KAMUNET AĞINA BAĞLANMA VE KAMUNET AĞININ DENETİMİNE İLİŞKİN USUL VE ESASLAR HAKKINDA TEBLİĞ

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç ve kapsam

MADDE 1 – (1) Bu Tebliğin amacı; KamuNet'e dâhil edilecek ve dâhil olan kamu kurumlarının KamuNet'e bağlı bilgi ve iletişim sistemlerine ilişkin olarak karşılaması gereken asgari gereklilikler ile bu kurumların denetlenmesine ilişkin usul ve esasların belirlenmesidir.

Dayanak

MADDE 2 – (1) Bu Tebliğ, 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanununun 5 inci maddesinin birinci fıkrasının (h) bendine dayanılarak hazırlanmıştır.

Tanımlar

MADDE 3 – (1) Bu Tebliğde geçen;

a) Bakanlık: Ulaştırma, Denizcilik ve Haberleşme Bakanlığını,

b) Bilgi Güvenliği Yönetim Sistemi (BGYS): Bilginin gizliliğini, bütünlüğünü veerişilebilirliğini sağlamak üzere; sistemli, kuralları koyulmuş, planlı, yönetilebilir, sürdürülebilir, dokümante edilmiş, kurumun yönetimince kabul görmüş ve uluslararası güvenlik standartlarının temel alındığı faaliyetler bütününü,

c) Bütünlük: Varlıkların doğruluğunu ve tamlığını koruma özelliğini,

ç) Erişilebilirlik: Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

d) Gizlilik: Bilginin yetkisiz kişiler, varlıklar ya da süreçlere kullanılabilir yapılmama ya da açıklanmama özelliğini,

e) İşletmeci: KamuNet'e ait altyapıyı işleten işletmeciyi,

f) Kamu kurumu: KamuNet'e dâhil olan ya da olacak kamu kurumu ve kuruluşunu,

g) KamuNet: Kamukurum ve kuruluşları tarafından özel ağ ile internet ortamından yalıtılmış şekilde hizmet, işlem ve veri trafiğinin aktarılacağı, fiziksel ve siber saldırılara karşı daha güvenli kapalı devre, kamu sanal ağı altyapısını,

ğ) Kurumsal SOME:Kamuda ve ilgili Sektörel Siber Olaylara Müdahale Ekibi tarafındanbelirlenen kritik altyapı işleten kurumlarda kurulan Siber Olaylara Müdahale Ekibini,

h) Sektörel SOME: Kritik sektörlerde, varsa sektörü düzenleyici ve denetleyici kurumlar, yoksa ilgili bakanlıklar bünyesinde kurulan Siber Olaylara Müdahale Ekibini,

ı) SOME: Siber Olaylara Müdahale Ekibini,

i) USOM: Ulusal Siber Olaylara Müdahale Merkezini,

j) Varlık: KamuNet için değeri olan herhangi bir şeyi,

ifade eder.

(2) Bu Tebliğde geçen ve birinci fıkrada yer almayan tanımlar için elektronik haberleşme mevzuatında yer alan tanımlar geçerlidir.

İKİNCİ BÖLÜM
Kamu Kurumu Yükümlülükleri ve Asgari Gereksinimler

Kamu kurumu yükümlülükleri ve asgari gereksinimler

MADDE 4 – (1) Kamu kurumu, KamuNet'e ilişkin aşağıda yer alan asgari gereksinimleri karşılar ve kayıt altına alır:

a) KamuNet'e bağlantı yapacak birimlerini ve sistemlerini kapsayacak BGYS'sini kurar ve işletir,

b) Kurmuş olduğu BGYS için, TS ISO/IEC 27001 veya ISO/IEC 27001 standardına göre belgesini alır ve güncelliğini sağlar. Bu belgeleri, TS ISO/IEC 27001 veya ISO/IEC 27001 standardı kapsamında Türk Akreditasyon Kurumu tarafından akredite edilen belgelendirme kuruluşları veya Uluslararası Akreditasyon Forumu Karşılıklı Tanınma Antlaşmasında yer alan ulusal akreditasyon kurumlarınca akredite edilmiş belgelendirme kuruluşlarından temin eder,

c) Kurum yönetimi tarafından onaylanmış bilgi güvenliği yönetim sistemi politikasına uygun olarak KamuNet ile ilgili politika tanımlar, dokümante eder, ilgili çalışanlarının ve tarafların söz konusu politikaya ilişkin farkındalığını sağlar,

