TÜRKİYE BİLİŞİM DERNEĞİ

2019/12 SAYILI CUMHURBAŞKANLIĞI BİLGİ VE İLETİŞİM GÜVENLİĞİ TEDBİRLERİ GENELGESİ SEKTÖR GERİBİLDİRİM RAPORU

16 EYLÜL 2019, ANKARA

Türkiye Bilişim Derneği
2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Sektör Geribildirim Raporu

Yayımcı Adı

TÜRKİYE BİLİŞİM DERNEĞİ (TBD)

Tel :+90 312 473 82 15 (pbx)
Faks :+90 312 473 82 16
Web : www.tbd.org.tr
e-posta : tbd-merkez@tbd.org.tr
Adres : Ceyhun Atuf Kansu Caddesi
1246 Sokak No:4/17 Balgat / ANKARA

Yayın Tarihi

16 Eylül 2019, Ankara

Yayın Sürümü

Sürüm 1.0

Editörler

Seçkin GÜRLER — TBD İcra Kurulu Üyesi, Siber Güvenlik Odak Eksen Başkanı – LABRİS Networks

Mehmet ÇAKIR — TBD İcra Kurulu Üyesi – BEAM Teknoloji

Barış ERDOĞAN — TBD İcra Kurulu Üyesi

TBD Yayın Numarası : 2019/10-1

Bilişim teknikbilimini ulusal bir kalkınma aracı olarak kullanacağız.

Prof. Dr. Aydın Köksal, 1968

TBD Kurucusu ve Onursal Başkanı

RAPORA KATKI SAĞLAYANLAR

İCRA KURULU SİBER GÜVENLİK ODAK EKSENİ ADINA

Seçkin GÜRLER	TBD İcra Kurulu Üyesi, Siber Güvenlik Odak Eksen Başkanı – LABRİS Networks
Mehmet ÇAKIR	TBD İcra Kurulu Üyesi – BEAM Teknoloji
Barış ERDOĞAN	TBD İcra Kurulu Üyesi

Çalıştay Teknik Alt Kurulu

Ahmet PEKEL	TBD
Güher KAYALI	Oracle
Kâzım BOZKURT	İnnovera
Serkan ÇINAR	Türk Telekom Regülasyon
Volkan EVRİN	Linux Kullanıcıları Derneği

Çalıştay Katılımcıları

Ahmet ATAY	Microsoft
Akif TEMUR	Türk Telekom Teknoloji
Aşkın TOKYAY	Türk Telekom Regülasyon
Aydın KOLAT	*TBD İCRA KURULU BAŞKANI – VERİSİS*
Burhanettin AL	TBD İcra Kurulu Üyesi – TURKCELL
Cem KIŞLA	Solitera Teknoloji
Cem ŞATANA	TBD İcra Kurulu Üyesi – Oracle
Ceyda SÜER	TBD Yönetim Kurulu Üyesi – Vodafone
Dilek KARAKAYA	TBD İcra Kurulu Üyesi – Sağlık Bakanlığı
Eren YILDIZ	Solitera Teknoloji
Fatma ERTÜRK	Safe-Tech

Furkan CİVELEK	Cumhurbaşkanlığı SBB
Gökhan ERZURUMLUOĞLU	TBD İcra Kurulu Üyesi – ISSD
Hakan GÜVEN	Oracle
Hande BAYRAK	Türk Telekom Regülasyon
Hanifi Burak YAMAN	Türk Telekom Siber Güvenlik
Koray ÇAKIR	ODTÜ Teknokent
Mahmut BALKİ	Türk Telekom Teknoloji
Mehmet Ali ORTAYATIRTMACI	TÜRKSAT
Mustafa YILMAZ	TR-TEST
Onur ARMUTCUOĞLU	YD Yazılım
Osman MURAT	Türk Telekom Teknoloji
Sinan ŞENOL	Aselsan
Suat YAMAÇ	Devlet Malzeme Ofisi
Tevfik ÖZHAN	Vodafone
Tahsin TÜRKDOĞAN	Türk Telekom Teknoloji

İsim sırası kullanılmıştır.

İÇİNDEKİLER

AMAÇ VE YÖNTEM

Cumhurbaşkanlığı 6.7.2019 tarihli "Bilgi ve İletişim Güvenliği Tedbirleri" genelgesinin yayınlanması sonrasında uygulamada oluşabilecek olası sorunların tespiti ve bunların giderilmesine yönelik çözüm önerilerinin Türkiye Bilişim Derneği (TBD) tarafından hazırlanarak Cumhurbaşkanlığı Dijital Dönüşüm Ofisi'ne (DDO) sunulması kararlaştırılmıştır.

TBD olarak, sektörün söz konusu genelge ile ilgili doğru bir resim ortaya koyabilmesi ve yine aynı genelge ile tarif edilen "Bilgi ve İletişim Güvenliği Rehberi"nin doğru temeller üzerinde oluşturulabilmesi için TBD İcra Kurulu Siber Güvenlik Odak Ekseni koordinasyonunda

- 3 çalıştay öncesi toplantı
- 1 çalıştay (33 kişi ile)
- 1 çalıştay sonrası teknik kurul toplantısı (10 kişi ile)

ile sektör temsilcileri bir araya gelmiş, yazılı ve sözlü geribildirimleri ile sektör görüşünü ekteki belgelerle 16.09.2019 tarihinde sonuçlandırmıştır.

Sektör görüşünü oluşturmak için Operatörler, Yabancı Üreticiler, Yerli Üreticiler, Entegratörler, Siber Güvenlik Danışmanları, Kamu Kurumları, Teknokentler, Üniversiteler, Kümelenmeler, Kamu Test Merkezi'nden oluşan geniş bir katılımcı kitlesi sürece dahil edilmiştir.

Çalışma hazırlanırken odağımız genelgenin güncellenmesi değil, DDO tarafından ortaya konulan insiyatifin, sektör tarafından nasıl sahiplenilebileceği olmuştur. Bu raporda değinilmesi gereken ek başlıklar ve yer verilmesi gereken tanımlara da işaret edilmiştir.

KISALTMALAR

Çalıştay 27.08.2019 Tarihinde TBD koordinasyonunda sektör temsilcilerinin katılımıyla gerçekleştirilen Operatörler, Yabancı Üreticiler, Yerli Üreticiler, Entegratörler, Siber Güvenlik Danışmanları, Kamu Kurumları, Teknokentler, Üniversiteler, Kümelenmeler, Kamu Test Merkezinin temsil edildiği "2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi Geribildirim Çalıştayı"dır.

Genelge 2019/12 Sayılı Cumhurbaşkanlığı Bilgi ve İletişim Güvenliği Tedbirleri Genelgesi

KVKK Kişisel Verilerin Koruması Kanunu

DDO Cumhurbaşkanlığı Dijital Dönüşüm Ofisi

SSS Sıkça Sorulan Sorular

REHBER ÖNCESİ

DDO tarafından hazırlanacak Sıkça Sorulan Sorular(SSS) Belgesi bazı alanları netleştirecek olsa da, temel ve teknik konuların ayrıntılı bir şemada ele alınması gereği göz önünde bulundurularak rehberin gerekiyorsa bölüm bölüm hızla yayınlanması önemli görülmektedir.

KVKK nın hazırladığı Rehber, SSS çalışmaları sektör tarafından beğenilmektedir. Sektör pratiklerinin ve standartlarının oturması açısından benzer bir formatta ilerlenebilir.
https://www.kvkk.gov.tr/Icerik/2030/Rehberler
https://www.kvkk.gov.tr/Icerik/5383/Diger-Dokumanlar

Rehber izlenebilir adımlardan oluşmalı, yalın olmalı herkes tarafından aynı şekilde anlaşılmalıdır, örneklerle pekiştirilmelidir.

TANIMLAR

VERİ GİZLİLİK DERECELERİ TANIMLARI

Detaylandırma Gereği:

Genelgede kullanılan veri tanımları ekli Çalıştay sunumunda renklendirilmiştir. Kullanılan tanımlar arasında "veri", "kritik bilgi", "kritik veri", "gizlilik dereceli veri", "kurumsal mahremiyet içeren veri", "kritik kurumların bulunduğu bölgelerdeki veri" gibi veri türlerinden bahsedilmektedir.

Rehber Önerisi:

Bu alanın referansının üzerinde çalışmaların devam ettiği Ulusal Veri Sözlüğü olması beklenmektedir. Konu üzerinde TBD İcra Kurulu'nda bir odak eksen oluşturulmuş ve DDO ile ortak hareket etmek için çalışmalarda eşgüdüm beklenmektedir.

Ulusal Veri Sözlüğünü beklemeden Türkiye'de yürürlükteki mevzuatla uyumlu bir "Veri Gizlilik Derecelerinin Sınıflandırılması"nın Rehber Veri Tanımları bölümünde yapılması beklenmektedir.

