Tarih	Kasım 2020	SSS No:1
Konu/Rehber Maddesi	Hedeflenen Durum (T/Ç/K/H/UD) Nasıl Doldurulacak?	
CBDDO'ya Sorulan Soru		
Formun "**Hedeflenen Durum (T/Ç/K/H/UD)**" alanının kullanım maksadını tam olarak anlayamadık. Normal şartlar altında hedeflenen durumun tüm tedbirler için "T" olması gerekmiyor mu? Kurum ve kuruluşların hedeflenen durum için "T" haricinde başka seçenek seçmeleri imkanı var mı? Bu durumda Rehber uyumu %100 nasıl sağlanacak? Bu alanın kullanım maksadı hakkında daha detaylı bilgi verebilir misiniz?		
CBDDO Tarafından Yapılan Açıklama		
Mevcut durum ve boşluk analizi çalışmaları çerçevesinde varlık grubu ile ilgili tedbirlerin uygulanmasında öncelikli hedef tedbirin "Tamamen" uygulanmasıdır. Ancak aynı varlık grubuna dâhil edilen varlıklara, ilgili tedbirlerin uygulanmasında iş süreçlerinin doğası gereği tamamen/kısmen uygulanma ihtimali bulunmaması; **personel, bütçe gibi kaynak planlamalarının yeterli olmaması** ve/veya telafi edici kontrollerin uygulanması söz konusu olmaktadır. Hedeflenen Durum alanı bu nedenle • Tedbir, varlık grubunda yer alan tüm varlıklara uygulanabilir ise "tamamen"(T) • Tedbir, varlık grubunda yer alan varlıkların çoğuna uygulanabilir fakat bazı varlıklara kısmen uygulanabilir ise "çoğunlukla" (Ç) • Tedbir, varlık grubunda yer alan bir kısım varlığa uygulanabilir veya tedbir kısmen uygulanabilir ise "kısmen"(K) • Tedbir uygulanamayacak ise "hiç" (H) • Tedbirin teknik olarak uygulanma ihtimali bulunmuyorsa "uygulanamaz"(UD) seçenekleri ile doldurulacak şekilde tasarlanmıştır.		

Tarih	Kasım 2020	SSS No:2
Konu/Rehber Maddesi	Özel Hastaneler Rehber Kapsamında mı?	

CBDDO'ya Sorulan Soru

CBDDO Rehberinin "Amaç ve Kapsam" başlıklı 1.1 maddesinde "Rehber, bilgi işlem birimi barındıran veya bilgi işlem hizmetlerini sözleşmeler çerçevesinde üçüncü taraflardan alan, devlet teşkilatı içerisinde yer alan kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmeleri kapsamaktadır" ifadesi bulunmaktadır.

Ulusal Siber Güvenlik Strateji dokümanları incelendiğinde "Elektronik Haberleşme, Enerji, Su Yönetimi, Kritik Kamu Hizmetleri, Ulaşım ve Finans" sektörlerinin Kritik Altyapı Sektörleri olarak tanımlandığın görülmektedir. Bahse konu dokümanlarda Sağlık Hizmetleri de Kritik Kamu Hizmeti olarak tanımlanmış durumdadır.

Bakanlığımıza bağlı sağlık hizmeti sunan sağlık tesislerimiz için Rehber'in bağlayıcı olduğu konusunda bir şüphe bulunmamaktadır. Ancak Rehber'in özel hastaneler için (bilhassa rehber uyum planlarının hazırlanması ve iki yıllık süreçte Rehber ile uyumlu olunması hedefi ile çalışma yapılması konusunda) bağlayıcı olup olmadığı konusunda tereddüde düşülmüştür. Bize bununla ilgili sorular gelmektedir. Bu sorulara ne şekilde cevap vermek gerekir.

CBDDO Tarafından Yapılan Açıklama

Bilgi ve İletişim Güvenliği Rehberinde kritik altyapı sektörleri *"Ulusal Siber Güvenlik Stratejisinde belirlenen kritik altyapı sektörleri"* ifade eder şeklinde tanımlanmıştır.

Strateji dokümanında ise kritik alt yapı sektörlerine:

"İşlediği **bilgi/verinin gizliliği, bütünlüğü veya erişilebilirliği** bozulduğunda,

- **Can kaybına,**
- Büyük ölçekli ekonomik zarara,
- Ulusal güvenlik açıklarına veya **kamu düzeninin bozulmasına** yol açabilecek bilişim sistemlerini barındıran altyapıları,"

ifade eder şeklinde yer verilmiştir.

Ayrıca, USOM tarafından yayımlanan Sektörel SOME Kurulum ve Yönetim Rehberi'nin "Kritik Kamu Hizmetleri Sektöründe Sektörel SOME'lerin Kurulacağı Kurumlar" başlığı altında **kritik kamu hizmetlerinin tanımı:**

"Kritik Kamu hizmetleri; vatandaşın gündelik hayatında sıklıkla etkileşimde bulunduğu nüfus, tapu, vergi, ticaret, sosyal güvenlik, sağlık (acil servis, tıbbı hizmetler, kan ve organ bankacılığı ve halk sağlığı), gıda, güvenlik (polis, jandarma, sahil güvenlik), yollar ve köprüler, barajlar, maaş ve adli işlemlerin yapıldığı ve kayıtlarının bulunduğu kritik sistemlerden sunulan servislerdir."

şeklinde yapılmıştır.

Yukarıda yer alan tanımlamalar doğrultusunda **özel hastaneler, kamu hizmeti sunma noktasında diğer hastanelerle aynı konumdadır ve Rehber özel hastaneler için de bağlayıcı niteliktedir.**

Tarih	Aralık 2020	SSS No:3
Konu/Rehber Maddesi	Kritik Verilerin Şifreli Olarak Herkese Açık Ortamlar Üzerinden Aktarılması	

CBDDO'ya Sorulan Soru

Malum olduğu üzere 2019/12 numaralı Cumhurbaşkanlığı Genelgesi ve CBDDO Rehberi uyarınca kurumsal verilerin yurt dışı bulut depolama ortamlarında saklanması, sosyal medya platformları ve herkese açık e-posta servisleri (Gmail vb.) üzerinden paylaşılması kesinlikle yasak. Bakanlık olarak biz zaten baştan beri bu kurala uygun olarak davranıyorduk. Sizin düzenlemelerinizin yayımlanması ile birlikte tüm kullanıcılarımıza her türlü vasıta ile yeniden duyuru yaptık ve aksine hareket etmenin sonuçları hakkında herkesi bilgilendirdik.

An itibarı ile durağan haldeki verileri, Bakanlığımız kullanıcıları arasında; Bakanlığımız kurumsal e-posta sistemi, kurumsal veri aktarım sistemi ve taşınabilir medya ortamları üzerinden yapıyoruz. Belli gizlilik derecesinin üzerindeki veriler için şifreleme zorunluluğu da getiriyoruz. Veri aktarımının tüm tarafları Bakanlığımız personeli olunca bu sürecin işletilmesinde bir sorunla karşılaşmıyoruz.

Bununla birlikte bahse konu durağan haldeki verilerin zaman zaman Kurumunuz kontrolündeki ortamlara erişimi olmayan üçüncü taraflar ile de (resmi maksatlarla) paylaşılması ihtiyacı oluyor. Bu durumda güvenli bir veri aktarım yöntemine ihtiyaç duyuyoruz. Biliyorsunuz veriler uygun kriptografik algoritmalar ve yeterli uzunlukta anahtar boyları ile şifrelendiğinde halka açık ağlar üzerinden paylaşılabiliyor. Örneğin web servisleri SSL/TLS ile güvenli hale getiriliyor. VPN servislerinde benzeri kriptografik işlemler kullanılıyor.

Yukarıdaki örneklere benzer şekilde; **kurumsal verilerimizi (örneğin AES 256 koruma sağlayan) bir şifreleme aracı ile kapatsak ve şifrelemede kullandığımız anahtarı ilgili kişilere SMS vb. yöntemler ile göndersek, bu şifreli (kapatılmış) veriyi üçüncü taraflar ile kurumumuz kontrolünde olmayan ortamlar üzerinden (yurt içi/yurt dışı bulut depolama ortamları, sosyal medya platformları veya herkese açık e-posta servisleri (Gmail vb.)) üzerinden paylaşsak, 2019/12 ve CBDDO Rehberini ihlal etmiş sayılır mıyız?**

CBDDO Tarafından Yapılan Açıklama

Bilgi ve İletişim Güvenliği Rehberi çerçevesinde uygulanması gereken tedbirlerin Rehber'de tanımlandığı şekli ile uygulanmasında teknik kısıtlar veya zorunluluklar olması durumunda tedbire yönelik telafi edici kontrol uygulanabileceği hususuna Rehber'de yer verilmiştir. Kurum, Rehberde yer verilen bir gereksinimi, üst yönetim tarafından onaylanmış teknik kısıtlamalar ve iş gereksinimlerinden dolayı rehberde tanımlandığı şekli ile karşılayamaması durumunda telafi edici kontroller uygulayabilir. Telafi edici kontroller, yerine uygulandıkları tedbir maddeleri ile aynı amaç ve etkiye sahip olmaları durumunda kullanılabilir olarak kabul edilecektir. Uygulanmasına karar verilen her bir telafi edici kontrol kayıt altına alınmalıdır.

