

VERİ MERKEZİ BİLGİ GÜVENLİĞİ STANDARDI

Versiyon 1.0

13 Kasım 2014

Giriş

Günümüzün küresel rekabet ortamında işletmeler verimliliklerini artırmak ve maliyetlerini düşürmek amacıyla bilginin depolanması ve işlenmesini gerektiren kurumsal bilgi teknolojileri uygulamalarına her geçen gün daha fazla ihtiyaç duymaktadır. Bu ihtiyaç söz konusu uygulamaların barındırıldığı ve sunulduğu veri merkezlerinin işletmeler için önemini ve değerini de artırmıştır. Diğer taraftan, veri merkezleri kurumsal bilgi ve uygulamaları toplu şekilde barındırmak için elverişli bir altyapı olsa da söz konusu bilgi ve uygulamaların değeri nedeniyle saldırganların da öncelikli hedefi haline gelmiştir. Sağladığı maliyet etkinliği nedeniyle bulut bilişim hizmetlerinin işletmelerce artan kullanımı da bu tehdidin boyutunu artırmaktadır. Bu nedenle, veri merkezlerinde bilgi güvenliğinin sağlanması her zamankinden daha fazla önem kazanmıştır.

Bu standard, veri merkezi kurup işletecek kamu kurumları ve özel sektör kuruluşlarının alması gereken bilgi güvenliği tedbirleri için kılavuzluğu ve bu standarda uygun veri merkezlerinin belgelendirilmesini amaçlamaktadır.

1. Kapsam

Bu standart, veri merkezlerinde bilgi güvenliğinin sağlanmasına yönelik asgari kriterleri kapsar. Söz konusu kriterler için iki farklı seviye belirlenmiş olup buna ilişkin detaylar Bölüm 4’de yer almaktadır.

2. Atıf Yapılan Mevzuat ve Standartlar

- Framework for Improving Critical Infrastructure Protection,

<http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf>

- Security and Privacy Controls for Federal Information Systems and Organizations (NIST Special Publication 800-53 Rev.4),

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

- Open Web Application Security Project (OWASP), www.owasp.org

- Media Destruction Guidance,

http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml

Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE),

<http://www.cert.org/resilience/products-services/octave>

3. Terimler, Tarifler, Semboller, Kısa Gösteriliş

AES : Advanced Encryption Standard

DMZ : Demilitarized Zone

DNS : Domain Name System

DSL : Digital Subscriber Line

ERP : Enterprise Resource Planning

FTP : File Transfer Protocol

HMAC: Keyed-Hash Message Authentication Code

HTTP : Hypertext Transfer Protocol

IP : Internet Protocol
IPSec : Internet Protocol Security
RAM : Random Access Memory
RPC : Remote Procedure Call)
RSA : Rivest-Shamir-Adleman
SMTP : Simple Mail Transfer Protocol
SSL : Secure Socket Layer
TCP : Transport Control Protocol
TLS : Transport Layer Security
UDP : User Datagram Protocol
VLAN: Virtual Local Area Network
VPN : Virtual Private Network
3DES : Triple Data Encryption Standard

4. Tanımlar

Bilgi güvenliği: Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin temin edilmesi.

Bilgi varlığı: Veri merkezinin işlevini sağlıklı şekilde yerine getirebilmesi için ihtiyaç duyulan sayısal ortamdaki bilgiler ile bu bilgileri işlemek, saklamak ve iletmek amacıyla kullanılan yazılım ve donanımların tümü.

Güvenlik kontrolü: Bilgi güvenliğini sağlamaya yönelik olarak alınan teknik ve/veya idari tedbir.

Güvenlik olayı: Bilgi güvenliğini tehdit edebilecek nitelikteki olay.

Veri merkezi: Belirli hizmetlerin sunulması amacıyla bilginin merkezi olarak saklanmasını ve işlenmesini sağlayan yazılım ve donanımlar ile bunları barındıran fiziksel altyapıdan müteşekkil tesis.

5. Seviyelendirme Sistemi

Bu standard veri merkezlerini, uygulanması gereken bilgi güvenliği tedbirleri açısından, Seviye-1 ve Seviye-2 olarak iki farklı kategoride ele almaktadır. Standardın öngördüğü bilgi güvenliği tedbirleri bu seviyelendirmeye göre farklılık gösterir. Seviye-2 veri merkezleri için öngörülen güvenlik tedbirleri Seviye-1 veri merkezleri için öngörülenlerden daha kapsamlıdır.

6. Bilgi Güvenliği Risk Yönetimi Yaklaşımı

Risk yönetiminin amacı, veri merkezlerinin karşı karşıya olduğu bilgi güvenliği tehditlerinden kaynaklanan riski tespit ederek, eldeki finansal kaynaklar ve insan kaynaklar çerçevesinde riski azaltmak için alınabilecek önlemlere karar vermektir. Bu standardda esas alınan bilgi güvenliği risk yönetimi yaklaşımı aşağıdaki beş ana fonksiyonu kapsamaktadır;

- i. **Tanımlama:** Bu fonksiyon bilgi varlıklarını, söz konusu varlıklara yönelik bilgi güvenliği tehditlerini ve bu tehditlerden kaynaklanan riskin ne şekilde yönetileceğini belirlemeyi amaçlar.
- ii. **Koruma:** Bu fonksiyon, bilgi varlıklarının bilgi güvenliği tehditlerine karşı korunması ve/veya tehditlerden kaynaklanabilecek zararın sınırlandırılması için alınacak tedbirleri kapsar.
- iii. **Tespit:** Bu fonksiyon, bilgi güvenliği olaylarının tespit edilmesine ilişkin tedbirleri kapsar.
- iv. **Müdahale:** Bu fonksiyon, tespit edilen bilgi güvenliği olaylarına ne şekilde müdahale edileceğini belirlemeyi amaçlar.
- v. **Kurtarma:** Bu fonksiyon, bir bilgi güvenliği olayı sonrası bilgi varlıklarının olay öncesindeki sağlıklı durumuna nasıl geri döndürüleceğine yönelik tedbirleri kapsar.

Bu fonksiyonlar, hem birbirlerini tamamlayacak hem de diğerlerinden bağımsız olarak her bir fonksiyonun kendi içinde iyileştirilmesi sağlanacak şekilde uygulanmalıdır. Örneğin; bir taraftan yeni tespit edilen saldırılara yönelik ilave koruma tedbirleri alınırken diğer taraftan tespit fonksiyonunun kapsamı da değişen tehdit algısına göre güncellenmelidir.

Yukarıda bahsi geçen beş ana fonksiyon Tablo-1’de gösterilen bilgi güvenliği kontrol gruplarını kapsamaktadır.

Tablo-1: Risk yönetimi ana fonksiyonları ve kontrol grupları

Fonksiyon	Kontrol Grubu
Tanımlama	Varlık yönetimi
	İş ortamı
	Risk yönetimi
Koruma	Erişim kontrolü
	Veri güvenliği
	Bilgi koruma süreçleri
	Bakım ve olay kayıtları
	Personel güvenliği ve eğitim
Tespit	Anomali tespiti
	Güvenlik izlemesi
Mudahale	İletişim ve analiz

	Olay müdahalesi
Kurtarma	Kurtarma planlaması
	İletişim planlaması

Risk yönetimi fonksiyonları hem Seviye-1 hem de Seviye-2 veri merkezleri için aynı şekilde uygulanacaktır. Söz konusu fonksiyonların kapsadığı kontrol grupları ile kontrol grupları bünyesindeki ve Bölüm 6'da tanımlanan bilgi güvenliği kontrolleri ise veri merkezi seviyesine göre farklılık gösterebilir.

Yukarıda tanımlanan risk yönetimi yaklaşımı, bir veri merkezinin bu standardda tanımlanan kontroller çerçevesinde bilgi güvenliği açısından durumunun değerlendirilmesi, eksikliklerinin tespiti, bu eksikliklerin giderilmesi için planlama yapılması ve kurumsal önceliklerin gerektirdiği durumlarda kontrol grupları kapsamına yeni kontrollerin ilave edilerek bunların mevcut kontrollerle ilişkisinin kurulabilmesine imkân sağlar.

7. Bilgi Güvenliği Kontrolleri

Bu bölümde, Seviye-1 ve Seviye-2 veri merkezleri için uygulanacak bilgi güvenliği kontrolleri ilgili fonksiyon ve kontrol grubu bazında tanımlanmıştır. Her güvenlik kontrolü için bir kod belirlenmiş olup ilgili güvenlik kontrollerinin listesi ile bunların detaylı açıklamaları EK-1 ve EK-2'de verilmiştir.

7.1. Seviye-1 Veri Merkezi için Kontroller

Seviye-1 veri merkezleri için Tablo-2'de belirtilen güvenlik kontrolleri uygulanmalıdır.

Tablo-2: Seviye-1 veri merkezi güvenlik kontrolleri

Fonksiyon	Kontrol Grubu	Kontrol	Kod
Tanımlama	Varlık yönetimi	Veri merkezi bünyesindeki fiziksel cihaz ve sistemlerin envanteri tutulacaktır.	S1.TA.VY-01
		Veri merkezi bünyesindeki yazılım platformları ve uygulamaların envanteri tutulacaktır.	S1.TA.VY-02
		Organizasyonel veri akışları dokümente edilecektir.	S1.TA.VY-03
		Harici bilgi sistemleri kataloglanacaktır.	S1.TA.VY-04
	İş ortamı	Enerji ve telekomünikasyon hizmet bağımlılıkları belirlenip dokümente edilecektir.	S1.TA.IO-01

		Bilgi güvenliğine ilişkin yasal yükümlülükler dokümanite edilecektir.	S1.TA.IO-02
	Risk Yönetimi	Veri merkezi için risk değerlendirmesi yapılacaktır.	S1.TA.RY-01
		Veri merkezi bilgi güvenliği mimarisi oluşturulacaktır.	S1.TA.RY-02
Koruma	Erişim Kontrolü	Kimlik yönetimi ve yetkilendirme sistemi oluşturulacaktır.	S1.KO.EK-01
		Bilgi varlıklarına fiziksel erişim kontrol edilecektir.	S1.KO.EK-02
		Bilgi varlıklarına uzaktan erişim kontrol edilecektir.	S1.KO.EK-03
		Veri merkezi ağı alt ağlara bölünecektir.	S1.KO.EK-04
	Veri Güvenliği	Duragan haldeki bilgiler korunacaktır.	S1.KO.VG-01
		Ag üzerinden gönderilen bilgiler korunacaktır.	S1.KO.VG-02
		İşletmeci kontrolü dışına çıkacak bilgi sistemi bileşenleri üzerindeki veriler imha edilecektir.	S1.KO.VG-03
		Veri merkezi bilgi sistemi potansiyel saldırılara karşı izlenip korunacaktır.	S1.KO.VG-04
	Bilgi Koruma Süreçleri	Bilgi sistemi bileşenleri için referans konfigürasyonlar oluşturulacak ve güncelliği sağlanacaktır.	S1.KO.BK-01
		Veri yedekleme mekanizması oluşturulacaktır.	S1.KO.BK-02
		Fiziksel işletim ortamına ilişkin politikalar belirlenecektir.	S1.KO.BK-03
		Bilgi sistemi zayıflık yönetim planı hazırlanıp uygulanacaktır.	S1.KO.BK-04
	Bakım ve Olay Kayıtları	Bilgi sisteminin kontrollü bakımı sağlanacaktır.	S1.KO.BO-01
		Olay kayıtları güvenli şekilde	S1.KO.BO-02

		saklanacaktır.	
	Personel Güvenliği ve Eğitim	Personel güvenliği süreçleri oluşturulacaktır.	S1.KO.PE-01
		Bilgi güvenliğiyle ilgili sorumlulukları olan personelin bu alandaki farkındalığı ve yetkinlikleri arttırılacaktır.	S1.KO.PE-02
Tespit	Anomali Tespiti	Güvenlikle ilgili olay kayıtları raporlanacak ve analiz edilecektir.	S1.TE.AT-01
	Güvenlik İzlemesi	Veri merkezi bilgi sistemi olası güvenlik tehditlerine karşı sürekli olarak izlenecektir.	S1.TE.GI-01
Müdahale	İletişim ve Analiz	Tespit edilen güvenlik olayları konusunda ilgili taraflar bilgilendirilecektir.	S1.MU.IA-01
	Olay Müdahalesi	Güvenlik olaylarına uygun şekilde müdahale edilecektir.	S1.MU.OM-01
Kurtarma	Kurtarma Planlaması	Veri merkezi kurtarma planı hazırlanacaktır.	S1.KU.KP-01

7.2. Seviye-2 Veri Merkezi için Kontroller

Seviye-2 veri merkezleri için Tablo-3'de belirtilen güvenlik kontrolleri uygulanmalıdır.

Tablo-3: Seviye-2 veri merkezi güvenlik kontrolleri

Fonksiyon	Kontrol Grubu	Kontrol	Kod
Tanımlama	Varlık yönetimi	Veri merkezi bünyesindeki fiziksel cihaz ve sistemlerin envanteri tutulacaktır.	S2.TA.VY-01
		Veri merkezi bünyesindeki yazılım platformları ve uygulamaların envanteri tutulacaktır.	S2.TA.VY-02
		Organizasyonel veri akışları dokümante edilecektir.	S2.TA.VY-03
		Harici bilgi sistemleri kataloglanacaktır.	S2.TA.VY-04

		Varlıklar için kritiklik değerlendirmesi yapılacaktır.	S2.TA.VY-05
	İş ortamı	Enerji ve telekomünikasyon hizmet bağımlılıkları belirlenip dokümente edilecektir.	S2.TA.IO-01
		Bilgi güvenliğine ilişkin yasal yükümlülükler dokümente edilecektir.	S2.TA.IO-02
	Risk Yönetimi	Bilgi sistemine yönelik tehditler dokümente edilecektir.	S2.TA.RY-01
		Veri merkezi risk analizi yapılacaktır.	S2.TA.RY-02
		Veri merkezi riskini kabul edilebilir seviyeye çekecek önlemler belirlenecektir.	S2.TA.RY-03
		Veri merkezi bilgi güvenliği mimarisi oluşturulacaktır.	S2.TA.RY-04
Koruma	Erişim Kontrolü	Kimlik yönetimi ve yetkilendirme sistemi oluşturulacaktır.	S2.KO.EK-01
		Bilgi varlıklarına fiziksel erişim kontrol edilecektir.	S2.KO.EK-02
		Bilgi varlıklarına uzaktan erişim kontrol edilecektir.	S2.KO.EK-03
		Veri merkezi ağı alt ağlara bölünecektir.	S2.KO.EK-04
	Veri Güvenliği	Duragan haldeki bilgiler korunacaktır.	S2.KO.VG-01
		Ağ üzerinden gönderilen bilgiler korunacaktır.	S2.KO.VG-02
		İşletmeci kontrolü dışına çıkacak bilgi sistemi bileşenleri üzerindeki veriler imha edilecektir.	S2.KO.VG-03
		Veri merkezi bilgi sistemi potansiyel saldırılara karşı izlenip korunacaktır.	S2.KO.VG-04
		Gelistirme ve test ortamı üretim ortamından ayrılacaktır.	S2.KO.VG-05
	Bilgi Koruma	Bilgi sistemi bileşenleri için referans	S2.KO.BK-01

	Süreçleri	konfigürasyonlar oluşturulacak ve güncelliği sağlanacaktır.	
		Veri yedekleme mekanizması oluşturulacaktır.	S2.KO.BK-02
		Fiziksel işletim ortamına ilişkin politikalar belirlenecektir.	S2.KO.BK-03
		Bilgi sistemi zayıflık yönetim planı hazırlanıp uygulanacaktır.	S2.KO.BK-04
	Bakım ve Olay Kayıtları	Bilgi sisteminin kontrollü bakımı sağlanacaktır.	S2.KO.BO-01
		Olay kayıtları güvenli şekilde saklanacaktır.	S2.KO.BO-02
	Personel Güvenliği ve Eğitim	Personel güvenliği süreçleri oluşturulacaktır.	S2.KO.PE-01
		Bilgi güvenliğiyle ilgili sorumlulukları olan personelin bu alandaki farkındalığı ve yetkinlikleri artırılacaktır.	S2.KO.PE-02
Tespit	Anomali Tespiti	Kullanıcıların ağ kullanım davranışlarına ve veri akışlarına ilişkin referans profiller oluşturulacaktır.	S2.TE.AT-01
		Olay kayıtları birbiriyle ilişkilendirilerek potansiyel saldırılar tespit edilecektir.	S2.TE.AT-02
		Güvenlikle ilgili olay kayıtları raporlanacak ve analiz edilecektir.	S2.TE.AT-03
	Güvenlik İzlemesi	Veri merkezi bilgi sistemi olası güvenlik tehditlerine karşı sürekli olarak izlenecektir.	S2.TE.GI-01
Müdahale	İletişim ve Analiz	Tespit edilen güvenlik olayları konusunda ilgili taraflar bilgilendirilecektir.	S2.MU.IA-01
	Olay Müdahalesi	Güvenlik olaylarına uygun şekilde müdahale edilecektir.	S2.MU.OM-01
Kurtarma	Kurtarma	Veri merkezi kurtarma planı	S2.KU.KP-01

	Planlaması	hazırlanacaktır.	
	İletişim Planlaması	Güvenlik olaylarına ilişkin kamuoyu iletişim planı hazırlanıp uygulanacaktır.	S2.KU.KP-02

EK-1: Seviye-1 Veri Merkezi Güvenlik Kontrolleri

Bu kısım Tablo-2’de yer verilen bilgi güvenliği kontrollerinin detaylı açıklamalarını içerir.

A-TANIMLAMA FONKSİYONU

Varlık Yönetimi Kontrol Grubu

Kontrol: Veri merkezi bünyesindeki fiziksel cihaz ve sistemlerin envanteri tutulacaktır.

