

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURULU KARARI

Karar Tarihi : 08.02.2012
Karar No : 2012/DK-16/53
Gündem Konusu : Elektronik Bilgi Güvenliği AŞ'nin Denetimi.

KARAR :Sektörel Denetim Dairesi Başkanlığının hazırladığı 02/02/2012 tarihli ve B.11.6.BTK.0.16.663.05/8368 sayılı karar ve ekleri incelenmiştir.

5070 sayılı Elektronik İmza Kanununun 15'inci ve 18'inci maddeleri, Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin 11'inci, 13'üncü ve 14'üncü maddeleri, ETSI TS 101 456 standardı maddeleri, Bilgi Teknolojileri ve İletişim Kurumunun Denetim Çalışmalarına İlişkin Yönetmeliğin 10'uncu ve 11'inci maddeleri ve ilgili diğer mevzuata istinaden;

1) 5070 sayılı Elektronik İmza Kanunu'nun "Denetim" başlıklı 15'inci maddesinin ikinci fıkrasında "*Denetleme sırasında, denetleme yapmaya yetkili görevliler tarafından her türlü defter, belge ve kayıtların verilmesi, yönetim yerleri, binalar ve eklentilerine girme, yazılı ve sözlü bilgi alma, örnek alma ve işlem ve hesapları denetleme isteminin elektronik sertifika hizmet sağlayıcıları ve ilgililer tarafından yerine getirilmesi zorunludur.*" hükmü yer almaktadır. Denetim sırasında denetçiler tarafından istenen 2010 yılı öncesi kayıtları da dâhil olmak üzere tüm sertifika kayıtlarını, 2010 yılı öncesinde yapılan işlemlere ilişkin logları ve 2007 yılından itibaren kullanılmayan gizli anahtar kopyalarının kullanım dışı bırakılmasına ya da imha edilmesine ilişkin kayıtları paylaşmakta gerekli özeni göstermediği tespit edilen e-Güven AŞ hakkında 5070 sayılı Kanun'un 18'inci maddesinin birinci fıkrasının (e) bendinde yer alan "*Bu Kanunun; e) 15 inci maddesi hükümlerine aykırı hareket eden elektronik sertifika hizmet sağlayıcısına otuzbin Türk Lirasından ellibin Türk Lirasına kadar idarî para cezası Telekomünikasyon Kurulu tarafından verilir.*" hükmü çerçevesinde 30.000 (otuz bin) Türk Lirası idarî para cezası uygulanması,

2) Yukarıda belirtilen idari para cezası tutarının yanında, tedbir niteliğinde olmak üzere e-Güven AŞ tarafından:

a) Bir felaket durumunda, ESHS'nin faaliyetlerine devam edebilmesi için alternatif güvenli bir sistem altyapısının 2012 yılı içerisinde kurulabilmesi için gerekli tedbirlerin alınarak iş planının oluşturulup Kuruma gönderilmesi ve söz konusu alternatif güvenli sistem altyapısının kurulmasını müteakip Kurumun bilgilendirilmesi,

b) Zaman Damgası Sunucusunda tutulan kayıtların bütünlüğünün ve gizliliğinin korunması ve olay bilgilerinin silinmeyecek veya tahrif edilmeyecek şekilde loglanması,

c) Tüm sunucuların UTC ile senkronizasyonunun güncel tutulması ve kontrol edilmesi,

ç) Sertifikalar kullanılarak giriş yapılan sistemlerde iptal işlemleri de dâhil olmak üzere tüm işlemlerin kim tarafından yapıldığının tespitini sağlayacak altyapının kurulması,

d) Kullanıcı sertifikalarının oluşturulmasına ve iptaline ilişkin işlemlerin güvenilir rolde bulunan en az iki kişinin gözetiminde yapılması,

e) HSM erişim kartlarının ve yedeklerinin tutulduğu kasa içerisinde bulunan operatör kartlarının güvenlik seviyesinin artırılması,

f) TSE ISO/IEC 27001 standardının A.7.2.2 maddesi uyarınca bilgi sınıflandırma şemasının oluşturulması, veri etiketleme/veri işleme için gerekli süreçlerin tanımlanması ve dokümantasyon değişikliklerinin gerçekleştirilmesi,

g) TSE ISO/IEC 27001 standardının A.9.2.1 maddesi uyarınca ESHS'nin faaliyetlerinde kullanılan teçhizatın fiziksel güvenliğinin de sağlanması,

