CBDDO BİGR DEĞERLENDİRME RAPORU

Raporu Hazırlayanlar

Cenk Erim TEZEL – Yönetim Kurulu Üyesi

Tayfun YAĞCI – Yönetim Kurulu Üyesi

Çalışma Gurubu Üyeleri

Ali DİNÇKAN – YK Başkan Yardımcısı

Ahmet ÖZÇAM – Dernek Üyesi

Emre ÇELİKKOL – Dernek Üyesi

F.Filiz ULVİ – Dernek Üyesi

Raporu Gözden Geçiren

Cem HACIZADE – Yönetim Kurulu Başkanı

Rapor Tarihi: 17.10..2024

İçindekiler

Giriş

2012/19 sayılı Cumhurbaşkanlığı Kararı Siber Vatan ilkesi ile kamu kurumları ve kritik altyapı şirketlerinden başlayarak siber dayanıklılığı sağlayacak yapının kurulmasını ve sürdürülmesini amaçlamıştır.

Bu doğrultuda önce Bilgi İletişim Güvenliği Rehberi ardından da Bilgi İletişim Güvenliği Denetim Rehberi yayınlanmış, denetçiler eğitilmiş ve seçilmiş sonrasında da bu denetimleri yapacak firmalar yetkilendirilmiştir. Buna paralel olarak 24 aylık uyum süreci başlamış ve bu süre içinde kamu kurum ve kuruluşları ile kritik altyapı şirketlerinin rehberin istediği güvenlik yapısını kurup uygulamaları beklenmiştir.

Değerlendirme Esasları

Bu rapor, Bilgi İletişim Güvenliği Rehberi ve Bilgi İletişim Güvenliği Denetim Rehberi'nin uygulanması ve denetim süreçlerine dair gözlemlerimizi ve önerilerimizi içermektedir. Raporda, rehberlerin içeriğine yönelik yapılan değerlendirmeler, uygulama sırasında karşılaşılan zorluklar ve geçmiş yıllardan elde edilen deneyimler ışığında geleceğe yönelik öneriler sunulmaktadır. Özellikle, rehberlerin uygulanabilirliğini artırmak amacıyla, mevcut kontrollerin sadeleştirilmesi, yurtdışı depolama ve trafik konularının ele alınması gibi önemli başlıklara odaklanılmıştır. Ayrıca, rehberlerin uygulanması, denetlenmesi ve denetim sonuçlarının analizi konusunda da önerilerimiz yer almaktadır.

Görüşler

Bilgi İletişim Güvenliği Rehberi, Bilgi İletişim Güvenliği Denetim Rehberi ve bu rehberlerin uygulanma süreçleri ile ilgili görüşlerimiz aşağıdaki gibidir:

1. Rehber içeriği ile ilgili öneriler
2. Rehberin uygulanması ile ilgili öneriler
3. Geçmiş yılların uygulamalarından gelecek yıllara aktarılmasında ışık tutacağını düşündüğümüz öneriler.

Rehber İçeriği

1. Rehberde tekrarlı olarak yer alan kontrollerin sadeleştirilmesi doğru olacaktır. Örneğin 3.2.7.x soruları (Uygulama Veritabanı Güvenliği) ile 5.2.1.x (Veritabanı Sıkılaştırma) grubu büyük ölçüde benzer soruları içermekte ve birbirini doğrudan referans vermektedir. Bu nedenle boşluk analizi veya denetim sırasına cevaplar ve değerlendirmeler doğrudan kopyalanmakta ve bir çapraz kontrol de sağlamamaktadır. Bu durumda olan kontrollerin sadeleştirilmesi ve toplam kontrol sayısının azaltılması rehber uygulamasını da denetimini de herhangi bir zaafa yol açmadan, kolaylaştıracaktır. Önerimiz bu kontrollerin varlık grubuna yönelik tedbirler tarafından eksiltilmesidir.
2. Yurtdışı depolama ve trafik konuları hemen tüm kamu kuruluşları ve kritik altyapı organizasyonları için sorunludur. Öncelikle şu hususun çözülmesi gerekmektedir: Kritik verinin yurtdışında saklanması yasaklanmıştır. Buradan çıkan sonuç olarak kritik olmayan verinin yurtdışında saklanabileceği değerlendirilebilir. Fakat herhangi bir