Kritik verinin üçüncü taraflar ile paylaşılması konusunda, öncelikli olarak yerli bulut dosya paylaşım ve depolama platformlarının kurum bünyesinde veya hizmet olarak kullanılması tercih edilmelidir. Bunun yanında zorunluluk durumunda kurum onayı alınarak, verinin uygun kriptografik algoritmalar ve yeterli uzunlukta anahtar boyları ile şifrelenerek paylaşılması ve şifreleme anahtarının ilgili kişilere farklı güvenilir kanallarla iletilmesini telafi edici kontrol kapsamında değerlendirmek mümkündür.

Tarih	Şubat 2021	SSS No:4
Konu/Rehber Maddesi	Çok Faktörlü Kimlik Doğrulama Kullanımı	
CBDDO'ya Sorulan Soru		
Rehberin Ağ ve BT Güvenliği ile ilgili bölümünde yer alan iki soruya ilişkin ilave açıklama talep etmekteyiz. 3.1.12.9 maddesinde kurum dışı paydaşların uzaktan erişiminde çok faktörlü kimlik doğrulama metotlarının kullanımı hususu zaten yer almaktadır. 3.1.12.15 maddesinde de benzeri bir gereksinim bulunmaktadır. 3.1.12.15 maddesinde sorulan konu, 3.1.12.9'da istenenden daha farklı bir gereksinim midir? Öyle ise bu madde ile ilgili daha detaylı açıklama yapabilir misiniz?		
CBDDO Tarafından Yapılan Açıklama		
Sorunuza ilişkin değerlendirmemiz aşağıda yer almaktadır: 3.1.12.9 maddesinde, kurum personeli haricinde yer alan dış paydaşların kurum sistemlerine uzaktan erişimi ve yapılan erişimin güvenliğini sağlamaya yönelik belirli kontroller yer almaktadır. 3.1.12.15 maddesinde ise kurum personeli dâhil dışarıdan kurum ağına yapılacak tüm erişimlerde çok faktörlü kimlik doğrulaması yapılması istenmektedir.		

Tarih	Şubat 2021	SSS No:5
Konu/Rehber Maddesi	3.1.9.8 Maddesi (Operasyon ve Test Ortamlarının İzolasyonu) İçin Açıklama Talebi	
CBDDO'ya Sorulan Soru		
CBDDO Rehber uyum çalışmaları kapsamında boşluk analizi yaparken, Rehber'de yer alan 3.1.9.8 maddesi için ne yapılması gerektiğini tam olarak anlayamadık. Bu madde, üst başlık olarak "3.1.9. Sanallaştırma Güvenliği" içerisinde yer alıyor. Bu başlık altında yer alan diğer tüm maddelerde, spesifik olarak sanallaştırma ortamları ile ilgili sorular var. Ancak 3.1.9.8 maddesi için kurumlardan (sanallaştırma güvenliği boyutuyla) istenen hususun ne olduğunu tam olarak anlayamadık. Bu maddenin altında yer aldığı başlıkta bir hata olabilir mi? Yeri doğru ise bu maddenin "sanallaştırma güvenliği" açısından ne şekilde anlaşılması gerektiği konusunda ilave açıklama yapabilir misiniz?		
CBDDO Tarafından Yapılan Açıklama		
Test ortamı ile operasyonel ortamların birbirlerinden ayrılması Bilgi ve İletişim Güvenliği Rehberi'nin farklı bölümlerinde de ele alınan önemli bir tedbir adımıdır. Rehber'in diğer bölümlerinde de; operasyon ve test ortamlarında farklı sunucuların kullanılması, test ortamında gerçek verilerin tutulmaması, operasyon ve test ortamına ait sunucuların yer aldığı ağlara yönelik segmentasyonun sağlanması, kullanılıyorsa veri tabanının veri tabanı yönetim sistemi ve kullanıcı seviyesinde izole edilmesi gibi tedbirler ele alınmıştır. Test ortamları, yapılan değişiklikler ile operasyon ortamlarının performansının etkilenmemesi, erişilebilirliğinin devamı, güvenlik zafiyetlerinin ve yazılımsal hataların önceden tespiti ve engellenmesi, operasyona geçilmeden önce iş tanımının beklentilerinin karşılanıp karşılanmadığının test edilmesi gibi bir çok nedenler ile kullanılmaktadır. Dolayısı ile operasyon ortamlarından farklı olarak üzerinde birçok test amaçlı değişikliğin gerçekleştiği, güvenlik boyutu ile ayrıca ele alınması gereken ortamlardır. Bilindiği üzere birçok kurum altyapısında operasyon ve test amaçlı kullanılacak sunucu ve sistem ortamları fiziksel kaynaklardan sanal kaynaklara doğru evrilmiştir. Bu nedenle test ve operasyon sanal ortamlarının güvenliği için alınacak temel tedbirlere sanallaştırma güvenliği altında da yer verilmiştir. Bu doğrultuda bahsi geçen tedbir kapsamında; sanallaştırma sistemlerinde yer alan test ve operasyonel ortamlar için kaynak yönetimi planlanmalıdır. Test ortamı ve operasyonel ortam için aynı kaynak kullanımı politikalarının bulunması ve eşit kaynak tahsisi operasyonel ortamdaki hizmet sürekliliğini olumsuz olarak etkileyebilecektir. Bu yüzden test ortamı için belirli bir kaynak limitinin bulunması, operasyonel ortamda ihtiyaç duyulacak kaynak gereksinimlerinin		

karşılanmasında olası problemleri önleyecektir. Benzer şekilde sanallaştırma ortamının yedekliliği veya felaket kurtarma gibi durumlarda operasyonel ortam önceliklendirilmeli, operasyonel ortam için yedeklilik ve iş sürekliliği gereksinimleri sağlandıktan sonra test ortamına yönelik faaliyetler gerçekleştirilmelidir.

Tarih	Şubat 2021	SSS No:6
Konu/Rehber Maddesi	Arka Kapı Taahhütnamesi	

CBDDO'ya Sorulan Soru

CBDDO tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberinin 3.2.6.3 numaralı maddesinde "**Tedarik edilen veya hizmet alımı ile geliştirilen uygulamalar için yazılımın kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) içermediğine/içermeyeceğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde (örneği Rehber'in EK.C-6'sında verilen) taahhütname alınmalıdır**" ifadesi yer almaktadır.

Aynı konu Cumhurbaşkanlığı tarafından yayımlanan 2019/12 sayılı Genelge'de "**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"** şeklinde ifade edilmiştir.

Rehber'in EK.C-6'sında verilen Taahhütname Örneğinde; arka kapı "**uygulama yazılımı, donanım ve işletim sistemleri veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistemlerde mevcut güvenlik önlemlerini aşarak erişim sağlamak üzere özel olarak tasarlanan ve/veya kasıtlı olarak dâhil edilmiş boşluklar veya güvenlik açıkları**", ürün ise "**kurum tarafından tedarik edilmesi planlanan uygulama yazılımı, donanım, işletim sistemi veya bu bileşenlerin bir ya da birkaçını üzerinde barındıran cihaz/sistem**" olarak tarif edilmiştir.

Yukarıda yer alan hususlar hep birlikte değerlendirildiğinde her ne kadar Rehber'in 3.2.6.3 maddesinde sadece "**uygulamalar ve yazılımlar**" için taahhütname alınması istenmiş gibi bir algı oluşmakla beraber aslında taahhütnamenin sadece "**kuruma özgü olarak geliştirilen yazılımları**" değil "**üzerinde arka kapı bulunması muhtemel herhangi bir yazılım çalışan her türlü cihaz (appliance), donanım ve sistemi**" kapsadığını anlamaktayız.

Bu doğrultuda aşağıdaki hususların sizden teyidini beklemekteyiz;

Kuruma özgü yazılım geliştirme işlemleri ve salt lisans alımları da dâhil üzerinde arka kapı bulunması muhtemel (işletim sistemleri dahil) herhangi bir yazılım çalışan her türlü cihaz (appliance), donanım ve sistem alımlarında bahse konu taahhütnameyi isteyecek miyiz?

1. 2019/12 sayılı Genelge'de yer alan "**imkanlar ölçüsünde**" ifadesini; "taahhütname öncelikle üreticiden, üreticiden alınamıyorsa dağıtıcıdan, her ikisinden de alınamıyorsa tedarikçiden alınacaktır" şeklinde mi anlamalıyız?
2. Genellikle bir alım içinde farklı üreticilere ait birden fazla ürün tedariki yapıldığı dikkate alındığında, eğer taahhütname ilgili ürünlerin üreticisinden veya dağıtıcısından alınamıyorsa, tedarikçiden "tüm ürünleri kapsayacak tek bir taahhütname" alınması yeterli olacak mıdır? Yoksa her bir ürün için ayrı ayrı taahhütname istenmesi mi gerekir?
3. Genellikle bir alım içinde farklı üreticilere ait birden fazla ürün tedariki yapıldığı dikkate alındığında, eğer taahhütname ilgili ürünlerin üreticisinden veya dağıtıcısından alınamıyorsa, tedarikçiden "tüm ürünleri kapsayacak tek bir taahhütname" alınması yeterli olacak mıdır? Yoksa her bir ürün için ayrı ayrı taahhütname istenmesi mi gerekir?

CBDDO Tarafından Yapılan Açıklama

Sorularınıza ilişkin değerlendirmemiz aşağıda yer almaktadır.

1. Sorunuz: Üzerinde arka kapı bulunması muhtemel uygulama ve yazılım içeren tüm bileşenler için taahhütname istenmelidir.
2. Sorunuz: "imkânlar ölçüsünde" ifadesi; kurumun tedarik sürecinde karşılaşabileceği olası farklı durumları işaret ekmektedir. "Taahhütname öncelikle üreticiden, üreticiden alınamıyorsa dağıtıcıdan, her ikisinden de alınamıyorsa tedarikçiden alınmalıdır" yaklaşımını da bu durumlardan biri olarak değerlendirmek mümkündür.
3. Sorunuz: Tüm ürünleri kapsayacak tek bir taahhütname alınması da yeterli olacaktır.