ç) Bilgi güvenliği ihtiyaçlarını karşılayacak şekilde bilgi varlıklarının gizlilik dereceleri sınıflandırılmasını Türk Standartları Enstitüsü tarafından Kritere Uygunluk Belgesi TSEK 523 Kriteri olarak yayınlanan Bilgi Varlıklarının Gizlilik Derecelerine Göre Sınıflandırılması Dokümanına uygun olarak yapar. Sınıflandırılan gizlilik derecelerine göre şifreleme tekniklerini kullanabilir,

d) KamuNet'e dâhil olan birimlerinde çalışan personeline yönelik BGYS ile birlikte siber güvenlikde dâhil olacak şekilde bilgilendirme ve eğitimler verir,

e) KamuNet'ten sorumlu bir ekip oluşturur. Bu ekibin iletişim bilgilerini Bakanlık ve İşletmeci ile paylaşır ve güncel tutar,

f) Sunucu ve istemci ağlarında internet üzerinden ve yerel ağ içerisinden düzenli zafiyet taramaları yapar, var olan zafiyetleri tespit ederek gerekli önlemleri alır,

g) KamuNet için kurum içi envanter ve topoloji oluşturur ve güncel tutar,

ğ) KamuNet'in bağlı olduğu sistemler üzerinde sızma/penetrasyon testleri gerçekleştirerek tespit edilen açıklıkların giderilmesi için çalışmalar yapar,

h) KamuNet'e bağlı sistemlere ait iz kayıtlarını herhangi bir anomaliye karşı sürekli olarak inceler,

ı) Sistem güvenliği için sunucu ve istemci ağlarını ayırır,

i) Sunucu ve istemci ağlarının birbirine erişiminde mutlaka bir güvenlik katmanı oluşturur,

j) KamuNet ağından gelebilecek tehditlere karşı kendilerini korumak ve KamuNet'e ilişkin bilgi sistemlerinde yer alan bilgilerin ve yazılımların gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması amacıyla (bilgisayar virüsleri, solucanlar, truva atları gibi zararlı yazılımlara ve benzeri) yazılımsal ve donanımsal önlemleri alır. Bu kapsamda güvenlik cihazları (güvenlik duvarı, saldırı önleme sistemi, içerik filtreleme, anti virüs veya birleşik tehdit yönetimi) kullanır,

k) İnternete açık servislerinin bulunması halinde bu servislerden gelen saldırıların KamuNet ağını da olumsuz etkilememesi için siber saldırılara (DDoS ve benzeri) karşı koruma ve güvenlik hizmetlerini alır,

l) İstemci ağı içerisinde dizin hizmetini kullanır ve kullanıcı bilgisayarlarını dizin hizmetine dâhil eder,

m) Dizin hizmeti üzerinde kullanıcı bilgisayarlarının KamuNet ağını olumsuz etkilememesi için işletim sistemi dâhil yüklü tüm programların güncellemelerini takip eder ve yapar,

n) KamuNet ağını olumsuz etkilememesi için dizin hizmeti üzerinde kullanılabilecek programları belirler ve kullanıcıların programlar üzerinde yetkisini (kurma, kaldırma) sınırlandırır,

o) KamuNet ağını olumsuz etkilememesi için Ağ Erişim Kontrolü (NAC-Network Access Controller) çözümleri ile

kullanıcıların yapılandırmasının güvenli olduğunu kontrol ederek kendi ağlarına dâhil eder,

ö) KamuNet ağında, bilmesi gereken prensibine göre sadece ilgili kurumlar ile veri paylaşır ve ilgisiz kurumların bilgiye erişimini kısıtlar,

p) KamuNet ağını olumsuz etkilememesi için kablosuz erişimi sağlayan modem veya erişim noktalarının yazılımlarını güncel tutar ve bu cihazların dizin hizmeti ile entegrasyonunu yapar,

r) Sunucuların bulunduğu sistem odalarını güncel ISO/IEC 27001 standardına uygun halegetirir, giriş ve çıkışları kontrol altında tutar ve bu konularda yetkilendirme yapar,

s) Sunuculardaki bilgi ve yazılımların kurtarılmasına imkân verecek şekilde yedek alınmasını sağlar,

ş) Sunucular üzerindeki kullanılmayan uygulamaları ve servisleri kapatır,

t) Sunucular üzerindeki işletim sistemleri ve uygulama yazılımlarını güncel tutar,

u) KamuNet'e bağlantı sağlayacak birimde görevlendirdiği çalışanlarıyla ve söz konusu birime ve ilgili sistemlere ilişkin mal veya hizmet alış verişinde bulunduğu üçüncü taraflarla yapacağı sözleşmelerde gizlilik hükümlerine yer verir ve imzalanan sözleşmeleri muhafaza eder,

ü) Kurumsal SOMEKurulum ve Yönetim Rehberine uygun şekilde Kurumsal SOME'sini kurar veulusal siber güvenliğin sağlanması amacıyla Bakanlık ve varsa bağlı olduğu Sektörel SOME'nin belirlediği esaslar çerçevesinde gerekli tedbirleri alır,

v) KamuNet'e ilişkin yapılan çalışmalarda Bakanlıkça hazırlanan Kurumsal SOME Kurulum veYönetim Rehberini esas alır,

y) İşletmeci ile arasındaki KamuNet ağı erişimini mümkünse farklı santrallerden ve farklı güzergâhlar ile yedekler.