- Verilerin Saklanması başlığı altında detaylandırıldığı gibi Genelge'yle alınacak önlemler, bir matrisin hücreleri üzerinden uygulanabilir gözükmektedir. Matrisin satırlarında "Veri Gizlilik Dereceleri", kolonlarında "Kurum Gizlilik Dereceleri"nin olması beklenmektedir.

Referans Bilgi ve Belgeler:

- Veri tanımlarının yeniden yapılması yerine mevcut mevzuatlar öncelikli ele alınmalıdır.

- Bilgi ve belge sınıflandırma ile ilgili dikkat edilecek hususlar eski Bakanlar Kurulu kararlarında yer alırken yeni kararda bulunmamaktadır. Veri ve Belgelerin gizlilik derecelerinin işaretlenmesi ile ilgili hususlar yeniden ele alınmalı ve mevzuatla sabitlenmelidir.

KURUM VE KURULUŞ GİZLİLİK DERECELERİ TANIMLARI

Detaylandırma Gereği:

Genelgede kullanılan kurum/kuruluş tanımları ekli Çalıştay sunumunda renklendirilmiştir. Kullanılan tanımlar arasında "kritik kurum", "stratejik önemi haiz kurum" gibi kamu kurum türlerinden bahsedilmektedir.

Rehber Önerisi:

Kamu Kurum ve Kuruluşları Tanımları bölümünde

- Kurum Gizlilik Derecelerinin Sınıflandırılması

- Kurum Merkez ve Uçlarının Sınıflandırılmasında farklılık varsa belirtilmesi

Referans Bilgi ve Belgeler:

DETSİS sisteminde kamu kurum ve bağlı teşkilatının kayıtları yapılırken aynı zamanda her bir birime gizlilik derecesi de atanması uygulama yöntemi olarak belirlenebilir.

KURUMSAL/KİŞİSEL TANIMLARI

Detaylandırma Gereği:

Genelgede kullanılan kurumsallık tanımları ekli Çalıştay sunumunda renklendirilmiştir. Kullanılan tanımlar arasında "kurumsal", "şahsi", "kişisel", "kurumsal olmayan" gibi uygulama hesapları ve eşya türlerinden bahsedilmektedir.

YERLİ VE MİLLİ TANIMLARI

Detaylandırma Gereği:

Genelgede geçen ve rehberde de büyük ağırlıkla ele alınacağını düşündüğümüz, yerli ve milli olma tanımlarının net olarak yapılması uygulamadaki karışıklıkların önüne geçecektir.

Rehber Önerisi:

Bazı Genelge maddeleri için yerli ve milli olmaktan kasıtlar net değildir. İlgili maddelerde konu hakkında detay verilmiştir.

Referans Bilgi ve Belgeler:

Yerli İşletme ve Kuruluş: ...

Milli İşletme ve Kuruluş: ...

YERLİ ÜRÜN VE MİLLİ ÜRÜN TANIMLARI

Detaylandırma Gereği:

Genelgede geçen ve rehberde de büyük ağırlıkla ele alınacağını düşündüğümüz yerli ve milli ürün tanımlarının net olarak yapılması uygulamadaki karışıklıkların önüne geçecektir.

Rehber Önerisi:

TBD'nin bu konudaki raporu sürüm 1.0 olarak 2018 yılı sonunda yayınlanmıştır. Rehberde bu tanımlar yapılırken, daha önceki çalışmaların ışığında TBD olarak destek olmak isteriz. TBD çatısı altında bu konuda sürekli bir çalışma grubu bulunmaktadır.

Referans Bilgi ve Belgeler:

"TBD YERLİ ve MİLLİ YAZILIM ENDÜSTRİSİ RAPORU (Sürüm 1.0)

https://www.tbd.org.tr/wp-content/uploads/2019/03/TBD_YERLI_MILLI_YAZILIM_ENDUSTRISI_RAPORU_SURUM1_01.pdf

Yerli Ürün (Sayfa 11) : Yerli ürün temelde yerli malı belgesine sahip olan ürün olarak tanımlanmaktadır. Yerli malı belgesi 4734 Sayılı Kamu Iħale Yasasının 63. Maddesinde yerli malı belirlenmesine ilişkin usul ve esasların "Bilim, Sanayi ve Teknoloji Bakanlığı" tarafından ilgili kurum ....(devamı raporda)

Milli Ürün (Sayfa 12) : Millî ürün kavramı incelenirken temelde fikrî ve sınai hakların durumunun göz önünde bulundurulması gerekmektedir. Kısaca millî ürün tüm fikri ve sınai hak sahiplerinin yabancı uyruklu gerçek veya tüzel kişide bulunmadığı ürünler

olarak ifade edilebilir. Yani millîlik kavramı, tasarım aşamasından başlayarak teknoloji geliştirme de dahil tüm üretim döngüsü içinde hak iddia edebileceklerin Türkiye'deki gerçek ve tüzel kişiler olması gerekliliğini ifade eder....(devamı raporda)"

KAMU KURULUŞU, KRİTİK KURUMLAR, KRİTİK ALTYAPI NİTELİĞİNDE HİZMET VEREN İŞLETMELER TANIMLARI

Detaylandırma Gereği:

Genelgenin kapsamında bahsi geçen "kritik kurumlar" ve "kamu kuruluşları" tanımlarında ve Kritik Altyapı niteliğinde olan işletmeler konusunda netlik gerekmektedir.

Rehber Önerisi:

Genel Kullanımda

"Kamu Kurum"ları, DETSİS sisteminde kayıtlı kamu kurum ve teşkilatlar,

"Kamu Kuruluşları" hisselerinin en az yarısı devlete ait olan ve kamu hizmeti yürüten her türlü şirket ve teşebbüsler

"Kritik Altyapı Niteliğinde Hizmet Veren İşletmeler" kamu olmayan ama kamuyu etkileyen kritik konumları nedeniyle kamunun özel denetimine tabi olan kurumlar (finans, ulaşım, enerji üretim, işletmeciler, veri merkezleri,..)

- Genelge ile sadece Kamu Kurum ve Kuruluşlarının mı ele alınmak istendiği yoksa belirlenecek düzenleyici kurumlar (Ör: BTK, BDDK, EPDK,..) tarafından denetlenen özel ve kamu-özel ortaklığı ile kurulan iştirakleri de kapsayıp kapsamadığı netleştirilmelidir. Kritik Altyapı Niteliğinde Hizmet Veren İşletmelerin de genelge kapsamına girdiği düşünülüyorsa ilgili işletmeler Ulusal Siber Güvenlik Stratejisi (2016-2019)'nde tanımlanmıştır.

- Kamu kuruluşu veya kritik altyapı niteliğinde hizmet veren işletmeler kapsamında olup, diğer kamu kurumlarının verilerini ve trafiklerini ağlarında barındıran kurumlar için, veri veya trafiği üreten kamu kurumunun sorumluk sınırları net olarak çizilmelidir. Veri veya trafiği üreten kamu kurumunun sorumluluğunu yerine getirmemesi halinde, bu veri ve trafikleri barındıran kamu kuruluşu ve kritik kurumların bir sorumluluğu bulunup bulunmadığı netleşmelidir. (Ör: Türk Telekom)

Referans Bilgi ve Belgeler:

Kritik Altyapı Niteliğinde Hizmet Veren İşletmeler (Ulusal Siber Güvenlik Stratejisi (2016-2019))

REHBER BAŞLIKLARI:

GİRİŞ

GENELGEYE NEDEN İHTİYAÇ DUYULDUĞU

Genelge Metni: Bilginin dijital (sayısal) ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla aşağıdaki tedbirlerin alınması uygun görülmüştür.

GENELGENİN KANUNİ DAYANAKLARI

Detaylandırma Gereği:

Metnin bir Genelge olarak hazırlanması ve hukuki yaptırımlarının ve kanuni dayanaklarının muğlak kalması, Genelge mevzuat uyumunun sağlanması

Rehber Önerisi:

Raporda değinilen İlgili madde ve tanımlarda mevzuat ilişkilerine de yer verilmektedir.

BÜTÇE VE ÖNCELİKLENDİRME

Detaylandırma Gereği:

Birçok kurumda bütçe kısıtlamaları olmakta, özellikle güvenlik bütçeleri sadece güncellemelere yetmektedir. Rehbere yazılacak maddelerle birlikte dönüşüm süreleri ve gerekecek bütçelerle ilgili önceliklendirme yönlendirmesinin yapılması beklenmektedir. DDO'nun önceliklendirmeyi ve kaynak planlamasını doğru yapması ve az olan kaynakları öncelikli yönlendirmesi bekleniyor.

Rehber Önerisi:

Getirilecek bazı uygulama kuralların (bir ürünün ulusal ya da uluslararası bir kalite belgesine sahip olması gibi) girişimcilerimizin pazara girişini zorlaştıracağı, özellikle yerli-milli ürünlere geçiş sürecinde Girişimcilik Ekosistemi ile bir araya gelinerek bir yol haritası oluşturulması gerekmektedir.