Tarih	Mart 2021	SSS No:7
İlgili Rehber Madde(s)(ler)i	Erişim Kayıtlarının Aktarımı	
CBDDO'ya Sorulan Soru		
Bakanlığımızda kişisel veriler ağırlıklı olarak (uygulamalar üzerinden erişilebilecek şekilde) veri tabanlarında saklanmaktadır. Veri tabanlarında tutulan verilere yapılan erişimler için uygulama ve veri tabanı (audit mekanizmaları) seviyesinde ayrı ayrı iz kayıtları alınmaktadır. Ayrıca sunucu, orta katman ve ağ cihazları düzeyinde de bazı iz bilgileri tutulmakta ve saklanmaktadır. Farklı seviyelerde tutulmakta olan iz bilgileri depolama vb. amaçlı olarak farklı araçlar kullanılmak suretiyle üretildikleri ortamlardan daha farklı ortamlara aktarılabilmektedir (dışarı aktarım). CBDDO Rehberi 4.1.2.4 maddesi incelendiğinde erişim kayıtlarının "dışarı" ve "içeri" aktarılmasından bahsedilmekte ve özellikle "içeri aktarım" için dikkat edilmesi gerek ilave kriterler (mevcut kayıtları yok etmeme veya değiştirmeme) bulunmaktadır. Rehberin bu maddesinde yer alan "içeri aktarma" işleminden ne kastedildiği konusunda daha ayrıntılı açıklama ihtiyacı olduğu değerlendirilmiştir.		
CBDDO Tarafından Yapılan Açıklama		
Sorunuza ilişkin değerlendirmemiz aşağıda yer almaktadır: Kurum ve kuruluşların bilgi güvenliği gereksinimlerine uygun olarak uygulamalara ilişkin erişim kayıtları belirli aralıklarla yedekleme ya da arşivleme amacıyla dışa aktarılmaktadır (export). Bu kayıtlara canlı sistem üzerinden tekrar erişim sağlanmak istendiğinde genellikle içeri aktarım (import) mekanizması kullanılmaktadır. 4.1.2.4 maddesinde bahsi geçen içeri aktarım işlemi, yedeklenen veya arşive alınan erişim kayıtlarının geri döndürülmesi ve canlı sistem üzerinden erişilebilir olmasıdır. Tedbir maddesinin amacı, yapılan içe aktarım işleminin mevcut erişim kayıtları üzerinde herhangi bir bozulmaya (güncelleme, silme veya üzerine yazma gibi) neden olmamasını sağlamaktır.		

Tarih	Nisan 2021	SSS No:8
İlgili Rehber Madde(s)(ler)i	Web Sunucusu Sıkılaştırma Tedbirleri Arasında Yer Alan İki Madde İçin İlave Açıklama	

CBDDO'ya Sorulan Soru

Başkanlığınız tarafından yayımlanan CBDDO Bilgi ve İletişim Güvenliği Tedbirleri Rehberinin aşağıda yer alan iki maddesi için ilave bilgi açıklama ihtiyacımız bulunmaktadır.

Bu iki madde kapsamında beklentinin tam olarak ne olduğunun daha açık olarak ifade edilmesinin uygun olacağı değerlendirilmektedir.

5.3.1.18 Burada kastedilen "özel anahtar" nedir? Sunucu tarafı SSL sertifikasının özel anahtarı mı? Yoksa başka bir bileşen mi?

5.3.1.20 Sunucuya IP adresi üzerinden yapılan erişimden ne kastedildiği tam olarak anlaşılamamıştır? Buradaki erişimin kim tarafından, ne maksatla yapılan erişim olduğu daha açık olarak yazılır ise daha uygun olacaktır.

CBDDO Tarafından Yapılan Açıklama

1. Soru

Tedbir 5.3.1.18 - Burada kastedilen "özel anahtar" nedir? Sunucu tarafı SSL sertifikasının özel anahtarı mı? Yoksa başka bir bileşen mi?

Cevap

İlgili tedbir maddesinde bahsedilen özel anahtar, sunucu üzerinde hizmet veren uygulamalara ait SSL sertifikalarına ait özel anahtarlardır. İlgili tedbir maddesi sunucu üzerinde bulunan tüm sertifikalara ait özel anahtarlar için uygulanmalıdır. Özel anahtarların ele geçirilmesi uygulamalar ile kullanıcılar arasında yapılan tüm iletişimin görüntülenebilmesine neden olacağı için, bu anahtarların korunması kritik öneme sahiptir. Bu amaçla dosya izninin kısıtlanması, özel anahtara erişimde güçlü parolaların kullanılması ve bu parolanın farklı bir sistemde güvenli bir şekilde saklanması gibi güvenlik kontrolleri uygulanmalıdır.

2. Soru

Tedbir 5.3.1.18 - Sunucuya IP adresi üzerinden yapılan erişimden ne kastedildiği tam olarak anlaşılamamıştır? Buradaki erişimin kim tarafından, ne maksatla yapılan erişim olduğu daha açık olarak yazılır ise daha uygun olacaktır.

Cevap

Sunucuya IP adresi üzerinden erişimden kasıt, sunucuya erişirken kullanılan URL içerisinde alan adı yerine doğrudan IP adresinin kullanılmasıdır. Günümüzde zararlı yazılımlar ve otomatik ağ tarama araçları, daha kolay otomatize edilebilmesi nedeniyle alan adı yerine daha çok IP adresi kullanmaktadır. Web sunucusuna IP adresi üzerinden erişimin engellenmesi ile bu tür otomatize araçların erişimi engellenecektir. Her ne kadar bu kontrol tek başına zararlı yazılımların yayılmasına veya otomatize araçların çalıştırılabilmesine tamamen engel olamayacaksa da, önemli bir savunma katmanı oluşturacaktır. Bu yüzden erişimin kimin tarafından ve ne amaçla yapıldığına bakılmaksızın, web sunucusuna IP adresi üzerinden yapılan erişimler engellenmelidir.

Tarih	Haziran 2021	SSS No:9
İlgili Rehber Madde(s)(ler)i	Personel Varlık Grubu Altında Yer Alan Varlıklara EK-C1 Anketin Uygulanması	
CBDDO'ya Sorulan Soru		
CBDDO Bilgi ve İletişim Güvenliği Rehberi kapsamında yapmış olduğumuz çalışmaları gözden geçirirken bir konu ile ilgili olarak sizlerden yeniden görüş alma ihtiyacı hissettik. Çalışmalara ilk başladığımızda **Varlık Gruplarını ve Kritiklik Derecelerini** belirlerken, ayrıntılı olarak varlık alt gruplarımızı belirledik ve sonrasında EK-C1'deki anket sorularını bu varlık alt grupları için yanıtlamaya çalıştık. Ancak ankette yer alan soruları, personel varlıklarına tam olarak uyarlayamadığımız için tersten gittik ve Rehberin 3.5 (Personel Güvenliği) bölümü altındaki tedbirlerin hangilerini, personel varlık gruplarımızda uygulayabiliyoruz diye baktık. Sonuçta 3.5 altında yer alan tedbirlerin **iki tanesi hariç** tamamı birinci seviye tedbir olduğu ve tüm personele zaten bu tedbirlerin uygulanması gerektiğinden hareketle, PERSONEL VARLIK GRUBU için ayrıca EK-C1'deki anketi uygulamadık. Yaptığımız bu işlem ile ilgili herhangi bir yorumunuz olabilir mi?		
CBDDO Tarafından Yapılan Açıklama		
Personel varlık grubu ana başlığı altındaki varlıklara 3.5.2.3 ve 3.5.3.10 tedbirlerini uygulamayı öngörüyorsanız anketi uygulamanıza gerek olmayacaktır.		

Tarih	Haziran 2021	SSS No:10
İlgili Rehber Madde(s)(ler)i	4.1.3.5 Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması	
CBDDO'ya Sorulan Soru		
Bilgi ve İletişim Güvenliği Tedbirleri Rehberi'nin 4.1.3.5 maddesinde "Çok Faktörlü Kimlik Doğrulama Mekanizmasının Kullanılması" başlıklı bir gereksinim var ve gereksinimin açıklamasında "Özel nitelikli kişisel verilerin tutulduğu ortamlara erişim için çok faktörlü kimlik doğrulaması yapılmalıdır" denilmektedir. Malum olduğu üzere "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 Kararında; "özel nitelikli kişisel verilerin işlendiği, muhafaza edildiği ve/veya erişildiği ortamlar elektronik ortam ise ve verilere uzaktan erişim gerekiyorsa en az iki kademeli kimlik doğrulama sisteminin sağlanması" istenmektedir. Bu şartlarda 4.1.3.5 maddesini, sadece uzaktan yapılan erişimler için mi dikkate alacağız? Yoksa örneğin özel nitelikli kişisel verilerin işlendiği bir uygulamaya (hastanelerimizdeki HBYS yazılımlarının tamamı bu şekildedir) yerel alan ağından erişen son kullanıcılar için de çok faktörlü kimlik doğrulama yapılması gerekir.		
CBDDO Tarafından Yapılan Açıklama		
Özel nitelikli kişisel verilerin Rehber kapsamında kritik bilgi/veri kategorisinde değerlendirilmesi sebebiyle, 4.1.3.5 maddesi uyarınca bu tür verilere yapılacak tüm erişimlerde çift faktörlü kimlik doğrulama mekanizmasının tesis edilmesi gerekmektedir. Rehber 3.2.1.10 maddesi de ilgili maddeyi destekleyici niteliktedir.		

