Bilişim Hukuku

Ünite 4 : Siber Güvenlik Kanunu
Kanun Numarası: 7545, Kabul Tarihi: 12.03.2025

Öğr. Gör. Zafer SERİN

Konular

- Kanunun Amacı, Kapsamı ve Temel İlkeleri
- Önemli Tanımlar
- Kurumsal Yapı (Başkanlık ve Kurul)
- Görev, Yetki ve Sorumluluklar
- Denetim Süreçleri
- Cezai Hükümler ve Yaptırımlar
- Geçiş Süreci ve Sonuç

Kanunun Amacı Nedir?

- Türkiye'nin siber uzaydaki unsurlarına yönelik tehditleri tespit etmek ve bertaraf etmek.
- Siber olayların etkilerini azaltmaya yönelik esasları belirlemek.
- Kamu ve özel sektörün siber saldırılara karşı korunmasını düzenlemek.
- Ülkenin siber güvenliğini güçlendirecek stratejileri belirlemek.
- Siber Güvenlik Kurulunun kurulmasını düzenlemek.

Bu Kanun Kimleri Kapsar?

- Siber uzayda faaliyet yürüten veya hizmet sunan:
  1. Kamu kurum ve kuruluşları.
  2. Kamu kurumu niteliğinde meslek kuruluşları.
  3. Gerçek ve tüzel kişiler (Şirketler, vatandaşlar vb.).
  4. Tüzel kişiliği olmayan kuruluşlar.

Neler Kapsam Dışındadır?

- Polis, Sahil Güvenlik ve Jandarma'nın yürüttüğü istihbari faaliyetler.
- Milli İstihbarat Teşkilatı (MİT) Kanunu uyarınca yürütülen faaliyetler.
- Türk Silahlı Kuvvetleri (TSK) İç Hizmet Kanunu uyarınca yürütülen faaliyetler.

Önemli Kavramlar: Siber Uzay ve Güvenlik

- Siber Uzay: İnternete, elektronik haberleşme veya bilgisayar ağlarına bağlı tüm bilişim sistemlerinden oluşan ortam.
- Siber Güvenlik: Bilişim sistemlerinin saldırıdan korunması; verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınması; saldırı tespiti, tepki verilmesi ve normale döndürme faaliyetleri bütünü.

Önemli Kavramlar: Tehditler

- Siber Olay: Bilişim sistemlerinin veya verinin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesi.
- Siber Saldırı: Veri gizliliğini, bütünlüğünü veya erişilebilirliğini ortadan kaldırmak amacıyla kasıtlı yapılan işlemler.
- Siber Tehdit: İhlale neden olabilecek potansiyel tehlikeler.
- Zafiyet: Bir siber tehdit tarafından istismar edilebilecek zayıflık veya güvenlik açığı.

Önemli Kavramlar: Altyapı

- Kritik Altyapı: İşlediği verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda;
  1. Can kaybına,
  2. Büyük ölçekli ekonomik zarara,
  3. Güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapılar.
- SOME: Siber Olaylara Müdahale Ekibi.

Kanunun Temel İlkeleri Nelerdir? (1)

- Siber güvenlik, milli güvenliğin ayrılmaz bir parçasıdır.
- Temel hedef, kritik altyapıları korumak ve güvenli bir siber uzay oluşturmaktır.
- Çalışmalar kurumsallık, süreklilik ve sürdürülebilirlik temelli yürütülür.
- Siber güvenlik tedbirleri, ürün ve hizmetlerin tüm yaşam döngüsü boyunca uygulanır.

Kanunun Temel İlkeleri Nelerdir? (2)

- Siber güvenliğin sağlanmasında öncelikle yerli ve milli ürünler tercih edilir.
- Tüm kamu kurumları, gerçek ve tüzel kişiler siber güvenlik tedbirlerinin alınmasından sorumludur.
- Hesap verebilirlik esastır.
- Nitelikli insan kaynağının artırılması teşvik edilir.
- Hukukun üstünlüğü, temel insan hakları ve mahremiyetin korunması esastır.

Kurumsal Yapı: İki Ana Direk

- Stratejik Seviye (Karar Alıcı): Siber Güvenlik Kurulu
- Operasyonel Seviye (Yürütücü): Siber Güvenlik Başkanlığı

Stratejik Çatı: Siber Güvenlik Kurulu

- Başkan: Cumhurbaşkanı (veya katılmadığında Cumhurbaşkanı Yardımcısı).
- Üyeler (Örnek): Adalet, Dışişleri, İçişleri, Milli Savunma, Sanayi ve Ulaştırma Bakanları, MİT Başkanı, MGK Genel Sekreteri, Savunma Sanayii Başkanı ve Siber Güvenlik Başkanı.
- Sekretarya: Başkanlık tarafından yürütülür.