KAMUNUN UYGULAMADA KARŞILAŞACAĞI SORUNLAR

Detaylandırma Gereği:

Soru işareti olan durumlarda başvurulacak kişiler ve başvuru yönteminin belirlenmesi

Rehber Önerisi:

Rehberin sürekli danışma gereksinimi duyulmayacak açıklıkta yazılacağını öngörüyoruz. Ek olarak DDO tarafından bir destek hattının tahsisi bir yöntem olarak uygulanabilir, bu destek hizmetine yeterli uzman atanamayacağı düşünülerek L1 ve L2 kurgulanması gerekebilir.

GENELGEYE UYGUN SATINALMA

Detaylandırma Gereği:

Satınalma sürecinde Genelge, Rehber ve bağlı SSS dokümanların yatırımdan imtina edilmeyecek şekilde açık ve yönlendirici olması gereği

Rehber Önerisi:

- Rehberde, Genelgeyle birlikte gelen şartlara uygun bir satınalma örneğine ve kontrol listesine yer verilebilir.

- Daha ileri bir uygulama olarak satın alınabilecek ürünlerin listesi katalog olarak düzenlenebilir. Bu katalogda yer alan üreticilerden ve ürünlerin hizmetini verecek kuruluşlardan Genelge'nin gereklerine dikkat etmeleri beklenebilir. Bu anlamda kamunun merkezi satınalma birimi olan DMO'nun, SSB Siber küme ve Tübitak gibi yerli üretimi destekleyen kümelenme ve kurumlarla işbirliği içinde yürüttüğü Teknokatalog

çalışması önemlidir. Belirlenecek yol haritasında kurumların Teknokatalog'la ilişkilendiirlmesi değerlendirilmelidir.

- DMO nun kataloğa girecek yerli ve yabancı ürünlere uyguladığı kıstaslar üzerinde çalışılmalıdır. Genel açıdan doğru olan kıstaslar, Teknokatalog gibi özel amaçlı kataloglarda değiştirilmeden uygulanmaya çalışıldığında, kataloğa giriş ve sürdürülebilirlik aşamalarında ciddi zorluklar yaşanmaktadır.

MİLLİ ÜRETİCİLERİN GENELGEYE UYUMU İÇİN TEŞVİKLER

Detaylandırma Gereği:

Genelgenin yürürlükte olması ve halen kamu kurum ve kuruluşlarını bağlaması, yerli ve milli tanımı içinde yüklenen görevlerin yerine getirilebilmesinde görev alabilecek kurum, girişim ve fonların hızlı hareket etmesini gerektirmektedir.

Rehber Önerisi:

- Genelgenin çıkması ile milli üreticilere ve hizmet sağlayıcılara büyük fırsatlar sunulmakta ve sorumluluklar yüklenmektedir. Hızlı adaptasyon için ürünü olan üreticilere ve sürece katkısı olacak hizmet sağlayıcılara sonuca yönelik teşvikler verilmesi planlanmalıdır.

- En iyi teşfiğin yeni müşteri ve gerçek trafik/sistemler üzerinde, kanun koyucu yönlendirmesinde çalışmak olduğu göz önünde tutulmalıdır.

- İthal ürünlerin, yerli üreticilerle rekabette piyasanın çok altında fiyat vermeleri veya ana yükleyiciler eliyle çok yüksek fiyatlara tedarik edilmeleri işlemleri incelenebilmelidir. Hayatın doğal akışına uymayan satınalmalar ulusal güvenlik ve piyasa koruma gerekçeleriyle mercek altına alınabilmelidir.

- Getirilen kuralların sonuçları olarak yerli ve milli ürünlerin özendirilmesi, Girişimcilik ve yatırım politikalarının bu Genelge'nin parçası olan Rehber'le şekillenmesi beklenmektedir.

KAMU VERİLERİNİN ANONİMLEŞTİRİLEREK ERİŞİLEBİLİR VE İŞLENEBİLİR BIR NOKTADA TOPLANMASI

Rehber Önerisi:

- Uygun koşullarda erişilebilir ve işlenebilir "Anonimleştirilmiş Türkiye Büyük Verisi"ne, Türkiye Endeksi çalışmaları, Yapay Zeka çalışmaları ve birçok konuda ihtiyaç duyulmaktadır. Rehber ile verinin kurumlarca nasıl anonimleştirileceği ve DDO kontrolünde nasıl merkezileştirileceği noktaları açıklanabilir. Genelge'nin güncellenmesi sırasında bu konuda bir madde Genelge'ye eklenebilir.

- Türkiye Endeksi, Kamu Veri Stratejisi, Ulusal Yapay Zeka Stratejisi konularında TBD İcra Kurulu'nda ayrı ayrı odak eksenler oluşturulmuş ve DDO ile ortak hareket etmek için çalışmalarda eş güdüm beklenmektedir.

GERİBİLDİRİM VE SORUNLU UYGULAMA BİLDİRİM YOLLARI

Detaylandırma Gereği:

Genelgenin uygulanmasındaki sorunların DDO ya iletilmesi ve Genelgenin sektör ve ilgili STK'lar tarafından sahiplenilmesi

Rehber Önerisi:

Genelgenin uygulanmasında en önemli takip mekanizması yine sektör ve ilgili STK'lar olacaktır. Uygulama ve satınalma sorunlarını şeffaflıkla dinleyecek ve sebeplerini sorgulayacak bir geribildirim mekanizmasının oluşması sektörün ve ilgili STK'ların, Genelge'nin açtığı yolu sahiplenmesini sağlayacaktır. Uygulama geribildirimleriyle ilgili Rehber'de bir bölümün bulunmasını önemli görüyoruz.

BİLGİ VE VERİLERİN SAKLANMASI

GENEL

DETAYLANDIRMA GEREĞİ:

Güvenli Veri Depolama Standardı'nın belirlenmesi: Kamu kurumları verilerinin depolama standardının tüm gizlilik dereceli veriler ve kurum/kuruluşlar için belirlenmesi gerekiyor.

REHBER ÖNERİSİ:

- Tanımlar bölümünde belirlenecek "Veri Tanımları" ve "Kurum ve Kuruluş Tanımları" bir matris oluşturmaktadır. Gizli bir verinin, kritik bir kurumda depolanması ile Çok Gizli bir verinin kritik olmayan bir kurumda depolanması arasında güvenlik yaklaşımı farkları oluşacaktır. Tanımlar belli olduktan sonra Matrisin her hücresi için ayrı bir veri depolama standardı belirlemek doğru olacaktır. Matris kurumsal veriler için tanımlanmalıdır, şahsi veriler matris dışında tutularak değerlendirilmelidir. Kurumsal ve şahsi tanımları yine tanımlar bölümünde yapılmalıdır.

- Bu sınıflandırma, dijital veri sınıflandırma uygulamaları ile desteklenmeli ve veri sahibi tarafından belirlenen veri sınıfının dijital veri ile kalıcı şekilde yaşaması, kontrolsüz değiştirilmemesi sağlanmalıdır.

- Depolanan verilerin gizliliği sağlanırken, kullanılacak kripto anahtarları ve algoritmaları tanımlanmalıdır.

- Bazı veri tipleri için saklama koşulları KVKK Kanunu, 5651 kanunu, USOM, Ulaştırma Bakanlığı ve benzeri mevzuatlarda yer almaktadır. Bu Genelge ve bağlı rehberin hazırlanmasında mevcut bu kanunlarda tanımlanan ve çerçevesi çizilen uygulamalarla uyum sağlanmalı, gereken noktalar bir ileriki safha olarak rehberde tanımlanmalıdır.

- Veri ve kurum sınıflandırmasına göre saklama süreleri tanımlanmalıdır. Verilerin saklandığı, yedeklendiği ve en üst felaket anında bu yedeklerden geri dönülebildiği merkezi bir kontrole tabi olmalıdır.

- Verilerin tanımı dahilinde yerli üretici ve kurumların yapay zeka ve uygulama geliştirme çalışmalarında kullanabilecekleri anonimleştirilmiş verinin tanımı ve paylaşılabilir anonim verilerle ilgili yetki ve onay mekanizmaları tanımlanmalıdır.

- Bu başlıkta finans sektöründe uygulandığı gibi saldırı anında kurum trafiklerini yurtdışı veri merkezlerine yönlendirme temelli çözümlere karşı önlem alınması

gerekmektedir. Rehberde konunun netleştirilmesini önemli görüyoruz. Ör: L4 DDoS saldırılarında yurtdışıyla bağlantılı verilen hizmetler.

- Kamudaki verilere verilen önemle ilişkili olarak halen Ulaştırma Bakanlığı tarafından yürütülen Kamu Veri Merkezi projesinin durumu ve kamunun yol haritası üzerine yönlendirmeler rehberde yer almalıdır. Kamu veri merkezinin oluşmasında ve işletilmesinde DDO yönlendirici olmalıdır.