Tarih	Temmuz 2021	SSS No:11
İlgili Rehber Madde(s)(ler)i	4.4. Kripto Uygulamaları Güvenliği Başlığı Altında Yer Alan Konular	
CBDDO'ya Sorulan Soru		
Rehber'in 4.4 Kripto Uygulamaları Güvenliği başlığı altında yer alan gereksinimleri incelediğimizde, bu başlıkların daha çok "**Kamu Kurum ve Kuruluşları İle Gerçek ve Tüzel Kişilerin Elektronik Haberleşme Hizmeti İçinde Kodlu veya Kriptolu Haberleşme Yapma Usul ve Esasları Hakkında Yönetmelik**" kapsamında yer alan "**Türk Silahlı Kuvvetleri, Jandarma Genel Komutanlığı, Sahil Güvenlik Komutanlığı, Milli İstihbarat Teşkilatı Müsteşarlığı, Emniyet Genel Müdürlüğü ve Dışişleri Bakanlığı ile bu kurumlara ait kodlu veya kriptolu elektronik haberleşme sistemlerinin kullanıldığı kamu kurum ve kuruluşları ile gerçek ve tüzel kişileri**" ilgilendirdiğini; Bakanlığımız gibi özel olarak kodlu ve kriptolu haberleşme yapmayan kurumlar için bu maddede yazan hususların nerede ise tamamına yakınının uygulanabilir olmadığını değerlendirdik. Bakanlık olarak hiçbir özel kripto cihaz veya sistemi kullanmıyoruz. Elbette kullandığımız yazılım ve sistemlerde birçok kriptografik işlem gerçekleştiriyoruz ama bu işlemlerin tamamı hazır ticari ürünler içinde yer alan yetenekler ile yapılıyor. Sadece varlık olarak düşünecek olur isek elimizde "SSL Sunucu Sertifikaları" ve e-imza işlemlerinde kullanılan "USB Token" gibi aparatlar var. Rehber'in diğer bölümlerinde, hazır ticari ürünler kullanılarak yapılan kriptografik işlemler için uygulanabilecek şekilde (bir kısmı aşağıda imza blokunun altında sıralanmıştır) birçok madde var. GAP analizlerimizi yaparken zaten bu maddeleri dikkate aldık. Bakanlık olarak CBDDO Rehberi yayımlanmadan önce de kullandığımız Sağlık Bakanlığı Bilgi Güvenliği Politikaları Kılavuzumuz var. Kılavuzun KRİPTOGRAFİK KONTROLLERİN KULLANIMI başlıklı 7'nci bölümünde birçok konu için (Kriptografik Politikalar, Kriptografik Araç ve Yöntemler, Algoritma ve Anahtar Uzunlukları, Web Trafiği Güvenliği, FTP İşlemleri Güvenliği, Uzaktan Yönetim Faaliyetleri, Sabit Ortamdaki Verilerin Şifrelenmesi vb.) standartlarımızı önceden ortaya koymuştuk. Kılavuzun tamamını da bu günlerde CBDDO Rehber gereksinimleri açısında yeniden gözden geçiriyoruz. **Sonuç olarak; Rehberin diğer bölümlerde aşağıda sıralandığı şekilde doğrudan bilgi varlıklarına uygulanması gereken bir çok madde varken; Bakanlık olarak "özel kodlu veya kriptolu haberleşme" yapmadığımızı da dikkate alırsak, Rehber'in 4.4 Kripto Uygulamaları Güvenliği başlığı altında yer alan gereksinimler için ayrıca bir analiz yapmaya ihtiyacımız var mı? Yoksa bu bölümde yer alan konuları; sadece 4.4.1.1, 4.4.1.2, 4.4.2.19 (E-İmza özel anahtarları ve SSL Sunucu sertifikaları açısından), 4.4.3.1 ve 4.4.3.4 numaralı gereksinimler için incelesek, diğer maddeler için UD (uygulanabilir değil) desek yanlış mı yapmış oluruz?**		
CBDDO Tarafından Yapılan Açıklama		
FTP, SMTP, http gibi protokollerin güvenli haberleşmesi için kullanılan SSL/TLS şifrelemesi 4.4. Kripto Uygulamaları Başlığı altında ele alınmamaktadır. SSL/TLS şifrelemesi kullanan web uygulamaları gibi varlıklar için 4.4 başlığı altında herhangi bir analiz çalışması yapmanıza gerek yoktur. Bu başlıktaki tedbirler bu nitelikteki varlıklar için ele alınmayacaktır. Ancak HSM cihazı, özel kodlu veya kriptolu elektronik haberleşme sistemleri, e-imza gibi uygulama ve cihazların kullanımı durumunda bahsi geçen ana başlıkta yer alan tedbirlerin uygulanabilirliğine yönelik analiz faaliyetleri gerçekleştirilmelidir.		

Tarih	Ağustos 2021	SSS No:12
İlgili Rehber Madde(s)(ler)i	2.1.4. Rehber Uygulama Yol Haritasının Hazırlanması	

CBDDO'ya Sorulan Soru

Rehberin "Rehber Uygulama Yol Haritasının Hazırlanması" başlıklı 2.1.4 maddesinde "boşluk analizi sonucunda tespit edilen eksikliklerin giderilmesi için gereken faaliyetler belirlendikten sonra planlama yapılması, Yapılacak çalışmalar belirlendikten sonra her çalışma için 2-3 aylık dönemler halinde hedefler belirlenmesi ve uygulama yol haritası kapsamında yapılan planlamaların EK-C.4'te yer alan form ile kayıt altına alınması" öngörülmektedir.

Rehberde yer alan "Rehberin Uygulanması" ve "Kurum BGYS süreçleri ile ilişkileri" hakkında maddeler incelendiğinde;

1.2 maddesinde "Rehber uygulama süreci, bilgi güvenliği yönetim süreçlerine alternatif olarak uygulanacak bir süreç olarak hazırlanmamış olup mevcut bilgi güvenliği yönetim süreçlerine teknik olarak katkı sağlayacak tedbirleri ve faaliyetleri içermektedir. **Kurumlar rehber uygulama süreci ile tanımlanan faaliyetleri, mevcut bilgi güvenliği yönetim süreçleri kapsamında ve uyarlama yaparak yürütmelidir."**

- 1.3 maddesinde "Kurumlar rehber uygulama sürecini, **yürüttükleri bilgi güvenliği yönetim süreçlerine entegre etmeli** ve bilgi güvenliği risk yönetimi faaliyetleri kapsamında rehberde tanımlanan tedbirleri uygulamalıdır."

şeklinde açıklamalar yer almaktadır.

Sağlık Bilgi Sistemleri Genel Müdürlüğü olarak 2014 yılından beri uygulamakta olduğumuz (kapsamı Genel Müdürlüğümüz faaliyetleri olan) bir ISO 27001 BGYS'miz var. BGYS'nin kapsamı Genel Müdürlüğümüz olmakla beraber, BT Hizmetlerinin sunumunun büyük bir kısmı merkezi olarak Genel Müdürlüğümüz tarafından yapıldığı için alınan tedbirler başta merkez teşkilat birimlerimiz olmak üzere tüm Bakanlığımızı da içine almaktadır.

Bu kapsamda Rehber'de yer alan tedbirler için boşluk analizlerini yaptığımız zaman eksik olarak tespit edilmiş konuların önemli bir kısmı için zaten halihazırda açılmış bir Düzeltici Faaliyet" veya "Takip Edilen Risk" bulunduğu ve eksikliklerin DF ve Risk İşleme faaliyetleri kapsamında zaten yönetilmekte (takip edilmekte) olduğunu gördük. Bu doğrultuda, Rehberin 1.2 ve 1.3 maddesinde yer alan açıklamalar uyarınca (amacı eksiklikler için planlama yapılması ve takibinin sağlanması olan) EK-C.4 formların doldurulması yerine, eksikliklerin (zaten yıllardır yaptığımız şekilde) BGYS süreçlerimiz içerisinde var olan DF ve Risk Yönetimi süreçleri ile takip edilmesinin uygun olacağını değerlendirdik. **Böylece Rehber Uygulama süreçlerini, BGYS Süreçlerine uyarladık ve her ikisini birbiri ile entegre etmiş olduk**. Aksini yapmış olsaydık benzer işler için iki ayrı süreç yaratmış olacak ve Rehberden kaynaklanan eksiklikleri (ki bunların çok büyük bir kısmı zaten BGYS süreçlerinde de tespit edilen ve takip edilen hususlardır) kağıt ortamlarda takip ederek gereksiz bürokratik süreçler yaratmış olacaktık.

Tabi ki boşluk analiz formlarına bir açıklama sütunu açarak, CBDDO Rehberinin izlenebilirliğini sağlamak maksadıyla, tespit edilen eksikliklerin hangi DF veya Risk ile takip edildiğini de kayıt altına aldık.

Yukarıda yapılan açıklamalar doğrultusunda size sormak istediğimiz husus şu şekildedir**: Yaptığımız işlem Rehber Uygulama süreçleri açısından uygun mudur? Hazırlık safhasının son aşaması olan yol haritasının belirlenmesi aşaması için mutlaka ayrıca Ek.C-4'te yer alan formların doldurulması zorunlu mudur?**

CBDDO Tarafından Yapılan Açıklama

BGYS ve BG Rehber uygulama sürecini e-postanızda bahsettiğiniz şekilde entegre olarak yürütmeniz bilgi güvenliği hususundaki benzer faaliyetlerin iki ayrı süreç olarak yürütülmemesi açısından doğru olarak atılmış bir adımdır.

