BİLGİ SİSTEMLERİ YÖNETİMİ TEBLİĞİ

(VII-128.9)

(5/1/2018 tarihli ve 30292 sayılı Resmi Gazetede yayımlanmıştır.)

Tebliğ Değişikliklerine İlişkin Liste:

1) *9/1/2020 tarihli ve 31003 sayılı Resmi Gazete'e Bilgi Sistemleri Yönetimi Tebliği (VII-128.9)'nde Değişiklik Yapılmasına Dair Tebliğ (VII-128.9.a) yayımlanmıştır.*

BİRİNCİ BÖLÜM
Amaç, Kapsam, Dayanak ve Tanımlar

Amaç

MADDE 1 - (1) Bu Tebliğin amacı, 2 nci maddede sayılan Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinin yönetimine ilişkin usul ve esasları belirlemektir.

Kapsam

MADDE 2 - (1) Aşağıdaki Kurum, Kuruluş ve Ortaklıklar, bu Tebliğ hükümlerine uymakla yükümlüdürler.

a) Borsa İstanbul A.Ş.,
b) Borsalar ve piyasa işleticileri ile teşkilatlanmış diğer pazar yerleri,
c) Emeklilik yatırım fonları,
ç) İstanbul Takas ve Saklama Bankası A.Ş.,
d) Merkezi Kayıt Kuruluşu A.Ş.,
e) Portföy saklayıcısı kuruluşlar,
f) Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş.,
g) Sermaye piyasası kurumları,
ğ) Halka açık ortaklıklar,
h) Türkiye Sermaye Piyasaları Birliği,
ı) Türkiye Değerleme Uzmanları Birliği.

(2) Birinci fıkrada sayılan Kurum, Kuruluş ve Ortaklıklardan, 6/12/2012 tarihli ve 6362 sayılı Sermaye Piyasası Kanunu'nun 136 ncı maddesi uyarınca banka ve sigorta şirketleri ile 21/11/2012 tarihli ve 6361 sayılı Finansal Kiralama, Faktoring ve Finansman Şirketleri Kanunu uyarınca finansal kiralama, faktoring ve finansman şirketlerinin bilgi sistemlerinin, kendi özel mevzuatlarında belirlenen ilkeler çerçevesinde yönetilmesi, bu Tebliğde öngörülen yükümlülüklerin yerine getirilmesi hükmündedir.

Dayanak

MADDE 3 - (1) Bu Tebliğ, 6362 sayılı Kanunu'nun 128 inci maddesinin birinci fıkrasının (h) bendine dayanılarak hazırlanmıştır.

Tanımlar ve kısaltmalar

MADDE 4 - (1) Bu Tebliğde geçen,

(a) Birincil sistemler: Kurum, Kuruluş ve Ortaklıkların Kanundan ve Kanuna ilişkin alt düzenlemelerden kaynaklanan görevlerini yerine getirmeleri için gerekli bilgilerin elektronik ortamda güvenli ve istenildiği an erişime imkan sağlayacak şekilde kaydedilmesini ve kullanılmasını sağlayan altyapı, donanım, yazılım ve veriden oluşan sistemin tamamını,

b) Bütünlük: Bilginin doğruluğu ve tamlığını koruma özelliğini,

c) Denetim izi: Finansal ya da operasyonel işlemler ile bilgi güvenliği ihlal olaylarının başlangıcından bitimine kadar adım adım takip edilmesini sağlayacak kayıtlar ile bu kayıtlar üzerinde yapılan işlemleri gösteren kayıtları,

ç) Düzeltici faaliyet: Bilgi sistemlerinde yaşanan herhangi bir acil durum, hata, arıza veya kötüye kullanım sonrasında olayın etkilerini azaltmak için yerine getirilen faaliyeti,

d) Erişilebilirlik: Bilginin yetkili kullanıcı, uygulama veya sistem tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğini,

e) Gizlilik: Bilgi sistemlerine ve bilgiye sadece yetkili kullanıcı, uygulama veya sistem tarafından erişilebilmesini,

f) Güvenli alan: Bilgi işleme, iletişim ve depolama donanımlarını barındıran alanı,

g) İkincil sistemler: Birincil sistemler aracılığı ile yürütülen faaliyetlerde bir kesinti olması halinde, bu faaliyetlerin iş sürekliliği planında belirlenen kabul edilebilir kesinti süreleri içerisinde sürdürülür hale getirilmesini ve Kanunda ve Kanuna ilişkin alt düzenlemelerde Kurum, Kuruluş ve Ortaklıklar için tanımlanan sorumlulukların yerine getirilmesi açısından gerekli olan bütün bilgilere kesintisiz ve istenildiği an erişilmesini sağlayan birincil sistem yedeklerini,

ğ) Kanun: 6362 sayılı Kanunu,

h) Kontrol: Bilgi sistemleri süreçleriyle ilgili olarak gerçekleştirilen ve iş hedeflerinin gerçekleştirilmesi, istenmeyen olayların belirlenmesi, engellenmesi ve düzeltilmesine ilişkin yeterli derecede güvenceyi oluşturmayı hedefleyen politikalar, prosedürler, uygulamalar ve organizasyonel yapıların tamamını,

ı) Kurul: Sermaye Piyasası Kurulu'nu,

i) Kurum, Kuruluş ve Ortaklıklar: 2 nci maddede sayılan kurum, kuruluş ve ortaklıkları,

j) Politika: Kurum, Kuruluş ve Ortaklıkların hedef ve ilkelerini ortaya koyan ve üst yönetimi tarafından onaylanmış dokümanı,

k) Prosedür: Süreçlere ilişkin işlem ve eylemleri tanımlayan dokümanı,

l) Sermaye piyasası kurumları: Kanun'un 35 inci maddesinde sayılan kurumları,

m) Süreç: Bir işin yapılış ve üretiliş biçimini oluşturan sürekli işlem ve eylemleri,

n) Üçüncü taraf: Kurum, Kuruluş ve Ortaklıklar ile müşteriler dışında kalan gerçek veya tüzel kişileri,

o) Üst yönetim : Yönetim kurulu tarafından belirlenen kişi ya da grubu, yönetim kurulu tarafından belirleme yapılmadığı durumlarda ise Kurum, Kuruluş ve Ortaklıklar'ın en üst yetkilisini,

ifade eder.

İKİNCİ BÖLÜM
Bilgi Sistemlerinin Yönetilmesi

Bilgi sistemleri yönetiminin oluşturulması ve hayata geçirilmesi

MADDE 5 - (1) Bilgi sistemlerinin yönetimi, kurumsal yönetim uygulamalarının bir parçası olarak ele alınır. Kurum, Kuruluş ve Ortaklıkların operasyonlarını istikrarlı, rekabetçi, gelişen ve güvenli bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejilerinin iş hedefleri ile uyumlu olması sağlanır, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde yer alır ve bilgi sistemlerinin güvenlik, performans, etkinlik, doğruluk ve sürekliliğini hedefleyerek doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilir.

