

YÖNETMELİK

Telekomünikasyon Kurumundan:

ELEKTRONİK HABERLEŞME GÜVENLİĞİ YÖNETMELİĞİ

BİRİNCİ BÖLÜM

Genel Hükümler

Amaç

MADDE 1 – (1) Bu Yönetmeliğin amacı, elektronik haberleşme güvenliğine ilişkin usul ve esasları düzenlemektir.

Kapsam

MADDE 2 – (1) Bu Yönetmelik, işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesi veya azaltılmasına ilişkin olarak alacakları tedbirlere yönelik usul ve esasları kapsar.

(2) Kişisel bilgilerin işlenmesi ve gizliliğinin korunması, bu Yönetmelik kapsamı dışındadır.

Dayanak

MADDE 3 – (1) Bu Yönetmelik, 4/2/1924 tarihli ve 406 sayılı Telgraf ve Telefon Kanununun 2 ve 4 üncü maddesi ile 5/4/1983 tarihli ve 2813 sayılı Telsiz Kanununun 7 nci maddesine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 4 – (1) Bu Yönetmelikte geçen;

a) Donanım-yazılım: Elektronik haberleşme altyapısı, bilgisayarlar, veri kaydetmek için kullanılan taşınabilir ve sabit diskler ile bunlarda kullanılan yazılım bileşenlerini,

b) Elektronik haberleşme: Elektriksel işaretlere dönüştürülebilir her türlü işaret, sembol, ses, görüntü ve verinin kablo, telsiz, optik, elektrik, manyetik, elektromanyetik, elektrokimyasal, elektromekanik ve diğer iletim sistemleri vasıtasıyla iletilmesini, gönderilmesini ve alınmasını,

c) Elektronik haberleşme altyapısı: Elektronik haberleşmenin, üzerinden veya aracılığıyla gerçekleştirildiği anahtarlama ekipmanları, donanım ve yazılımlar, terminaller ve hatlar da dahil olmak üzere her türlü şebeke birimlerini,

ç) Elektronik haberleşme hizmeti: Elektronik haberleşme tanımına giren faaliyetlerin bir kısmının veya tamamının hizmet olarak sunulmasını,

d) Elektronik haberleşme şebekesi: Bir veya daha fazla nokta arasında elektronik haberleşmeyi sağlamak için bu noktalar arası bağlantıyı teşkil eden anahtarlama ekipmanları ve hatlar da dahil olmak üzere her türlü iletim sistemleri ağını,

e) Güvenlik hassasiyetli alan: Elektronik haberleşme altyapısının işletmeci kontrolündeki bölümlerini,

f) İşletmeci: Kurum tarafından yapılan bir yetkilendirme çerçevesinde elektronik haberleşme hizmeti sunan ve/veya elektronik haberleşme şebekesi sağlayan ve alt yapısını işleten sermaye şirketini,

g) Kurul: Telekomünikasyon Kurulunu,

ğ) Kurum: Telekomünikasyon Kurumunu,

h) Şifreleme: Veri muhteviyatının, yalnızca yetkili kişi ya da kurumlarca veya haberleşmeyi gerçekleştiren taraflarca bilinmesini sağlamak ve üçüncü şahıslarla elde edilmesini önlemek üzere, söz konusu verinin formunun özel bir şablona göre değiştirilmesini,

ı) Veri: Abone ya da kullanıcının elektronik haberleşme şebekesi üzerindeki konum, zaman, trafik bilgileri ile elektronik haberleşmenin içeriğini,

i) Veri güvenliği: Verinin gizliliği, bütünlüğü ve devamlılığının sağlanmasını ifade eder.

İlkeler

MADDE 5 – (1) Bu Yönetmeliğin uygulanmasında aşağıda belirtilen temel ilkeler gözetilir:

a) Objektif nedenler aksini gerektirmedikçe, niceliksel ve niteliksel devamlılık, ayırım gözetmeme, düzenlilik, şeffaflık ve kaynakların etkin kullanılması,

b) Tüketici haklarının korunması,

c) Hizmet kalitesinin yükseltilmesi,

ç) Ulusal düzenleme ile ulusal ve/veya uluslararası standartların dikkate alınması.

İKİNCİ BÖLÜM

Elektronik Haberleşme Güvenliği Usul ve Esasları

Tehdit ve zafiyetler

MADDE 6 – (1) Elektronik haberleşmeye ilişkin başlıca tehditler;

a) Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi,

b) Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması,

c) Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi,

ç) Deprem, sel, su baskını, yangın gibi doğal afetler ile grev ve lokavt hali,

d) Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,

e) Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi,

f) Doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafta

gönderilmesi,

g) Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesidir.

