Kisbu Gayrimenkul ve Girişim Sermayesi Portföy Yönetimi Anonim Şirketi

Bilgi Güvenliği Olay ve Acil Durum Yönetimi Prosedürü

Adres : Levent Mah. Sülün Sokak, No:5 Beşiktaş / İstanbul / Turkey
Telefon :+90 (212) 875 45 44
Web : https://kisbuportfoy.com/

İÇİNDEKİLER

1.AMAÇ

Bu prosedür, Kisbu Gayrimenkul ve Girişim Sermayesi Portföy Yönetimi Anonim Şirketi bünyesinde meydana gelecek bilgi güvenliği olaylarının belirlenmesine, olay sonrası inceleme /analiz /iletişim gibi hususlarda sürdürülecek esasların tanımlanmasına, bilgi güvenliğinden kaynaklanan olaylarda tehdittin bertaraf edilmesine, olası zararların en aza indirilmesine ve iyileştirici aksiyonların belirlenmesine yönelik kuralları tanımlamayı ve bu tanımlamalar ile türü ve sebebi ne olursa olsun, herhangi bir kesinti ya da felaket durumunda, Kurum'un kritik iş süreçlerinin/aktivitelerinin sürekliliğini sağlayan iş sürekliliği planlaması amaçlanmaktadır.

2. KAPSAM

Bu prosedür, Kisbu Gayrimenkul ve Girişim Sermayesi Portföy Yönetimi Anonim Şirketi'ne konsolide olan ve Yönetim yetki ve erkine haiz olunan Kisbu Gayrimenkul ve Girişim Sermayesi Portföy Yönetimi Anonim Şirketi Bilgi Güvenliği Politikası' na aykırı durum oluşturan ve Kisbu Gayrimenkul ve Girişim Sermayesi Portföy Yönetimi Anonim Şirketi bilgi varlıkları ve bu bilgi varlıklarının bulunduğu kullanıcı, süreç ve sistemleri etkileyen tüm vakaları kapsamaktadır.

3.TANIMLAR VE KISALTMALAR

Bilgi Güvenliği Olayı; iletilen, saklanan veya sair şekilde işlenen verilerin kazara veya hukuka aykırı yollarla imha edilmesi, kaybı, değiştirilmesi, yetkisiz şekilde açıklanması veya bunlara erişime yol açan bir güvenlik açığı şekillerinde ortaya çıkabilen ihlallerdir.

Aşağıda yer alan durumlar genel olarak Bilgi Güvenliği Olayı olarak nitelendirilir:

- Gizli bilgilerin hukuka aykırı şekilde ifşası,
- Veri içeren e-postaların yanlışlıkla Şirket dışında ilgisiz kişilere iletilmesi, gönderimi,
- Bilgi işlem donanımlarına, sistemlerine ve ağlarına virüs veya diğer saldırıların (örneğin siber saldırı) gerçekleşmesi suretiyle verilere hukuka aykırı erişim sağlanması,
- Veri içeren fiziki dokümanların veya elektronik cihazların çalınması veya kaybolması,
- Kişiye özel kullanıcı adı ve parolaların yetkisiz kişilerce ele geçirilmesi.

Siber Olay (Vaka): Bilgi varlıklarının güvenliğine yönelik olarak gerçekleşen ve Bilgi Güvenliği Politikaları ile uyumsuzluk oluşturan durumlara, sistemlerde oluşabilecek beklenmeyen ve hizmet verdiği grup şirketlerinin gerek operasyonunu etkileyen gerek ise gizlilik gerektiren bilgilerin açığa çıkmasına; bilginin bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlal teşebbüsünde bulunulmasına sebep olabilecek olayları ifade eder. Bu olaylar aşağıdaki gibi çeşitlilik göstermektedir:

- Operasyonu durdurabilecek çevresel etmenler
- Kullanıcı hataları
- Fiziksel güvenlik önlemlerinin ihlali
- Şirket politikalarına uyulmaması
- Beklenmeyen konfigürasyon değişiklikleri
- Hardware ve Software hataları
- İzinsiz erişimler / Siber atak

Yukarıda belirtilen durumlar örnek mahiyetindedir. Şirket çalışanları, çalışan adayları, hizmet sağlayıcıları, ziyaretçiler ve diğer üçüncü kişilere ait veriler bu Plan kapsamında olup Şirketin sahip olduğu ya da Şirketimizce yönetilen verilerin işlendiği tüm kayıt ortamları ve veri işlenmesine yönelik faaliyetlerde bu Plan uygulanır.

Bilgi teknolojisi operasyonlarının güvenliğini tehdit eden veya belirlenmiş sorumlu kullanım politikalarını ihlal eden her türlü eylem, bilgi güvenliği olayı olarak değerlendirilebilir. Bu tehditler şüphe konusu

olabilir, başarılı olabilir veya teşebbüs edilmiş olabilir ve yetkisiz erişim, bilgi ifşası, kullanımı, kaybı, hasarı, ihlali veya değiştirilmesi riskine yol açabilir. Bu tür olaylara bazı örnekler şunlardır:

- Yüklü yazılımlarda yetkisiz değişiklikler
- Fiziksel ve çevresel güvenliğin tehlikeye atılması, örneğin şirket cihazlarının hasar görmesi.
- Hesapların ele geçirilmesi veya şifrelerin ve şifreleme anahtarlarının ifşa edilmesi
- Olayların ciddi (zarara yol açabilecek) olmadıkça bildirilme olasılığı düşük olsa da aşağıdaki nedenlerden dolayı kusursuz bir olay yönetim programı geliştirmek önemlidir.

Acil durum: işin yapıldığı binanın yok olması, operasyonlara ara verilmesi, işyerinin veya çevrenin fiziksel olarak zarar görmesi, firmanın finansal veya imaj olarak yıkılması ile sonuçlanabilir. Acil durum kapsamına giren olaylardan bazılar Yangın, Deprem, Patlama, Sel, Fırtına, Yıldırım düşmesi, Heyelan, Sabotaj/bombalamadır<

Acil Durum Yönetimi: Acil durumlarda kimlerin ne görevi olduğu ve planlamanın nasıl gerçekleştirileceği ilgili planlarda belirtilmiştir.