(2) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerinin yönetimine ilişkin politikaları, süreçleri ve prosedürleri tesis eder, düzenli olarak gözden geçirerek iş alanında gerçekleşen değişiklikler veya teknolojik gelişmeler doğrultusunda güncelliğini ve ilgili tüm birimlere duyurulmasını sağlar.

Bilgi güvenliği politikası

MADDE 6 - (1) Bilgi sistemlerinin kurulması, işletilmesi, yönetilmesi ve kullanılmasına ilişkin; bilginin gizliliğinin, bütünlüğünün ve gerektiğinde erişilebilir olmasının sağlanmasına yönelik olarak bilgi güvenliği politikası üst yönetim tarafından hazırlanır ve yönetim kurulu tarafından onaylanır. Onaylanan bilgi güvenliği politikası personele duyurulur. Bu politika, bilgi güvenliği süreçlerinin işletilmesi için gerekli rollerin ve sorumlulukların tanımlanmasını, bilgi sistemlerine ilişkin risklerin yönetilmesine dair süreçlerin oluşturulmasını, kontrollerin tesis edilmesini ve gözetimini kapsar.

Üst yönetimin gözetimi ve sorumluluğu

MADDE 7 - (1) Bilgi güvenliği politikasının uygulanması üst yönetim tarafından gözetilir. Bilgi güvenliği politikası kapsamında bilgi sistemleri üzerinde etkin ve yeterli kontrollerin tesis edilmesi yönetim kurulunun sorumluluğundadır.

(2) Yeni bilgi sistemlerinin kullanıma alınmasına ilişkin kritik projeler üst yönetim tarafından gözden geçirilir ve bunlara ilişkin risklerin yönetilebilirliği göz önünde bulundurularak onaylanır. Kritik projelerin Kurum, Kuruluş ve Ortaklıkların iç kaynaklarıyla veya dış kaynak yoluyla alınan hizmetlerle gerçekleştirilmesine bakılmaksızın personel uzmanlığının, projelerin teknik gereksinimlerini karşılayabilecek nitelikte olması esastır. Bu yapıyı desteklemek üzere oluşturulacak yönetsel rol ve sorumluluklar açıkça belirlenir.

(3) Kurum, Kuruluş ve Ortaklıkların üst yönetimi, bilgi güvenliği önlemlerinin uygun düzeye getirilmesi hususunda gereken kararlılığı gösterir ve bu amaçla yürütülecek faaliyetlere yönelik olarak yeterli kaynağı tahsis eder. Üst yönetim, asgari olarak aşağıdaki faaliyetlerin yerine getirilmesini temin edecek mekanizmaları kurar:

a) Bilgi güvenliği politikalarının ve tüm sorumlulukların her yıl gözden geçirilmesi ve onaylanması,

b) Bilgi sistemlerine ve süreçlerine ilişkin potansiyel risklerin etkileriyle birlikte tespit edilmesi ve bu çerçevede söz konusu risklerin azaltılmasına yönelik faaliyetlerin tanımlanmasını içeren risk yönetiminin gerçekleştirilmesi,

c) Bilgi güvenliği ihlallerine ilişkin olayların izlenmesi ve her yıl değerlendirilmesi,

ç) Tüm çalışanların bilgi güvenliği farkındalığını artırmaya yönelik çalışmaların yapılması ve eğitimlerin verilmesi.

(4) Bilgi sistemlerine ilişkin risklerin yönetimi amacıyla tesis edilen süreç ve prosedürler, Kurum, Kuruluş ve Ortaklıkların organizasyonel ve yönetsel yapıları içerisinde fiili olarak işleyecek şekilde yerleştirilir ve işlerliğine ilişkin gözetim ve takipler gerçekleştirilir.

(5) Bilgi sistemleri güvenliğine ilişkin süreç ve prosedürlerin gereklerinin yerine getirilmesinden ve takibinden sorumlu olan, bilgi sistemleri güvenliğiyle ilgili riskler ve bu risklerin yönetilmesi hususunda üst yönetime rapor veren ve yeterli teknik bilgi ve tecrübeye sahip bir bilgi sistemleri güvenliği sorumlusu belirlenir.

(6) Risk önceliklerine göre tüm kritik iş süreçlerinin sürekliliğini sağlamak için iş sürekliliği planı hazırlanır. Planda kritik iş süreçlerine ilişkin kabul edilebilir kesinti süreleri ile kabul edilebilir azami veri kaybı belirlenir.

Bilgi sistemleri risk yönetimi

MADDE 8 - (1) Kurum, Kuruluş ve Ortaklıklar bilgi sistemlerine ilişkin riskleri ölçmek, izlemek, işlemek ve raporlamak üzere risk yönetimi süreç ve prosedürlerini tesis eder ve güncelliğini sağlar.

(2) Bilgi sistemlerine ilişkin risklerin yönetilmesinde asgari olarak aşağıdaki hususlar değerlendirmeye katılır:

a) Bilgi teknolojilerindeki hızlı gelişmeler sebebiyle rekabetçi ortamda gelişmelere uymamanın olumsuz sonuçları, gelişmelere uyma konusundaki zorluklar ve yasal mevzuatın değişebilmesi,

b) Bilgi sistemleri kullanımının öngörülemeyen hatalara ve hileli işlemlere zemin hazırlayabilmesi,

c) Bilgi sistemlerinde dış kaynak kullanımından dolayı dış kaynak hizmeti veren kuruluşlara bağımlılığın oluşabilmesi,

ç) İş ve hizmetlerin önemli oranda bilgi sistemlerine bağlı hale gelmesi,

d) Bilgi sistemleri üzerinden gerçekleştirilen işlemlerin, verilerin ve denetim izlerine ilişkin tutulan kayıtların güvenliğinin sağlanmasının zorlaşması.

(3) Bilgi sistemlerine ilişkin risk analizi yapılır. Yılda en az bir defa veya bilgi sistemlerinde meydana gelebilecek önemli değişikliklerde tekrarlanır.

(4) Bilgi sistemlerinin teknik açıklarına ilişkin bilgi, zamanında elde edilir ve kuruluşun bu tür açıklara karşı zafiyeti değerlendirilerek, riskin ele alınması için uygun tedbirler alınır.

(5) Kurum, Kuruluş ve Ortaklıkların bilgi sistemleri, bilgi güvenliği gereklerinin yerine getirilmesi hususunda herhangi bir görevi bulunmayan ve sızma testi konusunda ulusal veya uluslararası belgeye sahip gerçek veya tüzel kişiler tarafından en az yılda bir kez sızma testine tabi tutulur.

(6) Sızma testinde bu Tebliğin 1 numaralı ekinde yer alan usul ve esaslar uygulanır.