ğ) TSE ISO/IEC 27001 standardının A.10.5.1 maddesi ve CWA 14167–1 5.1.8 [BK1.1] maddesi uyarınca verilerin ve yazılımların yedeklerinin yedekleme ilkelerine göre düzenli bir şekilde tutulması ve geri dönüş işlemlerinin kontrol edilmesi,

h) Taşınabilir medya araçlarının yönetimine ilişkin süreçlerin belirlenmesi ve risk yönetimi kapsamında kullanılmasına ilişkin düzenleyici faaliyetlerin gerçekleştirilmesi,

ı) ESHS uygulamalarında ve sistemlerde işlem yapan kişinin kimliğinin açıkça belirlenebilmesini teminen işletmenler, yöneticiler ve sisteme doğrudan erişim hakkı bulunan kullanıcılar için etkin bir kullanıcı erişim yönetiminin oluşturulması,

i) Kritik uygulamalarda başarısız kimlik doğrulama girişim sayısının kontrol edilebilmesini teminen başarısız kimlik doğrulama girişim sayısının izin verilen doğrulama girişimlerini aşması halinde güvenli sistem altyapısının bu girişimleri önlemesi,

j) ESHS alt kök sertifikalarının iptaline ilişkin işlemlerin güvenilir rolde bulunan en az iki kişinin gözetiminde yapılması,

k) *“Nitelikli elektronik sertifikanın iptaline ilişkin talepler; ESHS, sertifika sahibi ve sözleşme ile belirlenen kişiler tarafından yapılabilir. ESHS; bu duruma ilişkin taleplerin yapılabilmesini, asgari olarak telefonla ve kesintisiz sağlar. ESHS nitelikli elektronik sertifika sahibini söz konusu durum hakkında bilgilendirir”* hükmünü amir Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin “Nitelikli Elektronik Sertifikanın İptal Edilmesi” başlıklı 13'üncü maddesi kapsamında, iptal edilen veya askıya alınan sertifikanın değişen durum bilgisine ilişkin olarak sertifika sahibinin bilgilendirilmesi için gerekli tedbirlerin alınması,

l) *“ESHS, sertifika sahibinin onayını almak kaydıyla nitelikli elektronik sertifikayı kamuya açık bir dizinde yayımlar. ESHS, dizin hizmetinin kesintisiz olarak verilmesini sağlar.”* hükmünü amir Elektronik İmza Kanununun Uygulanmasına İlişkin Usul ve Esaslar Hakkında Yönetmeliğin “Nitelikli Elektronik Sertifikanın Yayımlanması” başlıklı 11'inci maddesi kapsamında kullanıcıların geçerli sertifikaları içinde bulunduran elektronik depo hizmetine tam ve kesintisiz bir şekilde erişimlerinin sağlanması,

m) Sertifika başvuru formlarının imzalanmasına gerekli özenin gösterilmesi,

n) ESHS'nin iç ağ alanlarını üçüncü kişilerin erişimine açık olan dış ağ alanlarına karşı korumak üzere gerekli kontrollerin yapılabilmesi için 3. katmanda yer alan bilgisayarın erişimlerine azami dikkat edilmesi,

o) ETSI TS 101 456 standardının 7.4.6 (d) maddesi uyarınca yardımcı programların kullanımının sınırlandırılabilmesi için ilgili prosedürlerde yer verilen hususların titizlikle uygulanması,

ö) BGYS'nin işletilmesine ve dosyalama sistemine gerekli özenin gösterilmesi

iin gerekli tedbirlerin mmkn olan en kısa sre iinde alınmak suretiyle yukarıda belirtilen tedbirlere iliřkin bilgi ve belgelerin iřbu Kurul Kararının e-Gven Ař'ye teblięini mteakip 60 gn ierisinde Kuruma iletilmesi hususlarına karar verilmiřtir.