Tahliye: Çalışanların, mekanik, otomatik ya da insan sesiyle yapılan uyarı sonrasında ya da uyarıya gerek kalmadan, bulundukları mekânları seri ve soğukkanlı biçimde terk etme işlemini ifade etmektedir.

Olağanüstü Durum: Deprem, yangın, toprak kayması, sel ve su baskını gibi doğal afet ile seferberlik hali ilanı, savaş, sabotaj, toplu halk hareketi ve yaygın terör faaliyeti gibi önüne geçilmesi imkânsız hallerde çalışanların can ve mal güvenliğini tehlikeye düşürme ihtimali olan herhangi bir durumdur.

Kriz Merkezi Çalışma Yeri: Olağanüstü bir durumda, “Kriz Merkezi” nin çalışmalarını sürdüreceği yerdir.

4. SORUMLULUKLAR

Yönetim Kurulu; Politikaya, kural ve düzenlemelere uyulmaması durumunda bildirim, inceleme ve yaptırım mekanizmalarının belirlenmesi ve işletilmesinin üst gözetiminden sorumludur.

İcra Kurulu; Politikanın oluşturulması, onaylanması, uygulanması ve gerektiğinde güncellenmesi konusunda yetkili onay mekanizmasıdır.

Bilgi Sistemleri Departmanı; Prosedürün işletilmesinden sorumludur, olay bildirimlerine ilişkin tüm iş birimlerinin desteğini beklemektedir.

Şirket Planın tüm şirkette işleyiş, faaliyet ve süreçlerinde ve uygulanmasında, hukuki yönden risklerin ve yakın tehlikenin önlenmesinde Şirket genelinde tüm çalışanlarımız, paydaşlarımız, misafirler, ziyaretçiler ve ilgili üçüncü kişiler iş birliği yapmakla yükümlüdür. Şirket’in tüm organ ve departmanları Şirket Bilgi Güvenliği Olay ve Acil Durum Yönetimi Prosedürünün uygulanmasından sorumludur.

5. VERİ GÜVENLİĞİNE İLİŞKİN YÜKÜMLÜLÜKLER

Bilgi Güvenliği Olay ve Acil Durum Yönetimi Prosedürünün amacı, kuruluşunuzun ihlaller, yetkisiz ifşa, bilgi imhası veya kaybı gibi bilgi güvenliği olaylarını yönetme ve raporlama konusunda sağlam bir yaklaşım sürdürmesini sağlamaktır.

Bir güvenlik olayı meydana geldiğinde hızlı ve etkili önlemler alınmalıdır. Bunu sağlamak için yönetim sorumlulukları ve prosedürleri belirlenmelidir. Yönetim sorumlulukları belirlenirken ve bilgi güvenliği prosedürleri geliştirilirken aşağıdaki hususlar dikkate alınmalıdır:

- Olay müdahalesinin planlanması ve hazırlanması

- Bilgi güvenliği olaylarının izlenmesi, tespiti, analizi ve raporlanması
- Olay yönetimi faaliyetlerinin kayıt altına alınması
- Adli delillerin ele alınması
- Bilgi güvenliği olaylarını ve zafiyetlerini değerlendirmek ve bunlara ilişkin kararlar almak.
- Hem dahili hem de harici bir güvenlik olayına müdahale etmek

Bilgi güvenliği olaylarının yetkin personel tarafından ele alınmasını ve bilgi güvenliği sorunlarının çözümü için hem kuruluş içinde hem de dışında uygun irtibat noktalarının belirlenmesini ve oluşturulmasını sağlayacak tüm prosedürlerin oluşturulması önemlidir.

Raporlama prosedürleri aşağıdakileri içermelidir:

Bilgi güvenliği olayı durumunda gerekli tüm işlemleri kaydeden ve raporlama eylemini destekleyen raporlama formları.

- Bilgi güvenliği olayının yaşanması durumunda izlenecek sonraki adımlar
- Güvenlik ihlali yapan çalışanlar hakkında izlenecek resmi disiplin süreci
- İlgili tarafların bildirilen bilgi güvenliği olaylarının ilerleyişi ve sonuçları hakkında bilgilendirilmesini sağlamak için organize edilmiş bir geri bildirim süreci.

Bilgi güvenliği olay yönetimiyle ilgili sorumluluk taşıyan herkes bu süreçlerden haberdar edilmeli ve tüm süreçler yönetimle mutabakata varılarak onaylanmalıdır.

İşlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, şirket tarafından alınması gereken önlemler tanımlanmıştır.

- Bilgi Güvenliği Politikaları:
- Bilgi Güvenliği Organizasyonu
- İnsan Kaynakları Güvenliği
- Varlık Yönetimi
- Erişim Kontrolü
- Kriptografi
- Fiziksel ve Çevresel Güvenlik
- Operasyonel Güvenlik
- İletişim Güvenliği
- Sistem Edinimi, Geliştirme ve Bakımı
- Tedarikçi İlişkileri
- Bilgi Güvenliği Olay Yönetimi
- İş Sürekliliği Yönetiminin Bilgi Güvenliği Yönleri
- Uyumluluk

Buna göre, İşlenen verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi hâlinde, Şirket söz konusu veri ihlalini, en kısa sürede (en geç 72 saat) söz konusu veri ihlalinden etkilenen kişilerin belirlenmesini müteakip makul olan en kısa süre içerisinde ilgili kişiye bildirmelidir.

İlgili kişinin iletişim adresine ulaşılabiliyorsa doğrudan, ulaşılamıyorsa Şirketin kendi web sitesi üzerinden yayımlanması gibi uygun yöntemlerle bildirim yapılmalıdır.

Şirket tarafından ilgili kişiye yapılacak olan ihlal bildiriminin açık ve sade bir dille yapılması ve asgari olarak;

- İhlalinin ne zaman gerçekleştiği,

- Veri kategorileri bazında (veri / özel nitelikli veri ayrımı yapılarak) hangi verilerin ihlalden etkilendiği,
- Veri ihlalinin olası sonuçları,
- Veri ihlalinin olumsuz etkilerinin azaltılması için alınan veya alınması önerilen tedbirler,
- İlgili kişilerin veri ihlali ile ilgili bilgi almalarını sağlayacak irtibat kişilerinin isim ve iletişim detayları ya da web sayfasının tam adresi, çağrı merkezi vb. iletişim yolları unsurlarına yer verilmesi gerekir.