Kod: S1.TA.VY-01

Açıklama: Veri merkezi hizmetlerinin sunumunda kullanılan fiziksel cihaz ve sistemlerin envanteri tutulacaktır. Bu envanter aşağıdaki şartları sağlamalıdır;

- Bilgi sisteminin mevcut durumunu doğru şekilde göstermelidir.
- Bilgi sistemi bileşenlerini envanter takibi yapmaya ve raporlamaya imkân verecek detayda göstermelidir. Envanter, en az, kendi başına belirli bir fonksiyon ifa eden her bir fiziksel cihazı kapsayacak detayda olmalıdır. Örneğin; sunucu donanımı, ethernet anahtar, monitör, bağımsız veri depolama veya yedekleme ünitesi, güvenlik duvarı donanımı, modem, kesintisiz güç kaynağı, vb. Söz konusu cihazların elektronik sistem bileşenleri (sabit disk, RAM, işlemci, anakart, dâhili güç kaynağı modülü, vb.) bu kapsamda değildir. Detaylandırmanın seviyesine bu çerçevede veri merkezi işletmecisi tarafından karar verilmeli ve bu seviye envanterin tutulduğu dokümanda açıklanmalıdır.
- Envanterdeki cihazların tanımlayıcı ve fonksiyonel özellikleri dokümante edilmelidir. Örneğin; cihaz üreticisi, modeli ve varsa seri numarası, sunucular için üzerindeki işlemci sayısı ve modeli, RAM miktarı, ethernet anahtarlar için port sayısı ve bant genişliği, vb.
- Ağ bağlantılı cihazlar (yönlendirici, ağ yazıcısı, modem, vb.) için cihazların ağ üzerindeki isimleri, fiziksel ve mantıksal adresleri kayıt altına alınmalıdır. Mantıksal ağ adresleri dinamik ise bu durum dokümantasyonda belirtilmelidir.
- Cihazların fiziksel olarak buldukları yer (oda, kabin, raf, vb.) açıklanmalıdır.
- Envanterdeki cihazların yönetiminden (kurulum, konfigürasyon, güncelleme, bakım, vb.) sorumlu personel belirlenip kayıt altına alınmalıdır.
- Yukarıdaki bilgilerde olabilecek değişikliklerin vakitlice envantere yansıtılabilmesi amacıyla veri merkezi işletmecisi tarafından envanter güncelleme süreci (güncelleme aralığı, veri güncellemekle görevli personel, vb.) tanımlanarak dokümantasyonda açıklanmalıdır. Envanter en az yılda bir kez güncellik açısından gözden geçirilmeli ve bilgi sisteminin güncel durumunu yansıttığı teyit edilmelidir.

Kontrol: Veri merkezi bünyesindeki yazılım platformları ve uygulamaların envanteri tutulacaktır.

Kod: S1.TA.VY-02

Açıklama: Veri merkezi hizmetlerinin sunumunda kullanılan tüm yazılım platformları ve uygulamaların envanteri tutulacaktır. Bu envanter aşağıdaki şartları sağlamalıdır;

- Bilgi sisteminin mevcut durumunu doğru şekilde göstermelidir.

- Bilgi sisteminde kullanılan yazılım bileşenlerini envanter takibi yapmaya ve raporlamaya imkân verecek detayda göstermelidir. Envanter, en az, kendi başına bağımsız olarak belirli bir fonksiyon ifa eden her bir yazılım bileşenini kapsayacak detayda olmalıdır. Örneğin; sanallaştırma platformu, web sunucu yazılımı, veritabanı yönetim sistemi, işletim sistemi, elektronik belge yönetim sistemi gibi kurumsal uygulamalar, yazılım geliştirme ortamları, müstakil yazılım kütüphaneleri (kendi başına belirli bir fonksiyonu icra eden müstakil yazılımlar bünyesindeki kütüphaneler bu kapsamda değildir; örneğin Windows işletim sisteminin kendi kütüphaneleri), belirli teknik/yönetimsel fonksiyonları (örneğin; belirli aralıklarla veri yedekleme, güvenlik konfigürasyonlarını otomatik olarak güncelleme, vb.) ifa etmek üzere geliştirilmiş kod parçaları, güvenlik yazılımları, vb. Detaylandırmanın seviyesine bu çerçevede veri merkezi işletmecisi tarafından karar verilmeli ve bu seviye envanterin tutulduğu dokümanda açıklanmalıdır.
- Envanterdeki yazılım ve uygulamaların tanımlayıcı özellikleri dokümante edilmelidir. Örneğin; yazılım adı ve sürümü, lisans bilgileri, üreticisi, vb.
- Envanterdeki yazılımların yönetiminden (kurulum, konfigürasyon, güncelleme, bakım, vb.) sorumlu personel belirlenip kayıt altına alınmalıdır.
- Ağ üzerinden haberleşen ve kendisine ait müstakil ağ arayüzü olan yazılım bileşenlerinin kullandıkları mantıksal ağ adresleri dokümante edilmelidir (örneğin; işletim sistemleri için IP adresleri). Söz konusu adresler dinamik ise bu durum dokümantasyonda belirtilmelidir.
- Uygulanabilir olduğu durumlarda, envanterdeki yazılımların işlediği veya erişimini kontrol ettiği ve kurumsal güvenlik açısından hassas bilgilerin niteliği açıklanmalıdır. Örneğin; veritabanı yönetim sunucusunun kontrolündeki kişisel bilgiler, e-posta sunucusunun kontrolündeki personel mesajları, elektronik belge yönetim sisteminin kontrolündeki resmi evraklar, personel bilgi sistemindeki ödeme/maaş bilgileri, vb. Kendisi bizzatıhi bu tür nitelikteki bilgileri işlemeyen veya bunlara erişimi kontrol etmeyen yazılımlar (sanallaştırma platformu, bu nitelikteki bilgiler dosya sisteminde müstakil olarak erişilebilir şekilde bulunmadığı durumda işletim sistemleri, vb.) bu kapsamda değildir.
- Yukarıdaki bilgilerde olabilecek değişikliklerin vakitlice envantere yansıtılabilmesi amacıyla veri merkezi işletmecisi tarafından envanter güncelleme süreci (güncelleme aralığı, veri güncellemekle görevli personel, vb.) tanımlanarak dokümantasyonda açıklanmalıdır. Envanter en az altı ayda bir kez güncellik açısından gözden geçirilmeli ve bilgi sisteminin güncel durumunu yansıttığı teyit edilmelidir.

Kontrol: Organizasyonel veri akışları dokümante edilecektir.

Kod: S1.TA.VY-03

Açıklama: Veri merkezinin kendi sistem bileşenleri arasındaki ve başka sistemlerle olan bağlantıları ile veri akışları aşağıda tanımlandığı şekilde dokümante edilecektir;

- Üçüncü parti bilgi sistemleri ve/veya ağlarıyla olan sürekli bağlantılar (örneğin; internet servis sağlayıcı ile veri merkezi arasındaki metro ethernet bağlantısı, veri

merkezi ile başka bir kurumsal bilgi sistemi arasındaki IP-VPN bağlantısı, vb.), bu bağlantılar üzerinden taşınan trafiğin karakteristiği (genel amaçlı IP trafiği, HTTP, FTP, SMTP, RPC gibi uygulama katmanı protokolleri, TCP/UDP portları, alıcı/gönderici adres blokları, vb.) mümkün olduğunca spesifik olacak şekilde dokümante edilecektir. Bu tür bağlantıların kurulması ve aktif hale getirilmesine onay verecek yetkili personel belirlenmelidir.

- Fiziksel cihaz envanterinde yer alan ve veri merkezinin ağ altyapısı üzerinde çalışan cihazlar arasındaki kablolu ve kablosuz bağlantılar ile bu bağlantıların ağ arayüz özellikleri (gigabit ethernet, port band genişliği, vb.) dokümante edilecektir. Bu amaçla fiziksel ağ topolojisini ve bağlantılarını açıklayan ağ haritası gibi gösterimler kullanılabilir.
- Yazılım platformları ve uygulamalar envanterinde yer alan yazılım bileşenleri arasındaki öngörülebilir veri akışları ve bunların karakteristiği dokümante edilecektir. Örneğin; web/uygulama sunucusu ile veritabanı sunucusu arasındaki veri akışı, doküman yönetim sistemiyle personel bilgi sistemi arasındaki veri akışı, vb. Burada kastedilen veri akışları sistemin yapısal/işlevsel tasarımıyla ilgili veri akışları olup geçici ve/veya önceden öngörülemez veri akışları (örneğin; ağ yöneticisinin konfigürasyon amacıyla bir ağ cihazına bağlanması, belirli bir kullanıcının dosya indirmek üzere FTP sunucusuna bağlanması, vb.) bu kapsamda değildir.
- Veri merkezinde kullanılan yazılım bileşenlerinin harici (veri merkezi dışındaki) uygulamalarla olan ve süreklilik arz eden veri akışları ile bunların karakteristiği dokümante edilecektir. Örneğin; veri merkezinde barındırılan bir kurumsal uygulamanın harici bir DNS sunucusundan hizmet alması gibi. Buradaki veri akışları, geçici ve/veya öngörülemez veri akışlarını (kullanıcıların çeşitli web sayfalarını görüntülemesi veya e-posta göndermesi, internet üzerinden oynanan oyunlar, vb.) kapsamaz. Bu madde kapsamındaki bağlantıların kurulmasını onaylayacak yetkili personel dokümantasyonda belirtilmelidir.
- Yukarıdaki maddelerde belirtilen bilgilerde olabilecek değişikliklerin vakitlice envantere yansıtılması amacıyla, veri merkezi işletmecisi tarafından güncelleme süreci (güncelleme aralığı, veri güncellemekle görevli personel, vb.) tanımlanarak dokümantasyonda açıklanmalıdır.

Kontrol: Harici bilgi sistemleri kataloglanacaktır.

Kod: S1.TA.VY-04

Açıklama: Veri merkezinin işlevini yerine getirmesi için rutin olarak bağlantı kurduğu veya sürekli şekilde bağlantıda olduğu harici bilgi sistemleri dokümante edilecektir. Harici bilgi sistemi, veri merkezi işletmecisinin doğrudan kontrol etmediği, başka bir kurum veya kuruluşca işletilen bilgi sistemidir. Örneğin; kurumsal bir uygulamayı barındıran ticari bulut bilişim hizmet sağlayıcının bilgi sistemi gibi. Bahse konu bilgi sistemleri veri merkezi bünyesindeki cihazların/yazılımlarının geçici veya öngörülemez şekilde bağlantı kurduğu harici bilgi sistemlerini (örneğin; kullanıcı talebi üzerine bağlantı kurulan internet üzerindeki herhangi bir e-posta veya web sunucusu) kapsamaz. Harici bilgi sistemleri aşağıdaki hususlar dikkate alınarak dokümante edilmelidir;

- Harici bilgi sisteminden temin edilen hizmetin niteliği, teknik detayları ve hizmete erişim için kullanılacak teknolojiler/protokoller açıklanacaktır. Örneğin; hizmet türü (e-posta, elektronik belge yönetimi, ERP sistemi, vb.), veri merkezinin harici bilgi sistemine erişimi için uygulanması gerekli teknolojiler (IPSec/SSL VPN bağlantısı, akıllı kart veya tek kullanımlık şifre benzeri kimlik doğrulama mekanizmaları, vb.) gibi.
- Veri merkezinin rutin işleyişinin harici bilgi sistemine ne ölçüde bağımlı olduğu açıklanmalıdır. Örneğin; harici bilgi sisteminde ortaya çıkabilecek bir hizmet kesintisinin veri merkezinin hizmet sunumunu ne şekilde etkileyebileceği/aksatabileceği gibi.
- Harici bilgi sistemine duyulan güvenin seviyesi (söz konusu bilgi sisteminin sahip olduğu güvenlik sertifikası, sistemi işleten organizasyonla olan güven ilişkisi, vb.) açıklanmalıdır. Bu açıklama, veri merkezi işletmecisi tarafından belirlenen bir ölçüğe dayalı (düşük, orta ve yüksek güven seviyeleri gibi) değerlendirme mekanizmasıyla desteklenebilir.
- Harici bilgi sistemleriyle ilişkileri teknik ve organizasyonel seviyede yürüten personel belirlenmeli ve kayıt altına alınmalıdır.
- Yukarıdaki bilgilerde olabilecek değişikliklerin vakitlice envantere yansıtılabilmesi amacıyla, veri merkezi işletmecisi tarafından envanter güncelleme süreci (güncelleme aralığı, veri güncellemekle görevli personel, vb.) tanımlanarak dokümantasyonda açıklanmalıdır.

İş Ortamı Kontrol Grubu

Kontrol: Enerji ve telekomünikasyon hizmet bağımlılıkları belirlenip dokümanite edilecektir.

Kod: S1.TA.IO-01

Açıklama: Veri merkezinin normal işleyişi için bağımlı olduğu telekomünikasyon ve enerji hizmetleri belirlenip açıklanacaktır. Bu dokümantasyon aşağıdaki hususları kapsamalıdır;

- Veri merkezinin harici bilgi sistemleri ve internet ağıyla haberleşmesi için temin edilen telekomünikasyon hizmetleri ve bunların özellikleri (ses/veri bağlantısı, fiziksel ve mantıksal bağlantı arayüzü özellikleri ve konfigürasyon bilgileri, hizmet sağlayıcı iletişim bilgileri).
- Yukarıdaki maddede belirtilen telekomünikasyon hizmetlerindeki olası kesintilerine karşı temin edilen yedek telekomünikasyon hizmetleri ve bunların özellikleri.
- Veri merkezinde kullanılan enerji hizmetleri, kesinti durumunda devreye alınacak alternatif enerji hizmetleri (örneğin; jeneratör enerjisi) ve bunların niteliği (jeneratör gücü, yakıt kapasitesine bağlı ortalama hizmet sağlama süresi, vb.).
- Kesintisiz güç kaynağı kullanımına ilişkin bilgiler (cihaz gücü, sayısı, cihazların sistemi besleyebilecekleri azami süre, vb.).
- Yukarıdaki bilgilerde olabilecek değişiklikler dokümantasyona yansıtılmalıdır.

Kontrol: Bilgi güvenliğine ilişkin yasal yükümlülükler dokümente edilecektir.

Kod: S1.TA.IO-02

Açıklama: Veri merkezinin işletimine ilişkin olarak yasal düzenlemelerden kaynaklanan yükümlülük ve ihtiyaçlar tanımlanıp dokümente edilecektir. Bu ihtiyaçlar, belirli nitelikteki verilerin (örneğin, sağlık verileri, finansal bilgiler, vb.) korunmasına veya bilgi sisteminin genel işleyişine ilişkin düzenlemelerden kaynaklanabilir. Söz konusu yükümlülükler değişen mevzuatı yansıtacak şekilde güncel tutulmalıdır.

Risk Yönetimi Kontrol Grubu

Kontrol: Veri merkezi için risk değerlendirmesi yapılacaktır.

Kod: S1.TA.RY-01

Açıklama: “Varlık Yönetimi” ve “İş Ortamı” kontrol grupları kapsamındaki kontroller dikkate alınarak veri merkezi için bilgi güvenliği risk değerlendirmesi yapılacaktır. Bu risk değerlendirmesi asgari olarak aşağıdaki hususları kapsamalıdır;

- Envanterde yer alan cihazlar için yetkisiz/hatalı müdahalenin (konfigürasyon değişikliği, fiziksel hasar, hatalı bağlantı/sökme, vb.) sebep olabileceği sorunlar.
- Envanterde yer alan cihazların donanım arızası gibi sebeplerle ortaya çıkabilecek sorunlar.
- Varsa, cihazlar üzerinde çalışan ve cihazın asli fonksiyonlarını yerine getiren yazılımların (örneğin; bir yönlendiricinin üzerinde çalışan yazılım - firmware) güvenlik açıklarından kaynaklanabilecek sorunlar. Sunucu gibi genel amaçlı donanımlar üzerine kurulan işletim sistemi, sanallaştırma platformu, e-posta sunucusu, vb. müstakil yazılımlar bu kapsamda değildir.
- Envanterde yer alan yazılımların yapısal güvenlik açıklarından kaynaklanabilecek sorunlar. Bu yazılımlar, hem ticari paket yazılımları hem de spesifik ihtiyaçlar için özel olarak geliştirilmiş kurumsal uygulamaları kapsar. Bu madde kapsamındaki güvenlik açıkları yazılımların kodundaki güvenlik açıkları (tampon bellek taşması, hatalı kriptografik protokol uygulaması, kullanıcı veri girişlerinin kod enjeksiyonuna karşı etkin şekilde kontrol edilmemesi, vb.) olup yazılımların hatalı kullanımı/konfigürasyonu kaynaklı sorunlar bu kapsamda değildir.
- Envanterde yer alan yazılımların yetkisiz/hatalı kullanımı ve/veya konfigürasyonundan kaynaklanabilecek sorunlar.
- Uzaktan yetkisiz erişim veya veri merkezi personelinin bilgi sistemine bilinçsiz/uygunsuz/kötü amaçlı müdahaleleri sonucu sisteme zararlı yazılım yüklenmesi nedeniyle ortaya çıkabilecek sorunlar.
- Veri merkezi ağı üzerindeki veri akışlarına yetkisiz müdahalelerin (veri trafiğinin yetkisiz kişilerce gözlenmesi, trafik içeriğinin değiştirilmesi, trafiğin kesilmesi/engellenmesi, vb.) sebep olabileceği sorunlar.
- Harici bilgi sistemleriyle olan veri akışlarına yetkisiz müdahalelerin ve servis dışı bırakma saldırılarının sebep olabileceği sorunlar.
- Veri merkezinin bağlantı sağladığı harici bilgi sistemlerindeki kesintilerin ortaya çıkarabileceği sorunlar.
- Dışarıdan temin edilen enerji ve telekomünikasyon hizmetlerindeki olası

kesintilerden kaynaklanabilecek sorunlar.

- Doğal afetlerin (yangın, su baskını, deprem, fırtına, vb.) sebep olabileceği sorunlar.