Kurul Ne Yapar? (Stratejik Görevler)

- Siber güvenlikle ilgili politika, strateji ve eylem planlarına yönelik kararları almak.
- Ülke çapında uygulanacak teknoloji yol haritasına yönelik kararlar almak.
- Teşvik verilecek öncelikli alanları belirlemek.
- Kritik altyapı sektörlerini belirlemek.
- Başkanlık ile diğer kamu kurumları arasındaki ihtilafları karara bağlamak.

Yürütme Gücü: Siber Güvenlik Başkanlığı

- Kanunun uygulanmasından sorumlu ana yürütme organıdır.
- Siber dayanıklılığın artırılması için faaliyet yürütür.
- Siber tehdit istihbaratı elde eder, oluşturur ve paylaşır.
- Zafiyet ve sızma testleri yapar veya yaptırır.

Başkanlığın Operasyonel Görevleri (1)

- Kritik altyapıları, kurumlarını ve konumlarını belirlemek.
- Kamu ve kritik altyapıların (veri envanteri dahil) varlık envanterinin tutulmasını sağlamak.
- Varlıkların kritikliğine göre güvenlik tedbirlerini almak veya aldırmak.
- SOME'ler kurmak, kurdurmak ve denetlemek.
- Siber güvenlik tatbikatları gerçekleştirmek.

Başkanlığın Regülasyon Görevleri (2)

- Siber güvenlik alanına ilişkin standartları hazırlamak veya uygun bulduklarını kabul etmek.
- Yazılım, donanım, ürün ve hizmetlere yönelik test ve sertifikasyon işlemlerini yürütmek.
- Siber güvenlik uzmanları ve şirketlerine yönelik sertifikasyon, yetkilendirme ve belgelendirme yapmak.
- Siber güvenlik denetimi gerçekleştirmek ve yaptırım uygulamak.

Başkanlığın Kritik Yetkileri (1)

- Siber saldırılara karşı caydırıcılık için gerekli tedbirleri almak veya aldırmak.
- Bilişim sistemlerine uygun bulunan yazılım ve donanımların kurulumunu sağlayabilir.
- Bu ürünlerce toplanan veri ve log kayıtlarını Başkanlık sistemlerine aktarabilir.
- Siber olaya maruz kalanlara yerinde veya uzaktan müdahale desteği sağlayabilir.

Başkanlığın Bilgi Toplama Yetkisi (2)

- Kanun kapsamındakilerden (tüm kurum ve şirketler) yürüttüğü faaliyetle sınırlı olarak bilgi, belge, veri ve kayıtları alabilir.
- Talepte bulunulanlar, kendi mevzuatındaki hükümleri gerekçe göstererek talebin yerine getirilmesinden kaçınamazlar.
- Elde edilen bilgi ve belgeler en fazla iki yıl çalışmaya konu edilir ve sonra imha edilir.
- Bilişim sistemlerindeki log kayıtlarını bünyesinde toplayabilir, saklayabilir ve değerlendirebilir.

Bizim Sorumluluklarımız Neler?

- Başkanlığın talep ettiği her türlü veri, bilgi, belge ve katkıyı öncelikle ve zamanında iletmek.
- Tespit ettikleri zafiyet veya siber olayları gecikmeksizin Başkanlığa bildirmek.
- Kamu ve kritik altyapılar, siber güvenlik ürünlerini Başkanlıkça yetkilendirilmiş uzman veya şirketlerden tedarik etmek zorundadır.

Denetim Nasıl Yapılacak?

- Başkanlık, Kanun kapsamındaki her türlü fiil ve işlemi denetleyebilir.
- Denetimi kim yapar?
  1. Başkanlık personeli.
  2. Yetkilendirilmiş bağımsız denetçiler.
  3. Bağımsız denetim kuruluşları.
- ÖNEMLİ: Kamu kurumları ve kritik altyapılarda denetimler, Başkanlık personelince veya refakatinde yapılır.

Denetçinin Yetkileri Nelerdir?

- Elektronik veriyi, belgeleri, cihaz, sistem, yazılım ve donanımları incelemek.
- Bunlardan kopya, dijital suret veya örnek almak.
- Konuyla ilgili yazılı veya sözlü açıklama istemek.
- Yükümlülük: Denetime tabi tutulanlar, ilgili sistemleri denetlemeye açık tutmak ve gerekli altyapıyı sağlamak zorundadır.

Arama ve El Koyma (Özel Durumlar)

- Suç veya siber saldırıların önlenmesi amacıyla;
- Konutta, işyerinde ve kamuya açık olmayan kapalı alanlarda arama yapılabilir.
- Kural: Hâkim kararı üzerine.
- İstisna (Gecikme Varsa): Cumhuriyet savcısının yazılı emri ile.
  - (Bu durumda 24 saat içinde hâkim onayına sunulur) .
- İstisna (Veri Merkezleri): Yetkili veri merkezlerinde sadece hâkim kararıyla arama yapılabilir.
- İstisna (Kamu): Kamu kurum ve kuruluşları bakımından hâkim kararı aranmaz.