Şirket tarafından Kurula haklı bir gerekçe ile 72 saat içinde bildirim yapılamaması halinde, yapılacak bildirimle birlikte gecikmenin nedenlerinin de Kurula açıklanması gerekmektedir.

Formda yer alan bilgilerin aynı anda sağlanmasının mümkün olmadığı hallerde, bu bilgiler gecikmeye mahal verilmeksizin aşamalı olarak sağlanmalıdır.

Şirket tarafından veri ihlallerine ilişkin bilgilerin, etkilerinin ve alınan önlemlerin kayıt altına alınması ve Kurulun incelemesine hazır halde bulundurulması sağlanmalıdır.

Veri işleyen nezdinde bulunan verilerin kanuni olmayan yollarla başkaları tarafından elde edilmesi halinde, veri işleyen bu konuda herhangi bir gecikmeye yer vermeksizin Şirket'e bildirimde bulunmalıdır.

Veri ihlalinin yurtdışında yerleşik şirket nezdinde yaşanması halinde, bu ihlalin sonuçlarının Türkiye'de yerleşik ilgili kişileri etkilemesi ve ilgili kişilerin sunulan ürün ve hizmetlerden Türkiye'de faydalanmaları durumunda, bu şirket tarafından da aynı esaslar çerçevesinde Kurula bildirimde bulunulmalıdır.

Veri ihlali gerçekleşmesi halinde şirket tarafından kendi nezdinde kimlere raporlama yapılacağı, Kanun kapsamında yapılacak bildirimler ile veri ihlalinin olası sonuçlarının değerlendirilmesi hususunda, kendi nezdindeki sorumluluğun kimde olduğunun belirlenmesi gibi konuları içeren bir Bilgi Güvenliği Olay ve Acil Durum Yönetimi Prosedürü hazırlanarak belirli aralıklarla bu plan gözden geçirilmelidir.

Bilgi Güvenliği Açıklarının Bildirilmesi

Kuruluşun bilgi sistemlerine ve hizmetlerine erişimi olan ve bunları kullanan tüm tarafların, gözlemlenen veya şüphelenilen herhangi bir güvenlik açığını ve olayı not alıp bildirmesi gerekmektedir. Bildirim prosedürü ve mekanizması kolayca erişilebilir olmalı, böylece taraflar olayların meydana gelmesini önlemek amacıyla güvenlik açıklarını mümkün olan en kısa sürede belirlenen irtibat noktasına bildirebilirler.

6- UYGULAMA ESASLARI

Siber olaylara hazırlık, tespit ve mücadele çalışmaları kapsamında yapılması planlanan çalışmalar bu doküman içerisinde belirtilmektedir.

- Hazırlık & İzleme
- Tespit & Müdahale & İletişim
- Onarım& İyileştirme
- Analiz & Raporlama

6.1. HAZIRLIK&İZLEME

• **Siber Olay Müdahale Komitesi'nin Kurulması:** Şirket en üst yönetiminin liderlik edeceği oturumlar ile krizin yönetilmesinden sorumludur. Öncelikle BT personelleri içinden olacak şekilde **Siber Olay Müdahale ekibi** kurulmalıdır. Siber Olay Müdahale Ekibi özellikle krizin yönetimi ve paydaşlarla iletişim, hukuki boyutun değerlendirilmesi, etkin risk yönetimi yapılmasının sağlanmasına yönelik

kurumsal iletişim; hukuk; denetim departmanlarından atanacak personel katılımı ile oluşturulacak Komitenin kimlerden oluşturulacağı Şirket Üst Yönetimi tarafınca belirlenir. Komitesi üyeleri, kriz süresince kendi rollerine ilişkin yedeklerini de belirleyip Komiteye bildirirler. Komite, Siber Olay Müdahale Ekibi ile beraber siber olaylarda yönetim; koordinasyon, test denetim; müdahale, bilinçlendirme ve analiz çalışmalarına yardımcı olacak veya yerine getirecektir. Belirlenecek olan Siber Olay Müdahale ekibi için; Ek-1'deki iletişim bilgileri formu doldurularak IT departmanı ile paylaşılacaktır. BT personelinin aşağıdaki içeriklerindeki eğitimleri alması zorunlu olup; müdahale ekibinin farklı departmandan olması halinde alınması önerilmekle birlikte; zorunlu değildir.

Zafiyet Analizi

- Güvenli Yapılandırma Denetimi Eğitimi
- Sızma Testleri Eğitimi
- Saldırı Teknikleri Eğitimi

Kayıt Yönetimi

- Saldırı Tespit ve Kayıt Yönetimi Eğitimi
- Merkezi Güvenlik İzleme ve Olay Yönetimi Eğitimi

Siber Olaylara Müdahale

- Siber Olaylara Müdahale Ekibi Kurulumu ve Yönetimi Eğitimi
- Bilişim sistemleri Adli Analizi Eğitimi
- Bilgisayar Adli Analizi - Derinlemesine Windows Eğitimi
- Ağ Adli Analizi Eğitimi
- Zararlı Yazılım Analiz Yöntemleri Eğitimi
- DDoS Saldırıları ve Korunma Yolları Eğitimi
- Bilişim Hukuku Eğitimi

Bilgi Güvenliği Yönetimi

- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Uygulama Eğitimi

Farkındalık Çalışmaları:

- Siber olay müdahale ekibinin organize edeceği çalışmalar;
- Kurum personeline periyodik olarak bilinçlendirme sunumu yapılması,
- Kurumun yemekhane, toplantı odaları gibi ortak kullanılan bölgelerine bilgi güvenliğiyle ilgili posterler asılması,
- Siber güvenlik ile ilgili periyodik olarak kurum içi bülten hazırlanması,
- Kurum çalışanlarına periyodik olarak bilgi güvenliğiyle ilgili hatırlatma e-postaları gönderilmesi,
- Varsa kurumun iç portalında siber güvenlik ile ilgili bir bölüm oluşturulması,
- Siber güvenlikle ilgili ekran koruyucuların ve arka plan resimlerinin hazırlanması,
- Kurumun bilgi güvenliği farkındalığını ölçecek anketlerin düzenli olarak yapılması şeklindedir.