Yukarıda belirtilen hususlar bilgi güvenliği riski oluşturabilecek genel sorun/saldırı sınıflarını göstermekte olup sınırlayıcı değildir. Veri merkezi risk değerlendirmesi, bu standardin koruma, tespit müdahale ve kurtarma fonksiyonları bünyesindeki kontrollerin doğası ve karşılık geldikleri bilgi güvenliği riskleri de dikkate alınmak suretiyle yapılmalıdır.

Risk değerlendirmesi, bilgi sisteminde yapılan kapsamlı değişiklikler sonrasında gözden geçirilmeli ve gerekli görüldüğünde güncellenmelidir. Kapsamlı değişiklik, bilgi sisteminin mimarisini ve işleyişini önemli ölçüde etkileyen işlevsel değişiklikler veya tasarım değişiklikleridir (örneğin; bilgi sisteminin çeşitli bileşenleriyle veri alışverişi yapan yeni bir modülün sisteme eklenmesi, yüksek güvenlik seviyesinde bilginin işlendiği yeni bir alt ağ oluşturulması, vb.). Risk değerlendirmesi en az yılda bir kez gözden geçirilerek gerek görülmesi durumunda güncellenmeli, bu gözden geçirmede bilgi sisteminin en son durumu dikkate alınmalıdır.

Kontrol: Veri merkezi bilgi güvenliği mimarisi oluşturulacaktır.

Kod: S1.TA.RY-02

Açıklama: Veri merkezi risk değerlendirmesi ve bilgi güvenliğine ilişkin yasal düzenlemeler doğrultusunda veri merkezi için bilgi güvenliği mimarisi oluşturulacaktır. Güvenlik mimarisi, farklı bilgi varlıklarının önem/hassasiyet derecesine paralel olarak söz konusu varlıklara yetkisiz erişimi zorlaştıracak katmanlı bir yapıda (defense-in-depth) tasarlanmalı, risk değerlendirmesinde ele alınan sorunları ortadan kaldırmaya veya olumsuz etkisini mümkün olduğunca azaltmaya hizmet etmelidir. Bu mimari en az aşağıdaki hususları kapsamalıdır;

- Veri merkezi bünyesindeki farklı fiziksel ve mantıksal güvenlik bölgeleri ve ağ segmentleri (internet üzerinden doğrudan erişilebilen hizmetlerin sunulduğu DMZ bölgesi, farklı departmanlara ilişkin uygulamaların üzerinde bulunduğu VLAN segmentleri, kritik bilgileri barındıran veritabanlarının bulunduğu fiziksel/mantıksal olarak izole edilmiş bölgeler/segmentler, vb.) ile bunlar üzerindeki cihaz ve yazılımlar.
- Bu bölgeler ve ağ segmentleri arasındaki fiziksel bağlantılar ve veri akışları için uygulanması gerekli güvenlik tedbirleri (güvenlik duvarı, saldırı tespit sistemi, veri kaybı önleme sistemi, zararlı yazılım kontrolü, trafik şifreleme, vb.).
- Veri merkeziyle harici bilgi sistemleri arasındaki bağlantılar, veri akışları ve bunlar için uygulanacak güvenlik tedbirleri.
- Yazılım ve uygulamalar için devreye alınacak güvenlik tedbirleri (e-posta sunucusuna ulaşan mesajların eklerini kontrol etmek için antivirüs yazılımı, uygulamalara kullanıcı veri girişlerinin kod enjeksiyonu türü saldırılara karşı kontrolü, web sunucusu gibi uygulamalara spesifik saldırı tespit sistemi, kullanıcı kimlik doğrulama, dosya bütünlüğü doğrulama, yazılım güvenlik

güncellemeleri, vb.).

- Fiziksel cihazlar ve yazılımlar için uygulanacak erişim kontrolü ve yetkilendirme mekanizmaları.
- Donanım sorunları nedeniyle ortaya çıkabilecek aksaklıkları giderecek/azaltacak mekanizmaları (örneğin; yük dengeleme modunda çalışan ethernet anahtarlar, yedekli şekilde çalışan veri depolama üniteleri, sanallaştırma platformu tarafından yönetilen sunucu havuzu, vb.).
- Dışarıdan temin edilen telekomünikasyon hizmetlerinde ortaya çıkabilecek sorunları giderecek/azaltacak yedekleme mekanizmaları (bağımsız işletmecilerden temin edilen telekomünikasyon hizmetleri, radyo link ve xDSL gibi farklı fiziksel ortam kullanan telekomünikasyon hizmetleri, vb.).
- Enerji kesintilerine yönelik önlemler.
- Veri merkezinin bulunduğu fiziksel ortamın güvenliğini sağlamaya yönelik tedbirler.
- Doğal felaketler durumunda veri merkezi hizmetlerinin devamlılığını sağlayacak veya aksaklıkların olası etkilerini en aza indirecek kurtarma mekanizmaları.

Koruma, tespit, müdahale ve kurtarma fonksiyonları bünyesindeki kontroller yukarıdaki maddelerde tanımlanan tedbirleri detaylandırmaya yöneliktir. Veri merkezi bilgi güvenliği mimarisi bahsi geçen kontroller dikkate alınarak oluşturulmalıdır. Bu mimari tek bir kapsamlı dokümanda bütün detaylarıyla açıklanabileceği gibi genel mimarinin açıklandığı bir doküman ve detaylar için atıf yapılan tamamlayıcı diğer dokümanlarla da oluşturulabilir. Dokümantasyonun ne şekilde oluşturulacağı veri merkezi işletmecisinin inisiyatifindedir.

B-KORUMA FONKSİYONU

Erişim Kontrolü Kontrol Grubu

Kontrol: Kimlik yönetimi ve yetkilendirme sistemi oluşturulacaktır.

Kod: S1.KO.EK-01

Açıklama: Veri merkezi bünyesinde uygulanacak kimlik yönetimi ve yetkilendirme sistemi oluşturulmalıdır. Bu sistem çerçevesinde;

- Veri merkezi bünyesinde kullanılacak hesap türleri (sistem yöneticisi, ağ yöneticisi, normal kullanıcı, ziyaretçi, geçici kullanıcı, dış kaynak hizmet sağlayıcı, vb.) tanımlanıp dokümanite edilmelidir.
- Bu hesap türleri için hesap yöneticileri olacak yetkili personel belirlenmelidir.
- Grup veya rol bazında yapılacak yetkilendirme tanımlamaları varsa, söz konusu grup ve rol üyelikleri için uygulanacak şartlar (belirli bir daire bünyesinde çalışma, spesifik bir projede görev alma, vb.) tanımlanmalıdır.
- Veri merkezi kullanıcıları, kullanıcıların grup ve rol üyelikleri, erişim yetkileri ve buna ilişkin diğer bilgiler (erişim zamanı, süresi, yapılabilecek işlemler gibi kullanıcı erişimine ilişkin kısıtlar, uzaktan erişim yetkileri, vb.) tanımlanmalıdır. Erişim yetkileri, ilgili kullanıcının görev/rol tanımının gerektirdiği en alt düzeyde tutulmalıdır (örneğin; ağ yöneticisi rolü için tanımlanan erişim yetkilerinin sadece

ağ cihazlarına müdahaleyi kapsamı ve veritabanı sunucularına müdahaleye izin vermemesi gibi).

- Hesap oluşturma, güncelleme ve kaldırma işlemleri için yetkilendirme/onay süreci oluşturulup dokümente edilmelidir. Bu süreç, ilgili kullanıcının kurum bünyesindeki rol ve sorumluluklarını bilen/belirleyen kurum yetkililerinin onaylarının alınmasını veya söz konusu rol ve sorumluluklar elektronik ortamda tanımlanmışsa yapılacak işlem öncesi bu kayıtların kontrolünü sağlamalıdır.
- Bir kullanıcı için farklı rollere ilişkin birden çok hesap oluşturulacağı durumda yukarıdaki maddede tanımlanan süreç tüm hesaplar için ayrı ayrı işletilmelidir. Söz konusu hesaplar için güncelleme ve hesabın kaldırılması işlemleri de bu kapsamdadır.
- Temel prensip olarak, kullanıcı kimlik doğrulaması harici kimlik doğrulama hizmetleri (Facebook, Google, Yahoo, vb.) yoluyla yapılmamalıdır. Eğer teknik/mali imkânsızlıklar nedeniyle bu tür kimlik doğrulama hizmetleri kullanılacaksa, böylesi kimlik doğrulama hizmetlerinin güvenlik politikalarının bu kontrol kapsamındaki tedbirlerle uyumu gözetilmelidir. Harici kimlik doğrulama hizmetleri hiçbir şekilde güvenlik açısından kritik hesaplar (ağ yöneticisi, veritabanı yöneticisi, sistem yöneticisi, vb.) için kullanılmamalıdır. Yasal gerekçelerle güvenli olduğundan emin olunan harici elektronik kimlik doğrulama hizmetleri (resmi elektronik kimlik kartı, yetkili bir kamu kurumu tarafından sunulan elektronik kimlik doğrulama hizmeti, vb.) bu kapsamda değildir.
- Güvenlik açısından hassas kullanıcı hesapları için belirli sayıdaki ardışık başarısız sisteme giriş denemeleri sonunda ilgili hesabı bloke ederek yetkili personel için uyarı üreten bir teknik mekanizma kurulmalıdır. Kaç ardışık başarısız sisteme giriş denemesi sonucunda ilgili hesabın bloke edileceği veri merkezi işletmecisi tarafından belirlenmelidir.
- Kullanıcı hesaplarına erişimle ilgili kritik olaylar (sisteme giriş, sistemden çıkış, başarısız giriş denemeleri, yeni kullanıcı hesabı oluşturma, yazılım kurulumu, konfigürasyon değiştirme, dosya görüntüleme, vb.) kayıt altına alınmalıdır. Hangi olayların bu kapsamda olduğu, ilgili hesap türünün niteliğine göre ve risk değerlendirmesi doğrultusunda, veri merkezi işletmecisi tarafından dokümente edilmelidir.
- Kullanıcı hesapları için tanımlayıcılar (kullanıcı adı, sicil numarası, vb.) her bir kullanıcı için farklı olacak şekilde belirlenmelidir.
- Farklı hesap türleri için uygulanacak kimlik doğrulama yöntemleri (şifre, akıllı kart, tek kullanımlık şifre, biyometrik tanımlama, vb.) tanımlanmalıdır. Ayrıca, bu yöntemler için uygulanacak güvenlik tedbirleri (şifre uzunluğu/karmaşıklığı, şifre veya akıllı kart yenileme periyodu, tek kullanımlık şifre için cep telefonu veya şifre üretici kullanımı, vb.) de açıklanmalıdır.
- Yukarıdaki maddede bahsi geçen kimlik doğrulama araçlarının (akıllı kart, şifre, tek kullanımlık şifre üretici, vb.) hesap sahibine güvenli şekilde ulaştırılması için uygulanacak prosedür tanımlanmalıdır. Mümkünse söz konusu kimlik doğrulama araçları hesap sahiplerinin yetkili personele kişisel başvurusu üzerine ve o esnada aktive edilerek kendilerine teslim edilmelidir.
- Bilgi sisteminde tutulan kullanıcı şifreleri mutlaka etkin ve güncel bir kriptografik mekanizmayla (şifreleme, kriptografik özet alma, vb.) korunmalı, şifreler hiçbir

zaman açık şekilde bilgi sisteminde saklanmamalıdır.

- Kullanıcıların hesaplarına ağ üzerinden erişimi durumunda kullanıcı cihazı ile kimlik doğrulamayı yapan uygulama arasındaki veri trafiği, en azından kimlik doğrulama süreci boyunca güvenli şekilde şifrelenmeli, kullanıcı şifreleri hiçbir şekilde ağ üzerinden açık olarak gönderilmemelidir. Şifreleme için etkin ve güncel kriptografik algoritmalar/protokoller kullanılmalıdır.
- Harici bilgi sistemleri üzerindeki uygulamaların kullanılması durumunda, ilgili uygulamanın kimliğini doğrulayacak uygun bir mekanizma (sayısal imza, SSL/TLS, IPSec VPN, vb.) kullanılmalıdır. Teknik sebeplerle bunun mümkün olmadığı durumlar (örneğin; DNSSec protokolunu desteklemeyen harici bir DNS sunucusunun kullanılması, harici bilgi sisteminin teknik tasarımının uygun olmaması, vb.) kayıt altına alınmalıdır. Bu tür harici uygulamalara bağlantıların güvenliği (örneğin; DNS sunucusunun bulunduğu adresin güvenilir olmayan bir başka hizmet sağlayıcı tarafından kullanılmaya başlanması, bağlantının yetkisiz müdahaleye karşı güvenliği, vb.) veri merkezi işletmecisi tarafından rutin olarak gözden geçirilmeli, buna ilişkin prosedür dokümanite edilmelidir.

Yukarıdaki maddelerde dokümanite edilmesi gerektiği belirtilen bilgilerde olabilecek değişiklikler en kısa sürede dokümantasyona yansıtılmalıdır.

Kontrol: Bilgi varlıklarına fiziksel erişim kontrol edilecektir.

Kod: S1.KO.EK-02

Açıklama: Veri merkezi envanterindeki bilgi varlıklarına fiziksel erişim kontrol edilecektir. Bu amaçla;

- Veri merkezinin bulunduğu bina, oda, vb. fiziksel yapılara giriş yetkisi olan personel belirlenip dokümanite edilmelidir. Veri merkezi birden çok sayıda ayrıştırılmış fiziksel birimden (oda, bina katı, vb.) oluşuyorsa, ilgili personelin veri merkezinin hangi kısımlarına giriş yetkisi olduğu tanımlanmalıdır. Bu yetkiler, ilgili personelin görevini yapmasına imkân verecek en alt seviyede tutulmalıdır. Görev değişikliği, işten ayrılma, vb. sebeplerle bu bilgilerde olabilecek değişiklikler en kısa sürede dokümantasyona yansıtılmalıdır.
- Söz konusu personelin fiziksel yapılara giriş için kullanacağı kimlik doğrulama araçları (personel kimlik kartı, akıllı kart, kapı anahtarı, biyometrik tanımlayıcılar, vb.) belirlenmeli ve ilgili personele güvenli şekilde teslim edilmelidir. Personel/görev değişikliği durumlarında söz konusu kimlik doğrulama araçları iptal edilmek veya geri alınmak suretiyle ilgili personelin bu kimlik doğrulama aracını kullanması engellenmelidir.
- Veri merkezini barındıran yapılara giriş ve çıkışları kontrol edebilmek için fiziksel kontrol tedbirleri (kilitli kapı, güvenlik görevlisi, elektronik alarm, vb.) alınmalıdır. Söz konusu yapılara fiziksel giriş-çıkışa imkân veren noktalarının tamamı için bu tedbirler uygulanmalıdır.
- Yetkili personelin veri merkezini barındıran fiziksel yapılara giriş ve çıkışları kayıt altına alınmalıdır. Söz konusu kayıtların bütünlüğünü ve mevcudiyetini koruyacak uygun mekanizmalar (fiziksel dokümanlar için ıslak imza ve güvenli bir yerde

saklama, elektronik kayıtlar için sayısal imzalama ve güvenli depolama, vb.) kullanılmalıdır.

- Veri merkezine giriş yetkisi olmayan kişilerin (ziyaretçiler, üçüncü parti hizmet sağlayıcıların çalışanları, vb.) fiziksel yapılara girişine ancak bu kişilere veri merkezine giriş yetkisi olan bir personelin eşlik etmesi durumunda izin verilmelidir. Yetkili personel, eşlik ettikleri kişilerin veri merkezinde bilgi güvenliği açısından tehdit oluşturmayacak şekilde davranmasını sağlamaktan sorumlu oldukları konusunda bilgilendirilmelidir.

Kontrol: Bilgi varlıklarına uzaktan erişim kontrol edilecektir.

Kod: S1.KO.EK-03

Açıklama: Veri merkezi bünyesindeki kamu kullanımına açık olmayan cihaz ve yazılımlara veri merkezi dışından harici ağlar üzerinden erişim kontrol edilecektir. Bu amaçla;

- Uzaktan erişim yetkisi olan kullanıcı hesapları, bunların uzaktan erişim yoluyla erişilebileceği bilgi varlıkları ve bunlar üzerinde yapabilecekleri işlemler dokümente edilmelidir. Uzaktan erişimin kapsamı mümkün olduğunca kısıtlı tutulmalı, veri merkezi operasyonları açısından zorunlu olmayan durumlar için uzaktan erişim yetkisi tanımlanmamalıdır. Söz konusu bilgilerde olabilecek değişiklikler en kısa sürede dokümantasyona yansıtılmalıdır.
- Uzaktan erişim yoluyla veri merkezine bağlanan kullanıcıların bağlantı bilgileri (hesap bilgileri, bağlantı IP adresi, bağlantıyı başlatma ve sonlandırma zamanı, bağlantı üzerinden yapılan kritik işlemler) kayıt altına alınmalıdır. Bu bilgilerin kapsamı, uzaktan erişime konu bağlantının niteliği ve risk değerlendirmesi dikkate alınarak, veri merkezi işletmecisi tarafından belirlenmeli ve dokümente edilmelidir.
- Uzaktan erişim yoluyla veri merkezi ağına gelen trafik belirlenmiş noktalarda toplanarak bu kontrol kapsamındaki tedbirlere uyumunu kontrol edecek teknik mekanizmalar uygulanmalıdır.
- Uzaktan erişim bağlantılarının trafik gizliliği ve bütünlüğünü korumak üzere uygun ve güncel kriptografik protokoller (IPSec, SSL/TLS, vb.) kullanılmalıdır.
- Eğer güvenlik açısından kritik kullanıcı hesapları (sistem yöneticisi, veritabanı yöneticisi, vb.) için uzaktan erişim yetkisi tanımlanacaksa, bu hesapların uzaktan erişimini denetlemek için en az iki faktörlü kimlik doğrulama mekanizmaları kullanılmalıdır. Mümkünse ikinci kimlik doğrulama faktörünün band dışı (out-of-band) olması sağlanmalıdır (cep telefonu vasıtasıyla tek kullanımlık şifre kullanımı gibi).

