, yorumlanmış veya zenginleştirilmiş bilgiyi,

i) Siber uzay: Doğrudan ya da dolaylı olarak internete, elektronik haberleşme veya bilgisayar ağlarına bağlı olan tüm bilişim sistemlerini ve bunları birbirine bağlayan ağlardan oluşan ortamı,

j) SOME: Siber olaylara müdahale ekibini,

k) Varlık: Elektronik veya fiziksel ortamlarda yer alan ve iletişim yoluyla aktarılabilen veriyi içeren tüm bilgi ve bilgi işleme olanaklarını, veriyi kullanan veya taşıyan personeli ve veriyi barındıran fiziksel mekânları,

l) Zafiyet: Siber uzayda yer alan varlıkların herhangi bir siber tehdit tarafından istismar edilebilecek zayıflık ve güvenlik açıklarını,

ifade eder.