EK – C.4 Rehber Uygulama Yol Haritası Belirleme Formu, mevcut durum ve boşluk analizi kapsamında yapılan çalışmalar göz önünde bulundurularak yapılması gereken iş paketlerini kayıt altına almak üzere oluşturulmuştur. Bahsi geçen form, eksikliklere yönelik uygulanacak düzeltici ve iyileştirici faaliyetlerin ya da risk yönetim süreçleri ile sağlanacak takip işlemlerinin kayıt altına alınması amacı taşımamaktadır. Dolayısıyla formun doldurulması, Kurum'a Rehber uyum faaliyetleri ile ilgili iş planlarını yazılı hale getirme ve buna istinaden gerekli kaynakları ayırma noktasında fayda sağlayacaktır.

Tarih	Kasım 2021	SSS No:13
İlgili Rehber Madde(s)(ler)i	3.1.12.13 Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması	
CBDDO'ya Sorulan Soru		
Rehber'in "3.1.12.13 Kimlik Yönetim ve Doğrulama Sistemlerinin Envanterinin Tutulması" maddesinde yer alan tedbir, "**Yerel veya uzak servis sağlayıcılarında bulunanlar da dâhil olmak üzere, kurumun tüm kimlik doğrulama sistemlerinin ve bu sistemlerle entegre uygulamaların envanteri tutulmalıdır**." şeklinde tanımlanmıştır. Bakanlık merkez teşkilat birimleri olarak sistem ve uygulamalarımız için temel kimlik doğrulama altyapısı olarak "merkezi kimlik doğrulama servisi" kullanıyoruz. Bu servis de aslında kendi içinde bir uygulama. Kimlik doğrulama işlevi 1) E-devlet, 2) Kurum Aktif Dizin Sunucusu, 3) E-İmza, 4) Mobil İmza, 5) TC Kimlik kartı ile yapılıyor ve kimliği doğrulanan kullanıcılar erişim ve yetki kontrolleri için ilgili uygulamalara yönlendiriliyor. Teknik nedenlerle merkezi kimlik doğrulama servisini kullanamayan bazı uygulamalarımız doğrudan Aktif Dizin üzerinden kimlik doğrulması yapıyor veya kendi içinde yer alan kullanıcı adı ve parolaya dayanan kimlik doğrulama mekanizmalarını kullanıyorlar. Elimizde, 1) Merkezi kimlik doğrulama servisi ile entegre çalışan, 2) Aktif Dizine erişip doğrulama yapan ve 3) Kendi kimlik doğrulamasını kendisi yapan uygulamaların ayrı ayrı listeleri mevcut. Bu şartlar altında 3.1.12.13 maddesinin gereğini yaptığımızı düşünebilir miyiz? Yoksa bu madde için başkaca bir çalışma yapmak gerekir mi?		
CBDDO Tarafından Yapılan Açıklama		
E-postanızda bahsettiğiniz tüm kimlik doğrulama sistemleri ve bunlarla ilişkili uygulamaları içeren bir envanter listesi oluşturulduğu durumda 3.1.12.13 maddesinin gereği sağlanmış olacaktır.		

Tarih	Kasım 2021	SSS No:14
İlgili Rehber Madde(s)(ler)i	Beyaz Liste Yönetimi	

CBDDO'ya Sorulan Soru

CBDDO Bilgi ve İletişim Güvenliği Tedbirleri rehberine **uygulamalar için** "Beyaz Liste" yönetimi ile ilgili olarak;

1. 3.1.1 Donanım Varlıklarının Envanter Yönetimi başlığı altında, 3.1.2.7 maddesinde **3'ncü seviye tedbir olarak** "Kurumun uygulama beyaz liste yönetimi, kurum onaylı beyaz liste yazılımları kullanılarak yapılmalıdır. Ayrıca yalnızca onaylı yazılım kütüphanelerinin (* .dll, * .ocx, * .so vb.) yüklenmesine izin vermelidir. Kurumun uygulama beyaz liste yönetimi, yalnızca onaylı ve dijital olarak imzalanmış betik dosyalarının (* .ps1, * .py, makrolar vb.) ilgili sistemde çalışmasına izin vermelidir",
2. 3.1.3. Tehdit ve Zafiyet Yönetimi başlığı altında, 3.1.3.2 maddesinde **1'nci seviye tedbir olarak** "Zararlı yazılımların kuruma ait ve/veya kurum tarafından yönetilen kullanıcı uç nokta cihazları ve altyapı bileşenleri üzerinde çalışmasını, kaydedilmesini ve aktarılmasını engellemek için politikalar/prosedürler tanımlanmalı ve işletilmelidir. Personelin beyaz listede bulunan uygulamalar haricinde uygulama kurmasının engellenmesine yönelik politika/prosedür oluşturulmalıdır. Politika/prosedürün uygulanmasını temin etmek üzere gerekli teknolojik altyapılar ve uyarı mekanizmaları aktif edilmelidir."
3. 3.1.3. Tehdit ve Zafiyet Yönetimi başlığı altında, 3.1.3.5 maddesinde **1'nci seviye tedbir olarak** "Son kullanıcıların, güvenlik sıkılaştırmaları kapsamında kurum tarafından uygulanması gerekli görülen konfigürasyonlara müdahale etmemesi ve beyaz listede bulunan programlar haricinde program kurmalarının engellenmesi için son kullanıcı hesaplarının yerel yönetici yetkileri kaldırılmalıdır."

şeklinde üç farklı gereksinim bulunmaktadır.

Bu üç madde hep birlikte değerlendirildiğinde;

1. Uygulamalar için beyaz liste yönetimini hangi seviye tedbir olarak değerlendirmek gerekir?
2. Yapılan anket sonucunda kritiklik seviyesi 1 (düşük) olarak belirlenmiş bir ağ ve BT sistemi dikkate alındığında;
    a. Kurumdaki son kullanıcı bilgisayarlarının etki alanında çalıştığı,
    b. Etki alanında yer alan bilgisayarlara, kurum bilişim teknik destek ekipleri tarafından standart (kurum tarafından belirlenmiş olan kısıtlı sayıda) yazılım kurulumu yapıldığı,
    c. Yerel yönetici yetkisinin kontrollü olarak (kısıtlı sayıda) kullanıcıya verildiği,
    d. Etki alanında bulunan cihazlarda zararlı yazılımlardan korunmak için güncel uç nokta güvenlik yazılımı kullanıldığını düşünürsek,

ayrıca beyaz liste yönetimi yapmak gerekli midir?

CBDDO Tarafından Yapılan Açıklama

1- 3. seviye olan 3.1.2.7 tedbir maddesinde belirtilen "Kurumun uygulama beyaz liste yönetimi, kurum onaylı beyaz liste yazılımları kullanılarak yapılmalıdır." ifadesi, bir "beyaz liste yönetim yazılımı" kullanılarak beyaz liste yönetimi yapılması durumunu belirtmektedir. Uygulamalar için beyaz liste yönetimi yapılması birinci seviye bir tedbirdir.

2- Kullanıcıların hangi programları yüklediğinin, hangi uygulamaları kullandığının bilinmesi ve kontrol edilmesi saldırı yüzeyinin tespit edilmesi için gereklidir. Belirttiğiniz şekilde önlemler alınsa da beyaz liste yönetiminin yapılması gereklidir.

Tarih	Kasım 2021	SSS No:15
İlgili Rehber Madde(s)(ler)i	4.3.1.12 Güvenli Veri Depolama Politikasının Uygulanması	

CBDDO'ya Sorulan Soru

CBDDO Bilgi ve İletişim Güvenliği Rehberi'nin Bulut Bilişim Güvenliği ile ilgili maddeleri altında "**4.3.1.12 Güvenli Veri Depolama Politikasının Uygulanması** " şeklinde bir tedbir bulunmaktadır. Tedbirin tanımı "**Bulut bilişim hizmeti sunacak servis sağlayıcının veri güvenliğini (ifşa, değiştirme, bozulma vb. durumlara karşı) sağlamak adına güvenli veri depolama politikası bulunmalıdır**" şeklinde yapılmış ve denetim soru önerisi olarak "**Bulut bilişim hizmet sağlayıcı tarafından güvenli veri depolama politikası hazırlanmış mıdır? Politika düzenli olarak gözden geçirilmekte midir? Politikanın ihlali durumunda hangi prosedür işletilmektedir**?" şeklinde kriterler belirlenmiştir.

Bakanlık olarak henüz bulut bilişim hizmeti almamakla birlikte kısa/orta vadede bazı projeler kapsamında bir kısım paydaşlarımızı bulut bilişim hizmet sağlayıcılara yönlendirmeyi planlıyoruz. Bu kapsamda konuyla ilgili detaylı çalışma yaparken, tedbirde yazılmış olan "**Güvenli Veri Depolama Politikası**"nın içeriğinde nelerin olması gerektiği konusunda tereddüt yaşadık. Güvenli Veri Depolama Politikası, ISO 27001 BGYS Standardı içinde yer alan zorunlu dokümanlar içerisinde de yer alan bir konu değil. Bu nedenle önümüzde bir örneği de yok. Bu Politika'nın belki de bulut bilişim hizmetlerine özgü özel bir gereksinim olabileceğini düşündük. Gerçi tedbirin tanımında "**verilerin ifşası, değiştirilmesi, bozulması gibi durumlar için alınması gereken güvenlik tedbirleri**" şeklinde bir ipucu bulunmakla birlikte, bu politikanın içeriğine yönelik daha detaylı kriterlerin ortaya konulmasına ihtiyaç olduğunu değerlendirdik.