trafiğin yurtdışından geçmemesi istendiği için bu veri yurtdışında depolanmak için ancak depolama aygıtları ile fiziki olarak taşınmak ve depolanmak durumundadır. Bundan daha önemlisi, az önce saydığımız rehbere tabi kurum ve kuruluşların büyük çoğunluğu, Office 365, Google, AWS gibi yurtdışı bulut ve depolama servislerini kullanmaktadır. Hatta kritik altyapı şirketlerinin bir kısmı yabancı ortaklı veya sahipli oldukları için bu trafikten kaçmaları mümkün değildir. Fiili durum ve rehberin isteklerinin bir şekilde uyumlu hale getirilmesinde fayda olduğunu düşünüyoruz.

3. Anlık mesajlaşma konusunda benzer bir sıkıntı vardır. Kimi çok kritik bakanlıklar dahil hemen tüm kamu kurumları ve kritik altyapı şirketleri yerli ve milli olmayan anlık mesajlaşma ve telekonferans uygulamaları kullanmaktadır. Örnek olarak, tüm belediyeler WhatsApp kullanırken Jandarma Genel Komutanlığı, İçişleri Bakanlığı, TSE dahil kritik kamu kurumları Zoom kullanmaktadır. Yine fiili durum ile rehberin isteklerinin uyumlu hale getirilmesinde fayda olacağı kanaatindeyiz.
4. Rehber kamuda dijitalleşmeyi hedeflese bunun güvenlik altyapısını çok öngörülü bir şekilde kurmaya çalışsa da bugün kamuda basılı bilgi kullanımı çok yaygındır. Adliyeler (UYAP'a rağmen), İcra Müdürlükleri, ilçe belediyelerinin İmar müdürlükleri başta pek çok kamu kuruluşu (tek tek sayınca sayıları binleri buluyor) basılı bilginin çok yoğun yer aldığı ve sirkülasyonunun olduğu kurumlardır. Bu bilginin güvenliği ise rehberi biraz özgürce yorumlayarak bilginin yer aldığı mekanların fiziki güvenliği üzerinden kontrol edilmeye çalışılmaktadır. Dönüşüm tamamlanana kadar basılı bilgiye daha fazla kontrol sağlanması bununla ilgili maddeler eklenmesi yerinde olacaktır.
5. Benzer bir durum fiziki mekanlar için de geçerli. Bugün Anadolu'da pek çok kamu kurum ve kuruluşunun rehberin istediği fiziki mekanları hayata geçirmesi veya dönüştürmesi mümkün değildir. Benim yaşadığım yer olan Bursa'nın bile bazı ilçelerinde belediye veya diğer kurumların rehberin istediği sistem odası güvenliği, fiziki koşullar, vb. şartları sağlaması çok uzun yıllarda gerçekleşecek hedeflerdir. Değerlendirmelerin bu durumu göz önüne almasında büyük fayda görüyoruz.
6. Bölüm 4 içerisinde 4.1 Kişisel Verilerin Güvenliği' konusunda yer alan maddelerden bazıları genel kontrol niteliği taşımakta ve kurum için bir kez yapılmaktadır. Örneğin 4.1.1.1 KV envanteri, 4.1.1.2 Kişisel Veri politikası vb.. Ancak rehber varlık grubu ile ilişkilendirme yöntemi üzerinden kurgulandığı için 4.1 ile ilişkilendirilen her varlık grubu için aynı soruya aynı yanıtın verilmesi gibi bir iş yükü oluşmakta ve güncelliğinin sağlanması sorun oluşturmaktadır. Rehberde varlık grubu bazında kontrollere ek olarak genel kontrollerin tanımlanması önerilmektedir. Doğrudan varlık grubu ile ilişkisi olmayan rehber maddeleri tespit edilmeli ve Genel Güvenlik Kontrolleri şeklinde bir ek başlık oluşturularak her kurumun bu konuları gerçekleştirmesi beklenmelidir. Ayrıca Kişisel Verilerin Korunması gibi konularda varlık grubuna özel olarak bulunan kontrollerin (örneğin 4.1.1.4 Veri Tabanının Dışarıya Aktarımının Yetkili Kullanıcı Tarafından Yapılması) 3. Bölümde ilgili tedbir grubuna taşınması değerlendirilebilir. Bu sayede Kişisel Verilerin Güvenliği konusunun tek sefer yapılan genel konuları genel kontroller kısmında, özel konuları ilgili varlık grubu bazında ele alındığından ilgili başlık iptal edilebilir.
7. Rehberde birbirine referans verilmiş pek çok kontrol tanımlıdır. Örneğin "4.6.1.2 Yazılım Varlık Envanterine Kayıt Edilmemiş Yazılımların Yönetimi" zaten Tedbir No: 3.1.2.4 altında ele alınmıştır. Bu gibi durumlar hem boşluk analizinde hem denetimlerde aynı cümlelere sahip olması nedeni ile gereksiz kopyalama ve yapıştırma eylemlerine neden olmaktadır. Birbirine referans verilmiş kontroller eğer birebir karşılıyor ise teke indirilebilir. Ayrıca 4.6 bölümü tüm varlık gruplarında seçilmesi gereken (her varlık grubunun zaten bir yeni geliştirme ve tedarik süreci olması gerekir diye düşünüyoruz) bir konu olması nedeni ile ilk öneride bulunan genel güvenlik kontrolleri başlığına taşınması değerlendirilebilir.
8. Rehber 4. Ve 5. Bölümlerin ne zaman seçileceğine dair bir kafa karışıklığı mevcuttur. Denetimlerimizde 3.1 Ağ ve Sistem Varlık Grubu üyesi iken 5.1 maddesini seçmeyen kuruluşlar olduğu gözlemlenmiştir. 3.1 ağ ve sistem grubunda olup işletim sistemi