(2) Elektronik haberleşmeye ilişkin başlıca zafiyetler;

a) Gelecekte gerçekleşmesi muhtemel tehditlerin öngörülememesi,

b) Bir sistem veya protokolün tasarımında yapılan yanlışlıklar,

c) Bir sistem veya protokolün kurulumu sırasında oluşan problemler,

ç) Geliştiricilerin hataları,

d) Uygulayıcıların hataları,

e) Sistemin işletimi sırasında oluşan uygunsuzluklar veya yetersizliklerdir.

Fiziksel alan güvenliği

MADDE 7 – (1) Bina içi güvenlik hassasiyetli alanlarda aşağıdaki hükümler uygulanır:

a) Giriş ve erişim yetkisi ile bu yetkinin kapsamı işletmeci tarafından önceden tanımlanarak, giriş ve erişim sadece yetkili kişilerle sınırlandırılır.

b) Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak, tarih, saat ve kimlik gibi bilgiler kaydedilerek, her ziyaretçinin sadece izin verilen yerlere girişi ve çıkışı sağlanır.

c) Tüm personel ve personel harici kişiler, kimlik bilgilerini, yetki ve erişim seviyelerini açık bir şekilde görünür kılabacak giriş veya kimlik kartı taşır.

ç) Güvenlik hassasiyetli alanlara giriş ve erişim yetkisi, düzenli olarak gözden geçirilerek güncellenir ve gerekli değilse iptal edilir.

(2) Bina dışı güvenlik hassasiyetli alanlarda aşağıdaki hükümler uygulanır:

a) Sahada yer alan, elektronik haberleşme altyapısını içeren bina, kule, dolap ve kutu gibi güvenlik riski oluşturabilecek alt yapı bileşenlerine erişim kontrol altında tutulur ve yetkisiz kişilerin kolaylıkla erişim sağlayamayacağı şekilde tesis edilir.

b) Elektronik haberleşme maksatlı kullanılan kule ve saha dolapları, yetkisiz kişilerin müdahale etmesini engellemek amacıyla uyarıcı levhalar ile donatılır.

(3) Güvenlik hassasiyetli alanlarda ilave olarak aşağıdaki tedbirler alınır:

a) Kötü niyetli faaliyetleri engellemek amacıyla planlanmamış çalışmalardan kaçınılır.

b) Ses ve/veya video kayıt cihazlarının güvenlik hassasiyetli alanlara, izinsiz olarak girişini engellemek amacıyla gerekli önlemler alınır.

c) Güvenlik hassasiyetli alanların, tehditlere karşı korunması amacıyla fiziki güvenlik tedbirleri planlanır ve gerekli önlemler alınır.

Personel güvenilirliği

MADDE 8 – (1) Elektronik haberleşme altyapısında istihdam edilen teknik personel, konusunda yeterli mesleki deneyime sahip ya da eğitim almış olmalıdır. Bu personelin görev tanım ve sorumlulukları açıkça belirlenmelidir.

(2) Elektronik haberleşme altyapısında istihdam edilecek personel hakkında adli sicil kaydı belgesi istenir.

(3) Personelin haberleşme gizliliğine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için her türlü önlem alınarak, işlerin ve hizmetlerin düzenli yürütülmesi sağlanır.

Veri güvenliği

MADDE 9 – (1) Veri güvenliği aşağıdaki hükümler uyarınca sağlanır:

a) Veri erişim yetkisi ve bu yetkinin kapsamı, veri türüne göre önceden belirlenir ve kayıt altına alınır.

b) Yetki sınırları dahilinde erişim sağlanması için kullanılacak teknolojilerin seçimi, işletmecinin tasarrufundadır.

Donanım-yazılım güvenliği ve güvenilirliği

MADDE 10 – (1) Elektronik haberleşme altyapılarında kullanılan donanım-yazılım güvenliği ve güvenilirliği aşağıdaki hükümler uyarınca sağlanır:

a) Donanım-yazılımın ulusal düzenleme ile ulusal ve/veya uluslararası standartlara uygun olması sağlanır.

b) Aynı fiziksel alanda ve/veya farklı fiziksel alanlarda bulunan donanım-yazılım bileşenleri arasındaki iç haberleşmeyi sağlayan kablolu ve/veya kablosuz ağ yönetimi sadece yetkili kişiler tarafından erişilecek şekilde şifrelenir.

c) Donanım-yazılım bileşenleri, herhangi bir güvenlik tehdidinin gerçekleşmesini önlemek üzere kontrol ve izleme altında tutulur.

ç) Donanım-yazılım bileşenlerinin, yasal olmayan elektronik haberleşme dinleme ve/veya izleme tehdidi oluşturacak unsurları içerip içermediğini belirlemek üzere satın alma, kullanım, bakım ve onarım sırasında kontrolleri yapılır. Donanım-yazılım bileşenlerinde bu tür bir unsurun varlığının saptanması durumunda ilgili bileşenin kullanımına son verilir. Bu durum kayıt altına alınarak raporlanır ve oluşan tehdidi bertaraf edecek önlemler ivedilikle alınır.

d) İşletmeci, elektronik haberleşmenin gizliliği, bütünlüğü ve devamlılığının sağlanması için kritik donanım-yazılım bileşenlerinin tespitini yapar. Tespit edilen kritik donanım-yazılım bileşenlerinin yedekli çalışması esastır.