ÜÇÜNCÜ BÖLÜM
Bilgi Sistemleri Kontrollerine İlişkin Esaslar

Bilgi sistemleri kontrollerinin tesisi ve yönetilmesi

MADDE 9 - (1) Kurum, Kuruluş ve Ortaklıkların üst yönetimi, bilgi güvenliği politikası kapsamında, bilgi sistemlerinden kaynaklanan güvenlik risklerinin yeterli düzeyde yönetildiğinden emin olmak için, bilgi sistemlerinin ve üzerinde işlenmek, iletilmek, depolanmak

üzere bulunan verilerin gizlilik, bütünlük ve erişilebilirliklerini sağlayacak önlemlere ilişkin kontrollerin geliştirilmesini, işletilmesini, güncelliğini sağlar ve gerekli yönetsel sorumlulukları tanımlar.

(2) Bilgi sistemleri kontrolleri kapsamında asgari olarak aşağıdaki hususlar dikkate alınır:

a) Her kontrol süreci için süreç sahibinin, rollerin, faaliyetlerin ve sorumlulukların açık bir şekilde tanımlanması,

b) Kontrol süreçlerinin periyodik biçimde tanımlanması,

c) Her kontrol sürecinin hedef ve amaçlarının açıkça tanımlanmış olması ve performansının ölçülebilir olması.

(3) Bilgi sistemleri kontrollerine ilişkin etkinlik, yeterlilik ve uygunluk ile öngörülen risk ya da risklerin etkisini azaltmaya yönelik faaliyetler devamlı bir şekilde takip edilir ve değerlendirilir. Değerlendirme neticesinde tespit edilen önemli kontrol eksiklikleri üst yönetime raporlanır ve gerekli önlemlerin alınması sağlanır.

Varlık yönetimi

MADDE 10 - (1) Kurum, Kuruluş ve Ortaklıklar, sahip oldukları bilgi varlıklarını ve bu varlıkların sorumlularını belirler, bu varlıkların envanterini oluşturur ve envanterin güncelliğini sağlar.

(2) Bilgi varlıkları önem derecelerine göre sınıflandırılır.

(3) Taşınabilir ortamlar, içerdiği bilgilerin hassasiyet derecesine göre kaybolma veya hırsızlık risklerine karşı korunur ve önem derecesi yüksek bilgileri veya bu bilgilere erişim sağlayan yazılımları barındıran taşınabilir ortamlar yetkilendirme olmaksızın kurum dışına çıkarılmaz.

(4) Depolama ortamları elden çıkarılmadan önce üzerinde kuruluşa ait veri, bilgi ve lisanslı yazılımın bulunmamasına yönelik gerekli önlemler alınır.

(5) Temiz masa ve temiz ekran ilkeleri benimsenir.

Görevler ayrılığı prensibi

MADDE 11 - (1) Bilgi sistemleri üzerinde hata, eksiklik veya kötüye kullanım risklerini azaltmak için görev ve sorumluluk alanları ayrılır. Sistem, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görevler ayrılığı prensibi uygulanır. Görev ve sorumluluklar belirli aralıklarla gözden geçirilir ve güncelliği sağlanır.

(2) Bilgi sistemleri süreçleri tasarlanırken kritik işlemlerin tek bir personele veya dış kaynak hizmeti sunan kuruluşa bağımlı olmaması göz önünde bulundurulur.

(3) Görevlerin tam ve uygun şekilde ayrılmasının mümkün olmadığı durumlarda oluşabilecek hata, eksiklik veya kötüye kullanımı önlemeye ve tespit etmeye yönelik telafi edici kontroller tesis edilir.

Fiziksel ve çevresel güvenlik

MADDE 12 - (1) Fiziksel erişimin yalnızca yetkilendirilmiş kişilerce yapılmasını sağlamak amacıyla, güvenli alanlar gerekli giriş kontrolleriyle korunur.

(2) Güvenli alanlara giriş ve çıkışlar gerekçelendirilir, yetkilendirilir, kaydedilir ve izlenir.

(3)Yangın, sel, deprem, patlama, yağma ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanır ve uygulanır.

Ağ güvenliği

MADDE 13 - (1) Ağların tehditlere karşı korunması ve ağları kullanan sistem, veri tabanı ve uygulamaların güvenliğinin sağlanması için kontroller tesis edilir ve etkin bir şekilde yönetilir.

(2) İletişim altyapıları dinlemeye ve fiziksel hasarlara karşı korunur.

(3) Mobil cihazların ağ erişimine ilişkin risklere yönelik güvenlik önlemleri alınır ve uygulanır.

(4) Bilgi sistemleri altyapısına yönelik yetkisiz erişimler engellenir ve gözetim süreçleri tesis edilir.

(5) Yüksek riskli uygulamaların güvenlik düzeyini artırmak için bağlantı süreleri ile ilgili kısıtlamalar kullanılır.

(6) İç kaynak yoluyla sağlanan veya dış kaynak kullanımı yoluyla alınan her türlü ağ hizmetinin güvenlik kriterleri, hizmet düzeyleri ve yönetim gereksinimleri tanımlanır ve hizmet anlaşmalarına dâhil edilir.

(7) Uzaktan erişim sağlayan kullanıcıları kontrol etmek için gerekli yetkilendirmeler yapılır. Bu kapsamda belirli konumlardan ve ekipmanlardan gelen bağlantıları yetkilendirmek için otomatik ekipman tanımlaması göz önüne alınır.

(8) Kurumsal ağ dışındaki ağlarla olan iletişimde, dış ağlardan gelebilecek tehditler için sürekli gözetim altında tutulan güvenlik duvarı çözümleri kullanılır.

(9) İç ağın farklı güvenlik gereksinimlerine sahip alt bölümleri birbirinden ayrılarak, denetimli geçişi temin eden kontroller tesis edilir.

Kimlik doğrulama

MADDE 14 - (1) Bilgi sistemleri üzerinden gerçekleşen işlemler için, risk değerlendirmesi sonucuna uygun kimlik doğrulama yöntemi belirlenir. Yöntem tercih edilirken, bilgi sistemleri üzerinden gerçekleştirilmesi planlanan işlemlerin niteliği, doğurabileceği finansal veya finansal olmayan etkilerinin büyüklüğü, işleme konu verinin, hassasiyeti ve kimlik doğrulama yönteminin kullanım kolaylığı göz önünde bulundurulur.

(2) Kimlik doğrulama yöntemi, müşterilerin ve personelin bilgi sistemlerine dâhil olmalarından, işlemlerini tamamlayıp sistemden ayrılmalarına kadar geçecek tüm süreci kapsayacak şekilde uygulanır. Kimlik doğrulama bilgisinin oturumun başından sonuna kadar doğru olmasını garanti edecek gerekli önlemler alınır. Parola kullanımı gerektiren kimlik doğrulama yöntemlerinde, parolaların tahmin edilmesi ve kırılması zor bir karmaşıklıkta ve uzunlukta olması sağlanır.

(3) Kullanılan kimlik doğrulama verilerinin tutulduğu ortamların ve bu amaçla kullanılan araçların güvenliğini sağlamaya yönelik gerekli önlemler alınır. Bu önlemler asgari olarak kimlik doğrulama verilerinin şifreli olarak saklanması, bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemlerin kurulması, yeterli denetim izlerinin tutulması ve güvenliğinin sağlanması hususlarını içerir. Kimlik doğrulama verilerinin aktarımı sırasında gizliliğinin sağlanmasına yönelik önlemler alınır.