içermeyen bir varlık grubu hayal edemiyoruz. Bu konuda Rehber içerisinde bir haritama veya hangi durumda bölüm 4 ve 5 için seçim zorunluluktur net olarak tariflenmelidir. İnisiyatife bırakılmaması tavsiye edilmektedir.

9. Müşteri kuruluşlarda bir kontrol tümüyle uygulanamıyorsa bu konuda telafi edici kontrol geliştirilebileceği kavramı oturmamış durumdadır. Bazı kurumlarda ilgili kontroller uygulanabilir olmasına rağmen mali veya teknolojik zorluklar (EKS de üreticinin sisteme dokunursanız garanti dışı kalır uyarıları) nedeni ile uygulanamamaktadır. Bu durumlarda kurumların nasıl hareket edecekleri rehberde daha net tanımlanmalıdır. Tanımlı olduğu düşünüyorsa farkındalık arttırılmalıdır.
10. Bilgi güvenliği ve gizliliğinin sağlanmasına yönelik olarak üst yönetimin liderlik etmesi, gerekli kaynakları taahhüt etmesi ve bunun duyurulması konusunda gerekli olan talimatlar yer almalıdır. Ayrıca yönetim gözden geçirme toplantıları konusunda vurgu yapılmalıdır. Yani yönetimsel süreçler daha belirgin olmadır. Her ne kadar rehber kapsamı içerisinde yönetimsel süreçlerden bahsediliyorsa da bu durum sistematik bir yaklaşım sergilemekten uzaktır. Bunun için dünya standardı ISO 27001 BGYS belli büyüklükte kurum ve kuruluşlara zorunlu olmalıdır ve Rehberin giriş bölümünde ifade edilen sistemler arası bütünlüğün sağlanması için eşleştirme tablosu ISO 27001:2022 için de oluşturulmalı ve yayınlanmalıdır. Bu durum yönetimsel işlemleri kolaylaştıracak, duplikasyonu önleyecek, daha etkin bir bilgi güvenliği yönetim sistemi kurulmasına vesile olacaktır.