Sonuç olarak Bulut Bilişim Hizmet Sağlayıcılar tarafından, kendisinden hizmet alan Rehber kapsamında yer alan kuruluişara "**Güvenli Veri Depolama Politikası**" adı altında farklı içerikte politikalar sunabileceği dikkate alındığında; bu politikadan ne anlaşılması gerektiği konusunda biraz daha detaylı bilgiye ihtiyaç duymaktayız.

CBDDO Tarafından Yapılan Açıklama

Güvenli Veri Depolama Politikası ile ilgili; ISO/IEC 27001 ve ISO/IEC 27002'nin "15.1.2 Tedarikçi anlaşmalarında güvenliği ifade etme" kontrol maddesi ile ISO/IEC 27017'nin "6.1.1 Bilgi güvenliği rolleri ve sorumlulukları" maddesinden faydalanılabilir. Aşağıda ilgili maddelerde yer alan ve Güvenli Veri Depolama Politikasında bulunmasının yerinde olacağı değerlendirilen hususlara yer verilmiştir. Kurumun bilgi güvenliği gereksinimleri doğrultusunda ilgili maddelerde yer alan hususlar geliştirilmeye açıktır.

· Kuruluşun bilgisine erişebilen, bunu işletebilen, depolayabilen, iletebilen veya kuruluşun bilgisi için bilgi teknolojileri altyapı bileşenlerini temin edebilen tedarikçilerin her biri ile anlaşılmalı ve ilgili tüm bilgi güvenliği gereksinimleri oluşturulmalıdır.

· Tespit edilen bilgi güvenliği gereksinimlerini karşılamak amacıyla anlaşmalara dâhil edilmesi için aşağıdaki şartlar dikkate alınmalıdır:

a) Sağlanacak ya da erişilecek bilginin tanımı ve bilgi sağlama ve erişim yöntemleri,

b) Kuruluşun bilgi sınıflandırma düzenine uygun bilgi sınıflandırması gerekirse kuruluşun kendi sınıflandırma düzeni ve tedarikçi sınıflandırma düzeni arasındaki eşleştirme,

c) Veri koruma, fikri mülkiyet hakları ve telif hakları dâhil yasal ve düzenleyici gereksinimler ve bunların nasıl karşılandığının açıklaması,

d) Erişim kontrolü, performans gözden geçirme, izleme, raporlama ve denetimi içeren üzerinde anlaşılmış bir kontrol kümesini uygulamak için her bir sözleşme tarafının yükümlülükleri,

e) Bilginin kabul edilebilir kullanıma dair kurallar,

f) Kuruluşun bilgisine erişmek veya almak için yetkili tedarikçi personelinin açık listesi ya da tedarikçi personeli tarafından kuruluşun bilgisine erişmek ve almak amacıyla yetkilendirme ve yetkilendirilmenin kaldırılması için prosedürler ya da şartlar

· Tüm varlıkların sahipliği ve bu varlıklarla ilişkili yedekleme ve kurtarma faaliyetleri gibi operasyonlar için sorumlulukları olan taraflar tanımlanmalı ve dokümante edilmelidir. Aksi takdirde bulut hizmeti sağlayıcısının, bu hayati görevleri bulut hizmeti müşterisinin yürüttüğünü varsayma riski doğar (veya tam tersi de olabilir) ve veri kaybı yaşanabilir.

Tarih	08.02.2022	SSS No:16
İlgili Rehber Madde(s)(ler)i	Güçlü Kimlik Doğrulama / Çok Faktörlü Kimlik Doğrulama	

CBDDO'ya Sorulan Soru

Kurumunuz tarafından yayımlanan Bilgi ve İletişim Güvenliği Rehberinin, özellikle hassas/kritik işlemlerin yapılması öncesinde kullanıcı kimliğinin doğrulanması için "**çok faktörlü kimlik doğrulaması yapılması**" öngörülmektedir. (3.1.4.18, 3.1.6.31, 3.1.6.34, 3.1.12.9, 3.1.12.11, 3.1.12.15, 3.1.14.7, 4.1.3.5)

Yine rehberin "Güçlü Kimlik Doğrulama Yöntemlerinin Desteklenmesi" başlıklı 3.2.1.10 nolu maddesinde hassas işlevler gerçekleştirilmeden önce "**yeniden kimlik doğrulama**, **daha güçlü bir mekanizmayla kimlik doğrulama**, **çok faktörlü kimlik doğrulama** veya **işlem imzalama"** gibi yöntemlerin uygulanması istenmektedir. Ancak bu yöntemlere ilişkin Rehber'in tanımlar bölümünde herhangi bir tanım yapılmamıştır.

KVKK tarafından yayımlanan bir Kamuoyu Duyurusunda (https://www.kvkk.gov.tr/Icerik/7073/BELEDIYELERE-ILISKIN-KAMUOYU-DUYURUSU) "*Bilindiği üzere, Kişisel Veri Güvenliği Rehberi (Teknik ve İdari Tedbirler) kapsamında kişisel verilere gerekmesi halinde uzaktan erişim için iki kademeli kimlik doğrulama kontrolünün uygulanması önerilmektedir. Bu kapsamda başkalarının kolayca ulaşabileceği örneğin kişinin TC kimlik numarası ve doğum günü bilgisinin sorgulanarak erişim imkânı veren sistemler **tek kademeli doğrulama** olarak kabul edilirken, kişinin TC kimlik numarasının yanı sıra kişiye özel oluşturulmuş şifre ya da kişinin daha önce bildirmiş olduğu telefon numarasına iletilen SMS kodu ile erişim sağlanan sistemler **iki kademeli doğrulama** olarak kabul edilmektedir.*" şeklinde bir tanım yapılmıştır.

Wikipedia'ya göre çok faktörlü kimlik doğrulamanın tanımı aşağıdaki gibidir. Buna göre iki kademeli doğrulama, aynı zamanda çok faktörlü doğrulama olarak tanımlanmaktadır.

1. Çok faktörlü kimlik doğrulma (MFA) bir bilgisayar kullanıcısına, kullanıcının kimlik doğrulama mekanizmasına başarılı bir şekilde **iki ya da daha fazla kanıt sağladığında** erişim sağlandığı bir kimlik doğrulama yöntemidir. (https://tr.wikipedia.org/wiki/%C3%87ok_fakt%C3%B6rl%C3%BC_kimlik_do%C4%9Frulamas%C4%B1)

2. Simple authentication requires only one such piece of evidence (factor), typically a password. For additional security, the resource may require more than one factor—multi-factor authentication, or two-factor authentication in cases where exactly two pieces of evidence are to be supplied. (Something the user has, Something the user knows, Something the user is, Somewhere the user is) (https://en.wikipedia.org/wiki/Multi-factor_authentication)

Yukarıdaki bilgiler doğrultusunda;

İki faktörlü kimlik doğrulama (örneğin Kurulun duyurusunda yer aldığı şekliyle *TC kimlik numarasının yanı sıra kişiye özel oluşturulmuş şifre*), Rehber'in bakış açısıyla çok faktörlü kimlik doğrulama olarak kabul edilebilir mi?

1. Rehbere göre çok faktörlü kimlik doğrulama için mutlaka bir üçüncü faktör (SMS vb.) mü olması gerekmektedir?
2. Rehber 3.2.1.10 maddesinin açıklamasında geçen "**daha güçlü bir mekanizmayla kimlik doğrulama**" ve "**çok faktörlü kimlik doğrulama**" arasındaki fark nedir? Daha güçlü kimlik doğrulama için ne gibi yöntemler kullanılabilir?

Biraz uzun bir soru oldu. Özellikle Kurul'un yukarıdaki kamuoyu duyurusu sonrasında kafamız biraz karıştı. Rehberin 3.2.1.10 maddesinde de güçlü kimlik doğrulama için farklı alternatifler sıralanınca bir kavram kargaşası oluşur gibi oldu. Bu doğrultuda yukarıdaki soruların yanıtları bizim için çok aydınlatıcı/yol gösterici olacaktır.