Yetkilendirme

MADDE 15 - (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerine erişim için uygun bir yetkilendirme ve erişim kontrolü tesis eder. Yetkilendirme düzeyi ve erişim haklarının atanmasında görev ve sorumluluklar göz önünde bulundurularak, gerekli olacak en düşük

yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yaklaşımı esas alınır. Atanacak yetkiler ve sorumluluklar görevler ayrılığı ilkesi ile tutarlı olur.

(2) Tüm yetkiler ve erişim hakları her yıl güncel durumla uyumlulukları açısından değerlendirilmeye tabi tutulur.

(3) Yetkilendirme verilerinin güvenliği sağlanır ve bu veriler üzerinde yapılacak her türlü değişikliği algılayacak sistemler kurulur. Yetkilendirme verilerinin tutulduğu ortamlara yetkisiz erişim teşebbüsleri kayıt altına alınır ve düzenli olarak gözden geçirilir.

(4) İstihdamın sonlanması durumunda, ilgili tüm yetkilendirmeler ivedilikle iptal edilir.

İşlemlerin, kayıtların ve verilerin bütünlüğü

MADDE 16 - (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri üzerinden gerçekleşen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli önlemleri alır. Bütünlüğü sağlamaya yönelik önlemler verinin iletimi, işlenmesi ve saklanması aşamalarının tamamını kapsayacak şekilde tesis edilir. Bilgi sistemlerine ilişkin dış kaynak hizmeti alınan kuruluşlar nezdinde gerçekleşen işlemler için de aynı yaklaşım gösterilir.

(2) Kritik işlemler, kayıtlar ve verilerde meydana gelebilecek bozulmaları saptayacak teknikler kullanılır.

Veri gizliliği

MADDE 17 - (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak önlemleri alır. Gizliliği sağlamak üzere yapılacak çalışmalar asgari olarak aşağıda belirtilen hususları içerir:

a) Bilgi sistemleri yapısı ile iş ve işlem çeşitliliği göz önünde bulundurularak verilerin önem derecesine uygun önlemlerin alınması,

b) Verilere erişim haklarının kişilerin görev ve sorumlulukları çerçevesinde belirlenmesi, erişimlerin kayıt altına alınması, bu kayıtların yetkisiz erişim ve müdahalelere karşı korunması,

c) Veri gizliliğini sağlamada şifreleme tekniklerinin kullanılması durumunda, güvenilirliği ve sağlamlığı ispatlanmış algoritmaların kullanılması; geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılmasının engellenmesi, verinin ve operasyonun önem düzeyine göre anahtarların değiştirilme sıklıklarının belirlenmesi.

(2) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri faaliyetleri kapsamında gerçekleşen işlemlere ilişkin iletilen, işlenen ve saklanan önem derecesi yüksek verilerin kasten veya yanlışlıkla kurum dışına sızmasını önlemeye yönelik olarak gerekli önlemleri alır.

Bilgi sistemlerine ilişkin dış kaynak yoluyla alınan hizmetlerin yönetimi

MADDE 18 - (1) Kurum, Kuruluş ve Ortaklıkların üst yönetimi tarafından, bilgi sistemleri kapsamında dış kaynak yoluyla alınacak hizmetlerin doğuracağı risklerin yeterli düzeyde değerlendirilmesine, yönetilmesine ve dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlarla ilişkilerin etkin bir şekilde yürütülebilmesine olanak sağlayacak bir gözetim mekanizması tesis edilir. Tesis edilecek gözetim mekanizması asgari olarak aşağıda belirtilen hususları içerir:

a) Dış kaynak yoluyla alınan bilgi sistemleri hizmeti kapsamındaki tüm sistem ve süreçlerin Kurum, Kuruluş ve Ortaklıkların kendi risk yönetimi, güvenlik, gizlilik ve müşteri gizliliğine ilişkin ilkelerine uygun olması,

b) Kurum, Kuruluş ve Ortaklıkların verilerinin dış kaynak yoluyla alınan bilgi sistemleri hizmeti sağlayan kuruluşa aktarılmasının gerekli olduğu durumlarda, söz konusu kuruluşun bilgi güvenliği konusundaki ilke ve uygulamalarının en az Kurum, Kuruluş ve Ortaklıkların uyguladığı düzeyde olması,

c) Dış kaynak yoluyla alınan bilgi sistemleri hizmetine ilişkin hususların Kurum, Kuruluş ve Ortaklıkların iş sürekliliği göz önünde bulundurularak düzenlenmesi ve gerekli önlemlerin alınması,

ç) Dış kaynak yoluyla alınan bilgi sistemleri hizmetlerinde ölçme, değerlendirme, raporlama ve güvenlik fonksiyonlarında nihai sorumluluğun Kurum, Kuruluş ve Ortaklıklarda olması,

d) Dış kaynak yoluyla alınan hizmetin, Kurum, Kuruluş ve Ortaklıkların yasal yükümlülüklerini yerine getirmelerini ve etkin biçimde denetlenmelerini engelleyici nitelikte olmaması,

e) Kurum, Kuruluş ve Ortaklıkların önem arz eden konulara ilişkin dış kaynak hizmeti aldıkları kuruluşlarla sözleşme imzalamadan önce ilgili kuruluş bünyesinde dış kaynak hizmetini istenilen kalitede gerçekleştirebilecek düzeyde teknik donanım ve altyapı, mali güç, tecrübe, bilgi birikimi ve insan kaynağı bulunup bulunmadığı hususlarını da dikkate alacak şekilde inceleme ve değerlendirme çalışması yapmaları ve bu çalışma sonucunda hazırlanacak teknik yeterlilik raporunun üst yönetime sunulması.

(2) Dış kaynak kullanımına ilişkin koşul, kapsam ve her türlü diğer tanımlama, dış kaynak yoluyla alınan hizmeti sağlayan kuruluşça da imzalanmış olacak şekilde sözleşmeye bağlanır. Sözleşme, asgari olarak aşağıdaki hususları içerir:

a) Hizmet seviyelerine ilişkin tanımlamalar,

b) Hizmetin sonlandırılmasına ilişkin koşullar,

c) Hizmetin, beklenmedik şekillerde sonlandırılması veya kesintiye uğraması durumunda uygulanacak yaptırımlar,

ç) Kurum, Kuruluş ve Ortaklıkların bilgi güvenliği politikası dâhilinde önem arz eden konulara ilişkin gereklilikler,

d) Sözleşme kapsamında üretilecek ürün bulunması halinde, ürünün sahipliği ile fikri ve sınai mülkiyet haklarını da göz önünde bulundurarak düzenleyen hükümler,

e) Sözleşmede dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlar için yükümlülük teşkil eden hükümlerin, alt yüklenici kuruluşlar ile yapılacak olan sözleşmelerde de bağlayıcı maddeler olarak yer almasını sağlayacak hükümler,

f) Hizmet sağlayıcı kuruluşun, sermaye piyasası mevzuatı kapsamında Kurul tarafından talep edilecek bilgileri istenen zamanda ve nitelikte sağlamasına ilişkin yükümlülüğü ve Kurul'un sözleşme kapsamında sunulan hizmet ile ilgili olarak hizmet sağlayıcı bünyesindeki gerekli gördüğü her türlü bilgi, belge ve kayda erişim hakkı.