Rehber Uygulaması

1. Rehber ve istekleri bugün bile yeteri kadar bilinmiyor. Geçen yıl rehber üzerine çalışan kurum ve şirketler rehber uyum çalışması yapmadılar. Sadece boşluk analizini takiben bir uyum planı oluşturdular.
2. 2022 yılında 12 Mayıs'ta yine baş denetçi olan bugünkü dernek başkanımız Cem Hacızade Doğu Karadeniz Belediyeler Birliği'nin davetlisi olarak rehber eğitimine gittiğimizde katılan 27 belediye ve diğer kurum temsilcilerinin sadece birisi rehbere sahipti ve pek çoğu rehberi orada öğrendi. Bu kadar yıl sonra Anadolu'nun çoğunda durum çok farklı değil. Rehberin içeriği ve gerekleri ile çok daha yoğun tanıtım ve bilgilendirme yapılması gerekiyor. Bakanlıklar aracılığıyla yapılan yazışmalar silsile içinde hedeflerine ulaştığında gerekli derecede etkili olmuyor.
3. Geçtiğimiz yıllarda ilçe belediyeleri ve kaymakamlıklar denetimden muaf tutulunca pek çoğu hiçbir çalışma yapmadı. Pek çok büyükşehir belediyesi bile 'adı üstünde rehber. Bir zorunluluk yok' şeklinde dönüş yaptılar. 2019/12 sayılı Cumhurbaşkanlığı genelgesi ve bunun içinde yer alan bağlayıcı hükümlerin altının bir daha çizilmesi gerekiyor. Hatta kamuya hizmet veren yazılım şirketleri bile rehberin isteklerine uygun değişiklikleri ürünlerine uygulamıyorlar.
4. Bir diğer uygulama olarak rehber bir yönetmelik veya kamu gözünde daha bağlayıcı görünen bir mevzuata dönüştürülebilir.
5. Bugün itibarıyla BİG Rehber faaliyetlerine başlamamış kurum ve kuruluşların ancak yine bir boşluk analizi yapması mümkün olacaktır. Haliyle denetim sonuçları da buna paralel olacaktır. Bu bile daha yaygın bilgilendirme ile mümkündür.
6. Bir diğer husus da hemen tüm yöneticilerin rehbere uymamanın cezasının ne olduğunu sormasıdır. Cezaların net ve caydırıcı hale getirilmesi ve yaygın bir şekilde duyurulması gereklidir.
7. Her kurumun öncelikle sistemine varlık sayısını ve varlık envanterlerini ilk aşamada kendileri girmeleri ve sonrasında dış denetim için firmalarımızın sistem tarafından adam gün hesaplanıp ücretlendirme hesaplanıp otomatik olarak atanması yoluna gidilebilir. Bilirkişilik süreçlerinde nasıl ki mahkeme hem ücreti belirleyip hem ataması yapıyor ise burada da aynı sistem olabilir ve her kurumun zorunlu denetim tarihi olur ve denetim yapacak firma belli olur burada hem fiyatlandırma hem adam gün hem denetimler kapsamında stabil bir süreç ortaya çıkar diye düşünüyoruz.