CBDDO Tarafından Yapılan Açıklama

a. Çok faktörlü kimlik doğrulama, doğrulanacak kimliğin iki veya daha fazla doğrulayıcı faktörle kontrol edilmesini ifade etmektedir. Dolayısıyla iki faktörlü kimlik doğrulama da çok faktörlü kimlik doğrulama olarak değerlendirilir. Kullanıcı adı olarak TCKN kullanılan uygulamalar için TCKN doğrulanacak öğedir, dolayısıyla doğrulayıcı bir faktör olarak değerlendirilemez. Kimlik doğrulama işleminde kullanıcı adı olarak alınan ve doğrulanan öğenin TCKN olması ve doğrulayıcı faktör olarak kişinin yalnızca kendisinin bildiği bir parolanın kullanılması, tek faktörlü kimlik doğrulama için verilebilecek bir örnektir. TCKN'nin doğrulanan öğe konumunda kullanıldığı durumda çok faktörlü kimlik doğrulama mekanizmasından bahsedebilmek için, yaygın biçimde birincil doğrulama faktörü olarak kullanılan parolaya ilave olarak en az bir doğrulayıcı faktör daha kullanılması gerekmektedir. Anılan ilave doğrulayıcı faktör; kayıtlı cep

telefonuna gönderilecek bir SMS, e-posta hesabına gönderilebilecek bir kod ya da bir biyometrik kontrol şeklinde örneklendirilebilir.

b. Kimlik doğrulama mekanizmaları 3.2.1.10 maddesinde de belirtildiği üzere sahip olunan, bilinen veya biyometrik faktörler içerebilmektedir. Bilgi ve İletişim Güvenliği Rehberi uyarınca bir kimlik doğrulama mekanizmasının çok faktörlü kimlik doğrulama uyguluyor olması, bu bahsedilen 3 unsurdan en az 2 tanesini kullanıyor olması ile ilişkilidir. Bu şekilde değerlendirildiğinde, kullanıcı adı ve parola ile giriş yapan bir kullanıcının daha sonra cep telefonuna SMS onay kodunun gönderilmesi bilinen ve sahip olunan faktörleri içerdiği için çok faktörlü kimlik doğrulama olarak değerlendirilmektedir. Bu kapsamda benzer şekilde kullanıcı adı ve parola kontrolüne ek olarak e-posta onay kodunun kullanılması da farklı bir kanal üzerinden doğrulama içerdiği için çok faktörlü kimlik doğrulama olarak değerlendirilmektedir.

c. 3.2.1.10 tedbir maddesi kullanıcı veya uygulama açısından kritik olabilecek işlevler öncesi ilave bir kimlik doğrulama mekanizmasının kullanılmasını amaçlamaktadır. Tedbir maddesi temelde hâlihazırda kullanıcının kimliğini doğrulamak için kullanılan yöntemlere ek olarak ilave bir kontrolün sağlanmasını talep etmektedir. Bu kapsamda hassas işlevler için kullanıcıdan ayrı bir parolanın istenmesi, kimliği doğrulanmış farklı bir kullanıcı tarafından onaylanması gibi yazılımsal kontroller de geçerli sayılmaktadır. Daha güçlü bir mekanizmayla kimlik doğrulama ise örneğin SMS onay kodu ile giriş yapılan bir uygulamada SMS onay kodu açık metin olarak gönderildiği için daha güçlü şifreli gönderilecek başka bir parola ile kritik işlemlerin yapılabilmesini amaçlamaktadır. Bu örneğe benzer şekilde uygulamanın ve sistemin tasarımına bağlı olarak daha güçlü bir mekanizma kullanımı da değişim gösterebilecektir. Bilgi ve İletişim Güvenliği Rehberi uyarınca güçlü bir kimlik doğrulama mekanizması kullandığı değerlendirilen uygulamalar ilgili tedbir maddesinde alternatif olarak sunulan yeniden kimlik doğrulama işlemi ile ilgili tedbir maddesine uyum sağlayabilir.

Tarih	Mart 2022	SSS No:17
İlgili Rehber Madde(s)(ler)i	Radyolink Devreleri İletişim Güvenliği	

CBDDO'ya Sorulan Soru

2019/12 sayılı Genelge'nin 21'nci maddesi (*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*) ile ilgili bir hususta bilginize başvurmak istiyoruz.

Aynı konu Rehber'in "4.5.3. Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri" başlığı altında 3'ncü seviye bir tedbir olarak (Madde 4.5.3.14) "Kritik Haberleşme Güvenliği (*Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır*)" tanımlanmıştır.

Her iki maddeye de baktığımızda tedbirlerin özne kısımlarında "**Telekom hizmeti veren işletmecilerin**" yer almakta olduğu görülmektedir.

- Bununla birlikte biz de Bakanlık olarak taşra birimlerimizde hem normal internet hizmeti, hem de MPLS VPN devreleri kullanılarak oluşturulan kapalı/korumalı ağımızda (Sağlık Bilişim Ağı/SBA) zaman zaman radyolink bağlantıları kullanıyoruz.
- SBA tarafında radyolink kullanılması ihtiyacı hasıl olduğunda, veri işlemede kullanılan uygulamaların sahip olduğu SSL/TLS koruması ve MPLS VPN'in sağladığı korumaya ilave olarak radyolink devresinin her iki ucunda mutlaka iletişimin kapatılması için kriptolama istiyoruz. Ancak buradaki kripto sistemleri (ulusal ve/veya uluslararası otoriteler tarafından güvenli olarak kabul görmüş algoritma ve anahtar boyları kullanılacak şekilde) donanım ve/veya yazılım tabanlı hazır ticari çözümler oluyor.
- İnternet tarafında radyolink kullanılması ihtiyacı hasıl olduğunda, radyolink hatları üzerinden geçen trafik için özel bir güvenlik sistemi talep etmiyoruz. Çünkü bu devreler üzerinden "özellikle" kritik bir veri işlenmiyor. Hastanelerin MERNİS (SGK) ve MEDULA (NVİ GM) gibi sistemlerle iletişimi SBA devreleri üzerinden KamuNET'e bağlanmak suretiyle gerçekleştiriliyor. Çok istisnai olarak (son kullanıcıların kendileri ile ilgili kişisel iş ve işlemleri için) bir veri işleme söz konusu olur ise zaten ilgili uygulamalar SSL/TLS ile bahse konu verileri şifreliyor.

Yukarıdaki bilgiler ışığında Genelge'nin 21 ve Rehber'in 4.5.3.14 maddesinin Bakanlığımız için uygulanabilirliği var mıdır?

CBDDO Tarafından Yapılan Açıklama

E-postanızda belirttiğiniz üzere 2019/12 sayılı Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi 21. Maddede "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." ifadesi yer almaktadır. Bahsi geçen Genelgede yer alan maddelerin uygulama pratiklerini detaylandırmak üzere çıkarılan Bilgi ve İletişim Güvenliği Rehberi'nin Elektronik Haberleşme Sektörü Özelinde Güvenlik Tedbirleri başlıklı 4.5.3.14 maddesinde ise "Telekomünikasyon hizmeti veren işletmelerce yerine getirilmek üzere, Cumhurbaşkanlığı ve milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumlarında iletişimin gizliliği ve güvenliğini artırmak amacıyla, bu kurumların merkez birimlerine ve talep edeceği diğer birimlerine doğrudan hizmet sağlayan haberleşme ve transmisyon altyapısında ilk toplama noktasına kadar radyolink vb. kablosuz teknolojiler kullanılmamalı, kullanımın zorunlu olması durumunda ihtiyaç duyulan gizlilik seviyesine uygun donanımsal veya yazılımsal milli kripto sistemleriyle birlikte kullanılmalıdır." ifadesi yer almaktadır.

Bu bağlamda, Sağlık Bakanlığı ve taşra teşkilatı faaliyet alanı olarak milli güvenliğin sağlanması noktasında doğrudan kanunla verilmiş bir görev icra etmediği için bahsi geçen güvenlik tedbiri Bakanlığınızı kapsamamaktadır. Bununla birlikte Kurumunuz tarafından yapılacak risk değerlendirilmesi çerçevesinde, radyolink ile veri iletimi sırasında yaşanabilecek bilgi güvenliği risklerinin Kurumunuza sirayet edebilecek olası etkilerinin göz önünde bulundurulmasında fayda olacağı düşünülmektedir.

Tarih	Mart 2022	SSS No:18
İlgili Rehber Madde(s)(ler)i	3.1.8.4 Detaylı Kayıt Tutulması- Zaman Damgası	
CBDDO'ya Sorulan Soru		
Başkanlığınız tarafından yayımlanan Bilgi ve iletişim Güvenliği Rehberi'nin 3.1.8.4 nolu maddesinde "*Sistem iz kayıtları; olay açıklaması, olay kaynağı, olay zamanı, kullanıcı/sistem bilgisi, kaynak adresleri, hedef adresleri ve işlem detayları bilgilerini içerecek şekilde tutulmalı ve bütünlüğü **zaman damgası** ile korunmalıdır.*" şeklinde bir tedbir bulunmaktadır. 5070 sayılı Kanunda "zaman damgası", "bir elektronik verinin, üretildiği, değiştirildiği, gönderildiği, alındığı ve / veya kaydedildiği zamanın tespit edilmesi amacıyla, **elektronik sertifika hizmet sağlayıcısı (ESHS) tarafından** elektronik imzayla doğrulanan kaydı" olarak tanımlanmıştır. 5651 sayılı kanun kapsamında çıkan yönetmeliklerde zaman damgası tanımı yer almamakta, metinler içerisinde de "verinin bütünlüğünün sağlanması için zaman damgası kullanılmasından ve korunmasından" bahsedilmekte, bu işlemin ESHS aracılığı ile yapılması gerektiğine yönelik bir ibare bulunmamaktadır. Yukarıdaki bilgiler ışığında CBDDO rehberinde belirtilen "zaman damgası" için ne söyleyebiliriz? Zaman damgasının ESHS tarafından üretilmesi şart mıdır? Ya da merkezi log yönetim sisteminin kendi ürettiği sertifika ile zaman damgası oluşturulması (CBDDO Rehberi gereksinimlerinin karşılanması açısından) yeterli midir?		
CBDDO Tarafından Yapılan Açıklama		
3.1.8.4 nolu tedbirde yer alan zaman damgasının, merkezi log yönetim sisteminin kendi ürettiği sertifika ile oluşturulması Rehber gereksinimlerinin karşılanması açısından yeterli olacaktır. Bununla birlikte, tutulan log kayıtlarının kritikliği, kurum dışı bir siber olayda veya adli bir olayda delil olarak kullanılma durumu, Kurum içerisinde kullanılan zaman sunucusunun doğruluğunun ve tutarlılığının ispatlanması gibi durumlar için, günlük veya haftalık periyotlarla ESHS tarafından sunulan zaman damgası kullanılması Kurumsal fayda sağlayacaktır.		