(3) Dış kaynak yoluyla alınan hizmeti sağlayan kuruluşlara verilen erişim hakları özel olarak değerlendirilir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılır, gerekiyorsa ek kontroller tesis edilir. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim türü, erişilecek verinin önemi ile erişimin bilgi güvenliği üzerindeki etkileri dikkate alınır. Alınan hizmetin sonlanması durumunda ilgili tüm erişim hakları iptal edilir.

(4) Kurum, Kuruluş ve Ortaklıkların üst yönetimi, dış kaynak yoluyla gerçekleştirilen hizmetler için hizmetin erişilebilirliğini, performansını, kalitesini, bu hizmet kapsamında

gerçekleşen güvenlik ihlali olayları ile dış kaynak yoluyla hizmet sağlayan kuruluşun güvenlik kontrollerini, finansal koşullarını ve sözleşmeye uygunluğunu yakından takip etmek için yeterli bilgi ve tecrübeye sahip sorumluları belirler.

Müşteri bilgilerinin gizliliği

MADDE 19 - (1) Kurum, Kuruluş ve Ortaklıklar bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin gizliliğini sağlamaya yönelik kontrolleri tesis eder ve bunların gerektirdiği önlemleri alır.

(2) Kurum, Kuruluş ve Ortaklıklar personelin kişisel verilerin korunması ve işlenmesine uygun davranışlarını temin etmelerine yönelik gerekli tedbirleri alırlar. Bu maddede yer almayan durumlarda 24/3/2016 tarihli ve 6698 sayılı Kişisel Verilerin Korunması Kanunu uygulanır.

Müşterilerin bilgilendirilmesi

MADDE 20 - (1) Kurum, Kuruluş ve Ortaklıklar tarafından elektronik ortamda sunulan hizmetlerden yararlanacak müşteriler, sunulan hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilir ve söz konusu hizmetlere ilişkin risklerin etkisini azaltmaya yönelik olarak benimsenen bilgi güvenliği ilkeleri ve bu risklerden korunmak için kullanılması gereken yöntemler müşterilerin dikkatine sunulur.

(2) Bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yaşayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmalar oluşturulur. Şikâyet ve uyarılar değerlendirilerek aksaklıkları giderici çalışmalar yapılır.

Üçüncü taraflarla bilgi değişimi

MADDE 21 - (1) Üçüncü taraflara Kurum, Kuruluş ve Ortaklıkların bilgi sistemine erişim hakkı vermeden önce gerekli güvenlik gereksinimleri tanımlanır ve uygulanır. Kurum, Kuruluş ve Ortaklıkların bilgi içeren ortamları, üçüncü taraflar ile yapılan bilgi aktarımları sırasında gerçekleşebilecek kötüye kullanım veya bozulmaya karşı korunur.

(2) Kurum, Kuruluş ve Ortaklıkların birinci fıkra kapsamında alacağı tedbirler Kurul'un bilgi alımı faaliyetlerine engel teşkil edemez.

Kayıt mekanizmasının oluşturulması

MADDE 22 - (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri üzerindeki riskleri, sistem veya faaliyetlerin karmaşıklığını ve kapsamının genişliğini göz önünde bulundurarak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması tesis eder. Bu sayede, bilgi sistemleri dâhilinde gerçekleşen ve Kurum, Kuruluş ve Ortaklıkların faaliyetlerine ait kayıtlarda değişiklik ve silmeye sebep olan işlemlere ilişkin denetim izlerinin yeterli detayda ve açıklıkta kaydedilmesi temin edilir. Kayıt mekanizmasının yetkisiz sistemsel ve kullanıcı erişimlerine karşı korunmasına yönelik önlemler alınır.

(2) Denetim izlerinin bütünlüğünün bozulmasının önlenmesi ve herhangi bir bozulma durumunda bunun tespit edilebilmesi için gerekli teknikler kullanılır. Denetim izlerinin bütünlüğü düzenli olarak gözden geçirilir ve olağandışı durumlar üst yönetime raporlanır.

(3) Denetim izlerinde asgari olarak aşağıdaki bilgiler tutulur:

a) Yapılan işlemlerin türü ve niteliği,

b) İşlemlere ilişkin yetkisiz erişim teşebbüsleri,

c) İşlemi gerçekleştiren uygulama,

ç) İşlemi gerçekleştiren kişinin kimliği,

d) Yapılan işlemlerin zamanı.

(4) Denetim izleri asgari 5 yıl saklanır. Denetim izlerinin, yeterli güvenlik düzeyine sahip ortamlarda korunması ve yedeklerinin alınması suretiyle, yaşanması muhtemel olumsuzluklar sonrasında da öngörülen süre için erişilebilir olmaları temin edilir.

(5) Dış kaynak hizmeti alınan kuruluşlar, müşteriler ve personel, bilgi sistemleri üzerindeki aktivitelerinin kaydının tutulduğu konusunda bilgilendirilir.

(6) Denetim izlerinin tutulması, mevzuatın diğer hükümleri gereği Kurum, Kuruluş ve Ortaklıkların belge saklamasına ilişkin yükümlülüklerini değiştirmez.

Zaman senkronizasyonu

MADDE 23 - (1) Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinde kullandıkları zaman bilgisi tek bir referans kaynağına göre senkronize edilir. Zaman bilgisi atomik saatler vasıtasıyla temin edilir.

Bilgi güvenliği ihlali

MADDE 24 - (1) Kurum, Kuruluş ve Ortaklıklar, bünyelerinde gerçekleşen her türlü bilgi güvenliği ihlal olayının ve bilgi sistemlerine ilişkin ortaya çıkan zayıflıkların yönetilmesini sağlayacak kontrolleri tesis eder. Bu kontroller asgari olarak aşağıdaki hususları içerir:

a) Gerçekleşen ihlal veya ortaya çıkan zayıflığın mümkün olan en kısa sürede kayda alınması ve çözülmesi için gerekli mekanizmaların kurulması, sorumlulukların belirlenmesi ve tüm personelin bilgilendirilmesi,

b) İhlal olayını veya zayıflığı bildiren kişinin, işlemin sonucu hakkında bilgilendirilmesi,

c) Bildirimi yapılan tüm ihlal olayı ve zayıflıkların kök sebebinin bulunması ve düzeltici faaliyetlerin uygulanması,

ç) Kritik ihlal olayları veya zayıflıkların üst yönetime raporlanması,

d) Tüm ihlal ve zayıflıkların; türü, ortaya çıkış zamanı, etkilediği bilgi sistemleri, iş süreçleri ve etki alanı ile buna karşı gerçekleştirilen düzeltici faaliyetler, harcanan zaman, maliyet ve işgücü miktarının kayda alınması,

e) Tekrarlayan veya benzer ihlal veya zayıflıklara organizasyonun hazırlıklı olmasının sağlanması.