8. Rehber denetimleri için kişi ve firma yetkilendirmeleri yapılmaktadır. Ancak denetimlerde fiilen denetim yetkisine sahip olmayan kişilerin denetçi gibi çalışarak denetimleri gerçekleştirdiği ve firmadan yetkilendirilen kişilerin denetim kayıtlarında adı geçtiği bilinmektedir. Denetimleri kimlerin yapabileceği net olarak denetim rehberinde tanımlıdır. Denetim firmalarının bu gibi uygunsuzlukları yapıp yapmadığı denetlenmeli ve gerekli yaptırımlar uygulanmalıdır.
9. Denetim yapan firmalarla denetlenen kurumlar ve şirketler arasındaki ticari bağ daha sıkı kurallara bağlanmalıdır. Denetimin diğer ürünlerle ilişkilendirilerek sunulması veya Bilgi ve İletişim Güvenliği Uyum danışmanlığının genel bilgi güvenliği hizmetleri ile ilişkilendirilerek veya adlandırılarak sunulması benzeri uygulamaların denetimlerin tarafsızlık ve etkinliğini olumsuz etkilemesinin önüne geçilmesi sağlanmalıdır. Bu ilişkiler daha yakından denetlenmeli ve sorgulanmalıdır.
10. Sektörel bazda regülatif kurumlar denetim gerçekleştirmemizi yasaklayabiliyorlar. Ancak bu sektörlerde bulunan iç denetim kadrolarını yetkinlik eksikliği nedeni ile sağlıklı bir denetim yapılmadığını gözlemliyoruz. Bir sektörde Rehber uyumu şartı mevcut ise DDO ve TSE'den yetki almış bizim gibi kuruluşların denetim yapmasının önüne geçilmemelidir. BDDK Eylül 2022 tarihinde yayınladığı bir yazı ile denetim kuruluşlarından hizmet almadan kendi iç denetim ekipleri ile söz konusu denetimlerin yapılmasını bankalardan istemiştir. Pek çok banka göstermelik olarak denetimleri yapmıştır. Bu denetimlerde dış kaynak kullanımı kısıtlanması sektörün siber güvenlik olgunluğunun arttırılmasının önünde bir engeldir. BDDK'dan yetkili kuruluşların yaptığı denetimlerin etkinliği ortada iken yüksek deneyime sahip DDO denetçilerinden hizmet alınmasının önüne geçilmemesi gerektiğini düşünmekteyiz. Ülkemizin kritik altyapısı olan finansal kuruluşlarda bu uygulama biçimi siber güvenlik olgunluğunun beklenen hızda artmasının önünde ciddi bir engeldir.
11. BİG Denetimlerini iç denetim olarak yapan kurumlardan tüm varlık gruplarını denetlenmesi istenmelidir. Bir satın almaya ve bütçe kısıtına tabi olmayan bu yöntemde sağlıklı sonuç alabilmek için yıla yayılmış olarak tüm varlık grupları denetlenmeli, eksiklikler belirlenmeli ve gerekli aksiyonlar başlatılmalıdır. Sonuçta denetimin bir sezonu yoktur. Sadece denetim sonuç ve raporlarının yüklenmesi için BİGDES'in açıldığı bir dönem söz konusudur. Yıl içinde denetimlerin sağlıklı bir şekilde yapılabilmesi için denetimin dönemsellik hissi ortadan kaldırılmalıdır. Geçtiğimiz dönemlerde denetim kapsamı dışında bırakılan kurum ve kuruluşlar da kapsama dahil olduğunda mevcut denetim sezonu yeterli olmayacak, BİGDES üzerinde de aşırı bir yük oluşturacaktır. Bu nedenle BİGDES'in açık olduğu sürenin, tüm yıla yayılamasa bile, daha uzun olması sağlıklı olacaktır.
12. Denetçilerin denetim raporlarının ilgili bölümlerini doğrudan BİGDES'e girmesini sağlayacak bir uygulamaya gidilebilir. Gerekli güvenlik önlemleri de alınarak bu girişin yapılması işleyişi hızlandıracağı gibi aynı zamanda denetçilerin performansının ve etkinliğinin de izlenmesini sağlayacaktır.