REFERANS BİLGİ ve BELGELER:

- 6698 sayılı Kişisel Verilerin Korunması Hakkındaki Kanun ile "Kimliği belirli veya belirlenebilir gerçek kişiye ilişkin her türlü bilgi" kişisel veri olarak tanımlanırken; "Kişilerin ırkı, etnik kökeni, siyasi düşüncesi, felsefi inancı, dini, mezhebi veya diğer inançları, kılık ve kıyafeti, dernek, vakıf ya da sendika üyeliği, sağlığı, cinsel hayatı, ceza mahkûmiyeti ve güvenlik tedbirleriyle ilgili verileri ile biyometrik ve genetik veriler" özel nitelikli kişisel veri olarak belirlenmiştir. Devam eden süreçte Kurul tarafından yayımlanan "Özel Nitelikli Kişisel Verilerin İşlenmesinde Veri Sorumlularınca Alınması Gereken Yeterli Önlemler ile ilgili Kişisel Verileri Koruma Kurulunun 31/01/2018 Tarihli ve 2018/10 Sayılı Karar" kapsamında özel nitelikli veriler açısından daha detaylı ve ağırlaştırılmış tedbirler belirlenmiştir.

- 5809 sayılı Elektronik Haberleşme Kanunu ve bu kanunla ilişkili veri saklama ve veri sınıflandırmaya ilişkin yönetmelikler bulunmaktadır.

- BTK e-SIM verilerinin depolanması kararı Madde2
https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf

GENELGE MADDE NO:1

Madde: Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.

DETAYLANDIRMA GEREĞİ:

Tanımlanan veriler, KVKK da belirtilen "Özel Nitelikli Kişisel Veri" tanımına uymaktadır. Daha dar bir tanımın yapılm

asının bir kargaşaya yol açabileceği düşünülmektedir.

REHBER ÖNERİSİ:

- KVKK web sayfalarında detaylı rehber ve klavuzları bulunan kanuna atıf yapılarak netleştirilebilir.

- "Yurtiçinde " tanımında kastedilenin yerli ve milli boyutu netleştirilmelidir. (madde 3 te yaptığımız açıklamalar ışığında aydınlatılatılabilir.)

- 2018/10 sayılı genelgede özel nitelikli kişisel veriler elektronik ortamda tutuluyor ise şifrelenmesi istenmektedir. Özellikle bu tür verileri yoğun olarak işlemesi gereken büyük veritabanlarına sahip kurumlarda, bilhassa VTYS'lerde saklanan bu tarzda verilerin şifreli olarak tutturulması ciddi sorunları da beraberinde getirmekte ve perfomans sıkıntıları ve lisans maliyetleri nedeniyle pratikte bunu gerçekleştirme imkânı olmayabilmektedir. Bu bakışla konunun ele alınması ve rehberde ayrıntılı yol gösterilmesi beklenmektedir. Yeni oluşturulacak sistemlerde konu ele alınabilecekken, eski sistemlerde dönüşümü planlamakta zorlanılmaktadır.

- Madde "Güvenli" tanımı için Genel bölümünde ifade ettiğimiz matris içinde bu veriler tanımlanarak güvenlik seviyesi netleştirilmelidir. Maddede tarif edilen "Özel Nitelikli Kişisel Veriler" le ilgili özel yöntem ve teknik uygulanacaksa rehberde tanımlanmalıdır.

- "Güvenli saklama yöntemi" ifadesi, verilerin disk, klasör ya da dosya bazında şifreli, erişim yetkileri tanımlanmış, erişim işlemleri kayıt altında olan saklama yöntemi olarak detaylandırılmalıdır.

- Özel Nitelikli Kişisel Veriler dahil olmak üzere bazı veriler, verilerin sahiplerine de maskelenmelidir. Kurum çalışanı veya yöneticisi olmak bu verilere erişim için yeterli olmamalıdır.

- Özel Nitelikli Kişisel verileri yurtdışına çıkarmak için kişi onayı yeterli olurken, genelgeyle yurtdışına çıkışı tamamen engellenmektedir. Kişi insiyatifi dışına çıkarılan bu durumla birlikte, verinin ithal ürünlerle yurtdışı bulut ortamlarına çıkarılması da engellenmiş olmaktadır. Bu durumda sağlık (kaza-hayat vb) sigortaları, biyometrik özellikleri kullanan teknolojiler/servisler ve ithal IoT ürünlerinin satış izinleri üzerine düşünülmelidir. Enabıza entegre giyilebilir teknolojilerin geleceği de bu anlamda ele alınmalıdır. Tarım alanlarında Tarım ve Orman Bakanlığı desteği ile zirai-meteorolojik verileri toplayan cihazları yabancı şirketlerden satın alan çiftçilerin verileri yurt dışında toplanmaktadır. Dolayısı ile Türkiye'de hangi ürünün ne zaman ne kadar üretileceği ve hangi ilacın pazarlanabileceği modeli yurt dışında oluşmaktadır.

GENELGE MADDE NO:2

Madde: Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda

kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.

REHBER ÖNERİSİ:

- Yukarıda bahsedilen matriste tanımlanacak bazı kurum ve verilerinin, internete kapalı olsa da intranete açık olacağı öngörülmektedir. Bu tür bir ağın internete kapalı olması yerli ağ geçidleriyle izole edilmesiyle mümkün olabilir. Dış veya iç bir ağdan gelebilecek erişim istekleri en üst düzeyde bahsi geçen ağ geçitleri ve sistemler üzerindeki güvenlik önlemleriyle alarmlanmalıdır. Bu alarmlar kruum SOME leri tarafından öncelikli ele alınmalıdır.

- İnternete kapalı ağlardan kasıt Sanal Hava Boşluğu veya Veri Diyodlarıysa veri ve kurum tipiyle matriste ilişkilendirilerek netleştirilmelidir.

- Tamamen internete kapalı ağlarda verilerin nasıl ve kim tarafından güncelleneceği, fiziksel işlem kayıtlarının nasıl tutulacağı detaylandırılmalıdır.

- Matriste kritiklik seviyesi yüksek kurum ve veriler için internet dışı şebekeler tercih edilmelidir.

- Sistemlere yapılabilecek fiziksel müdahalelerin (Disklerin alınması) önlenmesi için bu sistemlerin ayrı ve fiziksel güvenliği artırılmış(kamera, ek kapı,..), çift yetkilendirme gereken bir alanda tutmaları istenmelidir. Disklerin kriptolu olması ve kripto standartları(algoritma, anahtar) da yine bu başlıkla ilişkilendirilmelidir.

- Log kayıtlarının değiştirilmeye karşı önlem alarak saklanması konusu detaylandırılmalıdır. Önlemden kastın engelleme ve anlama olduğu değerlendirilmektedir. Logun erişilebilirliği, şifrelenme motodları, anlık uzak alana yedeklenmesi, logların değiştirilmesi karşısında alınacak önlemler, nitelikli zaman damgası kullanımı ve benzeri konular bahsi geçen matrise refere edilerek belirlenmelidir.

- Logların saklanmasıyla ilgili mevcut mevzuattan farklı bir gereksinim varsa belirtilmelidir. Süreler kurum sınıflandırılmasına göre yapılmalıdır.

REFERANS BİLGİ ve BELGELER:

- Log kayıtlarının saklanmasıyla ilgili BTK ŞEBEKE VE BİLGİ GÜVENLİĞİ YÖNETMELİĞİ

MADDE 29 – (1) İşletmeci, istenmeyen bilgi işleme faaliyetlerinin önlenmesi ve bilgi güvenliği ihlal olaylarının tanımlanması amacıyla kritik sistemleri izler ve asgari aşağıdaki hususların uygulanabilir olanlarını içeren kayıt dosyalarını en az 2 yıl süreyle tutar:

a) Kullanıcı kimlikleri.

b) Oturum açma/kapatma, veri ekleme/silme/değiştirme gibi işlemlerin tarihi, zamanı ve açıklamaları.

c) Bağlantı sağlanan ekipmanın kimliği ve yeri.

ç) Başarılı ve reddedilen sistem, veri ve diğer kaynaklara erişim girişimlerinin kayıtları.

d) Sistem ayarlarındaki değişiklikleri.

e) Kullanılan özel izinleri ve ayrıcalıkları.

f) Sistem araçlarının ve uygulamalarının kullanımı.

g) Erişilen dosyalar ve erişimin tipi.

ğ) Ağ adresleri.

h) Erişim kontrol sistemi tarafından üretilen alarmlar.

ı) Anti virüs yazılımı, güvenlik duvarı gibi güvenlik sistemlerinin aktif ve pasif hale getirilmeleri.

i) Sistem güvenlik ayarlarına ve kontrollerine ilişkin değişiklikler veya değişiklik girişimleri.

j) Sistem yöneticileri tarafından yapılan işlemler.

k) Kullanıcı veya sistem programları tarafından rapor edilen bilgi işlem ve haberleşme sistemlerine ilişkin hatalar.