Kontrol: Veri merkezi ağı alt ağlara bölünecektir.

Kod: S1.KO.EK-04

Açıklama: Veri merkezi ağı, gerek veri merkezi bünyesindeki gerekse veri merkeziyle harici bilgi sistemleri arasındaki veri akışları dikkate alınarak alt ağlara bölünecektir. Bu çerçevede;

- İnternet üzerinden erişilebilen kamuya açık veri merkezi hizmetleri, veri merkezi iç ağından mantıksal veya fiziksel olarak ayrılmış bir alt ağ üzerinden sunulmalıdır.
- Harici ağlar ve bilgi sistemleriyle olan bağlantılar kontrol edilen bir alt ağda sonlandırılmalı ve mutlaka veri merkezi işletmecisi tarafından yönetilen arayüzler (VPN sonlandırıcı, güvenlik duvarı, vekil sunucu, saldırı tespit/önleme sistemi, veri kaybı önleme sistemi, vb.) üzerinden geçirilmelidir. Söz konusu bağlantılar için hangi tür arayüzler kullanılması gerektiğine ilgili bağlantının risk değerlendirmesi doğrultusunda karar verilmelidir.
- Veri merkezi iç ağı fonksiyonel açıdan birbiriyle ilişkili ve/veya kritiklik açısından birbirine benzer olan cihaz, yazılım ve uygulamaları (örneğin; belirli bir organizasyonel birime hizmet veren uygulamalar, güvenlik açısından benzer derecede önemli bilgileri barındıran veritabanı sunucuları, vb.) aynı alt ağ üzerinde barındıracak şekilde alt ağlara ayrılmalıdır. Bu alt ağlar arasındaki veri akışları, veri akışlarının niteliğinin gözlenmesi ve kontrol edilmesine imkân verecek şekilde tek veya belirli sayıdaki fiziksel/mantıksal bağlantı noktaları üzerinden sağlanmalıdır.
- Alt ağlar arasındaki veri akışları, veri akışlarının niteliği ve bunlara ilişkin risk değerlendirmesi doğrultusunda belirlenen kriterlere göre (alıcı/gönderici IP adresleri ve/veya kullanıcıları, TCP/UDP portları, uygulama protokolleri, trafik içeriği, erişim zamanına ilişkin kısıtlar, vb.) filtrelenmeli/sınırlandırılmalıdır.

Veri Güvenliği Kontrol Grubu

Kontrol: Durağan haldeki bilgiler korunacaktır.

Kod: S1.KO.VG-01

Açıklama: Veri merkezi bünyesinde tutulan kullanıcı bilgileri ve sistem güvenliğine ilişkin bilgilerin güvenliği sağlanacaktır. Kullanıcı bilgileri, veri merkezi bünyesindeki yazılım ve cihazlar üzerinde barındırılan ve normal iş süreçlerinde kullanıcılar tarafından rutin olarak erişilen/işlenen/oluşturulan bilgilerdir (e-posta mesajları, elektronik doküman yönetim sistemindeki dosyalar, elektronik envanter kayıtları, kişisel sağlık kayıtları, vb.). Sistem güvenliğine ilişkin bilgiler ise bilgi güvenliği fonksiyonu olan cihaz ve yazılımların düzgün şekilde çalışması veya güvenlik fonksiyonlarının denetlenmesi için gerekli bilgilerdir (güvenlik duvarı ve saldırı tespit sistemi kural setleri ve olay kayıtları, erişim kayıtları, cihaz/yazılım güvenlik konfigürasyonları, vb.). Bu kontrol kapsamında;

- Kimlik doğrulama ve yetkilendirme sistemi çerçevesinde, cihaz ve yazılımlar üzerindeki kullanıcı bilgilerine erişimi kontrol edecek teknik mekanizmalar uygulanmalıdır. Bu mekanizmalar bütünleşik kimlik yönetimi sistemleri olabileceği gibi veri merkezi bünyesindeki farklı bilgi sistemi bileşenleri için kullanılan müstakil çözümler de olabilir.
- Kullanıcı bilgileri herhangi bir şekilde veri depolama cihazlarına yüklenerek fiziksel yollarla veri merkezi dışına çıkarılacaksa (örneğin; yedekleme veya veri aktarımı amacıyla), bu bilgiler mutlaka uygun şekilde şifrelenerek veri depolama cihazlarına yüklenmelidir. Şifreleme için endüstride yaygın kabul gören

kriptografik algoritmalar/protokoller (3DES, AES, RSA, openssl, truecrypt, vb.) kullanılabilir. Şifre anahtarları veri depolama cihazlarından bağımsız ve güvenli şekilde saklanmalı/iletilmelidir. Bu şekilde yapılacak şifrelemelere ve şifre anahtarlarının yaşam döngüsüne ilişkin süreç (üretim, kullanım, saklama, yok etme) veri merkezi işletmecisi tarafından dokümente edilmelidir.

- Kimlik doğrulama ve yetkilendirme sistemi çerçevesinde sistem güvenliğine ilişkin bilgilere erişimi ve müdahaleyi kontrol edecek teknik mekanizmalar uygulanmalıdır. Bu mekanizmalar ilgili tüm cihaz ve yazılımlara erişimi kontrol eden merkezi bir çözüm olabileceği gibi farklı cihaz ve yazılımlar için farklı mekanizmalar da kullanılabilir.
- Sistem güvenliğine ilişkin bilgilerin bütünlüğü periyodik aralıklarla gözden geçirilmeli ve referans konfigürasyonlarla karşılaştırmak suretiyle kayıtlarda bilinmeyen/istenmeyen değişiklikler yapılmadığından emin olunmalıdır. Bütünlük kontrolü söz konusu bilgilerin personel tarafından tek tek kontrol edilmesi veya bu bilgileri barındıran elektronik dosyaların özet değerlerinin kontrol edilmesi gibi yollarla yapılabilir. Bu madde kapsamındaki gözden geçirmeye ilişkin süreç (gözden geçirme aralığı, gözden geçirilecek kayıtların/bilgilerin listesi, ilgili personel, bütünlük kontrol yöntemi, vb.) veri merkezi işletmecisi tarafından dokümente edilmelidir.

Kontrol: Ağ üzerinden gönderilen bilgiler korunacaktır.

Kod: S1.KO.VG-02

Açıklama: Veri merkezi risk değerlendirmesi doğrultusunda, ağ üzerindeki veri akışlarının gizliliği ve bütünlüğü sağlanacaktır. Söz konusu veri akışları hem veri merkezi iç ağı üzerindeki (özellikle güvenlik hassasiyeti/tedbirleri açısından farklılık gösteren alt ağlar arasındaki trafik) hem de harici ağlarla olan veri akışlarını kapsar. Bu çerçevede, risk değerlendirmesi uyarınca bütünlük ve/veya gizliliğinin sağlanması gerektiği tespit edilen veri akışları için uygun ve güncel kriptografik mekanizmalar (IPSec, SSL/TLS, link seviyesinde şifreleme, HMAC, vb.) kullanılmalıdır. Bu amaçla kullanılan kriptografik anahtarların yaşam döngüsü (üretim, kullanım, saklama, yok etme) veri merkezi işletmecisi tarafından tanımlanıp dokümente edilmelidir.

Kontrol: İşletmeci kontrolü dışına çıkacak bilgi sistemi bileşenleri üzerindeki veriler imha edilecektir.

Kod: S1.KO.VG-03

Açıklama: Veri merkezinde kullanılan bilgi sistemi bileşenlerinden devre dışı bırakmak, başka bir kuruluşa devretmek, satmak, hurdaya ayırmak, vb. nedenlerle işletmecinin kontrolü dışına çıkacak olanlar üzerinde bulunan veriler güvenli şekilde imha edilecektir. Söz konusu bilgi sistemi bileşenleri sabit disk, flash bellek, optik disk, veri yedekleme amaçlı teyp üniteleri, üzerinde kritik bilgi barındıran müstakil cihazlar (örneğin; güvenlik konfigürasyonu yapılmış bir güvenlik duvarı cihazı), vb. elektronik/manyetik/optik cihazlardır. Bu çerçevede;

- Elektronik/manyetik/optik ortamdaki verilerin imhası için, ilgili veri depolama

ortamının niteliğine uygun veri imha yöntemleri uygulanmalıdır. Bu amaçla, http://www.nsa.gov/ia/mitigation_guidance/media_destruction_guidance/index.shtml adresinde açıklanan veya endüstride kabul gören diğer güvenli veri imha yöntemleri benimsenebilir.

- Kritik bilgi barındıran donanımın güvenli veri silme fonksiyonları varsa bunlar kullanılabilir. Böylesi durumlarda, söz konusu işlevlerin teknik olarak nasıl çalıştığı net olarak anlaşılmalı, verinin geri döndürülemez veya veri kurtarmayı çok zorlaştıracak şekilde silindiğinden emin olunmalıdır.
- Finansal, teknik, personel kısıtı, vb. sebeplerle yukarıdaki güvenli veri silme yöntemlerinin uygulanması mümkün değilse, imha edilecek veriyi barındıran cihaz veya depolama birimleri fiziksel olarak ve üzerindeki sayısal bilginin ele geçirilmesini imkânsız kılacak şekilde tahrip edilmelidir (kırama, parçalama, yakma, vb.).
- Benimsenen veri imha süreci (benimsenen veri imha yöntemleri, farklı türlerdeki veriler için imhayı onaylayacak yetkili personel, imha edilen verilere ve cihazların kayıt altına alınması prosedürleri) dokümente edilmelidir.

Kontrol: Veri merkezi bilgi sistemi potansiyel saldırılara karşı izlenip korunacaktır.

Kod: S1.KO.VG-04

Açıklama: İzleme faaliyetleri hem harici ağlarla veri merkezi arasındaki trafiğin hem de veri merkezi iç ağındaki trafiğin ve cihazların/yazılımların güvenlik tehditleri açısından izlenmesini kapsar. Bu kontrol kapsamında;

- Risk değerlendirmesi çerçevesinde, veri merkezi ağı üzerindeki kritik/hassas noktalarda saldırı tespit/önleme sistemi, zararlı kod koruma yazılımı, protokol analiz yazılımı, veri kaybı önleme sistemi, vb. araçlar kullanılmak suretiyle ağ trafiği olası saldırılara karşı izlenip korunacaktır. Özellikle dış ağlardan gelen trafik, iç ağdaki kritik uygulamaların giriş/çıkış trafiği (uygulama sunucusu ile veritabanı sunucusu arasındaki bağlantı gibi), kablolu ve kablosuz ağlar arasındaki trafik ile güvenlik nitelikleri (barındırılan veri ve uygulamaların hassaslığı, port ve uygulama katmanı protokolü gibi trafik özellikleri, vb.) itibarıyla birbirinden farklı ağ segmentleri arasındaki trafik bu kapsamda izlenmelidir.
- Harici ağlarla olan şifreli trafiğin içeriğinin izlenebilmesini sağlayacak uygun mekanizmalar (SSL vekil sunucu gibi) kullanılmalıdır. Söz konusu trafik, şifresi çözüldükten sonra, önceki maddede bahsi geçen uygun güvenlik araçlarıyla izlenmelidir. Bu tedbirler, kullanıcı mahremiyetine ilişkin yasal düzenlemelerle uyumlu olmalıdır.
- Bilgi sistemi bünyesinde kullanılacak kablosuz ağ cihazları için endüstride yaygın kabul gören güçlü ve güncel şifreleme protokolleri kullanılmalı ve kablosuz ağ erişimi yeterince güçlü/karmaşık şifrelerle korunmalıdır. Bu cihazların konumu ve sinyal gücü veri merkezi dışından sinyal alınmasını mümkün olduğunca zorlaştıracak şekilde belirlenmelidir.
- Uygulamaları olası saldırılara karşı korumak amacıyla, uygulamaların niteliği ve risk değerlendirmesi çerçevesinde, uygulamayı çalıştıran platform üzerinde, antivirüs yazılımı, saldırı tespit/önleme sistemi, protokol analiz yazılımı, zararlı

kod önleme sistemi, vb. araçlar kullanılmalıdır. Risk değerlendirmesinde, web tabanlı uygulamalar için OWASP (Açık Web Uygulama Güvenliği Projesi – Open Web Application Security Project – www.owasp.org) tarafından tanımlanan genel uygulama zayıflıkları da dikkate alınmalıdır.

- Veri merkezi işletmecisi bilgi sisteminde yetkisiz yazılımlar/uygulamalar çalıştırılmasını önlemek için gerekli teknik mekanizmayı oluşturmalıdır. Bu amaçla, beyaz liste oluşturma ve yazılım platformları üzerinde çalıştırılacak uygulamaları buna göre sınırlama (application whitelisting) gibi yöntemler benimsenebilir.

Bilgi Koruma Süreçleri Kontrol Grubu

Kontrol: Bilgi sistemi bileşenleri için referans konfigürasyonlar oluşturulacak ve güncelliği sağlanacaktır.

Kod: S1.KO.BK-01

Açıklama: Veri merkezi bünyesindeki cihaz ve yazılımların işletim esnasında sahip olması gereken konfigürasyonu gösteren referans konfigürasyonlar oluşturulacaktır. Bu amaçla;

- Bilgi sistemi bileşenlerinin normal çalışma konfigürasyonu dokümante edilecektir. Bu amaçla, ilgili cihaz veya yazılımın üreticisinin işletim ve güvenlik konfigürasyon kılavuzlarından faydalanılabilir. Açık veya ücretli kaynaklardan derlenecek bilgiler de bu amaçla kullanılabilir. Bu konfigürasyon belirlenirken, ilgili cihaz veya yazılımın bilgi sistemi açısından gerekli işlevlerini yerine getirmesine imkân verecek en sınırlayıcı konfigürasyon tercih edilmelidir. Normal çalışma konfigürasyonu, fiziksel cihazlar üzerine doğrudan kurulan yazılımları (örneğin; bağımsız sunucu donanımı üzerine kurulan Linux işletim sistemi veya bir sunucu havuzunu yöneten sanallaştırma platformu) ve bir platform yazılım üzerine kurulan diğer yazılımları (örneğin; Windows işletim sistemi üzerine kurulan ofis ve web sunucu yazılımları, sanallaştırma platformu üzerindeki bir sanal makineye kurulan Linux işletim sistemi, Firefox internet tarayıcısına eklenen plug-in yazılımlar, vb.) da kapsar.
- İlgili sistem bileşenlerinin işlevselliğini ve/veya güvenliğini artırmak amacıyla cihaz/yazılım üreticisi veya hizmet sağlayıcılar tarafından konfigürasyon değişikliği önerilmesi veya veri merkezi işletmecisi tarafından bu yönde karar verilmesi durumunda (saldırı tespit sistemi kural güncellemeleri, işletim sisteminin açık servislerinin değiştirilmesi, yazılım güvenlik yamalarının yüklenmesi, yazılım versiyon değişikliği, yeni yazılım yüklenmesi, vb.), yapılan bu değişiklikler referans konfigürasyona yansıtılarak dokümantasyonun güncelliğini koruması sağlanmalıdır.
- Referans konfigürasyonu ve konfigürasyonda yapılacak güncellemeleri onaylayacak personel belirlenip dokümante edilmelidir. Güncellemeler ancak belirlenmiş yetkili personel tarafından onaylandıktan sonra yine ilgili cihaz ve/veya yazılımlardan sorumlu personelce uygulanmalıdır. Konfigürasyon değişikliğini onaylayacak personel veri merkezi bilgi sisteminin genel teknik mimarisi ve risk analizi hakkında kapsamlı bilgi sahibi olan bir yetkili olmalıdır.

(güvenlik şefi, sistem yöneticisi, vb.). Konfigürasyon değişikliği uygulandıktan sonra, yapılan değişikliklerin daha önceden uygulanmakta olan güvenlik tedbirlerini etkisizleştirmeden emin olunmalıdır (örneğin; kapalı olan işletim sistemi servislerinin konfigürasyon değişikliği sonucunda açılması, güvenlik duvarının erişime kapalı tuttuğu portların açılması, vb.). Veri merkezi işletmecisi konfigürasyon güncellenmesine ilişkin süreci tanımlayıp dokümanete etmelidir.

- Referans konfigürasyon kayıtlarının geçmişe doğru kaydı tutulmalıdır. Bu, gerektiğinde eski konfigürasyonlara dönüşe imkân verir ve olay incelemesini kolaylaştırır.

Kontrol: Veri yedekleme mekanizması oluşturulacaktır.