Bilgi sistemleri edinimi, geliştirilmesi ve bakımı

MADDE 25 - (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemleri edinimi, geliştirilmesi ve bakımı için kontrolleri tesis eder. Bu kontroller asgari olarak aşağıdaki hususları içerir:

a) Kurum, Kuruluş ve Ortaklıkların kendi bünyesinde geliştirilecek, değiştirilecek veya dış kaynak hizmeti yoluyla edinilecek her türlü bilgi sisteminin, fonksiyonel gereksinimleri ile tasarım, geliştirme ve test aşamalarının her biri için teknik ve güvenlik gereksinimleri yazılı hale getirilir,

b) Temin edilecek bilgi sistemleri yapısının Kurum, Kuruluş ve Ortaklıkların ölçeği, faaliyetlerinin ve sunulan ürünlerin niteliği ve karmaşıklığı ile uyumlu olması zorunludur.

c) Bilgi sistemlerinin geliştirme, değişiklik veya edinimi faaliyeti boyunca, işin gelişimini takip edebilmek için proje gelişim raporları hazırlanır ve Kurum, Kuruluş ve Ortaklıkların yönetim kurulu tarafından onaylanır,

ç) Bilgi sistemlerinde yapılacak önemli güncellemelerin veya değişikliklerin iş süreçlerini aksatmaması ve bilgi güvenliği riski oluşturmaması için güncelleme veya değişikliklere ilişkin planlama, test ve uygulama adımları detaylı olarak ele alınır,

d) Uygulamalarda veri girişlerinin tam, doğru ve geçerli şekilde yapılmasını, veri üzerindeki işlemlerin doğru sonuçları üretmesini sağlayacak, veri ve işlem kaybını, verinin yetkisiz değiştirilmesini ve kötüye kullanımını önleyecek uygun kontroller tesis edilir,

e) Uygulama güvenliği ve erişilebilirlik gereksinimleri belirlenirken organizasyonun belirlemiş olduğu veri sınıflandırması ve risk öncelikleri göz önünde bulundurulur,

f) Bilgi sistemleri gerçek ortamda kullanıma alınmadan önce kabul kriterleri belirlenir, hazırlanacak bir plana göre fonksiyonel, teknik ve güvenlik gereksinimleri testlerine tabi tutulur, test verileri özenle seçilerek korunur ve kontrol edilir,

g) Gerekli hallerde değiştirilmiş veya yeni geliştirilmiş sistem, gerçek ortamda kullanıma alınmadan önce, belirli bir olgunluk seviyesine ulaşana kadar eski sistemle beraber çalıştırılmasına devam edilir; bu şekilde paralel işletimin mümkün olmadığı durumlarda ise, değiştirilmiş veya yeni geliştirilmiş sistem belirli bir olgunluk seviyesine ulaşana kadar eski sistem veri kayıpsız olarak devreye alınabilir halde tutulur,

ğ) Bilgi sistemlerinin kullanımı ile ilgili gerekli eğitim materyalleri oluşturulur,

h) Geliştirme, test ve gerçek ortamdaki işlemler ile bu işlemlerin gerçekleştiği ortamlar, yetkisiz erişim ve değişim riskine karşı birbirinden ayrılır.

Bilgi sistemleri sürekliliği

MADDE 26 – (1) Kurum, Kuruluş ve Ortaklıkların birincil ve ikincil sistemlerini yurt içinde bulundurmaları zorunludur.

(2) Kurum, Kuruluş ve Ortaklıklar faaliyetlerini destekleyen bilgi sistemlerinin sürekliliğini sağlamak üzere iş sürekliliği planının bir parçası olan bilgi sistemleri süreklilik planını hazırlar.

(3) Plan kapsamında ikincil sistem tesis edilir ya da bu hizmeti destek hizmeti kuruluşlarından tedarik etme hususunda güvence sağlayan anlaşmalar yapılır. İkincil sistemde, Kurum, Kuruluş ve Ortaklıkların veri ve sistem yedekleri kullanıma hazır bulundurulur.

(4) Plan, iş süreklilik planında belirlenen hedefleri de dikkate alacak şekilde, kritik iş süreçlerini destekleyen bilgi sistemleri hizmetlerine yönelik hazırlanır. Bu çerçevede hizmetlerin tekrar kullanıma açılmasını sağlayacak alternatifli kurtarma süreç ve prosedürleri tesis edilir ve gerekli önlemler alınır.

(5) Plan kapsamında, performans takibi ve kapasite planlaması yapılır, sistem kaynaklarının kullanımı izlenir.

(6) Bilgi sistemleri altyapısından kaynaklanabilecek kesintilere, işlem performansını düşürecek veya iş sürekliliğini aksatacak durumlara karşı gerekli önlemler alınır.

(7) Bilgi sistemlerinin sürekliliğini sağlamak amacıyla, risk değerlendirmesi, risk azaltma ve risk izleme faaliyetleri gerçekleştirilir.

(8) Plan, iş süreçlerini veya bilgi sistemlerini etkileyecek değişikliklerden sonra gözden geçirilerek güncellenir. Planın etkinliğini ve güncelliğini temin etmek üzere testler yapılır, testlere

varsa dış kaynak yoluyla hizmet alınan kuruluşlar da dâhil edilir ve test sonuçları üst yönetime raporlanır. Testler, her yıl tekrarlanır.

(9) Bilgi sistemleri, iş sürekliliği planındaki önceliklere uygun olarak yedeklenir ve yedekten geri dönülmesi için gerekli süreçler bilgi sistemleri sürekliliği planına ve testine dâhil edilir.

(10) Kurum, Kuruluş ve Ortaklıklar, bilgi güvenliği politikasının, bilgi sistemleri süreklilik planının, ağ topolojisinin, bilgi sistemleri varlık envanteri ile iş sürekliliği ve güvenliği açısından önem arz eden diğer dokümanların güncel sürümlerini ve bilgi sistemleri yönetimine ilişkin parolalarını güvenli ortamlarda saklar.