(2) Sistem yöneticilerinin kendi işlemlerine ilişkin kayıt dosyalarını silmelerini veya değiştirmelerini engelleyecek önlemler alınır.

(3) Kayıt dosyaları değişikliğe ve yetkisiz erişime karşı korunur.

- 5651 Kanunu Madde 5/3 ; Madde 6/b ve bağlı yönetmelik ve genelgeler

http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651-20150101.pdf

GENELGE MADDE NO:3

Madde: Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.

DETAYLANDIRMA GEREĞİ:

"Kurum kontrolündeki yerli hizmet sağlayıcılar" başlığının detaylandırılması

REHBER ÖNERİSİ:

- Tanımdan kastın gizlilik sözleşmesiyle bağlı ve erişimin yalnızca kurum tarafından yapıldığı sistemler olacağı öngörülmektedir. Yapılacak sözleşmenin bir formatının rehberde yer alması hizmet alacak kurumların işlemlerini rahatlatacaktır. Bu sözleşmede yer sağlayıcının matriste belirlenmiş veri ve kurum tiplerine göre hangi Seviye(Tier) da olacağı ve Hizmet Seviyesi Sözleşmesi (SLA) şartları belirlenmiş olmalıdır.

- Sistemler hizmet sağlayıcı ağından firewall, ips, ddos benzeri ağ geçidi güvenlik ürünleriyle ayrılmalıdır.

- Sistemlere yapılabilecek fiziksel müdahalelerin (Disklerin alınması) önlenmesi için kamu sistemlerinin ayrı ve fiziksel güvenliği artırılmış(kamera, ek kapı,..), çift yetkilendirme gereken bir alanda tutulması istenmelidir.

- Bazı kurum sistemleri ve üzerindeki veriler maddeye istisna olarak tanımlanabilir. Ör: herkese açık gizlilik seviyesinde veri içermeyen web sayfaları, anonim uygulamalar.. 2017 tarihli Ulusal Genişbant Stratejisi dokümanında Bulut Bilişim Yaygınlığının Artırılması hedeflenmiştir. Bu kapsamda bulut teknolojilerinden (yapılabiliyorsa sınırlarımız içinde kalarak) faydalanmak ve bu veri merkezlerini denetim altında tutmak, verileri şifrelemek ele alınmalıdır. Bulut bilişim sistemlerinin teknolojik avantajlarından yararlanırken Genelge ile ortaya konulan çekincelerin ortadan kalkması için madde sınırlarının ve hangi tip verilerin depolanabileceğinin detaylandırılmasına ihtiyaç vardır.

- Yerli hizmet sağlayıcılar tanımında geçen "yerli" kelimesinin milli kavramını da kapsamadığı böylece Amazon gibi yurtdışı sermayeli kuruluşların Türkiye de kuracakları veri merkezlerinin de kapsama girdiği düşünülmektedir. Yerlilikten kasıt buysa Amazon Türkiye ile ABD arasındaki veri transferlerinin nasıl denetleneceği açıklanmalıdır. Bu noktada milli olma isteği de varsa, millilik oranı ve milli bir sağlayıcının yurtdışına satılabilme koşulları da belirlenmelidir.

- Sektörde yerli/yabancı veya bulutta/kurum ağında(on premise) ayrımı yerine güvenlik kriterlerinin net olması gerektiği ifade edilmekte, yerli ve milli isterlerinin kısıtlı bir kurum ve veri için tanımlanması söz konusuysa matristeki hangi bölümle ilişkilendirileceği netleştirilmelidir.

- Kamuda sıklıkla kullanılan ve birçok modülü buluttan hizmet veren uygulamalar üzerinden, kurumların birçok verisi doğrudan bulutta tutulmaktadır. Ve bu tür ürünlerin

bulut altyapıları Türkiye'de değildir. Maddeyle bunun engellenmek istendiği bilinmekle birlikte, geçişteki zorluklar için kurumlar desteklenmeli ve yönlendirilmelidir (Örnek durumlarla ilgili TBD Siber Güvenlik Odak Ekseni ve Sektör Kurulu her zaman görüş vermeye hazırdır.).

REFERANS BİLGİ ve BELGELER:

11/12/2017 tarihli Ulusal Genişbant Stratejisi ve Eylem Planı (2017-2020) Stratejik Amaç 2. Genişbant Talebinin Oluşturulması Madde 14 Bulut Bilişim Yaygınlığının Artırılması

BİLGİ VE VERİLERİN PAYLAŞILMASI

GENEL

DETAYLANDIRMA GEREĞİ:

Verilerin Depolanmasında ele alınan konular verinin iletilmesi başlığında da ele alınmalıdır.

REHBER ÖNERİSİ:

- Veri depolama başlığında bahsi geçen matrise göre sınıflandırılmış veri ve kurumların veriyi nasıl taşıyacağı belirlenebilir.

- KamuNet ağına bağlanacak kurumsal ağlar için ISO 27001 istenmesine karşın bu gereksinimin bakanlığın tüm birimleri için mi, yoksa KamuNet'e fiilen bağlantı yapılan ağ için mi olduğu yönüne bazı soru işaretleri dile getirilmiştir. Rehber'de netleştirilmesi yararlı olacaktır.

- Kurumlar arasında yapılacak veri aktarım anlaşması içeriği için standart oluşturulması gerekmektedir. TSE tarafından hazırlanan fakat henüz resmen yayınlanmayan "KAMU GÜVENLİ VERİ PAYLAŞIM KRİTERİ"nin Rehber ile netleşmesi veya TSE tarafından netleştirilecek konuya atıf yapılması beklenmektedir.

- Veri sızıntısını önlemeye yönelik, kurumlara özel belirlenen politika ve kurallar çerçevesinde uygun bir DLP çözümü kullanılarak kritik verinin paylaşılması noktasında verinin güvenliği sağlanmalıdır.

GENELGE MADDE NO:4

Madde: Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

DETAYLANDIRMA GEREĞİ:

Kullanılacak ürünler konusunda netleşme

REHBER ÖNERİSİ:

- Yetkilendirilmiş kurumların rehberde daha açık belirtilmesi veya yanda belirtilmiş yönetmeliğe atıfta bulunulması uygun olacaktır.

- Trafik şifreleme ihtiyacının büyüklüğü göz önüne alınınca, maddeyle belirtilmiş ürünlerin yerli tedarikle karşılanabilmesi için mobil uygulamaların gereklerinin(kripto, anahtar,..) belirlenerek yerli üretimin teşvik edilmesi sağlanabilir.

- Kurumlardaki mobil uygulamalar sadece son kullanıcıların kullandığı uygulamalar olarak düşünülmemelidir. Maddenin bu anlamda ayrıntılandırılmaması yerli ve yabancı ürün kullanan ve mobil eklentileri olan sistemler için sıkıntı yaratabileceği düşünülmektedir.Ör: SSL VPN Clientler, Mobil İmza uygulamaları, CRM ERP Clientları ve benzeri

REFERANS BİLGİ ve BELGELER:

23 Ekim 2010 - 27738 Sayılı Kamu Kurum ve Kuruluşları ile Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik

GENELGE MADDE NO:5

Madde: Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

REHBER ÖNERİSİ:

- Güzlilik dereceli evrakların EBYS sistemlerinde işlenmediğinden, sadece yetkilendirilmiş kişiler tarafından erişilebildiğinden emin olunmalıdır.

REFERANS BİLGİ ve BELGELER:

23 Ekim 2010 - 27738 Sayılı Kamu Kurum

BİLGİ VE VERİLERİN İŞLENMESİ

GENEL

REHBER ÖNERİSİ:

- Gizlilik dereceli evrakların EBYS sistemlerinde işlenmediğinden, sadece yetkilendirilmiş kişiler tarafından erişilebildiğinden emin olunmalıdır.

GENELGE MADDE NO:7

Madde: Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.

REHBER ÖNERİSİ:

- Diğer maddelerde olduğu gibi gizlilik dereceleri kurumun sınıflandırmasına göre belirlenmelidir.

- Tempest koşullarının ağır olduğu ve ek büyük kaynaklar gerektireceği için bilgilerin işlendiği yerler tanımı bilgilerin toplu işlendiği yerler şeklinde değiştirilmesi gerekmektedir.

REFERANS BİLGİ ve BELGELER:

Tempest ortam gereklilikleri ve bu gerekliliklerin nasıl denetleneceği MSB ilgili güvenlik yönergelerinde, Tesis Güvenlik Belgesi isterlerinde yer almaktadır.

GENELGE MADDE NO:8

Madde: Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.

REHBER ÖNERİSİ:

Rehbere önerilen Personel Farkındalığı başlığı ile, bu ve diğer konular orada detaylı ele alınmalıdır.

GENELGE MADDE NO:9

Madde: Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.

REHBER ÖNERİSİ:

Rehbere önerilen Personel Farkındalığı başlığı ile, bu ve diğer konular orada detaylı ele alınmalıdır.