Kod: S1.KO.BK-02

Açıklama: Doğal afet, hatalı işletim, sabotaj, donanım arızası, siber saldırı, vb. durumlarda veri kaybının önüne geçmek amacıyla, veri merkezinde barındırılan bilgiler yedeklenecektir. Söz konusu bilgiler hem elektronik ortamdaki kullanıcı bilgilerini (e-posta mesajları, elektronik dokümanlar, kişisel sağlık bilgileri, finansal kayıtlar, vb.) hem de sistemin güvenli işletimiyle ilgili bilgileri (konfigürasyon dosyaları, erişim yetkileri, güvenlik cihazı kural setleri, güncel sanal makine imajları, vb.) kapsar. Bu çerçevede;

- Veri merkezi işletmecisi, yedeklenmesi gerekli bilgilerin kategorik listesini oluşturmalı ve dokümanete etmelidir.
- Farklı kategorilerdeki bilgiler için yedekleme periyodu belirlenip dokümanete edilmelidir. Yedekleme periyodunun tespitinde ilgili kategorideki bilgilerin güncellenme sıklığı ve bu bilgilerin kaybindan kaynaklanabilecek risk dikkate alınmalıdır.
- Yedekleme sistemi, veri akışını etkin biçimde kontrol edebilecek şekilde, ana bilgi sisteminden fiziksel veya mantıksal olarak ayrıştırılmış olmalıdır. Ana bilgi sisteminden yedekleme sistemine veri aktarımı otomatik olarak yapılacaksa, bu ikisi arasındaki veri akışının ilgili bilgi kategorilerinin güncelleme periyoduna göre olmasını sağlayacak teknik mekanizmalar kurulmalı ve dokümantasyonda açıklanmalıdır.
- Yedekleme sistemi mümkünse ana bilgi sisteminin bulunduğu lokasyondan farklı bir yerde barındırılmalıdır. Teknik/finansal nedenlerle bunun mümkün olmadığı durumlarda, yedekleme sistemi ana bilgi sisteminin bulunduğu fiziksel bina bölümünden (oda, kat, fiziksel güvenliği sağlanmış müstakil kabin, vb.) farklı ve giriş/çıkış kontrolü yapılabilen ayrı bir bölümde olmalıdır. Yedekleme sisteminin bulunduğu bina bölümüne girme veya bu sisteme ağ üzerinden bağlanma yetkisi olan personel belirlenmelidir. Hiçbir çalışanın binanın bu bölümüne tek başına girişine izin verilmemeli, söz konusu bölüme giriş için en az iki yetkili personelin fiziksel mevcudiyetini sağlayacak teknik/ıdari mekanizmalar kurulmalıdır. Bu mekanizmalar, fiziksel müdahale gerektiren acil durumlarda (yangın, su baskını, vb.) yetkili bir personel (sistem yöneticisi, güvenlik şefi, vb.) tarafından devre dışı bırakılabilecek şekilde tasarlanmalıdır. Yedekleme sisteminin yönetimi (sistem konfigürasyonu, veri silinmesi, verilerin başka bir ortama aktarımı, vb.) amacıyla bu sisteme ağ üzerinden erişim sağlanacaksa, yapılacak işlemler için en az iki

yetkili personelin onayını gerektiren teknik mekanizmalar kurulmalıdır.

- Yedeklenen bilgiler harici bir hizmet sağlayıcının altyapısı üzerinde barındırılacaksa, bu bilgiler yetkisiz kişilerin erişimini engelleyecek şekilde uygun ve güncel kriptografik algoritmalar/protokoller kullanılarak şifrelenmeli ve şifreleme için kullanılan anahtarlar veri merkezi işletmecisinin kontrolünde tutulmalıdır. Bu nitelikteki şifrelemeye ve şifre anahtarlarının yaşam döngüsüne ilişkin süreç veri merkezi işletmecisi tarafından tanımlanıp dokümante edilmelidir. Yedeklenen bilgilerin tutulduğu altyapı ilgili kamu otoriteleri tarafından bu amaçla yetkilendirilmiş bir işletmeci tarafından işletiliyorsa ve mevzuat uyarınca söz konusu işletmeciye bilgi güvenliği gereksinimleri açısından güvenmek mümkünse (örneğin; ilgili mevzuata uygun şekilde yetkilendirilmiş bir kamu kurumu tarafından işletilen felaket kurtarma merkezi gibi) bu maddede öngörülen tedbirlerin alınmaması tercih edilebilir.

Kontrol: Fiziksel işletim ortamına ilişkin politikalar belirlenip uygulanacaktır.

Kod: S1.KO.BK-03

Açıklama: Veri merkezi bilgi sisteminin fiziksel işletim ortamının güvenliğini sağlamaya yönelik politikalar tespit edilerek bunların uygulanmasını sağlayacak teknik mekanizmalar kurulacaktır. Bu çerçevede;

- Enerji besleme sistemi, acil durumlarda (yangın, su baskını, vb.) veri merkezi bilgi sisteminin tüm enerjisini kesebilecek şekilde yapılandırılacaktır.
- Olası enerji kesintisi durumlarında bilgi sisteminin güvenli şekilde işletilmesi veya geçici olarak devre dışı bırakılmasını sağlayacak şekilde sisteme kesintisiz güç kaynağı beslemesi sağlanacaktır.
- Olası enerji kesintisi durumlarında bilgi sisteminin bulunduğu bina bölümlerini yeterince aydınlatacak bir aydınlatma sistemi (batarya beslemeli sabit/hareketli acil durum lambaları gibi) kurulmalıdır.
- Bilgi sistemini barındıran bina bölümleri için otomatik yangın tespit ve söndürme sistemi kurulmalıdır.
- Bilgi sistemini barındıran bina bölümleri için gerçek zamanlı nem ve sıcaklık izlemesine imkân verecek bir mekanizma kurulmalıdır.

Kontrol: Bilgi sistemi zayıflık yönetim planı hazırlanıp uygulanacaktır.

Kod: S1.KO.BK-04

Açıklama: Veri merkezi bilgi sisteminin yazılım güvenlik açıkları ve konfigürasyon hatalarından kaynaklanan güvenlik zayıflıklarını tespit edip giderecek bir zayıflık yönetim planı hazırlanıp uygulanacaktır. Bu çerçevede;

- Bilgi sistemindeki zayıflıkları tespit etmek üzere periyodik aralıklarla zayıflık taraması yapılacaktır. Bu amaçla ağ üzerinde otomatik tarama yapan yazılım araçları kullanılabilir. Bu tür araçlar kullanıldığında, bunların güncel zayıflıkları tespit edebilecek nitelikte olmasına dikkat edilmelidir. Zayıflık taramalarının periyodu veri merkezi işletmecisi tarafından planda belirlenmelidir. Zayıflık

taramaları en az yılda bir kez yapılmalıdır. Bu işlem veri merkezi işletmecisi tarafından yapılabileceği gibi üçüncü parti hizmet sağlayıcılardan hizmet satın alma yoluyla da yapılabilir.

- Tarama sonucunda tespit edilen zayıflıklar ilgili güvenlik personeli tarafından gözden geçirilmeli, risk değerlendirmesi doğrultusunda giderilmesi gerektiğine karar verilen zayıflıkları ortadan kaldıracak önlemler (yama yükleme, konfigürasyon güncelleme, güvenlik yazılımı kullanma, vb.) alınmalıdır. Bu çerçevede, tespit edilen zayıflıklar, bunlara ilişkin risk değerlendirmesi ve uygulanacak tedbirler kayıt altına alınmalıdır.
- Tarama sonucu tespit edilen zayıflıkların giderilmesine ilişkin önlemlerin etkin şekilde çalıştığı test edilmelidir. Bu amaçla, zayıflık taraması tekrarlanarak sonuçları değerlendirilebilir veya daha önce tespit edilmiş zayıflıklar kullanılarak sisteme sızmaya çalışılabilir. Alınan önlemlerin belirlenen zayıflıkları ortadan kaldırdığını test etmeye ilişkin süreç veri merkezi işletmecisi tarafından tanımlanıp planda dokümente edilmelidir.
- Bilgi sisteminin normal işleyişi sürecinde tespit edilecek zayıflıklar (yazılımlar için yeni yama yayınlanması, gerçekleşen bir saldırı sonucunda tespit edilen zayıflıklar, personelin rastlantısal şekilde tespit ettiği zayıflıklar, vb.) için de uygun tedbirler alınmalıdır. Bu tür tedbirler için de yukarıdaki maddelerde tanımlanan süreçler uygulanmalıdır.

Bakım ve Olay Kayıtları Kontrol Grubu

Kontrol: Bilgi sisteminin kontrollü bakımı sağlanacaktır.

Kod: S1.KO.BO-01

Açıklama: Veri merkezi bilgi sistemi bileşenlerinin bakımları kontrollü şekilde yapılacaktır. Bu amaçla;

- Cihaz ve/veya yazılım üreticisinin tanımladığı veya kurumsal gereksinimler doğrultusunda yapılacak planlı bakımların zamanları belirlenip dokümente edilmelidir.
- Bakımı yapılacak cihaz ve/veya yazılımların bakımları, bunlardan sorumlu veri merkezi personelinin gözetiminde veya söz konusu personel tarafından yapılmalıdır. Yapılan bakım çalışmalarının detayları dokümente edilmelidir.
- Bakım işlemlerinin tamamlanmasının ardından, ilgili cihaz ve/veya yazılımlar için uygulanan güvenlik kontrollerinin (yamalar, konfigürasyon, açık ağ servisleri, vb.) etkin olduğu kontrol edilmelidir. Bakım çalışmaları kapsamında sistemde yapılacak kalıcı değişiklikler referans konfigürasyona yansıtılmalıdır.
- Bakım amacıyla veri merkezinde kullanılacak cihaz ve yazılımların güvenilir olduğu kontrol edilmelidir. Bu amaçla, ilgili cihaz ve yazılımların güvenilir üreticilerden temin edilip edilmediği ve/veya bu cihaz ve yazılımları kullanan hizmet sağlayıcının güvenilirliği sorgulanabilir. Her durumda, bahsi geçen cihaz ve yazılımlar ancak sistem yöneticisi veya eşdeğer konumdaki personelin onayıyla ve bakımı yapılacak sistem bileşenlerinden sorumlu veri merkezi personelinin gözetiminde kullanılmalıdır.
- Bakım çalışmaları uzaktan erişim yöntemiyle yapılacaksa, bu amaçla

yetkilendirilen hizmet sağlayıcı personeli ve yetkilendirme kapsamı kayıt altına alınmalıdır. Söz konusu personel için veri merkezi bünyesinde kullanılan kimlik doğrulama ve yetkilendirme mekanizmasında erişim yetkisi tanımlanmalı ve uzaktan erişim yoluyla yapılan bakım çalışmalarının kaydı tutulmalıdır. Bakımı yapılan cihaz veya yazılımlardan sorumlu personelin söz konusu bakım çalışmalarını izleyebilmesini sağlayacak teknik mekanizmalar kurulmalıdır. Bakım çalışmaları tamamlandıktan sonra bu nitelikteki uzaktan erişim yetkileri iptal edilmelidir. Uzaktan erişim bağlantıları mutlaka güvenli ve güncel şifreleme protokolleri kullanılmak suretiyle korunmalıdır.

Kontrol: Olay kayıtları güvenli şekilde saklanacaktır.

Kod: S1.KO.BO-02

Açıklama: Olay kayıtları, veri merkezi bilgi sistemi bileşenleri üzerinde/aracılığıyla gerçekleşen ve güvenlik açısından önem arz eden olayların (sunucuya başarısız giriş denemeleri, sunucu üzerinde yapılan yeni hesap oluşturma, şifre değiştirme, kullanıcı yetki değişiklikleri gibi güvenlik açısından hassas işlemler, güvenlik duvarının oluşturduğu olay kayıtları, saldırı tespit sisteminin tespit ettiği saldırı girişimlerine ilişkin kayıtlar, antivirüs yazılımının tespit ettiği zararlı yazılımlara ilişkin kayıtlar, işletim sisteminin ve uygulama yazılımlarının kendi olay kayıtları, vb.) kayıtlarıdır. Veri merkezi işletmecisi bu kayıtları oluşturup güvenli şekilde saklamalıdır. Bu çerçevede;

- Veri merkezi işletmecisi bilgi sistemi bileşenleri üzerinde toplanacak olay kayıtlarını listeleyip dokümanete etmelidir. Hangi olay kayıtlarının toplanacağına, fiziksel cihaz ve yazılım envanterinde yer alan bilgi sistemi bileşenlerinin nitelikleri ve bunlara ilişkin risk değerlendirmesi doğrultusunda karar verilmeli ve söz konusu kayıtların bir güvenlik olayının analizinde nasıl yardımcı olabileceği açıklanmalıdır. Derlenecek olay kayıtları güvenlik izlemesi kontrol grubundaki kontroller kapsamında izlenmesi öngörülen faaliyetlerin takibini sağlayacak nitelikte olmalıdır.
- Olay kayıtları belirli aralıklarla ilgili bilgi sistemi bileşenlerinden toplanıp merkezi şekilde kayıt altına alınmalıdır. Hangi olay kaydının ne sıklıkta toplanacağı belirlenip dokümanete edilmelidir. Bu yapılırken, ilgili cihaz ve yazılımların ne hızda/hacimde olay kaydı oluşturduğu ve bunların lokal veri depolama kapasiteleri de dikkate alınmalıdır.
- Merkezi olarak depolanan olay kayıtlarının ne süreyle saklanacağı ilgili kaydın niteliğine bağlı olarak veri merkezi işletmecisi tarafından belirlenip dokümanete edilmelidir. Bu kayıtların mümkün olduğunca uzun süre saklanması, bir saldırı durumunda olayın nasıl gerçekleştiğini aydınlatmak amacıyla sistem üzerinde gerçekleşen işlemlerin geriye doğru takibini ve birbiriyle ilişkisini kurmayı kolaylaştırır.
- Merkezi olarak toplanan olay kayıtları, üzerlerinde değişiklik yapılmasını engeleyecek şekilde korunmalıdır. Bu amaçla sayısal imzalama, optik disk gibi bir kez kayıt yapılabilen ortamlarda saklama, vb. yöntemler benimsenebilir.

Personel Güvenliđi ve Eđitim Kontrol Grubu

Kontrol: Personel güvenliđi s¼reçleri oluřturulacaktır.

Kod: S1.KO.PE-01

Açıklama: Veri merkezi personelinden kaynaklanabilecek olası riskleri azaltmak amacıyla personel güvenliđi s¼reçleri oluřturulacaktır. Bu kapsamda;

- Personel rolleri için kritiklik/önem seviyesi tespit edilmelidir (örneğin; sistem yöneticisi için yüksek kritiklik/önem seviyesi, bakım personeli için düşük kritiklik/önem seviyesi, vb.).
- İlgili rolün kritiklik/önem seviyesine göre söz konusu rolü üstlenecek personelin taşıması gereken güvenlik nitelikleri (yüz kızartıcı bir suçtan dolayı ceza almamış olmak, aşırı/uç politik/ideolojik görüşleri benimsememek, önceki işyerlerinden alınan olumlu referanslar, karakter özellikleri, tamamlanan eğitimler, güvenlik kleransı, vb.) belirlenip dokümente edilmelidir.
- Veri merkezinde güvenlikle ilgili bir role atanacak personel bu nitelikler açısından amirlerince değerlendirilmeli ve bu doğrultuda ilgili role atanmalıdır. Bu değerlendirmeyi yapacak yetkililer belirlenip dokümente edilmelidir.
- Görevinden/rolünden ayrılan personelin ilgili görev/rol uyarınca veri merkezi bilgi sistemi üzerinde sahip olduđu erişim yetkileri derhal kaldırılmalıdır. Eğer belirli bilgi sistemi bileşenlerine erişim için gerekli araçlar (anahtar, akıllı kart, şifre üretici, vb.) bu personelin kontrolündeyse onlar da geri alınmalı veya iptal edilmelidir.
- Veri merkezi bilgi sisteminin güvenlik mimarisi ve teknik özellikleri hakkında detaylı bilgiye sahip personelle (sistem yöneticisi, ağ yöneticisi, güvenlik mimarı, vb.) gizlilik sözleşmesi yapılmalı, bu personelden ilgili görevden/rolden ayrılması durumunda sahip olduđu bu nitelikteki bilgileri üçüncü taraflarla paylaşmayacağına dair yazılı taahhüt alınmalıdır.
- Veri merkezinde bakım, onarım, teknik destek, kurulum, danışmanlık, vb. amaçlarla geçici veya sürekli olarak görev alacak üçüncü parti hizmet sağlayıcı personeli veya bağımsız uzmanlar için personel güvenliđi kriterleri belirlenip dokümente edilmelidir. Söz konusu çalışanlar bilgi sisteminin güvenlik mimarisi ve teknik özellikleri hakkında detaylı bilgiye sahip olabilecek durumdaysa, bu personelin kendisiyle ve/veya işvereniyle de gizlilik sözleşmesi yapılmalıdır.
- Bilgi güvenliđiyle ilgili rolü olan personelin sorumluluklarını geređince yerine getirmemesi durumunda karşılaşılabilecek yaptırımlar belirlenip dokümente edilmeli ve ilgili personel bu konuda bilgilendirilmelidir.

Kontrol: Bilgi güvenliđiyle ilgili sorumlulukları olan personelin bu alandaki farkındalıđı ve yetkinlikleri arttırılacaktır.

Kod: S1.KO.PE-02

Açıklama: Veri merkezi bünyesinde görev yapan ve güvenlikle ilgili görevleri bulunan personele (sistem yöneticileri, ağ yöneticileri, yazılım geliştiriciler, güvenlik mimarları, vb.) yönelik periyodik eğitim programları düzenlenecektir. Bu programların periyodu ve içeriđi veri merkezi işletmecisi tarafından belirlenmeli, eğitim alan personelin kayıtları tutulmalıdır. Eğitim programlarının mümkün olduğunca yoğun olması, personelin güncel

güvenlik tehditleri ve tedbirler konusunda daha yetkin olmasına ve sistem güvenliğini artırmaya yardımcı olur.

C-TESPİT FONKSİYONU

Anomali Tespiti Kontrol Grubu

Kontrol: Güvenlikle ilgili olay kayıtları raporlanacak ve analiz edilecektir.