Sızma Testi ve Denetim Çalışmaları:

Metodoloji: Sızma testleri, aşağıda detaylandırılan kullanıcı profilleri ile tanımlanan erişim noktalarından gerçekleştirilecek testlerden oluşur. Testler, sistem tespiti, servis tespiti ve açıklık taraması, araştırması adımları ile başlar ve her bir erişim noktası kapsamında uygulanacak adımlar ile devam eder. Bu testler sonrası saptanan açıklık ve bulgular, Kapsam bölümünde belirtilen ve ilişkili olduğu her bir başlık altında ayrıntılı olarak incelenerek raporlanır. Sızma testleri gerçekleştirilirken her bir test başlığı kapsamında saptanan açıklık ve bulgular, ayrı ayrı değerlendirilmenin yanında, bir araya

geldiklerinde oluşturabilecekleri riskler ve açıklıklar açısından da değerlendirilir ve bu birlikte değerlendirme sonucu ortaya çıkan yeni açıklık ve bulgularda raporlanır. Bulgular, Bulgu Önem Dereceleri bölümünde yer verilen dereceler kullanılarak “Bulgu Formatı” bölümünde tariflenen formata uygun olacak şekilde sunulur. Bu kapsamda bulgu önem dereceleri belirlenirken varlığın değeri dikkate alınmaz. Varlık değerlendirmesi yapmak ve varlıkların önem derecelerine göre aksiyon almak Kurum, Kuruluş ve Ortaklıkların sorumluluğundadır. Sızına testleri gerçekleştirilirken, Kurum ve Ortaklıklar faaliyetlerinin aksamasına ve hizmet kesintisine yol açmayacak yöntemler kullanılmasına dikkat edilir. Hizmet kesintisine yol alabilecek tüm testler Kurum ve Ortaklıklar ile koordineli bir şekilde planlanarak gerçekleştirilir.

a) Geniş kapsamlı test ve denetim:

Grup şirketlerinde yılda en az bir kez aşağıdaki kapsamda test ve denetimler yapılır veya TSE tarafından belgelendirilmiş firmalara yaptırılır.

- İletişim Altyapısı ve Aktif Cihazlar
- Dış ağa açık bileşenlerde bulunabilecek zafiyetlerin taranması
- Dışa açık web uygulamalarının sızma testleri
- Etki alanı ve son kullanıcı bilgisayarları yapılandırma testleri
- Veri tabanı yapılandırma testleri
- Web Uygulamalar
- Mobil Uygulamalar
- Kuruma özel geliştirilmiş yazılımlar
- DNS servisi testleri
- E-posta servisi testleri
- Sosyal mühendislik testleri
- Sadece kurum içinden erişilen web uygulamaları sızma testleri
- Dağıtık servis dışı bırakma (DDoS) testleri
- Sanallaştırma sistemleri testleri
- Kablosuz ağ testleri
- Güvenlik duvarı testleri
- URL ve içerik filtreleme testleri

b) Test sonuç raporlarının içermesi beklenen minimum bilgi aşağıda listelenmiştir:

- Zafiyetin önem derecesi (Yüksek, Orta, Düşük)
- Zafiyetin etkisi
- Zafiyetin bulunduğu bileşenler
- Zafiyetin açıklaması ve nasıl tespit edildiği
- Alınması gereken önlemler

c) Varlık ve risk değerlerinin belirlenmesi:

Siber müdahale ekibi; üstünde zafiyet bulunduğu tespit edilen varlıklar için başta bilgi işlem birimi olmak üzere kurumun ilgili birimleri ile iş birliği içinde varlık değerlerini belirler. Test sonuç raporundan gelen zafiyet değerleri ile varlık değerlerini kullanarak risk değerlerini hesaplar. Böylece, “Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi” raporunu hazırlar ve Kriz Komitesi ile değerlendirerek öncelikli olarak Şirket Üst Yönetimi’ne, bununla birlikte, Yüksek Önem Derecesindeki riskleri İcra Kurulu’na da sunar.

d) Testlerin Gerçekleştirileceği Erişim Noktaları

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

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

ii. Kurum, Kuruluş iç ağı: Kurum, Kurmuş ve Ortakların iç ağında yer alan ve test kapsamında ele alınan sunucular Kurum, Kuruluş ve Ortaklıklar iç ağı üzerinden erişilerek sızma testleri gerçekleştirilir. Ağ ve ağ trafiği üzerinde gerçekleştirilecek testler için de bu ağ kullanılır ve testi gerçekleştirecek şahıslara kullanımı cn yaygın olan çalışan bilgisayarı profilinde bilgisayarlar sağlanır.

b. Testlerin Gerçekleştirileceği Kullanıcı Profilleri

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

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

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

iii. Kurum, Kuruluş ve Ortaklıklar çalışanı profili: Kurum, Kuruluş ve Ortaklıklar personelinin çalışma ortamını kullanarak sahip olduğu yetkiler ile sistemde oluşturabileceği tehditleri tespit etmek ve ilgili zayıflıkları bertaraf etmek adına gerekli çözümler oluşturmak amacıyla bu profil kullanılmalıdır. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile gerçekleştirilecek testlerde, Kurum, Kuruluş ve Ortaklıklarda çapında en yaygın olarak kullanılan çalışan profilinin seçilmesinin yanında, yerel yönetici (loca1 admin) yetkisine sahip çalışma profilleri ile de sızma testleri gerçekleştirilir. Kurum, Kuruluş ve Ortaklıklar çalışanı profili ile yapılan testlerde, testi yapan kişi kuruluşa Kurum, Kurmuş ve Ortaklıklar tarafından tanımlanan erişim yetkileri ve verilen izinler raporda açıkça ifade edilmelidir.