KAMU SİSTEMLERİNE BAĞLI CİHAZ VE KULLANICILAR

GENELGE MADDE NO:10

Madde: Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.

DETAYLANDIRMA GEREĞİ:

"Kurum sistemlerine bağlanmak " "kurum sistemi" "kaynağından emin olmak" "kriptolamak" tanımının netleştirilmesi

REHBER ÖNERİSİ:

- Kurum tarafından dış bağlantı için tanımlanmış sistemlere, ağlara, güvenlik önlemleri alınmak kaydıyla bağlanmak mümkün olmalıdır. Kurum dış kullanım ve iç kullanım ağları tanımlanabilir. Ör: Üniversite ve kurumlar misafir ağları, Kurum web sayfası,..

- Kaynağından emin olmak tanımı, kurumun envanterinde olan veya kurumun bağlanan cihazların güvenliğini kendi yönettiği, güvenlik önlemlerini kontrol ettiği bir çerçeve olarak tanımlanmalıdır.

- Kriptolamaktan kasıt netleştirilmelidir. Kripto algoritması, yöntemi belirlenmelidir. Şifrelenmiş verinin kurum dışında nerede, nasıl ve kim tarafından açılabileceği belirtilmelidir.

GENELGE MADDE NO:15

Madde: Üst düzey yöneticiler de dahil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.

REHBER ÖNERİSİ:

- Madde ele alınırken Sıfır Güven (Zero Trust) ve en az yetki (Least Privilege) modeli açıklanmalıdır.

- Güvenlik zafiyetlerinin en çok güvenliğin yönetilememesinden kaynaklandığından çıkışla, merkezi kimlik ve erişim yönetim sistemine sahip olması yönlendirilmelidir.

YERLİ VE MİLLİ KRİPTO VE GİZLİLİK DERECELİ HABERLEŞME

GENELGE MADDE NO:11

Madde: Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.

REHBER ÖNERİSİ:

- Özellikle madde 4 ve 21 göz önüne alınarak, şifreleme ihtiyacının büyüklüğü ortadadır. Maddeyle belirtilmiş ürünlerin yerli tedarikle karşılanabilmesi için uygulama gereklerinin(kripto, anahtar,..) belirlenerek yerli üretimin teşvik edilmesi sağlanmalıdır.

- Özellikle kamu uçlarının merkez ağlara bağlantılarında kriptonun kullanılması, yerli üreticilerle işbirliği yapılarak yaygınlaştırılmalıdır.Yerli üreticilere kullanılması gereken kripto (algoritma, anahtar) yönlendirmesi yetkilendirilmiş kurum veya kuruluşlar aracılığıyla yapılabilir.

- Kamu uçlarının MPLS ve benzeri altyapılar üzerinde şifreleme içermeyen yöntemlerle merkezlere taşınması sonucu, trafiğin kurumda olmadığı alanlarda kurum dışından birilerinin takibine açık olduğu kabul edilmelidir. Bu maddedeki amacı gerçekleştirebilmek için kullanılan/kullanılacak MPLS ağları üzerinde VPN yöntemi uygulanmalıdır. VPN/Kriptoların yapılandırılması sorumluluğu verinin sahibi kurumda olmalı ve kurumlar bu yapıları kendi yönetimlerinde işletmelidir.

- Kriptonun nerede başlayacağı ve nerede sonlandırılacağı netleştirilmelidir. Sunucu ile ağ geçitleri arasındaki trafiğin ifrelenme ihtiyacı değerlendirilmelidir.

- Kripto sistemlerinin kurumların satınalma sorumluluğunda olduğu düşünülmekte, işletmecilerin bu konuda bir yatırım yapmayacağı öngörülmektedir. Konunun netleştirilmesi gerekmektedir.

- Genelge kapsamında yerli ürün gereksinimleri sadece kripto temelinde ele alınmıştır. Siber güvenlik tehditlerinin büyük çoğunluğu katman7'ye kaymış ve yeni nesil güvenlik duvarı, web filtreleme, antivirüs, saldırı tespit ve önleme sistemleri gibi ürünlerle engellenmektedir. Ülkemizde bu ürünler çoğunlukla yabancı menşelidir. Uygun kurum ve veri tiplerinde yerli kripto cihazlarıyla birlikte, yerli siber güvenlik ürünleri veya özgür yazılım / açık kaynak kodlu ürünler zorunluluk olarak ele alınmalıdır.

- Genelge'nin milli güvenliği yükseltmenin yanında siber güvenlikte cari açık dengesizliğinin de önüne geçmek amacında olduğunu düşünüyoruz. Bu anlamda kamuda sıklıkla kullanılan siber güvenlik ürünlerinin de yerli ve milli olmasıyla ilgili Rehber'de açıklama beklenmektedir.

KAMU TARAFINDAN TEDARİK EDİLEN YAZILIM VE DONANIM ÜRÜNLERİNİN GÜVENİLİRLİĞİ

GENEL

REHBER ÖNERİSİ:

12. Maddenin COTS(rafta) 13. Maddenin Kurum özel geliştirilen yazılımlar için yazıldığı öngörülmektedir. COTS veya kurum özel olmasından bağımsız olarak, ürün üretiminde hatalar doğal şekilde de olabilmektedir. Bunların olmamasını hiç kimse (üretici, dağıtıcı, satıcı,..) garanti edemeyecektir. Her üreticinin iş takip sistemlerinde herhangi bir anda geliştirme ekibinde düzeltilmekte olan hatalar da vardır. Bu nedenle hataların bulunmaması gibi bir taahhüdü hiçbir üretici veremeyecektir.

DDO nun üreticilere yaklaşımı, hataların olmasını engelleyecek geliştirme süreçlerinin uygulanıp uygulanmadığı ve hatalara nasıl müdahale edildiği noktasında taahhütler almak olmalıdır. Ürün üreticisi,

i. güvenli geliştirme süreçlerini uyguladığını taahhüt etmeli ve sertifikasyon ile ispatlamalıdır.
ii. hata ve açıkları bildirme için halka açık bir yöntemi sunmalıdır.
iii. hataların ve açıkların düzeltilmesi (flaw remediation) ile ilgili prosedürleri uygulandığını taahhüt etmeli ve bir sertifikasyonla ispatlamalıdır.

Bu hassasiyet ortaya konulurken, yerli üreticilerin uluslararası sertifikasyonlarının Türkiye'de yapılabilmesi önemlidir.

GENELGE MADDE NO:12

Madde: Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.

REHBER ÖNERİSİ:

- Maddenin bu şekilde kalması yurt dışı üreticilerin vermeyecekleri, yerli üreticilerin ise bu taahhütleri vermek için zorunluk baskısı altında kalacakları bir ortam oluşturacaktır.

- Bunun yerine "Güvenli olmasını istiyorsan kendin test et" mantığıyla kamuda sıkça kullanılan ürünler önceliklendirilerek, TR Test altında yerli veya yabancı bakmadan bir masumiyet (arka kapı) sertifikasyonu gereği bulunmaktadır. Bu sertifikasyon ürünün yapısına, kullanım amacına, hizmet şekline ve teknolojisine göre çeşitlenebilir ve kritiklik/gizlilik gibi unsurlara göre derecelendirilebilir. Bir başka yöntem de TR Test'in kamuda kullanılan ürünleri ürün sağlayıcıdan bağımsız olarak, her hangi bir başvuruya gerek duymadan test edebilmesinin önünün açılması, özel durumlarda kaynak kodlarının ve derleme ortamlarının tamamının incelenmesinin sağlanması ve KİK aracılığıyla gerekli tedbirlerin alınabilmesinin sağlanmasıdır. Ürün üreticileri bu tür bir teste ürün ve uzman personel sağlamayı taahhüt etmelidir.

- TR Test'in yükünün hafifletilmesi için Türkiye test merkezlerinden alınmış Ortak Kriterler EAL4+ sertifikalı ürünler için masumiyet sertifikası şartı aranmayabilir. Türkiye Ortak Kriterler test merkezlerinin süreçlerinde uyguladıkları arka kapı analizleri gözden geçirilebilir.

- Taahhütlerin üreticiler yerine ihaleyi alan iş ortakları ve entegratörlerden alınması yine anlamlı bir yol olarak görülmemektedir. İş ortakları ve entegratörler yukarıda bahsedildiği gibi bilinçsiz bir zorlama ile karşı karşıya kalacaklardır. Çoğu iş ortağı uluslararası üreticilerle, kabul ettiğimi kabul et (back to back) mantığında çalışmakta, üreticinin vermediği taahhütleri kurumlara vermemektedir.

- Kamu kaynaklarıyla ulusal tehdit oluşturan ürün ve uygulamaların tespit edilmesi halinde KİK eliyle kullanımının yasaklanması için mevzuat düzenlemesi gereği bulunmaktadır. Halen bir sistemi kırmak ve orada kalmak suçken, buna yol açan kapıların bilinçli olarak bırakılması suç olarak kabul edilmemektedir.