Kod: S1.TE.AT-01

Açıklama: Gerek yazılımlar ve güvenlik cihazları gerekse veri merkezi personeli tarafından tespit edilen güvenlik olayları analiz edilerek sebepleri araştırılacak ve bunlar raporlanacaktır. Bu çerçevede;

- Yazılımlar ve güvenlik araçları tarafından üretilen olay kayıtları (erişim ve işlem kayıtları, saldırı girişimlerine ilişkin kayıtlar, zararlı yazılım tespitleri, vb.) ve sistemin rutin işletimi sürecinde personel tarafından tespit edilen güvenlik olayları sistematik şekilde raporlanacaktır. Bu raporlama, cihazlar/yazılımlar tarafından oluşturulan olay kayıtlarının merkezi olarak otomatik şekilde derlenmesi yoluyla olabileceği gibi ilgili cihaz/yazılım sorumlusu personel tarafından manuel olarak da yapılabilir. Raporlamanın amacı, ilgili personelin güvenlik olaylarını analiz etmesine yardımcı olmaktır. Raporlamanın ne şekilde (otomatik, manuel, raporlama periyodu, görevli personel, vb.) yapılacağına veri merkezi işletmecisi tarafından karar verilmelidir. Raporlama periyodunun kısa olması olası bir saldırının veya bilgi güvenliği tehdidinin erken tespitine yardımcı olur.
- Oluşturulan raporların ilgili personelce güvenlik tehditleri, hedefler, sistem zayıflıkları ve saldırı yöntemleri açısından analiz edilmesini sağlayacak süreç tanımlanmalıdır. Bu süreç, belirli rollerdeki personelin (güvenlik mimarı, ağ yöneticisi, vb.) söz konusu raporları topluca belirli aralıklarla değerlendirmesi şeklinde olabileceği gibi veri merkezi işletmecisinin atayacağı bir personelin raporların farklı kısımlarını ilgili veri merkezi uzmanlarının değerlendirmesini sağlaması şeklinde de olabilir. Bu şekilde yapılacak değerlendirmelerin nihai sonucu, gerektiği durumda raporlanan olaylara müdahale edecek personel ve/veya birimlerin belirlenerek bunların olası güvenlik zayıflıkları ve potansiyel saldırılar hakkında farkındalıklarının artırılması ve gerekli tedbirleri almasının sağlanmasıdır.
- Tespit edilen güvenlik olaylarının hangi sistem bileşenlerini etkilediği analiz edilmelidir. Bu amaçla, farklı cihaz ve yazılımların ürettiği olay kayıtları ve ağ trafiğine ilişkin kayıtlar değerlendirilerek güvenlik olayının hangi sistem bileşenlerini etkilemiş olabileceği belirlenmeli ve bu şekilde tespit edilen sistem bileşenlerinin bahse konu bilgi güvenliği olayından olumsuz şekilde etkilenip etkilenmediği araştırılmalıdır. Bu çalışmanın nihai çıktısı, güvenlik olayından olumsuz etkilenen sistem bileşenlerinin ve bu olumsuz etkinin niteliğinin tespit edilmesidir. Bu tespitler dokümanite edilmelidir.

Güvenlik İzlemesi Kontrol Grubu

Kontrol: Veri merkezi bilgi sistemi olası güvenlik tehditlerine karşı sürekli olarak izlenecektir.

Kod: S1.TE.GI-01

Açıklama: Veri merkezi ağı ve ağ üzerindeki cihaz ve yazılımlar olası güvenlik tehditlerine karşı sürekli olarak izlenecektir. Bu çerçevede yapılacak izleme asgari aşağıdaki hususları kapsamalıdır;

- Risk değerlendirmesi doğrultusunda hassas olduğu değerlendirilen cihaz ve yazılımlara yönetim/konfigürasyon amaçlı kullanıcı erişimlerinin belirlenen erişim yetkileri ve kısıtları (sunucu üzerinde yapılan yeni hesap oluşturma veya hesap kaldırma gibi işlemler, konfigürasyon değişiklikleri, veri ekleme/değiştirme/silme gibi hassas işlemler) çerçevesinde olup olmadığı incelenmelidir. Bu amaçla, erişim kontrolü ve yetkilendirme sistemi çerçevesinde oluşturulan sistem kayıtları ile ilgili cihazın/yazılımın olay kayıtları esas alınabilir. Bahse konu incelemeler otomatik veya manuel yöntemlerle yapılabilir. İncelemeye konu hassas cihaz ve yazılımlar veri merkezi işletmecisi tarafından tanımlanmalı ve dokümanite edilmelidir. Bunlar tipik olarak hassas verileri barındıran veya onlara erişimi kontrol eden cihaz/yazılım araçları ile güvenlik araçlarıdır. Bu incelemelerde tespit edilen anormallikler raporlanmalıdır.
- Yazılım envanterinde yer alan yazılımların bütünlüğü periyodik olarak kontrol edilmelidir. Bütünlük kontrolü hem aktif haldeki yazılımları hem de varsa bu yazılımların sanal makine imajlarını kapsar. Bu amaçla; envanterdeki yazılımların güvenilir olduğu bilinen bir zamanda bütünlük bilgileri (örneğin; sistem dosyaları özet değerleri) kayıt altına alınmalı, yazılımlarda değişiklik/güncelleme yapılması durumunda söz konusu bütünlük bilgileri de güncellenmelidir. Yazılımların bütünlüğü, veri merkezi işletmecisinin belirleyeceği aralıklarla ve en az dört ayda bir kez, yukarıda bahsi geçen bütünlük bilgileriyle karşılaştırılmak suretiyle kontrol edilmelidir. Bütünlük kontrolünden geçemeyen yazılımlar güvenli olduğu bilinen en son durumuna döndürülmeli, ayrıca yazılım bütünlüğünün bozulmasına sebep olan hususlar araştırılıp raporlanmalıdır.
- Gerek veri merkezi ağı üzerindeki gerekse veri merkezi ağı ile harici ağlar arasındaki trafik saldırı tespit sistemleri kullanılarak izlenmelidir. Hangi bağlantıların izlenmesi gerektiğine risk değerlendirmesi doğrultusunda karar verilmelidir. Harici ağlarla olan bağlantılar, kablolu ve kablosuz ağlar arasındaki bağlantılar, veri merkezi ağı üzerindeki hassas uygulamalar arasındaki bağlantılar (web sunucusu ile veritabanı sunucusu arasındaki bağlantı gibi) ve güvenlik nitelikleri farklı alt ağlar arasındaki trafik bu bağlamda özellikle dikkate alınmalıdır.
- Risk değerlendirmesi doğrultusunda hassas olduğu değerlendirilen yazılım platformları ve uygulamalar için uygulama bazlı zararlı yazılım ve saldırı tespit/önleme mekanizmaları kurulmalıdır. Bu mekanizmalar imza ve/veya davranış temelli antivirüs yazılımları, saldırı tespit sistemleri, veri kaybı önleme sistemi, vb. olabilir.
- Veri merkezini barındıran fiziksel ortam (bina, odalar, bölümler, katlar, vb.) olası güvenlik olaylarına karşı izlenmelidir. Bu çerçevede, hassas fiziksel bölümlerin

giriş/çıkış noktalarının kameralarla izlenip kayıt altına alınması, yetkisiz giriş teşebbüsü durumunda uyarı üreten alarm sistemleri kurulması, vb. tedbirler alınabilir. Veri merkezi işletmecisi hangi fiziksel alanların bu şekilde izleneceğini risk değerlendirmesi doğrultusunda belirleyip dokümente etmelidir.

- Veri merkezi ağı üzerindeki olası yetkilendirilmemiş cihazlar ve fiziksel ağ bağlantıları tespit edilmelidir. Bu amaçla, ağa bağlanacak cihazlar için merkezi bir yetkilendirme sistemi kurulabileceği gibi personel tarafından veri merkezi ağının fiziksel olarak incelenerek cihaz envanteri ve fiziksel ağ bağlantılarına ilişkin dokümantasyonla karşılaştırılması da sağlanabilir. Bu kapsamda alınacak tedbirler ve ne şekilde uygulanacağı dokümente edilmelidir.

D-MÜDAHALE FONKSİYONU

İletişim ve Analiz Kontrol Grubu

Kontrol: Tespit edilen güvenlik olayları konusunda ilgili taraflar bilgilendirilecektir.

Kod: S1.MU.IA-01

Açıklama: Koruma ve tespit fonksiyonları bünyesindeki kontroller kapsamında raporlanan güvenlik olayları konusunda, bu olaylara müdahale edebilecek durumdaki personele (genellikle ilgili cihaz veya yazılımın işletim ve bakımından sorumlu personel) ve ilgili diğer kurumsal birimlere bilgi verilecektir. Bu çerçevede;

- Güvenlik olaylarının analizi sonucunda belirlenen teknik ve/veya yönetsel güvenlik zayıflıkları dokümente edilmeli ve bu zayıflıklara müdahale etmekle görevli birim/personel bu konuda bilgilendirilmelidir.
- Tespit edilen güvenlik olaylarının ve sistem zayıflıklarının veri merkezinin bağlı bulunduğu ve/veya hizmet sunduğu üçüncü taraf bilgi sistemlerini olumsuz etkileme riski varsa (örneğin; sistemlere zararlı yazılım bulaşması, yetkisiz konfigürasyon değişikliği, vb.), ilgili taraflar söz konusu güvenlik olayları ve olası etkileri konusunda bilgilendirilmelidir.

Olay Müdahalesi Kontrol Grubu

Kontrol: Güvenlik olaylarına uygun şekilde müdahale edilecektir.

Kod: S1.MU.OM-01

Açıklama: Raporlanan güvenlik olaylarının yapılan analizi sonucunda veri merkezi açısından azaltılması veya ortadan kaldırılması gereken bir risk teşkil ettiği değerlendirilen güvenlik olaylarına müdahale edilecektir. Bu çerçevede,

- Öncelikle, güvenlik olayının olası olumsuz etkilerini sınırlandırmak amacıyla, ağ yapısı, sistem bileşenlerinin bağımlılıkları, veri akışları ve güvenlik olayından etkilenmesi öngörülen cihazların/yazılımların destekledikleri hizmetlerin kritikliği ve gerektiğinde güvenlik olayının adli analizini yapmak için ihtiyaç duyulabilecek kayıtların (ağ trafiği kayıtları, işletim sistemi olay kayıtları, güvenlik cihazlarının oluşturduğu kayıtlar, vb.) oluşturulması hususları dikkate alınarak, güvenlik olayının diğer sistem bileşenlerine sirayet etmesini önleyecek tedbirler (belirli ağ

bağlantılarının kesilmesi/kısıtlanması, belirli cihazların ağdan ayrılması, birtakım servislerin kapatılması, vb.) alınmalıdır.

- Belirlenip dokümanite edilen teknik veya yönetsel güvenlik zayıflıklarını azaltacak veya ortadan kaldıracak tedbirler uygulanarak ilgili dokümantasyon bu doğrultuda güncellenmelidir (örneğin; eksik bir yazılım yamasının kurulması durumunda yazılım referans konfigürasyonunun buna göre güncellenmesi, sisteme yeni bir güvenlik yazılımı eklenmesi durumunda bunun güvenlik mimarisine ve envanter kayıtlarına yasıtılması, vb.).
- Hızlı müdahale gerektiren ve etraflı değerlendirme için yeterli vakit olmayan güvenlik olaylarına (örneğin; sistemden kritik bilgilerin çalındığına yönelik güçlü şüphe, sunucuların servis dışı bırakma saldırısı altında olması, vb.) ne şekilde müdahale edileceğini belirleme yetkisi olan personel tespit edilmelidir. Bu personelin, bilgi sisteminin genel mimarisi, güvenlik fonksiyonları, yasal yükümlülükler ve potansiyel riskler konusunda yeterli ölçüde bilgili olması gereklidir. Pratikte bu rol güvenlik mimarı/şefi veya benzer bir görevli tarafından üstlenilebilir. Her durumda, güvenliği artırmak amacıyla bu şekilde sisteme yapılan kalıcı müdahaleler daha sonra ilgili dokümantasyona yasıtılmalıdır.
- Güvenlik olaylarına müdahale etkinliğini artırmak amacıyla, yaşanan güvenlik olaylarının sebepleri, olay müdahalesinde yaşanan aksaklıklar ve benzer durumlarda güvenlik olaylarına daha etkin müdahale için alınabilecek tedbirler hususunda ilgili personel dönemselsel olarak bilgilendirilmelidir. Bu bilgilendirme, güvenlik mimarı/şefi veya benzeri pozisyondaki bir yetkili tarafından yapılabilir. Bilgilendirme aralığı veri merkezi işletmecisi tarafından, yaşanan bilgi güvenliği olaylarının yoğunluğu ve insan kaynağı imkânlarına göre belirlenmelidir.
- Güvenlik olayının yasal olarak suç teşkil eden ve/veya raporlanması gereken bir saldırıdan kaynaklanması durumunda ilgili kamu otoritelerine bildirimde bulunulmalıdır.
- Veri merkezi işletmecisi, bu kontrol kapsamındaki tedbirlerin uygulanmasına ilişkin bir müdahale planı hazırlamalıdır. Bu plan, kurumsal öncelikler ve risk değerlendirmesi çerçevesinde, belirli kategorilerdeki saldırılar veya güvenlik tehditleri ortaya çıktığında nasıl tepki verileceğini tanımlamalı ve öncelikleri ortaya koymalıdır. Örneğin, e-posta sunucusunun servis dışı bırakma saldırısı altında olması durumunda internet servis sağlayıcıdan band genişliğinin azaltılmasının talep edilmesi veya hassas bilgileri barındıran veritabanından bilgi çalındığının tespiti durumunda başka hiçbir öncelik gözetilmeksizin veritabanının ağ bağlantısının tümüyle kesilmesi gibi. Plan, olaylara müdahaleyle görevli personel ve bunların yetki sınırlarını da netleştirmelidir. Örneğin; bir virüs saldırısına müdahale için sistem yöneticisi antivirüs yazılımlarının imza veritabanını güncelleyebilir veya hassas verilerin çalınması riski ortaya çıktığında güvenlik şefi tüm ağ bağlantılarını kesebilir.

E-KURTARMA FONKSİYONU

Kurtarma Planlaması Kontrol Grubu

Kontrol: Veri merkezi kurtarma planı hazırlanacaktır.

Kod: S1.KU.KP-01

Açıklama: Veri merkezinin olası bir güvenlik olayı sonrası normal çalışma şartlarına dönmesini sağlamak üzere kurtarma planı hazırlanacaktır. Bu plan;

- Olası bir güvenlik olayı sonrasında geçici veya kalıcı olarak devre dışı kalan bilgi sistemi bileşenlerinin normal çalışma şartlarına dönmesi için gerekli kullanıcı ve sistem bilgilerini kategorik olarak tanımlamalı ve bunlara nasıl (kurum bünyesindeki yedekleme sistemi, harici hizmet sağlayıcıda barındırılan veri yedekleri, vb.) erişileceğini göstermelidir. Veri merkezinin normal işletimi sürecinde yukarıda bahsi geçen bilgi kategorilerinde ortaya çıkabilecek değişiklikler plana yansıtılmalıdır.
- Veri merkezi hizmetlerinin önem seviyesine ve risk değerlendirmesine bağlı olarak, kurtarma faaliyetlerinde farklı sistem bileşenleri için nasıl bir önceliklendirme yapılması gerektiğini açıklamalıdır. Bu açıklamalar, bahsi geçen hizmetlerin niteliğine bağlı olarak, belirli sistem bileşenlerini ve/veya hizmetleri devreye almak için hedeflenen azami süreyi de tanımlayabilir.
- Veri merkezi operasyonlarının güvenliği ve devamlılığı açısından kritik önemdeki cihazlar ve yazılımlarda yaşanabilecek kesintileri/sorunları en kısa sürede çözümlenmek için ilgili tedarikçilerden temin edilecek destek hizmetleri önceden planlanmalıdır.
- Üçüncü parti hizmet sağlayıcılardan temin edilen telekomünikasyon ve enerji hizmetlerindeki olası kesintilere karşı devreye alınabilecek ve hazırda bekletilen yedek hizmetler için, bu tip kesintiler boyunca veri merkezinin ihtiyaç duyacağı kapasite göz önünde bulundurularak planlama yapılmalıdır. Kesinti durumunda söz konusu yedek hizmetlerin ne şekilde devreye alınacağı da ilgili hizmet sağlayıcıların iş süreçleri göz önünde bulundurularak önceden planlanmalıdır.
- Kurtarma çalışmalarında tespit edilen aksaklıkların nedenleri incelenmek suretiyle kurtarma planı sürekli olarak iyileştirilmelidir.
- Kurtarma planı, güvenlik mimarı/şefi veya benzeri üst seviye role sahip bir veri merkezi yetkilisi tarafından onaylanıp kurtarma faaliyetlerinde rol alması muhtemel personel plan hakkında bilgilendirilmelidir.
- Herhangi bir bilgi güvenliği olayı sonrasında kurtarma çalışmalarının tamamlanmasının ardından ilgili sistem bileşenlerinin referans konfigürasyon dokümantasyonunda öngörülen nitelikte olduğu kontrol edilmelidir. Bu husustaki olası aksaklıklar giderilmeden ilgili sistem bileşenleri devreye alınmamalıdır. Hizmet sürekliliği zorunlulukları nedeniyle hızlı hareket edilmesi gereken durumlarda konfigürasyon kontrolü bahse konu sistem bileşenlerinin devreye alınması sonrasında bırakılabilir. Böylesi durumlarda bu kontrollerin en kısa sürede yapılması sağlanmalıdır. Kurtarma planı, bu süreci takip edip gerekli kararları verecek yetkili personeli tanımlamalı, bu personel kurtarma faaliyetlerindeki rolleri ve verecekleri kararların olası sonuçları konusunda bilgilendirilmelidir. Söz konusu personelin, veri merkezi hizmet ihtiyaçlarını ve güvenlik risklerini iyi anlamış çalışanlar olması gereklidir.

EK-2: Seviye-2 Veri Merkezi Güvenlik Kontrolleri

Bu kısım Tablo-3'de yer verilen bilgi güvenliği kontrollerinin detaylı açıklamalarını içerir.

A-TANIMLAMA FONKSİYONU

Varlık Yönetimi Kontrol Grubu

Kontrol: Veri merkezi bünyesindeki fiziksel cihaz ve sistemlerin envanteri tutulacaktır.