Tarih	Ağustos 2022	SSS No:19
İlgili Rehber Madde(s)(ler)i	3.2.8.1 Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi	

CBDDO'ya Sorulan Soru

Genel Müdürlüğümüzde uygulanan BGYS kapsamında kullanmakta olduğumuz Güvenli Yazılım Geliştirme Kontrol Listesinin "**Mimari, Tasarım ve Tehdit Modelleme**" başlığı altında, "**Uygulamadaki bileşenler hata durumlarında varsayılan olarak güvenli durumlara geçmelidir**." şeklinde bir gereksinimimiz bulunmaktadır. Bu gereksinim, büyük oranda Rehberin 3.2.8.1 (Hataların Yakalanması ve Varsayılan Olarak Güvenli Duruma Geçmesi) maddesinde yazan tedbire karşılık gelmektedir.

Yazılımcılarımız ile hata yakalama işlemlerini nasıl yaptıklarını ve bunu nasıl dokümante ettiklerini konuştuğumuzda "***hata yakalama ve ele alma işlemlerinin bir kısmının zaten kullanılan yazılım geliştirme platformu tarafından otomatik olarak sağlandığı, kod içinde yazılımcı tarafından kontrol edilmesi gereken hatalar için (try, catch, throw gibi komutlar/bloklar kullanılmak suretiyle) gerekli kontrollerin eklendiği, geliştiricilerin hata ile karşılaştığına nasıl bir önlem aldığını (kodun nasıl reaksiyon verdiğini) kod içine "comment" olarak yazdıklarını, oluşan hatalar için iz kaydı ürettiklerini ve log dosyalarına yazdıklarını, çok iyi dokümante edilmiş az sayıda projede yazılım analiz ve tasarım dokümanlarında hata yakalama ile ilgili hususların da yer alabildiğini***" ifade ettiler.

Rehberin 3.2.8.1 maddesi için yazan denetim soru önerisine baktığımızda "*Uygulamalarda hata ile karşılaşılması durumunda takip edilecek adımlar/faaliyetler tanımlanmış mıdır*?" şeklinde bir ifade bulunmaktadır. Ancak soru cümlesinde geçen "adımların/faaliyetlerin" nasıl bir dokümanda/sistemde yer alması gerektiğine yönelik soru önerisinde herhangi bir açıklama bulunmamaktadır. Bu durum, özellikle yazılım geliştirme alanında tecrübesi olmayan denetçilerin, bu maddenin denetimini yapmasını zorlaştırmaktadır. Denetçi uygulama sahibinden bu madde için ne istemesi (neyi göstermesi) gerektiğini anlayamamaktadır.

Biz bu maddeyi **mülakat yöntemi ile denetlerken**;

- Uygulamanın kaynak kodunda hata yakalama işlemleri için "*try, catch, throw (veya kullanılan platforma bağlı olarak benzeri benzeri)*" bloklar olup olmadığını,
- Bu bloklar için "yakalanan hatanın ne olduğu ve böyle bir hata yakalandığında yazılımın ne yapacağına ilişkin açıklama (comment)" yazılıp yazılmadığını,
- Kullanıcıya gösterilen hata mesajlarında gereksiz detayların olup olmadığını kontrol ediyoruz.

Sizce (mülakat yöntemi ile bu madde kontrol edilirken) bu şekilde yapılan bir denetim yeterli midir? Yeterli değil ise daha farklı nasıl bir yöntem izleyebiliriz?

Cevabınız evet ise Rehberin bir sonraki sürümü için denetim soru önerisinin "***Uygulamalarda hata ile karşılaşılması durumunda takip edilecek adımlar/faaliyetler (yazılım analiz ve tasarım dokümanlarında/yazılım kaynak kodları içerisinde yer alan açıklamalarda yeterli düzeyde) tanımlanmış mıdır? Kullanıcılara gösterilen hata mesajlarına gereksiz detaylara yer verilmekte midir?***" şeklinde düzeltilmesinin uygun olacağını düşünüyoruz.

CBDDO Tarafından Yapılan Açıklama

Bilgi ve İletişim Güvenliği Rehberi kapsamında 3.2.8.1 maddesine yönelik iletmiş olduğunuz öneri için öncelikle teşekkür ederiz. Rehber içerisinde yer alan denetim maddeleri, ilgili oldukları güvenlik tedbirlerinin uygulanıp uygulanmadığının kontrolü için kullanılabilecek denetim yöntemlerini ve soru örneklerini içermektedir. Dolayısıyla denetimi gerçekleştirmesi planlanan denetçi tarafından denetim görüşünün oluşturulmasına makul güvence sağlayacak düzeyde denetim kanıtının, yalnızca Rehberde dokümante edilmiş olan denetim maddeleri ile sınırlı kalmayacak şekilde farklı sorular ve yöntemleri içerecek şekilde zenginleştirmesi mümkündür.

3.2.8.1 maddesine ilişkin tedbir maddesinin mülakat yöntemi ile değerlendirilmesi aşamasında e-postanızda belirtmiş olduğunuz soru içeriklerinin faydalı olacağı değerlendirilmekle birlikte "Bu bloklar için "yakalanan hatanın ne olduğu ve böyle bir hata yakalandığında yazılımın ne yapacağına ilişkin açıklama (comment)" yazılıp yazılmadığını" sorgulamak güvenlik açısından değil, uygulamanın geliştirilmesinin devamlılığı için zaruridir. Ancak, kullanılan denetim yöntemi doğrultusunda yapılan değerlendirmeler kapsamındaki soruların yeterliliğine yönelik sorumluluk denetçiye aittir.

İlaveten, Rehber içeriğinin güncellenmesine yönelik yapılan çalışmalar kapsamında ilgili tedbir maddesinin denetim soruları ve bu kapsamda iletmiş olduğunuz değerli önerileriniz mutlaka dikkate alınacaktır.

Tarih	Xxxx 2022	SSS No:20
İlgili Rehber Madde(s)(ler)i	3.6.3 Elektromanyetik Bilgi Kaçaklarından Korunma Yöntemleri (TEMPEST)	

CBDDO'ya Sorulan Soru

Bilindiği üzere TEMPEST özellikli cihazların kullanılması, cihazlar için TEMPEST onayı alınması, tesisatın TEMPEST kurallarına uygun olarak imal edilmesi gibi konular (TSK/MSB'nın konuyla ilgili mevzuatının zaten uzun yıllardır var olması nedeniyle) ülkemizde bu zamana kadar sadece askeri tesislerde (özellikle muhabere merkezleri, kripto sistemleri, kripto odalarında aranan) veya askeri birimler için hizmet üreten savunma sanayi firmalarının tesis güvenlik belgesi alınması süreçlerinde söz konusu olan ve sağlık sektörü için hiç gündemde yer almayan bir konu idi.

TEMPEST ile ilgili konularda yeterli bilgi ve tecrübemizin olmaması ve konuyla ilgili açık kaynaklarda yeterince bilgi bulunmaması nedeniyle, CBDDO Rehberinde yer alan TEMPEST bağlantılı tedbirlerle alakalı olarak bazı sorularımız olacak.

Şöyle ki;

1. Rehberin 3.6.3.2 maddesinde sistem odası/veri merkezinde kullanılan tüm gizlilik seviyeli bilgi işleyen cihazlar için TEMPEST onayı olması istenmiştir. Bu zamana kadar kamu kurum ve kuruluşlarında kullanılan sunucu cihazlarının piyasada mevcut standart sunucular olduğu dikkate alındığında, TEMPEST kaynaklı bilgi kaybı riskinin olasılığı da dikkate alındığında, mevcut sunucuların TEMPEST özellikli cihazlar ile değiştirilmesi (veya yeni tedarik edilecek sunucuların TEMPEST özellikli olarak satın alınması) mutlaka gerekli ve maliyet/etkin midir? Bu madde milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumları dışında yer alan diğer kamu kurum ve kuruluşlarını da bağlamakta mıdır? Bu maddede belirtilen "cihazların TEMPEST onayları" nereden, nasıl alınmalıdır?
2. Aynı konu ile ilgili olarak 4.4.3.6 maddesinde kripto cihazları için istenen bir özelliğin, 3.6.3.2 maddesinde 2'nci seviye kritik olarak belirlenen bir sistem odasındaki sunucular için de istenmiş olması kendi içinde tutarlı mıdır? Rehber kaleme alınırken 3.6.3.2 maddesinin seviyesi (veya bir bütün olarak mevcudiyeti) konusunda sehven bir hata yapılmış olması mümkün müdür?
3. Sunucu/sistem odası 3.6.3.3 maddesinde belirtildiği şekilde TEMPEST tesisat kurallarına uygun olarak imal edilirse (tesisatın elektromanyetik ortamdaki sinyallerden kaynaklanan sızıntıyı önleyeceği varsayımı ile) 3.6.3.2 maddesini "Uygulanabilir Değil (UD)" olarak mı düşünmek gerekir?
4. 3.6.3.3 maddesinin açıklama kısmında yer alan "kurallar/mevzuat" hangileridir? Bunlara nereden, nasıl ulaşabiliriz?
5. Rehberin bir sonraki sürümünde (3.6.3.2 ve 3.6.3.3 maddesinde yer alan) TEMPEST ile ilgili gereksinimler için (doğrudan milli güvenliğin sağlanması kapsamında görev yürüten kamu kurumları dışında yer alan) kamu kurum ve kuruluşları açısından bir esneklik sağlanması/ bu maddelerde revizyona gidilmesi düşünülmekte midir?

CBDDO Tarafından Yapılan Açıklama

Henüz cevap verilmedi