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

c. Sistem Tespiti, Servis Tespiti ve Açıklık Taraması

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

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

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

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

d. Sızma Testleri

i. internet üzerinden gerçekleştirilecek temel sızma testleri: Kurum, Kuruluş ve Olasılıklar açısından bağımsız bir lokasyondan, Kurum, Kuruluş ve Ortaklıkların internet üzerinde sahip olduğu IP ağı taranarak sistem tespiti, servis tespiti ve açıklık taraması adımları gerçekleştirilir.

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

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

e. Sızma Testi Sonuçlarımın Takibi

Kurumsal Siber Güvenlik Değerlendirme ve Risk Analizi raporunun içermesi beklenen minimum bilgi aşağıda listelenmiştir:

- Varlık değeri
- Zafiyetin önem derecesi (Yüksek, Orta, Düşük)
- Zafiyetin etkisi
- Zafiyetin bulunduğu bileşenler
- Zafiyetin açıklaması ve nasıl tespit edildiği
- Alınması gereken önlemler
- Risk değeri

e) Dar kapsamlı test ve denetim:

Siber müdahale ekibinin; a maddesinde tanımlanan testlerden 6 ay sonra, a maddesinin ilk 5 adımını tekrar gerçekleştirmesi tavsiye edilir. Ayrıca, bilgi işlem altyapısında değişiklik olması durumunda da 6 aylık süreyi beklemeden aynı test adımları gerçekleştirilir. Kurumsal Siber Güvenlik Değerlendirme ve

Risk Analizi raporunda gerekli güncellemeleri yapar. Bulunan zafiyetlerin ilgili bilgi işlem personeli / firma tarafından kapatılmasını koordine ederler. Zafiyetler kapatıldıktan sonra doğrulama testlerini yaparlar veya yaptırırlar.

f) Yapılan güvenlik testleri sonucunda suç olabilecek iz, delil ve emare (zararlı yazılım, sızma vb.) görülmesi durumunda birim amiri ve kurum hukuk müşavirliği ile görüşülerek gecikmeksizin aksiyon alınır.

g) Kurum yönetimi ve bilgi işlem birimi ile periyodik toplantılar yaparak, gerçekleşen siber olayları, mevcut riskleri ve düzeltici/önleyici faaliyetlerin durumunu gözden geçirir.

h) Profesyonel saldırganların hedefi durumunda olan şirketler için, ransomware simülasyonu yaptırılır. Ransomware simülasyonu, direkt olarak içeride sahip olunan bir mail box ile tamamen hedef odaklı saldırı ile harekete geçer. Sistemler üzerinde bir açık bulup, fidye yazılımını ayağa kaldırana kadar devam eder. Üretim, ar-ge gibi iş birimleri olan, yüksek hacimde kişisel veri bulunduran, operasyonel devamlılığı ağırlıklı olarak sistem destekli yürüyen firmaların riski büyük olduğu için yılda bir kez hem penetrasyon (sızma) testi, hem de ransomware simülasyonu yapılması tavsiye edilmektedir.

- Altyapı Çalışmaları

a. Kurum BT envanterinin tutulması ve düzenli şekilde güncellenmesi gerekmektedir. Bu envanterin güvenliğinin sağlanması öncelikli konular arasında yer almaktadır.

b. Kurum envanterindeki bilgisayarların ve sunucuların güvenlik ve sistem yamalarının düzenli şekilde kontrol edilmesi ve yapılması gerekmektedir. Envanterde bulunan donanım ve yazılımlara ait üretici sayfalarının ve bildirimlerinin takip edilmesi ve yayınlanan acil kodlu yamaların geçilmesi olası saldırıların önüne geçmek açısından kritik öneme sahiptir.

c. Envanterde bulunan her türlü kullanıcı bilgisayarı, sunucu ya da mobil cihazda zararlı yazılım ya da saldırıları tespit eden uç nokta güvenlik yazılımı konumlandırılmalı ve güncel tutulmalıdır.

d. Saldırı tespit ve engelleme sistemlerinin konumlandırılması, doğru şekilde konfigüre edilmesi ve güncel tutulması bir diğer önemli aksiyondur. Gerçekleşmekte olan bir saldırının öncelikle tespit edilmesi ve otomatik aksiyonlar ile durdurulması kurum kaynaklarının efektif şekilde kullanılması açısından önemlidir.

e. Bu amaçla kurum içerisinde tespit amaçlı donanım ve sistemler konumlandırılmalı ve bildirim ayarlamaları yapılmalıdır. İlgili bildirimlerin ulaşacağı kişi ve/veya kişiler önceden belirlenmeli ve alacakları aksiyonlar netleştirilmelidir. Yeterli insan kaynağının bulunmaması durumunda hizmet alımı planlanmalıdır.

f. Olası bir saldırının önceden tespiti ya da sonraki aşamalarda analizi için her türlü sisteme ait önemli işlem kayıtlarının (log) merkezi bir sistemde tutulması ve bu noktada gerekli korelasyonların yazılarak alarm oluşturması sağlanmalıdır. Düzenli olarak bu log kayıtları incelenmeli ve olası anomaliler detaylı incelemeye alınarak kök sebepleri bulunmalıdır.

g. Destek alınan hizmet sağlayıcılar kurumun bilgi güvenliği bakış açısına hakim olmalı ve aynı seviyede dikkat etmelidirler. Birçok saldırının 3. parti hizmet sağlayıcıları üzerinden geldiği unutulmamalı ve erişim izinleri buna göre verilmelidir.

h. Kurum içerisindeki erişimlerin sadece gerektiği kadar sağlanması yetki prensibi açısından önemlidir, bu noktada da erişim talepleri detaylı değerlendirilmeli ve gereksiz/süresiz erişimler düzenli olarak

tespit edilerek kaldırılmalıdır. Ayrıca kullanıcı ağının sınıflandırılması, kritik departmanların farklı ağ/VLAN'da bölünmesi risk yönetimi açısından önemlidir.

i. Test / anonim hesaplar tutulmamalı, kullanılmayan hesaplar ve şifre yönetimi kontrol altında tutulmalıdır.

j. Bir diğer önemli nokta ise kurumun yedekleme politikası ve bu sistemlerin siber saldırılardan etkilenmeyecek bir yapıda oluşturulma gerekliliğidir. Olası bir siber saldırı sonrası güvenilir olmayan ya da erişilemeyen yedeklerin olması durumunda kurum açısından ciddi kayıplar oluşacaktır.