Kod: S2.TA.VY-01

Açıklama: Veri merkezi hizmetlerinin sunumunda kullanılan fiziksel cihaz ve sistemlerin envanteri tutulacaktır. Bu envanter aşağıdaki şartları sağlamalıdır;

- Bilgi sisteminin mevcut durumunu doğru şekilde göstermelidir.
- Bilgi sistemi bileşenlerini envanter takibi yapmaya ve raporlamaya imkân verecek detayda göstermelidir. Envanter, kendi başına belirli bir fonksiyon ifa eden her bir fiziksel cihazı göstermelidir. Örneğin; sunucu donanımı, ethernet anahtar, monitör, bağımsız veri depolama veya yedekleme ünitesi, güvenlik duvarı donanımı, modem, kesintisiz güç kaynağı, vb. Söz konusu cihazların bakım, kapasite yükseltme, vb. sebeplerle cihazdan ayrılabilir ve diğer sistem bileşenlerinden bağımsız olarak tanımlanabilecek elektronik sistem bileşenleri (sabit disk, RAM, işlemci, anakart, dâhili güç kaynağı modülü, vb.) de envantere gösterilmelidir. Bu çerçevede, hangi cihaz ve elektronik bileşenlerin envantere yer aldığı açıklanmalıdır.
- Envantere kaydedilecek elektronik sistem bileşenlerine, bu bileşenleri ayrı ayrı takip etmeye imkân verecek kod, kayıt numarası, vb. atayarak ilgili bileşenler uygun şekilde (barkod, etiket, vb.) işaretlenmelidir. İlgili sistem bileşenini tekil olarak tanımlayabilecek bir bilgi (üretici seri numarası gibi) mevcutsa bu da aynı amaçla kullanılabilir.
- Envanterdeki cihazların tanımlayıcı ve fonksiyonel özellikleri dokümante edilmelidir. Örneğin; cihaz veya elektronik sistem bileşeninin üreticisi, modeli ve seri numarası, sunucular için üzerindeki işlemci sayısı ve modeli, ethernet anahtarlar için port sayısı ve bant genişliği, vb.
- Ağ bağlantılı cihazlar (yönlendirici, ağ yazıcısı, modem, vb.) için cihazların ağ üzerindeki isimleri, fiziksel ve mantıksal adresleri kayıt altına alınmalıdır. Mantıksal ağ adresleri dinamik ise bu durum dokümantasyonda belirtilmelidir.
- Cihazların fiziksel olarak buldukları yer (oda, kabin, raf, vb.) açıklanmalıdır.
- Envanterdeki cihazların yönetiminden (kurulum, konfigürasyon, güncelleme, bakım, vb.) sorumlu personel belirlenip kayıt altına alınmalıdır.
- Yukarıdaki maddelerde bahsi geçen envanter takip işlemlerini yapmaya imkân veren merkezi bir elektronik sistem kurulmalıdır. Bu sistem envanterdeki tüm cihaz ve elektronik sistem bileşenlerini kapsamalı, ayrıca envanterdeki elektronik sistem bileşenleri ile cihazlar arasındaki bağımlılık/kullanım ilişkisini (örneğin; sunucu donanımı ve bunun parçası olan sabit disk ve RAM, yönlendirici cihazı ve bunun parçası olan dâhili güç ünitesi, vb.) de göstermelidir.
- Bakım, onarım, kapasite artırımı, cihaz değişikliği/ilavesi, vb. durumlarda yukarıdaki bilgilerde olabilecek değişikliklerin derhal envantere yansıtılabilmesi amacıyla veri merkezi işletmecisi tarafından envanter güncelleme süreci

tanımlanarak dokümente edilmelidir. Envanter en az yılda bir kez güncellik açısından gözden geçirilmeli ve bilgi sisteminin güncel durumunu yansıttığı teyit edilmelidir. Cihazların bünyesindeki elektronik sistem bileşenlerinin envanter kayıtlarıyla karşılaştırılması ilgili cihaza fiziksel müdahale gerektirebileceğinden, bu gibi durumlarda sistem kesintisini minimum düzeyde tutmak amacıyla, bir önceki gözden geçirme döneminde fiziksel müdahalede bulunulmadığı bilinen cihazlar için bu tür kontroller yapılmayabilir.

Kontrol: Veri merkezi bünyesindeki yazılım platformları ve uygulamaların envanteri tutulacaktır.

Kod: S2.TA.VY-02

Açıklama: Bu kontrolün kapsamı S1.TA.VY-02 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Bu kontrol kapsamındaki yazılım envanter takibi işlemlerini yapmaya imkân veren merkezi bir elektronik sistem kurulmalıdır.

Kontrol: Organizasyonel veri akışları dokümente edilecektir.

Kod: S2.TA.VY-03

Açıklama: Bu kontrolün kapsamı S1.TA.VY-03 kodlu kontrolle aynıdır.

Kontrol: Harici bilgi sistemleri kataloglanacaktır.

Kod: S2.TA.VY-04

Açıklama: Bu kontrolün kapsamı S1.TA.VY-04 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Harici bilgi sistemiyle kurumsal bilgi paylaşılacaksa (sağlık bilgisi, finansal bilgiler, diğer kişisel bilgiler, mühendislik tasarımları, idari kayıtlar, vb.) bu bilginin niteliği ile bunların hassasiyet derecesi açıklanmalıdır. Veri merkezi işletmecisi, paylaşılan verinin niteliğine/hassasiyetine bağlı olarak, ilgili harici bilgi sisteminin sağlaması gerekli asgari güvenlik kriterlerini (güvenlik sertifikasyonu, bilgi güvenliği süreçlerinin varlığı ve olgunluğu, yasal yetkilendirme, vb.) tanımlamalıdır. İlgili mevzuat uyarınca herhangi bir harici bilgi sistemiyle paylaşılması gereken veriler bu kapsamda değildir.

Kontrol: Varlıklar için kritiklik değerlendirmesi yapılacaktır.

Kod: S2.TA.VY-05

Açıklama: Bu kontrol kapsamında veri merkezi bünyesindeki varlıklar (cihazlar, yazılımlar ve veri) için kritiklik/hassasiyet değerlendirmesi yapılacaktır. Varlıkların kritiklik/hassasiyet değerlendirmesi, söz konusu varlıkların geçici veya kalıcı olarak kullanılamaz hale gelmesi, yok olması, bütünlüğünün zarar görmesi, ilgisiz/yetkisiz kişilerin eline geçmesi gibi olumsuzlukların veri merkezi işletmecisine, kullanıcılarına

ve/veya bağlantılı olduğu harici bilgi sistemlerine verebileceği zarar göz önüne alınarak yapılmalıdır. Bu değerlendirme için veri merkezi işletmecisinin belirleyeceği bir ölçek kullanılabilir (yüksek/orta/düşük kiritiklik seviyeleri gibi). Bu çerçevede;

- Veri merkezi bilgi sisteminde kullanılan fiziksel cihaz ve yazılımlar için kritiklik/hassasiyet değerlendirmesi yapılacaktır.
- Veri merkezi bünyesinde barındırılan, işlenen veya oluşturulan veriler gruplandırılarak (resmi yazışmalar, kişisel sağlık bilgileri, fikri mülkiyete konu bilgi varlıkları, personel bilgileri, vb. ve uygun olduğu durumda bu türdeki bilgilerin alt kırılımları) bunlar için kritiklik/hassasiyet değerlendirmesi yapılmalıdır. Veri merkezi işletmecisi söz konusu veri gruplarını belirleyerek dokümanete etmelidir.
- Veri merkezi bilgi sisteminde teknik değişiklik yapılması, yeni hizmetlerin devreye alınması, farklı türlerde veri barındırılmaya/işlenmeye başlanması gibi durumlarda kritiklik/hassasiyet değerlendirmesi söz konusu değişiklikler dikkate alınarak gözden geçirilmelidir. Veri merkezi işletmecisi buna ilişkin süreci tanımlayıp dokümanete etmelidir.

İş Ortamı Kontrol Grubu

Kontrol: Enerji ve telekomünikasyon hizmet bağımlılıkları belirlenip dokümanete edilecektir.

Kod: S2.TA.IO-01

Açıklama: Bu kontrolün kapsamı S1.TA.IO-01 kodlu kontrolle aynıdır.

Kontrol: Bilgi güvenliğine ilişkin yasal yükümlülükler dokümanete edilecektir.

Kod: S2.TA.IO-02

Açıklama: Bu kontrolün kapsamı S1.TA.IO-02 kodlu kontrolle aynıdır.

Risk Yönetimi Kontrol Grubu

Kontrol: Bilgi sistemine yönelik tehditler dokümanete edilecektir.

Kod: S2.TA.RY-01

Açıklama: Veri merkezi bünyesinde kullanılan cihaz ve yazılımlara yönelik tehditlere ilişkin bilgiler ilgili kaynaklardan derlenip dokümanete edilecektir. Bu amaçla;

- Bilgi güvenliğiyle ilgili güncel zayıflıklar ve tehditler ilgili çevrimiçi forumlar, uzmanlık grupları, kamuya açık güvenlik zayıflık veritabanları, güvenlik şirketleri, ilgili kamu otoriteleri ve araştırma kurumları, diğer veri merkezi işletmecileriyle olan bilgi paylaşımları, vb. kaynaklar vasıtasıyla düzenli şekilde takip edilecektir.
- Bu bilgilerden veri merkezi bilgi sistemi bileşenlerinin güvenliğiyle ilgili olabilecekler derlenip dokümanete edilecektir.
- Veri merkezi işletmecisi bu süreci yürütecek personeli belirlemelidir.

Kontrol: Veri merkezi risk analizi yapılacaktır.

Kod: S2.TA.RY-02

Açıklama: Bilgi sistemine yönelik tehditlere ilişkin olarak derlenen bilgiler dikkate alınarak veri merkezi bilgi sistemi için bilgi güvenliği risk analizi yapılacaktır. Bu kapsamda;

- Bahse konu tehditlerin veri merkezi operasyonları açısından sebep olabileceği zarar ve bunun ne kadar olası olduğu belirlenecektir. Yeterli bilgi mevcutsa bu değerlendirme için sayısal zarar ve olasılık tahminleri kullanılabilir. Buna imkân yoksa zarar ve olasılıklar bir ölçek çerçevesinde (düşük/orta/yüksek gibi) uzman görüşleri temel alınarak öngörülebilir. S2.TA.VY-05 kodlu kontrol kapsamındaki değerlendirmeler bu bağlamda dikkate alınmalıdır.
- Söz konusu zarar ve olasılık öngörülerini dikkate alınarak ilgili tehditlerin veri merkezi operasyonları için oluşturduğu risk hesaplanmalıdır.
- Risk analizi çalışması için <http://www.cert.org/resilience/products-services/octave> adresinden ulaşılabilen OCTAVE metodu veya benzer başka standartlar/çalışmalar kullanılabilir.
- Risk analizi, veri merkezi altyapısında yapılacak önemli değişiklikler (bilgi sistemine yeni bileşenler eklenmesi, bazı bileşenlerin devreden çıkarılması veya mevcut bileşenlerde güvenliği etkileyebilecek değişiklikler) sonrasında gözden geçirilmeli ve gerektiğinde güncellenmelidir. Benzer şekilde, bilgi güvenliği tehditlerine ilişkin bilgiler güncellendikçe bunun mevcut risk analizini ne şekilde etkilediği de düzenli olarak gözden geçirilmelidir.
- Veri merkezi işletmecisi bu kontrol kapsamında yapılacak çalışmalara ilişkin süreci ve bunların ne şekilde dokümente edileceğini tanımlamalıdır.

Kontrol: Veri merkezi riskini kabul edilebilir seviyeye çekecek önlemler belirlenecektir.

Kod: S2.TA.RY-03

Açıklama: Veri merkezi risk analizi çerçevesinde belirlenen riskleri azaltarak veri merkezi işletmecisi açısından kabul edilebilir seviyeye çekecek teknik/idari tedbirler belirlenip dokümente edilecektir. Bu kapsamda;

- Belirlenen riskleri azaltacak teknik/idari tedbirlerin maliyeti öngörülecektir.
- Bu maliyetler ilgili tedbirlerin sağlayacağı marjinal faydayla karşılaştırılıp söz konusu tedbirlerin önceliğine ve uygulanıp uygulanmayacağına karar verilecektir.
- Bu süreçte yapılan değerlendirmeler dokümente edilecektir.
- Veri merkezi risk analizinde olabilecek değişiklikler ve/veya riski azaltmak için uygulanabilecek tedbirlerin mahiyetinin/maliyetinin değişmesi durumunda yukarıdaki öngörü ve kararlar gözden geçirilecek ve gerektiğinde güncellenecektir.

Kontrol: Veri merkezi bilgi güvenliği mimarisi oluşturulacaktır.

Kod: S2.TA.RY-04

Açıklama: Bu kontrolün kapsamı S1.TA.RY-02 kodlu kontrolle aynıdır.

B-KORUMA FONKSİYONU

Erişim Kontrolü Kontrol Grubu

Kontrol: Kimlik yönetimi ve yetkilendirme sistemi oluşturulacaktır.

Kod: S2.KO.EK-01

Açıklama: Bu kontrolün kapsamı S1.KO.EK-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Güvenlik açısından kritik hesaplara erişim için en az iki faktörlü kimlik doğrulama kullanılmalıdır.
- Bu kontrolün öngördüğü işlevselliğe sahip merkezi bir elektronik kimlik yönetimi ve yetkilendirme sistemi kurulmalıdır.
- Kullanıcı kimlik doğrulaması hiçbir şekilde harici kimlik doğrulama hizmetleri (Facebook, Google, Yahoo, vb.) yoluyla yapılmamalıdır. Yasal gerekçelerle güvenli olduğundan emin olunan harici elektronik kimlik doğrulama hizmetleri (resmi elektronik kimlik kartı, yetkili bir kamu kurumu tarafından sunulan elektronik kimlik doğrulama hizmeti, vb.) bu kapsamda değildir.
- Tüm kullanıcı hesapları için belirlenmiş sayıda başarısız sisteme giriş denemesi sonrasında ilgili hesabı bloke edecek bir teknik mekanizma kurulmalıdır.

Kontrol: Bilgi varlıklarına fiziksel erişim kontrol edilecektir.

Kod: S2.KO.EK-02

Açıklama: Bu kontrolün kapsamı S1.KO.EK-02 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezinin bulunduğu fiziksel bina bölümlerine kendilerine eşlik edecek yetkili personel eşliğinde girecek ziyaretçi, bakım/destek personeli, vb. kişilerin kimlikleri tespit edilerek giriş-çıkış zamanları ve söz konusu bölümlerde bulunma gerekçeleri kayıt altına alınmalıdır.

Kontrol: Bilgi varlıklarına uzaktan erişim kontrol edilecektir.

Kod: S2.KO.EK-03

Açıklama: Bu kontrolün kapsamı S1.KO.EK-03 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezi işletmecisi gerektiğinde istenen uzaktan erişim bağlantılarını derhal ve otomatik olarak sonlandırabilecek bir teknik mekanizma oluşturmalıdır.
- Uzaktan erişim yoluyla veri merkezi bilgi sistemine bağlanmak için kullanılacak terminaller veri merkezi işletmecisi tarafından önceden tanımlanmış ve gerekli güvenlik konfigürasyonu (işletim sistemi açık servisleri, cihazda yüklü yazılımlar, antivirüs ve saldırı tespit sistemi gibi güvenlik araçlarının kurulması) yapılmış

cihazlar olmalıdır. Bu konfigürasyon söz konusu terminallerin kullanılabilceği harici ađlar ve ortamların güvenlik niteliđi göz önünde bulundurularak belirlenip dokümente edilmelidir. Bu çerçevede, söz konusu cihazların veri merkezine uzaktan bağlantıları için uygun bir cihaz kimliđi doğrulama mekanizması oluşturulmalıdır.

- Hassas verilerin kullanıcı terminallerine transferine mümkün olan en sınırlı kapsamda izin verilmeli, böylesi durumlarda da söz konusu verileri kullanıcı terminalinde ancak yetkili cihaz kullanıcısının açabileceđi şekilde şifreleyerek saklayacak bir teknik mekanizma oluşturulmalıdır. Bu amaçla oluşturulacak şifreleme anahtarlarının yaşam döngüsünün yönetimine ilişkin süreç tanımlanmalıdır.
- Uzaktan erişim bağlantısı üzerinden veri merkezi ađıyla gerçekleşen trafik, şifresinin açılmasının ardından, veri merkezi bünyesinde kullanılan güvenlik araçlarıyla (antivirüs yazılımı, saldırı tespit/önleme sistemi, veri kaybı önleme yazılımı) gözlenmelidir. Bu güvenlik araçlarının tespit ettiđi bir saldırı veya güvenlik riski durumunda bahse konu uzaktan erişim bağlantısı otomatik olarak kesilmelidir.

Kontrol: Veri merkezi ađı alt ađlara bölünecektir.

Kod: S2.KO.EK-04

Açıklama: Bu kontrolün kapsamı S1.KO.EK-04 kodlu kontrolün kapsamıyla aynıdır.

Veri Güvenliđi Kontrol Grubu

Kontrol: Durađan haldeki bilgiler korunacaktır.

Kod: S2.KO.VG-01

Açıklama: Bu kontrolün kapsamı S1.KO.VG-01 kodlu kontrolle aynıdır.

Kontrol: Ađ üzerinden gönderilen bilgiler korunacaktır.

Kod: S2.KO.VG-02

Açıklama: Bu kontrolün kapsamı S1.KO.VG-02 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- İceriđi şifrelenmiş dahi olsa ađ üzerinde gözlemlenebilen trafik özelliklerinden (zaman, hacim, veri aktarım aralıđı, haberleşme uç noktaları, vb.) yapılacak çıkarsamaların güvenlik riski oluşturabileceđi değerlendirilen veri akışları (özellikle harici bilgi sistemleriyle olan trafik bu kapsamda değerlendirilmelidir) için bu gözlemleri anlamsız/kullanışsız kılacak şekilde trafik yapısı yapay olarak deđiştirilmelidir. Bu amaçla, rastgele aralıklarla rastgele hacimde gereksiz/anlamsız bilgi iletimi gibi taktikler kullanılabilir.