Değişiklik yönetimi

MADDE 27- (1) Kurum, Kuruluş ve Ortaklıklar, bilgi sistemlerini oluşturan her türlü yazılım, donanım ve altyapı bileşenlerine, dokümantasyona ve bilgiye yapılan değişiklikleri yönetebilmek amacıyla kontroller geliştirir. Bu kontroller en az aşağıdaki hususları içerir:

a) Yapılacak her türlü değişiklik için; değişikliğin sebebini, kapsamını, etkisini, içerdiği riskleri, beklenen faydasını, değişikliği yapacak kişileri, maliyetini, gerekli test ve eğitim faaliyetlerini tanımlayan kayıtlar oluşturulur,

b) Planlanan değişiklikler onay sürecinden geçmedikçe işleme konulmaz,

c) Planlanan değişiklikler, devreye alınma tarihleri, test ve eğitim faaliyetleriyle ilgili düzenlemeler ilgili tüm taraflara önceden duyurulur,

ç) Değişikliğin uygulanmasında ortaya çıkan hatalar ve öngörülemeyen durumlarda uygulamaya alınacak geri dönüş prosedürleri ve bunlarla ilgili sorumluluklar önceden belirlenir,

d) Gerçekleştirilen değişikliklerin sonuçları gözden geçirilir,

e) Gerçekleştirilen, iptal edilen veya reddedilen tüm değişiklikler gerekçeleriyle birlikte kayda geçirilir ve saklanır.

DÖRDÜNCÜ BÖLÜM
Muafiyetler, Diğer Hususlar, Yürürlük ve Yürütme

Muafiyetler

MADDE 28 - (1) Asgari özsermaye yükümlülüğü 5 milyon TL ve daha az olan portföy yönetim şirketleri ve Sermaye Piyasası Lisanslama Sicil ve Eğitim Kuruluşu A.Ş. 24 üncü ve 27 nci maddeleri uygulamak zorunda değildir.

(2) Dar yetkili aracı kurumlar, varlık kiralama şirketleri, ipotek finansmanı kuruluşları, Türkiye Sermaye Piyasaları Birliği, Türkiye Değerleme Uzmanları Birliği, bağımsız denetim, derecelendirme ve değerleme kuruluşları, halka açık ortaklıklar, varlık finansmanı fonları, kolektif yatırım kuruluşları, emeklilik yatırım fonları, konut finansmanı fonları 7 nci maddenin beşinci fıkrası, 8 inci maddenin dördüncü, beşinci ve altıncı fıkralarını, 14 üncü maddenin üçüncü fıkrasını, 15 inci maddenin üçüncü fıkrasını, 17 nci maddenin ikinci fıkrasını, 18 inci maddenin dördüncü fıkrasını, 22 nci maddenin ikinci fıkrasını, 24 üncü maddeyi, 25 inci maddenin birinci fıkrasının (b), (d) ve (ğ) bendini, 26 ncı maddenin üçüncü fıkrasını ve 27 nci maddeyi uygulamak zorunda değildir.

(3) Kurul bu maddenin birinci ve ikinci fıkralarında belirlenen muafiyetleri kısmen veya tamamen kaldırmaya, bunların kapsam ve içeriğini Kurum, Kuruluş ve Ortaklıklar bazında değiştirmeye yetkilidir.

(4) **(EK:RG-09/01/2020-31003)**) Birinci fıkrada belirtilen asgari özsermaye yükümlülük tutarı için, 2/7/2013 tarihli ve 28695 sayılı Resmî Gazete'de yayımlanan Portföy Yönetim Şirketleri ve Bu Şirketlerin Faaliyetlerine İlişkin Esaslar Tebliği (III-55.1)'nin 28 ve 41 inci maddeleri kapsamında Kurulca yeniden değerleme kapsamında belirlenen ve ilan edilen tutarlar esas alınır.

Diğer Hususlar

MADDE 29 - (1) Bu Tebliğ hükümleri esas olmak üzere, tezgahüstü türev araç işlemi gerçekleştiren aracı kurumların bilgi işlem altyapılarına ilişkin olarak ilgili Kurul düzenlemelerinde belirlenen ilke ve esaslara uyulur.

Yürürlük

MADDE 30- (1) Bu Tebliğ yayımı tarihinde yürürlüğe girer.

Yürütme

MADDE 31 - (1) Bu Tebliğ hükümlerini Kurul yürütür.

EK-1

Bilgi Sistemleri Sızma Testleri Usul ve Esasları

1) Amaç: Sızma testlerinin amacı, Kurum Kuruluş ve Ortaklıkların bilgi sistemlerinde tespit edilen açıklıkların ve zafiyetlerin kullanılmasıyla sistemlere sızma girişimlerinin önceden tespit edilmesi ve düzeltilmesidir.

2) Kapsam: Sızma testleri kapsamında gerçekleştirilecek testler asgari olarak aşağıdaki başlıkları kapsar:

a. İletişim Altyapısı ve Aktif Cihazlar
b. DNS Servisleri
c. Etki Alanı ve Kullanıcı Bilgisayarları
ç. E-posta Servisleri
d. Veritabanı Sistemleri
e. Web Uygulamaları
f. Mobil Uygulamalar
g. Kablosuz Ağ Sistemleri
ğ. Dağıtık Servis Dışı Bırakma Testleri
h. Sosyal Mühendislik Testleri

3) Metodoloji: Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonrası saptanan açıklık ve bulgular, Kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgular da raporlanır. Bulgular, **"Bulgu Önem Dereceleri"** bölümünde yer verilen dereceler kullanılarak "**Bulgu Formatı**" bölümünde tariflenen formata uygun olacak şekilde sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır. Sızma testleri gerçekleştirilirken, Kurum, Kuruluş ve Ortaklıklar faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol açabilecek tüm testler Kurum, Kuruluş ve Ortaklıklar ile koordineli bir şekilde planlanarak gerçekleştirilir.

a. Testlerin Gerçekleştirileceği Erişim Noktaları

Sızma testlerinin gerçekleştirileceği asgari erişim noktaları aşağıda tanımlanmaktadır. Bu noktalardan sisteme erişildikten sonra, sızma testleri gerçekleştirilir.

i. İnternet: Kurum, Kuruluş ve Ortaklıkların internet üzerinden erişilebilen tüm sunucu ve servislerine İnternet üzerinden erişilerek sızma testleri gerçekleştirilir ve devamında ve detaylı sızma testleri uygulanır.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağı: Kurum, Kuruluş ve Ortaklıkların iç ağında yer alan ve test kapsamında ele alınan sunuculara Kurum, Kuruluş ve Ortaklıklar iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ

kullanılır ve testi gerçekleştirecek şahıslara kullanımı en yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.

b. Testlerin Gerçekleştirileceği Kullanıcı Profilleri

Sızma testlerinin sağlıklı bir şekilde gerçekleştirilebilmesi ve testlerin gerçek hayata uygun olması için, yukarıda tanımlanan erişim noktalarına bu ortamların doğasına uyacak şekilde aşağıdaki kullanıcı profilleri ile sızma testleri gerçekleştirilir.

i. Anonim kullanıcı profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıkların web servislerine erişebilen ancak web uygulamalarına giriş yetkilerine sahip olmayan kullanıcıyı temsil eder. Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olmayan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

ii. Kurum, Kuruluş ve Ortaklıklar müşterisi profili: İnternet üzerinden, Kurum, Kuruluş ve Ortaklıklar'ın web servislerine erişebilen ve web uygulamalarına giriş yetkilerine sahip olan kurumsal veya bireysel kullanıcıları temsil eder. İnternet üzerinde Kurum, Kuruluş ve Ortaklıklara ait web uygulamalarının üyesi olan kullanıcıların sistem için oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır.