- Bir diğer olası yöntem ithal edilen donanımsal bilişim ürünlerinin gümrükten çekilmesi sürecine bu ürünleri ithal eden tarafın taahhütname vermesi şartının eklenmesidir.

- Taahhütname uygulanacaksa bir sözleşme niteliğinde olmalı ve sonraki güncellemeleri de kapsamalıdır. Taahhütname alındığı tarihten sonra sistemler sürekli güncellemeler yoluyla yeni kodlar ve imzalar almaktadır.

- Kamuda kullanılan ürünlerin güncellemlerinin Türkiye'de bulunan veri merkezleri üzerinden yapılması ve bu sunuculara yurtdışından yapılan bağlantıların denetim altında tutulması bir yöntem olarak ele alınmalıdır.

- Kurumun yapacağı satın alma sonucunda, yurdışındaki üreticilerin sistem ve sahibiyle ilgili hangi bilgilere sahip olduğu denetlenmelidir. Üreticilerdeki bilgiler kurumu tanımlamamalı, üretici veri tabanlarındaki kurumlarla ilgili bilgiler anonim olmalıdır.

- Güncellemeler dahil olmak üzere kamu sistemlerinin herhangi bir amaçla yurtdışı sunuculara kendiliğinden bağlantı kurmaları ve veri göndermeleri engellenmelidir, şartnamelerde bu madde standart hale gelmelidir.

- Geçmiş dönemlerde NSA in raporları sızdırılmış ve burada bazı dış devletlerin üreticiler tarafından bilinçli veya bilinçsiz bırakılan arka kapıları satın aldığı, sattığı, bazı

üreticilerle bu amaçla iş birliği yaptığı belgelerle ortaya konulmuştur. Fakat bu bilgiler elde olmasına karşı hiçbir tedbir alınamamıştır.

- Madde çerçevesinde özgür yazılım / açık kaynak kodlu ürünler teşvik edilmeli fakat özgür yazılımların da arka kapı barındırmadığına dair güvenceler alınmalıdır.

- Yazılımların yanında test yapılacak alan olarak hızlandıcı kartlar (FPGA,ASIC,GPU..) üzerindeki yazılımlar da ele alınmalıdır. Bu kapsamda bir ileriki aşama olarak donanım sürücüleri de ele alınabilir.

- Yine bu madde başlığında üreticilerden alınacak kaynak kodlarının ve ürünün çalıştırılabilir hale gelmesini sağlayan derleme kaynaklarının / kütüphanelerinin bir bütün olarak, bu işe özel ve en üst düzeyde korunan bir makama yeddiemin olarak teslim edilmesi şartı konulması ve bu kodlar üzerinde kaynak kod analizi yapılması zor ama değerlendirilmesi gereken bir noktadır.

GENELGE MADDE NO:13

Madde: Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.

DETAYLANDIRMA GEREĞİ:

Tedbirler ve güvenlik testlerinin detaylandırılması

REHBER ÖNERİSİ:

- Madde ile kurum özel geliştirilen yazılımların hedeflendiği anlaşılmaktadır.

- Yerli üreticilerin COTS ürünleri de yabancı ürünlerle aynı kategoride değerlendirilmeli, kurum özel yazılım geliştiriyor muamelesiyle karşı karşıya kalmamalılardır.

- Bahsi geçen güvenlik testi şemalarının çıkarılması ve yayınlanması gerekmektedir. Asgari olarak aşağıdaki gereklilikler belirtilmelidir.

Statik kaynak kod analizi

Dinamik web uygulama taraması

Geliştirme ortamı ile canlı ortamın birbirinden izolasyonu

Görevler ve sorumluluklar ayrımı ilkesine göre yetkilerin sınırlandırılması ve ayrıştırılması

YENİ BAŞLIK ÖNERİSİ: KAMU TARAFINDAN TEDARİK EDİLEN HİZMET VE DANIŞMANLIKLAR

GENEL

DETAYLANDIRMA GEREĞİ:

Genelge ile Kamu kurumlarının hedeflenmesi fakat kamunun özel sektörle ilişkisinden bahsedilmemesi

REHBER ÖNERİSİ:

Genelgede Özel sektörün bahsi geçen sistemlere ve verilerin bulunduğu alanlara destek, danışmanlık hizmetlerini nasıl vereceği, bu sistemleri nasıl kuracağı, bu dış kaynaklardan hangi güvenlik kriterlerinin aranacağı noktalarının aydınlatılması gerekmektedir.

SİBER TEHDİT BİLDİRİMLERİ

GENELGE MADDE NO:14

Madde: Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.

REHBER ÖNERİSİ:

- Madde SOMEleri ilgilendirse de , USOM un ürettiği tehdit bildirimlerinin yeterliliği ve uluslararası bildirimleri kamuya ne kadar tatbik edebildiği de düşünülmelidir.

- Siber tehdit bildiriminin üst seviyeli olması durumunda, 24x7 , gerçek zamanlı aksiyon alınması için gerekli yazılım altyapısının sağlanması ve süreçlerin tanımlanması; yapılan işlemlerin kayıt altına alınması; tehdide ilişkin, olay sırasında ve sonrasında, olay analizinin yapılabilmesi için gerekli teknolojik ve idari altyapının hazırlanması; süreç ve tedbirler planlanırken, yurtiçi referansları olan, yerli ve milli kaynaklarla oluşturulmuş çözüm ve ürünlerin öncelikli olarak değerlendirilmesi gibi konular Rehber'de ele alınmalıdır.

ENDÜSTRİYEL KONTROL SİSTEMLERİNİN GÜVENLİĞİ

GENELGE MADDE NO:16

Madde: Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.

REHBER ÖNERİSİ:

Endüstriyel kontrol sistemleri tanımı yapılmalıdır. İnternete kapalı olsa bile kritik tanımı yapılacak sistemler çin güvenlik tedbirleri alınmalıdır. Olası güvenlik tedbirleri diğer maddelerde belirtilen kapsamdan daha düşük olmamalıdır.

PERSONEL GÜVENLİĞİ

GENEL

REHBER ÖNERİSİ:

- Bu tür personelle yapılacak sözleşme gizlilik ekinin detaylı ve tek tip olması beklenmektedir.

- Bu başlıkta personelin teknik güvenilirliği de ele alınabilir, gerekli sertifikasyonlara sahip olmayan kişilerin sistem güvenliğini sağlayamayacakları öngörülmektedir.

GENELGE MADDE NO:17

Madde: Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.

REHBER ÖNERİSİ:

- Bu kurumlara hizmet veren özel işletmelerin de güvenlik soruşturmasından yararlanabilmesinin yolu açılmalıdır. Halen Tesis Güvenlik Belgesi olmayan COTS ürünü bulunan yerli üreticiler personellerini bu süreçlere sokamamaktadır. Yabancı ürün ve hizmet sağlayıcıları da aynı şekilde yararlanamamaktadır.

- Kritik önemi haiz personel hakkında hangi mevzuat ya da yönetmelik çerçevesinde güvenlik soruşturması ve arşiv araştırması yapılacağı, altı ayda bir adli sicil belgelerinin yenilenmesi, güvenlik önlemleri hakkında eğitilmeleri, giriş çıkışlarının kayıt altına alınması vb. gerekli önlemleri içerecek şekilde detaylandırılması beklenmektedir.

- Kamuda nitelikli personelin en kıt kaynak olduğundan çıkışla, bir personelin görevlendirilmesi veya işe alımı öncesinde çok uzun süreler beklenmesi mümkün olamamaktadır. Sürecin hızlandırılması adına önlemler Rehber'de yer alabilir.

KAMU E-POSTA SİSTEMLERİ

GENEL

REHBER ÖNERİSİ:

- Kurum e-posta sistemleri yerine şahsi e-posta hesaplarının kullanılmasının ana nedeni olarak kurumlardaki sistemlerdeki kota sınırları ve kullanıcıya yansıyan yönetim zorluklarıdır.

- Türkiye'de merkezi ve milli bir kamu e-posta sisteminin tüm kurumlarımız tarafından kullanılması ve kurumlardaki çoğu yabancı menşeili yerel e-posta sunucuları kaldırılabilir.

- Sistemlerin yanında personel parola güvenliği ve benzeri siber güvenlik önlemleri e-posta sistemleriyle sınırlı olmamak üzere tarif edilebilir. Rehbere önerilen Personel Farkındalığı başlığı ile bu ve diğer konular orada detaylı ele alınmalıdır.

GENELGE MADDE NO:18-19

Madde:

18. Kamu e-posta sistemlerinin ayarlan güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.

19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

REHBER ÖNERİSİ:

E-posta sistemlerinin güvenlik gereksinimleri tarif edilmelidir.

- SSL/TLS ile iletimin zorunlu tutulması,

- SPF, SenderID, DKIM v.b. gönderici doğrulama özelliklerinin etkinleştirilmesi,

- E-posta boyutu limiti konulması,

- Spam e-postalara karşı tedbirlerin etkinleştirilmesi,

- Open relay v.b. ile yetksiz erişim ve kullanımın engellenmesi,

- E-posta sistemi, kayıt/iz bilgilerinin uygun süre ile saklanması

gibi...