ÜÇÜNCÜ BÖLÜM

İşletmecilerin Yükümlülükleri

Elektronik haberleşme güvenliğini sağlama yükümlülüğü

MADDE 11 – (1) İşletmeci, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlüdür. Yetkilendirilen işletmeciler yetkilendirme tarihinden itibaren bir yıl içerisinde söz konusu standarda uygunluğu sağlar. Belirtilen süre içerisinde söz konusu standarda uygunluğu sağlayamayan işletmecilere Kurul tarafından gerekli görülmesi halinde ilave süre verilebilir.

(2) İşletmeci, elektronik haberleşme güvenliği kapsamında, başta 6 ncı maddede belirtilen tehdit ve zafiyetler olmak üzere, kendi teknik ve idarî yapılanmasına göre yılda en az bir kez risk analizi yapar veya bu analizi tarafsız kuruluşlara yaptırır. Bu çerçevede tespit edilen tehdit ve zafiyetlere ilişkin riski değerlendirerek gerekli önlemleri alır.

Kuruma bilgi verme yükümlülüğü

MADDE 12 – (1) Elektronik haberleşme güvenliğine ilişkin rapor her yıl yenilenir ve Şubat ayı sonuna kadar Kuruma gönderilir. Söz konusu rapor;

a) 11 inci madde kapsamında yapılan risk analizinde tespit edilen tehdit ve zafiyetler ile bunların yüksek, orta veya düşük şeklinde tasnifi ile gerçekleşme olasılıkları ve önlemleri,

b) Bir tehdit ve/veya zafiyetin gerçekleşmesi durumunda yürütülecek faaliyetleri ve bu faaliyetlerde görev alacak personel ile bunların yetki ve sorumluluklarının neler olacağını içeren iş akış diyagramları ve acil eylem planlarını,

c) Donanım-yazılım bileşenlerinin kurulumu, kullanımı ve işletimi ile bakım ve onarımı sırasında ortaya çıkan ve raporlanan problem ile uygunsuzlukları içerir.

Alt yüklenici firmadan sorumlu olma yükümlülüğü

MADDE 13 – (1) Alt yüklenici firma ile çalışılması halinde, alt yüklenici firma tarafından bu Yönetmelik hükümlerinin ihlal edilmesi durumunda söz konusu ihlalin işletmeci tarafından yapıldığı kabul edilir.

DÖRDÜNCÜ BÖLÜM

Çeşitli ve Son Hükümler

Müeyyideler

MADDE 14 – (1) Bu Yönetmelik hükümlerinin ihlali durumunda; 5/9/2004 tarihli ve 25574 sayılı Resmi Gazete’de yayımlanan Telekomünikasyon Kurumu Tarafından İşletmecilere Uygulanacak İdari Para Cezaları ile Diğer Müeyyide ve Tedbirler Hakkında Yönetmelikte söz konusu ihlale karşılık gelen idari para ceza oranları uygulanır. İdari para cezalarının uygulanması, tahsili, ihlalin tekrerrü gibi durumlarda, söz konusu Yönetmelik hükümleri uygulanır.

(2) Birinci fıkrada belirtilen Yönetmelikte yer almayan; haberleşmenin güvenliğine yönelik tehdit ve zafiyetlere ilişkin gerekli önlemlerin alınmaması ile bina içi ve dışı güvenlik hassasiyetli alanlarda yeterli önlemlerin alınmaması durumunda işletmecinin bir önceki takvim yılındaki cirosunun % 1 (yüzde bir)’ine kadar idari para cezası uygulanır. Kurul tarafından gerekli görülen durumlarda idari para cezası verilmeden önce, ilgili işletmeciye söz konusu durumun düzeltilmesi için yeterli süre verilebilir.

Standarda uygunluğu sağlama

GEÇİCİ MADDE 1 – (1) Bu Yönetmeliğin yayımlanmasından önce yetkilendirilen işletmeciler, Yönetmeliğin yayımı tarihinden itibaren bir yıl içerisinde 11 inci maddede belirtilen standarda uygunluğu sağlar. Belirtilen süre içerisinde söz konusu standarda uygunluğu sağlayamayan işletmecilere Kurul tarafından gerekli görülmesi halinde ilave süre verilebilir.

Yürürlük

MADDE 15 – (1) Bu Yönetmelik yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 16 – (1) Bu Yönetmelik hükümlerini Telekomünikasyon Kurulu Başkanı yürütür.