iii. Kurum, Kuruluş ve Ortaklıklar çalışanı profili: Kurum, Kuruluş ve Ortaklıklar personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile gerçekleştirilecek testlerde, Kurum, Kuruluş ve Ortaklıklarda çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici(local admin) yetkisine sahip çalışan profilleri ile de sızma testleri gerçekleştirilir. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile yapılan testlerde, testi yapan kişi/kuruluşa Kurum, Kuruluş ve Ortaklıklar tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

iv. Diğer kullanıcı profilleri: Sızma testlerinin, yukarıda tanımlanan diğer dört kullanıcı profiline uymayan bir kullanıcı profili ile gerçekleştirilmesi durumunda, kullanılan her bir profil için tanımlanan hak ve yetkiler bu başlık altında açıkça ifade edilir.

c. Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

Sızma testleri aşağıda tanımlanan sistem tespiti, servis tespiti ve açıklık taraması/araştırması adımları ile başlar. Sistem tespiti, servis tespiti ve açıklık taraması/araştırması tüm bilgi sistemi varlıklarına uygulanır.

i. Sistem tespiti: Sunucu veya aktif/pasif ağ cihazlarının sistem/yapılandırma bilgilerinin tespit edilmeye çalışıldığı adımdır.

ii. Servis tespiti: Kurum, Kuruluş ve Ortaklıklar bilgi sistemlerinde yer alan varlıkların port taramasının gerçekleştirildiği ve dış dünyaya/genel erişime açık olan portların sunduğu servislerin tespit edilmeye çalışıldığı adımdır.

iii. Açıklık taraması/araştırması: Kurum, Kuruluş ve Ortaklıkların bileşenleri ve bu bileşenlerin sunduğu servislerin açıklık tarayıcıları ile güncel açıklıklara karşı tarandığı ve muhtemel güvenlik açıklıklarının belirlenmeye çalışıldığı adımdır. Bu adımda ayrıca, tespit edilen muhtemel açıklıklar için açıklık veritabanları gibi kaynaklar kullanılarak bu açıklıkların bileşenlere ve bileşenlerin etkileşimde olduğu sistemlere güvenlik açısından etkileri araştırılır.

d. Sızma Testleri

i. İnternet üzerinden gerçekleştirilecek temel sızma testleri: Kurum, Kuruluş ve Ortaklıklar ağından bağımsız bir lokasyondan, Kurum, Kuruluş ve Ortaklıklar'ın internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

ii. Kurum, Kuruluş ve Ortaklıklar iç ağından gerçekleştirilecek sızma testleri: Kurum, Kuruluş ve Ortaklıkların iç ağında sistem tespiti, servis tespiti ve açıklık taraması adımlarının yanında aşağıdaki faaliyetlerin gerçekleştirilmesi sağlanır:

- Kurum yerel ağ haritası tespiti
- Belirlenen açık portlar üzerinden içerik filtreleme, güvenlik duvarı atlatma ve bilgi kaçırma testlerinin gerçekleştirilmesi
- Yerel alan ağı içerisinde zafiyet taraması yapılması
- Kurum yerel ağında araya girme teknikleri ile hassasiyet derecesi yüksek bilgilerin elde edilmeye çalışılması
- Elde edilen bilgiler ışığında kullanıcı bilgisayarları, sunucu sistemleri ve aktif cihazlara yönelik ele geçirme saldırılarının gerçekleştirilmesi
- Ele geçirilen sunucu ve kullanıcı bilgisayarları üzerinden daha kritik bilgilere ulaşılmaya çalışılması

4) Sızma Testi Sonuçlarının Takibi

Kurum, Kuruluş ve Ortaklıklar, sızma testleri sonucu tespit edilen bulguları, bulguların önem derecelerini, birlikte oluşturabilecekleri riskleri, tespit edildiği varlıkların değerini ve sızma testi raporlarında yer alan önerileri dikkate alarak, Kurum, Kuruluş ve Ortaklıklar yönetim kurullarınca onaylanan ve bu bulguların en kısa sürede giderilmesini amaçlayan bir aksiyon planı çerçevesinde takip eder. Sızma testleri sonucu ortaya çıkan tespitler, gerekli görülmesi halinde Kurum, Kuruluş ve Ortaklıkların teftiş kurullarının iç denetim planına da dâhil edilir. Sızma testi raporları, tamamlanmasını müteakip bir ay içinde Kurula gönderilir.

Bulgu Önem Dereceleri

Bulgu önem dereceleri beş kategoride ele alınır. Acil, kritik, yüksek, orta ve düşük şeklinde olan bu kategorilere ilişkin açıklamalar aşağıda yer almaktadır:

Önem Derecesi	**Açıklama**
Acil	Niteliksiz saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Kritik	Nitelikli saldırgan tarafından Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve sistemin tamamen ele geçirilmesi ile sonuçlanan saldırılara sebep olan açıklıklardır.
Yüksek	Kurum, Kuruluş ve Ortaklıklar dış ağından gerçekleştirilen ve kısıtlı hak yükseltilmesi veya hizmet dışı kalma ile sonuçlanan, ayrıca yerel ağdan ya da sunucu üzerinden gerçekleştirilen ve hak yükseltmeyi sağlayan saldırılara sebep olan açıklıklardır.
Orta	Yerel ağdan veya sunucu üzerinden gerçekleştirilen ve hizmet dışı bırakılma ile sonuçlanan saldırılara sebep olan açıklıklardır.
Düşük	Etkilerinin tam olarak belirlenemediği ve literatürdeki en iyi sıkılaştırma yöntemlerinin izlenmemesinden kaynaklanan eksikliklerdir.

Bulgu Formatı

Kapsam bölümünde belirtilen başlıkların her biri altında raporlanacak bulguların sunuluş biçimi aşağıda yer almaktadır:

Bulgu Referans No	**Rapordaki her bulguyu tekil olarak niteleyen harf/rakam dizisi**
Bulgu Adı	Bulguyu özet olarak ifade eden tanımlayıcı isim
Önem Derecesi	Bulgunun, EK-1'de yer verilen önem derecesi
Etkisi	Bulguda yer verilen açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel sonuç
Erişim Noktası	"3.a Testlerin Gerçekleştirileceği Erişim Noktaları" bölümünde yer verilen testin gerçekleştirildiği erişim noktası
Kullanıcı Profili	"3.b Testlerin Gerçekleştirileceği Kullanıcı Profilleri" bölümünde yer verilen testin gerçekleştirildiği kullanıcı profili
Bulgunun Tespit Edildiği Bileşen/Bileşenler1	Bulgunun tespit edildiği bileşeni niteleyen IP Numarası, URL, Sistem, Servis, Sunucu veya Varlık adı gibi bilgiler
Bulgu Açıklaması	Bulgunun detaylı açıklaması
Çözüm Önerisi	Bulgunun giderilmesi için testi gerçekleştiren kuruluş tarafından yapılacak çözüm önerisi