Kontrol: İşletmeci kontrolü dışına çıkacak bilgi sistemi bileşenleri üzerindeki veriler

imha edilecektir.

Kod: S2.KO.VG-03

Açıklama: Bu kontrolün kapsamı S1.KO.VG-03 kodlu kontrolle aynıdır.

Kontrol: Veri merkezi bilgi sistemi potansiyel saldırılara karşı izlenip korunacaktır.

Kod: S2.KO.VG-04

Açıklama: Bu kontrolün kapsamı S1.KO.VG-04 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezinin harici ağlarla olan bağlantıları üzerinden taşınan trafiğin metadata bilgilerini kayıt altına alacak teknik mekanizmalar kurulmalıdır. Bu kayıtlar, trafik içeriğini izlemeksizin, trafik özelliklerinin (IP adresleri, haberleşme portları, bağlantı zamanı ve süreleri, trafik hacmi, vb.) analiz edilmesi yoluyla anomali/saldırı tespitine yardımcı olur. Söz konusu kayıtların saklanma süresi, güvenlik olay kayıtlarının saklanması için belirlenen süreyle uyumlu olacak şekilde, veri merkezi işletmecisi tarafından belirlenmelidir. Bu tür bir tedbir, risk değerlendirmesi doğrultusunda, veri merkezi iç ağı üzerindeki güvenlik açısından hassas ve trafik izlemesinin saldırı tespiti açısından yararlı olabileceği değerlendirilen noktalarda (örneğin; işlenen/saklanan bilgilerin güvenlik hassasiyetinin, kullanıcıların oluşturduğu ağ trafiği deseninin ve/veya kullanılan uygulama katmanı protokollerinin birbirinden önemli ölçüde farklı olduğu alt ağlar arasındaki bağlantılar) da uygulanabilir.
- Veri merkezi ağı harici ağlardan gelebilecek servis dışı bırakma saldırılarına karşı korunmalıdır. Bu kapsamda, saldırının geldiği adres bloklarının trafiğini internet servis sağlayıcı seviyesinde veya veri merkezi ağı girişinde yavaşlatma, gerektiğinde hızlı şekilde devreye alınabilecek ilave telekomünikasyon hizmet kapasitesini yedekte tutma, vb. önlemler alınmalıdır ve bunlar dokümanite edilmelidir.
- Kablosuz ağ cihazlarının kontrolsüz/yetkisiz şekilde veri merkezi ağına eklenmesini engelleyecek teknik bir mekanizma kurulmalıdır. Bu amaçla merkezi bir cihaz yetkilendirme mekanizması kurulup işletilebilir.

Kontrol: Geliştirme ve test ortamı üretim ortamından ayrılacaktır.

Kod: S2.KO.VG-05

Açıklama: Geliştirme ve test ortamları, bu nitelikteki çalışmaların ihtiyaç duyduğu esnekliğe paralel olarak, üretim ortamına nispetle daha esnek güvenlik tedbirlerinin uygulanmasını gerektirebilir. Bu nedenle, veri merkezi bünyesinde oluşturulan geliştirme ve test ortamı mantıksal veya fiziksel olarak üretim ortamından ayrılmalıdır. Aksini gerektiren zorlayıcı gereksinimler yoksa bu ayrıştırma fiziksel olarak yapılmalıdır (örneğin; fiziksel olarak diğer ağlarla bir bağlantısı olmayan bağımsız bir ağ kurmak suretiyle). Eğer ayrıştırma mantıksal seviyede yapılacaksa, geliştirme ve test ortamıyla üretim ortamı arasındaki bağlantılar, fiziksel bağlantı noktaları, bağlantı üzerinden geçirilecek trafiğin niteliği (haberleşme portları, adresler, yetkili kullanıcılar, trafik hacmi, bağlantı zamanı, vb.) açısından mümkün olan en üst seviyede kısıtlanmalıdır.

Bilgi Koruma Süreçleri Kontrol Grubu

Kontrol: Bilgi sistemi bileşenleri için referans konfigürasyonlar oluşturulacak ve güncelliği sağlanacaktır.

Kod: S2.KO.BK-01

Açıklama: Bu kontrolün kapsamı S1.KO.BK-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Referans konfigürasyonun yönetimine ilişkin olarak bu kontrol kapsamında tanımlanan işlevleri gerçekleştirecek ve/veya gerçekleştirilen işlemlerin takibini yapmaya imkân sağlayacak merkezi bir konfigürasyon yönetim sistemi kurulmalıdır.
- Referans konfigürasyonda yapılması onaylanan değişikliklerin ilgili cihaz/yazılımdan sorumlu personel tarafından uygulanması esnasında veya bunu muteakip söz konusu konfigürasyon değişikliğinin doğru şekilde yapıldığını kontrol edip rapor edecek ikinci bir personel belirlenmelidir. Bu tedbir, personel hatası veya kötü amaçlı girişimlerden kaynaklanabilecek olası zararları azaltmayı amaçlar.

Kontrol: Veri yedekleme mekanizması oluşturulacaktır.

Kod: S2.KO.BK-02

Açıklama: Bu kontrolün kapsamı, aşağıda belirtilenler hariç, S1.KO.BK-02 kodlu kontrole aynıdır;

- Yedekleme sistemi ana bilgi sisteminin bulunduğu lokasyondan farklı bir yerde barındırılmalıdır. Bu lokasyonun seçiminde doğal afet olasılığının daha düşük ve bağımsız olduğu bir bölge seçilmesi önem taşır.

Kontrol: Fiziksel işletim ortamına ilişkin politikalar belirlenip uygulanacaktır.

Kod: S2.KO.BK-03

Açıklama: Bu kontrolün kapsamı S1.KO.BK-03 kodlu kontrole aynıdır.

Kontrol: Bilgi sistemi zayıflık yönetim planı hazırlanıp uygulanacaktır.

Kod: S2.KO.BK-04

Açıklama: Bu kontrolün kapsamı S1.KO.BK-04 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezi hizmetleri için özel olarak geliştirilmiş yazılımların zayıflık incelemesi yapılmalıdır. Bu amaçla, statik ve dinamik yazılım güvenliği test yöntemleri uygulanabilir. Bu şekilde tespit edilecek zayıflıklar ve zayıflığı gidermek üzere alınan tedbirler dokümanite edilmelidir. Veri merkezi işletmecisi bu çerçevede yapacağı testlere ilişkin süreci (kullanılan test yöntemleri, hangi tür güvenlik zayıflıkları için test yapıldığı, test personeli, güvenlik testlerinin yazılım geliştirme sürecindeki yeri, vb.) tanımlamalıdır.

Bakım ve Olay Kayıtları Kontrol Grubu

Kontrol: Bilgi sisteminin kontrollü bakımı sağlanacaktır.
Kod: S2.KO.BO-01
Açıklama: Bu kontrolün kapsamı S1.KO.BO-01 kodlu kontrolle aynıdır.

Kontrol: Olay kayıtları güvenli şekilde saklanacaktır.
Kod: S2.KO.BO-02
Açıklama: Bu kontrolün kapsamı S1.KO.BO-02 kodlu kontrole ilave olarak aşağıdakileri kapsar; <ul style="list-style-type: none">• Merkezi olarak toplanan olay kayıtlarına inceleme, başka bir bilgi sistemine aktarım, silme, vb. amacıyla erişebilecek personel tanımlanmalıdır. Söz konusu kayıtlara sadece yetkili personelin erişimini sağlayacak teknik mekanizma oluşturulmalıdır.• Önceden belirlenmiş ve otomatik olarak uygulanan kayıt silme ve aktarım işlemleri dışında olay kayıtlarının silinmesi veya aktarımı ancak en az iki yetkili personelin onayıyla yapılmalıdır. Buna ilişkin teknik mekanizma ve idari süreç tanımlanıp dokümante edilmelidir.

Personel Güvenliği ve Eğitim Kontrol Grubu

Kontrol: Personel güvenliği süreçleri oluşturulacaktır.
Kod: S2.KO.PE-01
Açıklama: Bu kontrolün kapsamı S1.KO.PE-01 kodlu kontrole ilave olarak aşağıdakileri kapsar; <ul style="list-style-type: none">• Güvenlik açısından kritik rollerdeki personelin işyerindeki davranışlarındaki (iş arkadaşlarıyla ilişkileri, işe geliş-gidiş zamanları, rolün gerektirdiği özeni gösterme, veri merkezi işletmecisinin belirlediği genel işyeri kurallarına uyum, vb.) beklenmeyen/sıradışı/olumsuz değişiklikler personel yönetimi birimi veya eşdeğer idari birim tarafından yakından takip edilmelidir. Böylesi durumlar bahse konu personelin bilgi sistemi üzerindeki faaliyetlerini olası kötü amaçlı müdahalelere karşı daha yakından takip etmeyi gerektirebilir. Veri merkezi işletmecisi bu tür değerlendirmelerin ve incelemelerin yapılmasına ilişkin süreci tanımlayıp dokümante etmelidir.

Kontrol: Bilgi güvenliğiyle ilgili sorumlulukları olan personelin bu alandaki farkındalığı ve yetkinlikleri arttırılacaktır.
Kod: S2.KO.PE-02
Açıklama: Bu kontrolün kapsamı S1.KO.PE-02 kodlu kontrolle aynıdır.

C-TESPİT FONKSİYONU

Anomali Tespiti Kontrol Grubu

Kontrol: Kullanıcıların ağ kullanım davranışlarına ve veri akışlarına ilişkin referans profiller oluşturulacaktır.

Kod: S2.TE.AT-01

Açıklama: Veri merkezi bilgi sistemine erişim yetkisi olan kullanıcılar için bu kullanıcıların ağ üzerinde oluşturdukları veri trafiğine ilişkin referans profiller oluşturulacaktır. Söz konusu profiller, kullanıcıların ağ kullanım davranışlarındaki değişiklikleri gözlemleyerek olası saldırıların tespitine yardımcı olur. Bu kapsamda;

- Kullanıcıların (belirli kullanıcı yetkileriyle otomatik olarak ağ üzerinde trafik yaratan işlemler yapan sunucular gibi yazılımlar da bu kapsamdadır) veri merkezi ağı üzerinde oluşturdukları trafiğin profili oluşturulacaktır. Profilin unsurları (bağlantı alıcı/gönderici port ve adres bilgileri, trafik hacmi, bağlantının gün/hafta içinde oluşma zamanı, süresi ve tekrarlamaya sayısı, bağlantı üzerinden aktarılan paket sayısı ve ortalama büyüklüğü, vb.) kullanıcı gruplarının erişim yetkileri, kullandıkları hizmetler ve risk değerlendirmesi doğrultusunda veri merkezi işletmecisi tarafından belirlenip dokümanite edilmelidir.
- S2.KO.VG-04 kodlu kontrol kapsamında derlenecek trafik metadata bilgileri yukarıdaki maddede açıklanan profili oluşturmak için kullanılabilir. Ancak, söz konusu metadata bilgilerinin ağ üzerinde izlendiği/toplandığı noktalardaki kullanıcı trafiğinin gerçek kullanıcı trafiğini yüksek doğrulukta temsil ediyor olması önem arz eder. Örneğin; her bir kullanıcının veri merkezi ağına bağlantısının sağlandığı ilk noktada (kullanıcı terminalinin ethernet anahtara bağlandığı nokta gibi) kullanıcı trafiğinin tamamını gözlemlemek mümkünken harici ağlarla iletişimi kontrol eden vekil sunucunun bulunduğu noktada gözlemlenecek trafik sadece harici ağlarla etkileşimin niteliği konusunda bilgi verebilir. Bu çerçevede, kullanıcı ağ trafiği profillerini oluşturmak amacıyla derlenecek trafik metadata bilgilerinin ağ üzerinde hangi stratejik noktalarda izleneceğine/toplanacağına farklı kullanıcı gruplarının ağ üzerinde oluşturdukları trafiğin yeri ve risk değerlendirmesi doğrultusunda karar verilmelidir.
- Belirlenen stratejik noktalarda izlenen kullanıcı trafiğini kullanıcı profilleriyle karşılaştırıp gözlemlenen belirgin sapmaları otomatik şekilde güvenlik olay kaydı olarak raporlayacak bir teknik mekanizma kurulmalıdır. Profilin unsurlarındaki hangi miktar değişimin belirgin sapma olarak kabul edileceği veri merkezi işletmecisi tarafından belirlenip dokümanite edilmeli ve bahse konu teknik mekanizmanın konfigürasyonu bu doğrultuda yapılmalıdır.

Kontrol: Olay kayıtları birbiriyle ilişkilendirilerek potansiyel saldırılar tespit edilecektir.

Kod: S2.TE.AT-02

Açıklama: Yazılımlar ve güvenlik araçları tarafından derlenen olay kayıtlarını birbiriyle ilişkilendirip potansiyel güvenlik olaylarını tespit edip raporlayabilecek bir teknik mekanizma oluşturulmalıdır. Bu amaçla güvenlik bilgi ve olay yönetimi (Security Information and Event Management - SIEM) araçları kullanılabilir.

Kontrol: Güvenlikle ilgili olay kayıtları raporlanacak ve analiz edilecektir.

Kod: S2.TE.AT-03

Açıklama: Bu kontrolün kapsamı S1.TE.AT-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- S2.TE.AT-01 ve S2.TE.AT-02 kodlu kontroller kapsamında üretilen güvenlik olay kayıtları da bu kontrol kapsamında raporlanıp analiz edilmelidir.

Güvenlik İzlemesi Kontrol Grubu

Kontrol: Veri merkezi bilgi sistemi olası güvenlik tehditlerine karşı sürekli olarak izlenecektir.

Kod: S2.TE.GI-01

Açıklama: Bu kontrolün kapsamı S1.TE.GI-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezi işletmecisi bilgi sisteminde yetkisiz yazılımlar/uygulamalar çalışıp çalışmadığını tespit etmek üzere gerekli teknik/idari mekanizmaları oluşturmalıdır. Bu amaçla, işletim sistemlerindeki aktif proseslerin belirli aralıklarla veya rastgele zamanlarda otomatik şekilde veya personel tarafından el yordamıyla kontrolü gibi yöntemler benimsenebilir. Bu tedbire ilişkin süreç tanımlanıp dokümente edilmelidir.

D-MÜDAHALE FONKSİYONU

İletişim ve Analiz Kontrol Grubu

Kontrol: Tespit edilen güvenlik olayları konusunda ilgili taraflar bilgilendirilecektir.

Kod: S2.MU.IA-01

Açıklama: Bu kontrolün kapsamı S2.MU.IA-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Güncel bilgi güvenliği tehditleri konusunda irtibat halinde olunan uzmanlık grupları, araştırma/güvenlik kuruluşları veya kamu otoriteleri tespit edilen güvenlik olaylarının detayları (saldırı yöntemi, araçları, alınabilecek tedbirler, vb.) konusunda bilgilendirilmelidir. Bu bilgilendirme, özellikle paylaşılan bilgiyi görebilecek kişilerin güvenilirliğinin önceden öngörülmesinin zor olduğu durumlarda (çevrimiçi bloglar gibi) veri merkezi bilgi sisteminin teknik özellikleri ve güvenlik fonksiyonları konusunda minimum ölçüde çıkarsama yapmaya imkan verecek şekilde yapılmalıdır.

Olay Müdahalesi Kontrol Grubu

Kontrol: Güvenlik olaylarına uygun şekilde müdahale edilecektir.

Kod: S2.MU.OM-01

Açıklama: Bu kontrolün kapsamı S1.MU.OM-01 kodlu kontrolle aynıdır.

E-KURTARMA FONKSİYONU

Kurtarma Planlaması Kontrol Grubu

Kontrol: Veri merkezi kurtarma planı hazırlanacaktır.

Kod: S2.KU.KP-01

Açıklama: Bu kontrolün kapsamı S1.KU.KP-01 kodlu kontrole ilave olarak aşağıdakileri kapsar;

- Veri merkezi işletmecisi bilgi sistemindeki işlem (transaction) temelli uygulamalar için işlem kurtarma mekanizmalarını tanımlayıp uygulamalıdır.
- Kurtarma planı veri merkezi işletmecisi tarafından belirlenip dokümante edilen aralıklarla ve prosedürlere göre test edilecektir. Söz konusu testler kurtarma prosedürlerinin hayali senaryolar üzerinde adım adım uygulanması veya belirlenen bir güvenlik olayının simülasyonu şeklinde olabilir. Bu testlerde tespit edilen aksaklıklar dokümante edilip kurtarma planı bu doğrultuda iyileştirilmelidir.

İletişim Planlaması Kontrol Grubu

Kontrol: Güvenlik olaylarına ilişkin kamuoyu iletişim planı hazırlanıp uygulanacaktır.

Kod: S2.KU.KP-02

Açıklama: Veri merkezi işletmecisi farklı kuruluşları ve toplum kesimlerini etkileyebilecek kişisel bilgilerin çalınması, kritik hizmetlerde kesinti, vb. sonuçları olan güvenlik olayları sırasında/sonrasında kamuoyunu yeterince ve doğru şekilde bilgilendirmeli ve bu amaca yönelik bir iletişim planı oluşturmalıdır. Söz konusu plan veri merkezi işletmecisi adına basın-yayın organlarıyla iletişim kuracak ve gerek bu kanallar gerekse sosyal medya gibi ortamlar üzerinden bilgilendirme yapacak personeli belirlemelidir. Plan, kamuoyuyla iletişim gerektiren güvenlik olayları sonrasında basın-yayın araçlarında ve sosyal medyada ortaya çıkabilecek ve veri merkezi hizmetlerine duyulan güveni zedeleyebilecek olası bilgi kirliliğinin ve olumsuz yorumların izlenerek (örneğin; sosyal medya kanallarının otomatik araçlarla izlenmesi, basın-yayın organlarının belirlenen personel tarafından takibi, vb.) kamuoyuyla paylaşılacak mesaj ve bilgilerin bu olumsuz etkiyi en aza indirecek şekilde tasarlanmasını sağlayacak mekanizmayı tanımlamalıdır.