Kurum, Kuruluş ve Ortaklıklar, sızma testleri sonucunda tespit edilen bulguları;

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

Bulgu Önem Dereceleri

Bulguların önem dereceleri beş kategoride ele alınır:

Acil, Kritik, Yüksek, Orta, Düşük.

Bulgu Formatı

Her bulgu aşağıdaki başlıklar altında raporlanır:

- Bulgu Referans No: Her bulguyu tekil olarak niteleyen harf-rakam dizisi
- Bulgu Adı: Bulguyu özetleyen tanımlayıcı isim
- Önem Derecesi: EK-1'de belirtilen önem derecesi
- Etkisi: Açıklığın/eksikliğin kötüye kullanılması durumunda oluşabilecek potansiyel Sonuç
- Erişim Noktası: Testin gerçekleştirildiği erişim noktası
- Kullanıcı Profili: Testin gerçekleştirildiği kullanıcı profili
- Tespit Edildiği Bileşen/Bileşenler: IP numarası, URL, sistem, servis, sunucu veya varlık adı
- Bulgu Açıklaması: Bulgunun detaylı açıklaması
- Çözüm Önerisi: Bulguyu gidermek için testi gerçekleştiren kurum tarafından önerilen çözüme ulaşılmaya çalışılması

6.2. TESPİT & MÜDAHALE & İLETİŞİM

a) Tespit ve Müdahale: Herhangi bir olay, çalışanlar tarafından fark edildiğinde zaman kaybetmeksizin Bilgi Güvenliği Yöneticisi' ne bildirilir. Tüm çalışanlar tüm iletişim kanallarını kullanarak bir bilgi güvenliği vakasını iletebilirler. Bu noktada dikkat edilmesi gereken hususlar bulunmaktadır.

- Olası bir saldırı ihtimali fark edildiğinde kurumun tüm sistemleri ile internet ağı yalıtılmalıdır.
- Olası saldırı durumunda mutlak surette Bilgi Güvenliği Yönetimi bilgilendirilmeli ve gerekirse aşağıdaki aksiyonların alınmasına yönelik Bilgi Güvenliği Yönetimi'nden destek & yönlendirme talep edilmesi esastır.
- Saldırının gerçekleştirildiği nokta tespit edilene kadar sunucu ve kullanıcı ağına tüm erişimler mümkünse kesilerek izolasyon sağlanmalıdır.

- Operasyonların kesintiye uğramaması için alternatif yöntemler değerlendirilmeli, gerekli yönlendirmeler yapılmalıdır.
- Saldırının türüne göre gerekli izleme detaylı şekilde sağlanmalıdır.
- Saldırının türüne bakılmaksızın tüm yüksek yetkili hesapların şifreleri değiştirilerek, kullanımı askıya alınmalıdır. Yeni yüksek yetkili bir hesap oluşturulmalıdır.
- Saldırının gerçekleştiği tespit edilen cihazlar ağ dışarısına alınarak izolasyon sağlanmalıdır.
- Hiçbir bilgisayar ya da sunucu yeniden başlatılmamalıdır. Yeniden başlatma işlemi, bellekte önemli verilerin/delillerin kaybına yol açacaktır.
- Saldırının gerçekleştiği tespit edilen sistemler güvenilir bir yerde incelenmek üzere muhafaza edilmelidir.
- Olası bir saldırı durumunda güvenlik sistemlerinden sorumlu personel tüm ürünlerin aktif çalıştığını ve erişilebilir olduğunu teyit etmelidir. Güvenlik ürünlerinin local hesap bilgileri değiştirilmelidir.
- Sistem ve network ekibinin tüm kritik sistemlerde ve bilgi ifşasına neden olabilecek sunuculardaki local erişim bilgilerini değiştirmesi, kaynaklarda bulunan logların sağlıklı bir şekilde akmaya devam ettiğinin teyit etmesi gereklidir.
- Olay bildiriminde aşağıdaki konulara ilişkin detay bilgilerin verilmesi önem taşımaktadır:
- Bilgi Güvenliği Olayının oluştuğu tarih ve zaman
- Olayın nasıl fark edildiği ve vaka hakkında genel açıklama
- Olaydan etkilendiği düşünülen iş süreçleri, bilgi varlıkları ve kişiler
- Olay hakkında bilgisi olan kişiler
- Olay ile ilgili alınan ilk aksiyon

b) Ön Analiz Çalışmaları

- Olay bildiriminin yapılmasını takiben bilgileri alan Bilgi Güvenliği Yöneticisi, bildirilen vakanın gerçek bir vaka olup olmadığını tespit etmek amacı ile ön analiz yapar. Bu ve aşağıdaki süreçlerin tamamında Bilgi Güvenliği Yönetimi'nden destek & yönlendirme talep edilmesi esastır. Bu aşamada vaka bildirimini yapan kişilerden detaylı bilgi alınması, vakadan etkilenen iş süreçleri ve bilgi varlıklarının incelenmesi gibi bazı temel araştırma faaliyetleri yapılır.
- Bilgi Güvenliği Yöneticisi, gerek duyduğu takdirde tüm çalışanlardan yardım isteyebilir.
- Analizde aşağıdaki konular sorgulanarak bazı temel soruların cevaplarına ulaşılmaya çalışılır:
- Gerçekten vaka olup olmadığı (Belirtilen durumun gerçekleşip gerçekleşmediğinin incelenerek karara bağlanması)
- Vakanın tipi (Bilgi sızıntısı problemi, bilgi doğruluğu problemi v.b)
- Vakadan etkilenen bilgi varlıkları, vakanın etkisi ve bu etkiye bağlı olarak vakanın önem derecesi
- Vaka analiz çalışmasına katılması gereken çalışanlar

c) Önem Derecesinin Belirlenmesi

Vakanın kullanıcıları, bilgi varlıkları veya iş süreçleri üzerinde yarattığı etki ve verdiği veya vereceği zararlar göz önüne alınarak aşağıda belirtilen uygun kategorideki önem derecesi belirlenir.