Geçmiş Yıllara Ait Uygulamalar

1. Bir önceki maddeden devamla geçen yıl rehbere tabi olan, denetim yükümlülüğü olan fakat bunu gerçekleştirmeyen kurum, kuruluş ve şirketler ile yöneticileri ile ilgili işlem başlatılmalı ve cezasızlık hissinin önüne geçilmelidir. Yoksa diğer yöneticiler de benzer yollara girmeyi tercih edebilirler. Bu veritabanına çok kolay ulaşılabilir.
2. Bir diğer konu da işin denetim ayağı. Denetimlerin ne kadar sağlıklı yapıldığı ve sonuçların ne kadar objektif olduğunu da analiz edeceğiniz kanaatindeyiz. Rehberin mevcut hali ve asgari şartlarda delil toplama, inceleme vb. süreciyle bile aldığı süre sizin de malumunuzdur. Gerek iç denetim gerekse dış denetim olarak elinize ulaşan raporları incelemeniz, denetim süreleri, içeriği, doğruluğu, tutarlılığı açısından analiz etmenizde fayda vardır. TSE de yetki belgelerinin ara denetimini yaparken süreçte yapılan denetimlerin sayılarını ve sürelerini değerlendirmeye almalıdır.

3. Son bir not: TSE’nin denetçi sınavları iyi bilişimcileri seçiyor fakat iyi denetçileri yeteri kadar ayırt etmiyor. Sınavda başarılı olmuş pek çok denetçi/baş denetçi, özellikle, denetim rehberini doğru yorumlayamıyor.
4. Kamu kurumu personeline İç tetkik yapma koşulunda 27001 BGYS sertifika sahip olmak değil ataması yapılmış denetçi olmak diye düzenlenmesi getirilmelidir. Karmaşık bir süreç olan BİG Denetimlerinin sadece iç denetçi belgesine sahip kişilerce sağlıklı olarak yapılması ve DDO’ne sağlıklı sonuçlar döndürmesi mümkün değildir. Aslında temelde Türkiye Cumhuriyeti’nin bekası ve Siber Vatan’ın tüm unsurlarıyla güvence altında olduğunun denetiminin BDDK, TCMB vb. kurumların yönetmeliklerinde olduğu gibi Bağımsız Denetim kurumlarınca yapılması çok daha sağlıklı olacaktır.

Sonuç

Bilgi İletişim Güvenliği Rehberi ve Denetim Rehberi'nin uygulanmasında karşılaşılan zorluklar, rehberlerin içeriğinin daha fazla sadeleştirilmesi ve uygulama süreçlerinin daha esnek hale getirilmesi gerektiğini ortaya koymaktadır. Rehberlerin dijitalleşme hedeflerine uygun olarak, basılı bilgi güvenliği ve fiziki mekanların güvenliği konularında daha fazla düzenlemeye ihtiyaç duyulduğu gözlemlenmiştir. Ayrıca, rehberlerin uygulama süreçlerinin, kamu kurumlarında daha geniş çapta tanıtım ve bilgilendirme ile desteklenmesi gerekmektedir. Geçmiş yıllara ait uygulamalardan elde edilen deneyimler, rehberlerin daha etkin bir şekilde uygulanabilmesi için cezaların netleştirilmesi ve yaygın bilgilendirme yapılmasının önemini vurgulamaktadır.

Bilgi İletişim Güvenliği Rehberi'nin yeni versiyonunda bu önerilerin dikkate alınması, ülkemizin siber güvenlik altyapısını daha sağlam temellere oturtarak siber vatana büyük fayda sağlayacaktır. Bu sayede, kritik bilgi varlıklarının korunması ve bilgi güvenliği süreçlerinin etkin yönetimi ile siber vatanın bütünlüğü ve güvenliği daha güçlü bir şekilde sağlanabilecektir. Bu rapor, Bilgi İletişim Güvenliği Rehberi'nin gelecekteki uyum çalışmalarına ışık tutmayı ve ülkemizin siber güvenliğine katkı sağlamayı amaçlamaktadır.