ÜÇÜNCÜ BÖLÜM
Denetim ve Yükümlülükler

Bakanlığın yükümlülükleri

MADDE 5 – (1) Bakanlığın yükümlülükleri şunlardır:

a) KamuNet'e dâhil olacak kamu kurumlarını belirler,

b) KamuNet üzerindeki veri iletişiminin daha güvenli bir ortamda yapılabilmesini teminen gerekli hizmetleri ve çözümleri belirler,

c) KamuNet'e dâhil olmak isteyen kamu kurumlarını bu usul ve esaslar kapsamında uygunluk denetimini yapar veya yaptırır. Denetimin üçüncü tarafa yaptırılması durumunda gizlilik sözleşmesi imzalar,

ç) Uygunluk denetimi sonucunda asgari gereklilikleri sağlayan kamu kurumunun KamuNet'e dâhil olma sürecini başlatır. Asgari gereklilikleri sağlayamayan kamu kurumlarının, eksiklerini tamamlamalarına müteakip yeniden değerlendirme yapılır,

d) Periyodik denetim sürelerini belirler,

e) Periyodik denetimler sırasında tespit edilen eksikliklerini zamanında gidermeyen veya ağ güvenliğini tehdit eden durumlarda ilgili kamu kurumlarının KamuNet erişimini askıya alır veya çıkarır.

Denetlenen kamu kurumu ve işletmecinin yükümlülükleri

MADDE 6 – (1) Denetlenen kamu kurumu ve işletmeci:

a) Denetimle ilgili elverişli bir çalışma ortamı sağlar ve KamuNet'e ilişkin her türlü bilgi, belge ve yazılı açıklamayı belirlenen süre içerisinde verir,

b) Denetime ilişkin gerekli altyapıyı temin eder ve denetim süresince çalışır vaziyette bulundurur,

c) KamuNet'e ilişkin faaliyetler ve denetim süreci ile ilgili irtibat kurulabilecek personel bilgilerini Bakanlığa iletir,

ç) İşletmeci, KamuNet altyapısının kesintisiz, yedekli, fiziksel ve siber saldırılara karşı uluslararası standartlara uygun hizmet sürekliliğinin sağlanması için gerekli tedbirleri alır.

Denetim faaliyetleri

MADDE 7 – (1) Denetim faaliyetleri aşağıdaki maddeler kapsamında gerçekleştirilir:

a) Bakanlık tarafından belirlenen periyodik sürede KamuNet'e dâhil olan kamu kurumları ile işletmeci denetlenir veya denetlettirilir,

b) İşletmeci ve her bir kamu kurumu için denetim raporu hazırlanır,

c) Denetim raporunu ilgili kamu kurumu ve işletmeci ile paylaşır, varsa eksikliklerin süresi içerisinde tamamlanması istenir,

ç) Denetlenen kamu kurumundan ve işletmeciden denetim ile ilgili KamuNet'e ilişkin her türlü bilgi, belge ve yazılı açıklama istenir,

d) Denetlenen kamu kurumu ve işletmecinin yönetim ve yürütme işlerini aksatmayacak şekilde denetim gerçekleştirilir,

e) Denetim sürecinde edinilen bilgi ve belgelerin gizliliği sağlanır, gizli bilgiler, ticari sırlar ve benzeri bu konuda kanunen yetkili kılınanlardan başkasına açıklanamaz ve doğrudan veya dolaylı şekilde kendisi ya da üçüncü kişilerin yararına kullanılamaz,

f) Denetim ekibi gerekli teknik bilgiye ve mesleki yeterliliğe sahip en az üç personelden oluşur,

g) Denetim esnasında, KamuNet ağını ve ulusal siber güvenliği olumsuz yönde etkileyebilecek hususların tespit edilmesi durumunda bunların ivedilikle giderilmesi istenir.

DÖRDÜNCÜ BÖLÜM
Son Hükümler

Yürürlük

MADDE 8 – (1) Bu Tebliğin 4 üncü maddesinin birinci fıkrasının (a), (b) ve (c) bentlerine ilişkin hükümleri yayımı tarihinden iki yıl sonra, diğer hükümleri ise yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 9 – (1) Bu Tebliğ hükümlerini Ulaştırma, Denizcilik ve Haberleşme Bakanı yürütür.