ÖNEM DERECESİ:

- Yüksek [Y]: Acil olarak BS müdürü ve Bilgi Güvenliği Komitesi'ne raporlanmalı.
- Orta [O]: Acil olarak BS müdürüne raporlanmalı. Düzenli olarak Bilgi Güvenliği Komitesi'ne raporlanmalı.
- Düşük [D]: Sadece BS Müdürüne raporlanmalı. Düzenli olarak Bilgi Güvenliği Komitesi'ne raporlanmalı

- Ön analiz sonucunda vakanın gerçekleşip gerçekleşmediği belirlenir. Eğer vaka gerçekleşmemiş ise elde edilen bulgular ve bu bulgular ışığında ilgili kişilere gereken bildirim yapıldıktan sonra vaka kapatılır. Ön analiz sonucunda elde edilen bulgular, vakadan etkilenen iş sürecinin veya bilgi varlığının iş ve teknik sahiplerine gerektiği ölçüde aktarılır.

d) İletişim: Şekilde gösterildiği üzere siber olay müdahale ekibi siber olay öncesi, bilgi işlem varlıkları üzerinde rutin güvenlik testi çalışması yapar veya yaptırır. Kayıt yönetimi sistemi ara yüzünden rutin olarak iz kayıtlarını takip eder. Siber olay esnasında ise, bilgi işlem biriminin yapacağı müdahaleyi izler; yardımcı olur ve gerekli koordinasyonu sağlar.

6.3. ANALİZ VE RAPORLAMA

Yukarıda belirtilen vaka analiz adımlarına paralel olarak elde edilen düzenli kayıtlar vakaya ait incelemeler tamamlandıktan sonra “Yüksek” önem derecesine sahip vakalar için “Bilgi Güvenliği Vaka/Olay Analiz Raporu” hazırlanır. (Ek-2)

- Vakanın Tanımı, Ne Zaman Tespit Edildiği
- Vakanın Nedeni
- Vakanın Türü
- Vaka Analiz Çalışmaları / Olay Açıklaması (kronolojik sıralama)
- Vaka Sonucu
- Vakadan Etkilenen İş Süreçleri ve Bilgi Varlıkları (İş süreçlerine veya BS servislerine olan etkisi)
- Vakadan Etkilenen İlgili Birimler (Olayın Etkisi)
- Alınan Aksiyonlar
- Yapılacaklar
- Değerlendirme/Tavsiyeler

6.4. İLETİŞİM

Yukarıda belirtilen Olay Müdahale Akış adımları doğrultusunda vakıa iletişimi yapılması esastır. Bunun yanında, gerekli görüldüğü durumlarda kamu otoriteleri başta olmak üzere tüm paydaşlara bilgi sunulması gerekebilir. Bu bakımdan konunun Kriz Komitesi ve/veya Risk Yönetim Başkanlığı’na intikalinden itibaren süreç ve iletişimi aşağıdaki mercilerle beraber değerlendirilir.

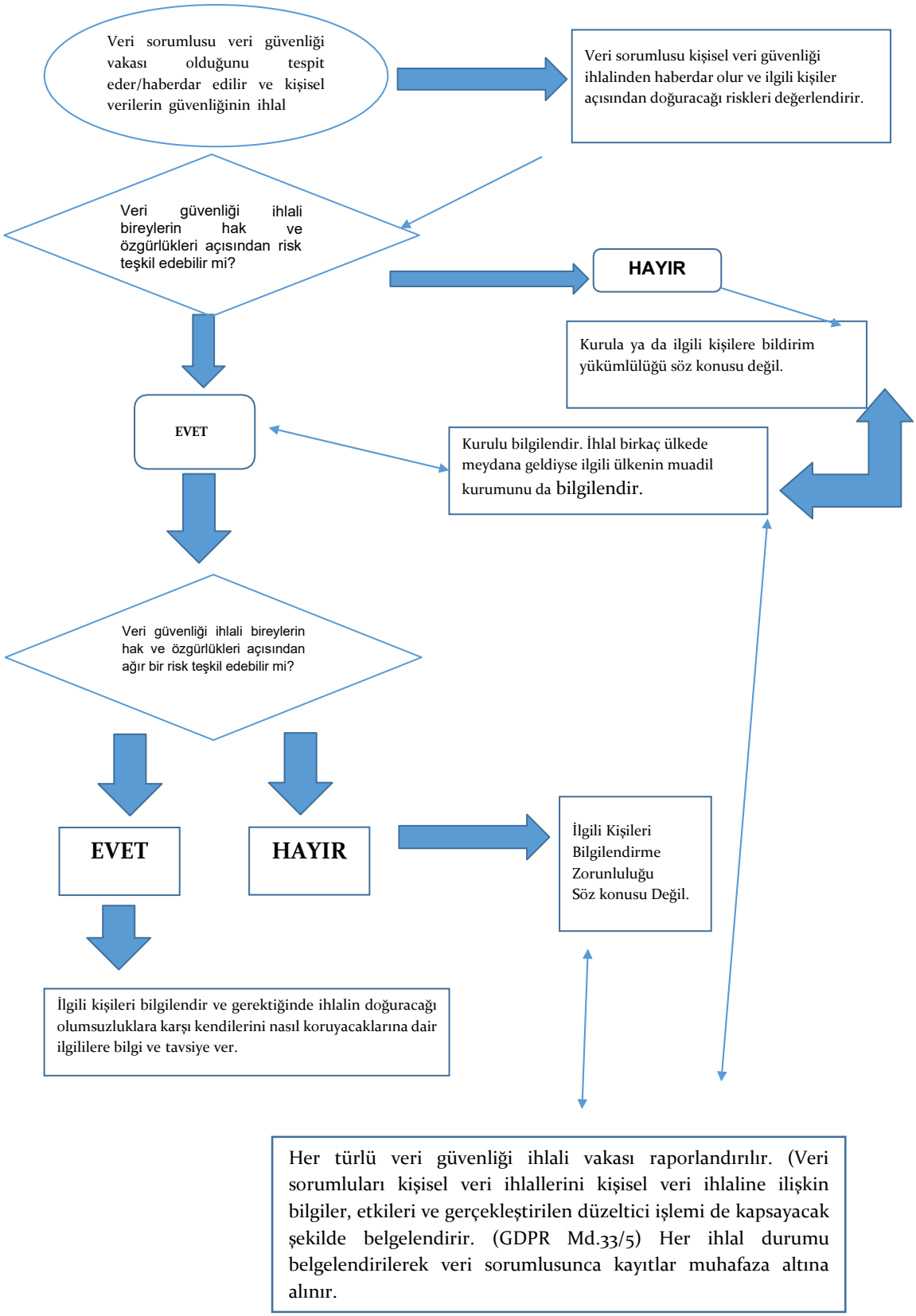
- Kriz Komitesi
- Yönetim Kurulu
- İcra Kurulu