Yaptırımlar: Hapis Cezaları (1)

- 1-3 Yıl Hapis: Denetim görevlilerinin istediği bilgi/belgeyi vermeyenler (kamu hariç).
- 2-4 Yıl Hapis: Gerekli izin/yetkiyi almadan faaliyet yürütenler.
- 4-8 Yıl Hapis: Sır saklama yükümlülüğünü yerine getirmeyenler (Madde 13).
- 3-5 Yıl Hapis: Başkanlıktan ayrıldıktan sonra 2 yıllık yasağa uymayanlar (Madde 12).

Yaptırımlar: Hapis Cezaları (2)

- 3-5 Yıl Hapis: Sızan kişisel veya kritik verileri izinsiz paylaşan/satışa çıkaranlar.
- 2-5 Yıl Hapis: Halkta panik yaratmak amacıyla yalan veri sızıntısı haberi yayanlar.
- 8-12 Yıl Hapis: Türkiye'nin siber unsurlarına yönelik siber saldırıda bulunanlar.
- 10-15 Yıl Hapis: Bu saldırıdan elde ettiği veriyi yayan veya satışa çıkaranlar.

Cezayı Artıran Durumlar

- Suçun kamu görevlisi tarafından işlenmesi (Üçte bir artırım).
- Suçun birden fazla kişi tarafından işlenmesi (Yarı oranında artırım).
- Suçun bir örgütün faaliyeti çerçevesinde işlenmesi (Yarısından iki katına kadar artırım).

Yaptırımlar: İdari Para Cezaları

- 1 Milyon TL - 10 Milyon TL:
  1. Zafiyet veya siber olayı Başkanlığa bildirmeyenler.
  2. Yetkisiz şirketlerden ürün tedarik eden kritik altyapılar.
- 10 Milyon TL - 100 Milyon TL:
  1. Siber güvenlik şirketlerinin yurt dışı satış, birleşme, devir gibi işlemlerinde Başkanlık onayı almayanlar (Madde 18) .
- 100 Bin TL - 1 Milyon TL:
  1. Denetimde sistemlerini incelemeye açmayanlar.
  2. (Bu ceza ticari şirketler için brüt satış hasılatının %5'ine kadar çıkabilir).

Siber Güvenlik Şirketlerine Özel Düzenlemeler

- Siber güvenlik ürünlerinin yurt dışına satışı, Başkanlıkça belirlenecek usul ve esaslara tabidir (İzne tabi olabilir).
- Bu şirketlerin;
  1. Birleşme,
  2. Bölünme,
  3. Pay devri veya satış işlemleri Başkanlığa bildirilmek zorundadır.
- Şirket üzerinde kontrol hakkı sağlayan işlemler Başkanlık onayına tabidir.
- Onay alınmadan yapılan işlemler hukuki bir geçerlilik kazanmaz.

Mevcut Durumdan Yeni Düzene Geçiş

- BTK (Bilgi Teknolojileri ve İletişim Kurumu) ve Dijital Dönüşüm Ofisi'ndeki ulusal siber güvenlik faaliyetleri, varlıkları ve ilgili personeli 6-9 ay içinde yeni Başkanlığa devredilecektir.
- ÖNEMLİ: Halen siber güvenlik alanında faaliyet gösteren dernek, vakıf ve ticaret şirketleri, düzenlemeler yürürlüğe girdikten sonra 1 YIL İÇİNDE Başkanlığın belirlediği sertifikasyon ve yetkilendirme işlemlerini tamamlamak zorundadır.
- Bu yükümlülüğü yerine getirmeyenler, siber güvenlik alanında faaliyette bulunamaz.

Son Hükümler

- Yürürlük (Madde 20): Bu Kanun yayımı tarihinde (19/3/2025) yürürlüğe girer.
- Yürütme (Madde 21): Bu Kanun hükümlerini Cumhurbaşkanı yürütür.
- Uygulama (Geçici Madde 1): Kanunun uygulanmasına ilişkin yönetmelik vb. düzenlemeler 1 yıl içinde yürürlüğe konulur.

Teşekkürler

- Kanun (7545), siber güvenliği "milli güvenliğin" bir parçası olarak tanımlamıştır.
- Stratejik kararlar için Siber Güvenlik Kurulu, yürütme ve denetim için Siber Güvenlik Başkanlığı kurulmuştur.
- Kamu, özel sektör ve kritik altyapılar için net sorumluluklar (olay bildirimi, yetkili satıcı) getirilmiştir.
- Başkanlığa geniş denetim, bilgi toplama ve yaptırım yetkileri verilmiştir.