VERİNİN ULUSAL SINIRLARI VE YERLİ ÜRÜN

GENEL

REHBER ÖNERİSİ:

- Verinin ulusal sınırları çizilirken yerli ürün ve özgür yazılım/açık kaynak kodlu kullanım noktaları belirlenebilir. Özgür yazılım ve açık kaynak koda yönlendirirken, kurumların bu ürünleri tercih ederken kullanılabilirlik, performans, entegrasyon, uyumluluk konularında mutlaka uzman girişimlere ihtiyaç duyacakları değerlendirilmelidir. Kamu kurumlarımız için başarılı pilot çalışmalar önemlidir.

- Açık kaynak kodlu yazılımların çok değerli bilgiler içeren bir kütüphanedir ama gerçek hayata sektör tarafından entegre edilmesi gerekmektedir.Bazı özgür yazılımlarda doğrudan kullanım mümkünken, bazılarında girişimlerin bu kodlara dayanarak ürün çıkarması özendirilmelidir. Her iki durumda da eğitim müfredatlarının ve kurulum, konfigürasyon, destek bilgi birikiminin oluşturularak kurumlar hizmetine sunulması için girişimlerin kurulması ve var olanların büyütülmesi, kurumsallaştırılması önemlidir. Bu

bilgi birikiminin kurumlarımıza kobi seviyesindeki girişimlerce verilmesi rekabet ve inovasyon için kritik önemdedir.

GENELGE MADDE NO:20-6

Madde:

20. Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.

6. Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.

REHBER ÖNERİSİ:

İşletmeciler tarafından UAB ve BTK ile detaylı çalışmalar yapıldığı, maddenin Rehberde veya rehber dışında BTK üzerinden ele alınması gerektiği ifade edilmektedir.

İŞLETMECİ ALTYAPILARININ GÜVENLİĞİ

GENELGE MADDE NO:21

Madde: İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.

REHBER ÖNERİSİ:

- Ele alınmak istenen bölgenin sınırlı ve kritik önemde olduğu da düşünülerek bu maddeyle ilgili yönlendirmelerin rehber yoluyla değil, BTK üzerinden işletmecilere yazılı tebligatla yapılmasının daha doğru olacağı düşünülmektedir.

- Bölgenin kısıtlı bir alan olarak tanımlanacağı düşünülerek işletmecilerin bu düzenlemeye bir itirazları bulunmamaktadır. Alanın geniş ve parçalı tarif edilmesi, kırsalın da kapsanması uygulamada sorunları büyütebilecektir.

- Tarif edilen alandaki kurumların uçlarıyla ilgili aynı hassasiyetin bulunup bulunmadığı netleştirilmelidir. Uçların merkeze bağlantılarında kriptonun kullanılması, yerli üreticilerle işbirliği yapılarak yaygınlaştırılmalıdır. VPN/Kriptoların yapılandırılması sorumluluğu verinin sahibi kurumda olmalı ve kurumlar bu yapıları kendi yönetimlerinde işletmelidir.

- Uçların da kapsama dahil edilmesi halinde fiber şebekenin kısıtlılığı göz önünde bulundurularak alternatifler gündeme alınmalıdır.

- Yerli üreticilere kullanılması gereken kripto (algoritma, anahtar) yönlendirmesi yetkilendirilmiş kurum veya kuruluşlar aracılığıyla yapılabilir.

YENİ BAŞLIK ÖNERİSİ: ÜRÜNLERİN KULLANILABİLİRLİĞİ

REHBER ÖNERİSİ:

Sistemlerin güvenliğinin sağlanamamasında en büyük etkin, ürünlerin yeterkince yetkin kullanılamamasıdır. Bu anlamda Türkçe arayüze ve kullanım klavuzuna sahip olmayan güvenlik ürünleri ve güvenlik bileşenine sahip ürünlerin satışına izin verilmemelidir. Türkiye yeterince büyük bir pazardır ve birçok yurt dışı üretici böyle bir zorunluluk hissetmedikleri için Türkçe yönetim arayüzü ve dokümantasyon hazırlığına girmemektedir.

YENİ BAŞLIK ÖNERİSİ: İŞ SÜREKLİLİĞİ

REHBER ÖNERİSİ:

CIA (Confidentiality Integrity Availability) üçlüsü, Erişilebilirlik(Availability) ayağından Genelge'de bahsedilmemiştir.

Sistemlerin yedekliliği, yedeklerin çalışabilir olması, kurum sınıfına göre ISP yedekliliği, Coğrafi Yedeklilik gibi konular rehberde bu başlık altında yer alabilir.

YENİ BAŞLIK ÖNERİSİ: KAMU AĞLARININ DÜZENLİ TEST VE SERTİFİKASYONU

REHBER ÖNERİSİ:

- Genelgede kamu ağlarının nasıl test edileceği ve hangi sertifikasyonlara sahip olacağından bahsedilmemiştir. Sıma testleri, ISO 27001 ve benzeri önlemler ve bu önlemleri alırken kullanılacak dış kaynakta aranacak nitelikler netleştirilmelidir.

- Düzenleyici kurumlara verilecek tatbikat görevleri de yine bu başlıkta ele alınabilir.

YENİ BAŞLIK ÖNERİSİ: GÜVENLİK YÖNETİMİ

REHBER ÖNERİSİ:

- Center of Internet Security (CIS)'in 20 Güvenlik Kontrolü referans alınabilir Örnek olarak en temel ve başlangıç güvenlik kontrolleri, "Varlık/envanter Yönetimi" ile "Zafiyet ve Yama Yönetimi" başlıkları Genelge'de yer almamış olmakla beraber asgari gerekliliklerdir.

- Rehberde Risk Yönetimi bölümüyle, alınan tedbirler risklerle ilişkilendirilmelidir.

YENİ BAŞLIK ÖNERİSİ: PERSONEL FARKINDALIĞI

REHBER ÖNERİSİ:

- Birçok maddenin hakkıyla uygulanabilmesi için personel farkındalığının yüksek olması gerekliliği ortadadır. Bu Genelge ile tarif edilmeyen birçok personel farkındalığı konusu, rehberde ayrı bir başlık altında ele alınmalıdır.

- Sosyal mühendislik yöntemlerine karşı bilinç yükseltilmelidir.

- Bu konuda verilen eğitimlerin bir kamu kültürü oluşturma amacı olmalıdır.

REHBERİN UYGULANMASI VE DENETİM

UYGULAMA: GENELGE SON BÖLÜM PARAGRAF 2

Madde: Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur. Mevcut bilgi teknolojisi altyapıları, güvenlik seviyesi öncelikleri dikkate alınarak yayımlanmasını müteakip Rehberde yer alacak plan çerçevesinde kademeli olarak bu esaslara uyumlu hale getirilecektir. Uyum çalışmalarında ve yeni kurulacak bilgi sistemlerinde, belirtilen adreste yayımlanan güncel sürüm dikkate alınacaktır.

REHBER ÖNERİSİ:

- Mevcut sistemlere tanınan zaman netleşmelidir. Mevcut sistemlerin güncelleme yoluyla devamı Genelge'nin uygulanması önünde bir engel olabilir.

- Geçiş süreci bazı veriler ve uygulamalar için öncelikli olarak ele alınmalı ve mevcut sistemlerin 2-3 yıl daha güncellemesi devam ediyor olsa bile Genelge hükümleri mevcut sistemler için belirlenecek tarihten sonra geçerli olmalıdır.

DENETİM: GENELGE SON BÖLÜM PARAGRAF 3

Madde: Milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçlan ile yapılan düzeltici ve önleyici faaliyetler, Rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.

REHBER ÖNERİSİ:

- Denetleme raporlarının bir üst kuruma veya düzenleyici kurullara iletilmesi gerektiğini düşünüyoruz. Sorumluluğun kurumlarda kalması denetlemenin yeterince yapılamayacağı tereddütlerini beraberinde getirmektedir.

- Rehberde denetimin nasıl yapılacağı , hangi yöntemin uygulanacağı belirlenmelidir. Ayrıca, Kurumlar içinde oluşturulacak denetleme mekanizmalarının yapısı, yetkinlikleri, görev alanları ve görev alacak denetçilerin özellikleri belirlenmelidir.

- Denetim raporu, akredite edilmiş firmalar tarafından yapılmalıdır. Akreditasyonu olmayan kişi ve kuruluşlar tarafından yapılan denetim ve raporlar geçersiz sayılmalıdır. Olası dış kaynak kullanımının da gerekleri ve şartları için yönlendirmeler yapılmalıdır.

- SKEP sonuçlarının denetim sonuçlarına eklenmesi ele alınmalıdır.

TÜRKİYE BİLİŞİM
1971
DERNEĞİ

www.TBD.org.tr