İlgili tüm paydaşlara zamanında, doğru ve eksiksiz bilgi sunulması Şirket itibar yönetimi açısından son derece önem arz eder. Bu bakımdan, “Yüksek Önem Derecesindeki vakıalarda, yukarıdaki organlar harici, Şirket ve ilgili birimleri de kriz yönetimi boyunca teyakkuzda ve yedekli şekilde çalışırlar. Kamu otoritelerine yapılacak açıklamaların zamanında, eksiksiz ve doğru yapılmasından ilgili Şirket Hukuk Birimleri ile beraber Şirket Yönetimi sorumludur. Her türlü bildirim öncesi Kriz Komitesi’nin konuyu görüşmesi, “Yüksek Önem Derecesindeki vakıalarda İcra Kurulu’nu bilgilendirmesi esastır. Bu gibi vakıalarda, kamu otoritelerine verilecek bilginin ne şekilde olacağı (sözlü / yazılı), iletişim yöntemi, iletişimi kimlerin yapacağı hususlarında Şirket Hukuk Birimi görüşü alınması gereklidir.

Görsel / Yazılı Basın ve/veya Şirket resmi web sitesi, sosyal medya hesaplarından yapılacak olan açıklamaların zamanında, eksiksiz ve doğru yapılmasından Şirket Kurumsal İletişim Birimi ve Şirket Yönetimi sorumludur. Yüksek Önem Derecesindeki vakıalarda, her türlü iletişim öncesi Kriz

Komitesi'nin konuyu görüşmesi, gerektiği durumlarda İcra Kurulu'nu bilgilendirmesi gereklidir. Sürecin kurumsal iletişim şekli ve yöntemine ilişkin de ilgili Başkan Yardımcılığı'ndan destek talebi yapılmalı, bilgi sunulmalıdır. Ayrıca paydaşlara yapılacak her türlü bildirim şekli ve içeriği itibarı ile, Kriz Komitesi bilgi / onayına sunulmalıdır.

İhlal Bildirim Mükellefiyetine İlişkin Akış Şeması



Her türlü veri güvenliği ihlali vakası raporlandırılır. (Veri sorumluları kişisel veri ihlallerini kişisel veri ihlaline ilişkin bilgiler, etkileri ve gerçekleştirilen düzeltici işlemi de kapsayacak şekilde belgelendirir. (GDPR Md.33/5) Her ihlal durumu belgelendirilerek veri sorumlusunca kayıtlar muhafaza altına alınır.

6.5. ONARIM VE İYİLEŞTİRME

Vaka analizinin raporlanmasından sonra, tespit edilen aksaklıkların iyileştirilmesi veya ortadan kaldırılmasına yönelik çalışmalar başlatılır.

Aksaklıkların iyileştirilmesi sağlandıktan sonra, gerçekleşen vakanın nedenine bağlı olarak vakaya dahil sistemlerin belirli bir süre gözlenmesi sağlanmalıdır. Yaşanan problemin devamlılığının olup olmadığı belirlenir.

Vakadan etkilenen bilgi varlıklarının güçlendirilmesinin yanı sıra, Bilgi Güvenlik Yöneticisi veya Bilgi Güvenliği Komitesi tarafından gerekli görülür ise bu bilgi varlıklarının bulunduğu sistemin yenilenmesi istenebilir.

Yaşanan siber olaya ilişkin iş ve işlemlerin anlatıldığı siber olay müdahale raporu İcra Kurulu bilgisine sunulur.

7. ACİL DURUM EYLEM PLANI

Türü ve sebebi ne olursa olsun, herhangi bir kesinti ya da felaket durumunda, Kurumun kritik iş süreçlerinin/aktivitelerinin sürekliliğini sağlayan iş sürekliliği planlamasına ilişkin hususlar belirtilmiştir.

7.1. OLMASI GEREKENLER

İş sürekliliği planı kapsamında dikkate alınan varsayımlar aşağıdaki gibidir;

- Alternatif lokasyonlar ve lokasyonların Altyapı Sistemleri kullanılabilir durumdadır.
- Çalıştırılacak uygulama ve işletilecek sistemler/aktiviteler için Kabul edilebilir kesinti süreleri ve veri kurtarma noktası hedefleri, iş kritik sistemler için RTO/RPO değerleri belirlenen değerdedir (RTO: Olası felaket durumunda sistemin devreye alınma süresi).
- BT bileşenleri için gerekli veri kurtarma noktası hedeflerine (RPO) Uygun Yedekleme mekanizmaları kurulmuş ve test edilmiş durumdadır.
- Uzaktan çalışma talimatları, gerekli donanımlar, donanım üzerindeki uygulamalar, (notebook, telefon, vpn hesapları) hazır durumdadır.
- Acil ve olağanüstü durumda görev alacak ekiplerin hem kendi hem ekip üyelerinin de diğer ekiplerdeki üyelerin erişim bilgileri mevcuttur. Kullanılabilen tüm iletişim araçları ile haberleşme sağlanabilir.
- Acil ve olağanüstü durumda çalışacak minimum personel sayısı ve hangi personelin çalışacağı belirlenmiş durumdadır. Bu personel, acil ve olağanüstü durumda nasıl davranacakları, kiminle bağlantıya geçecekleri ve işlerini nasıl devam ettirecekleri konusunda bilgi sahibidir.
- Kurum, kontrol dışı/beklenmedik ve hizmet kesintileri yaratabilecek olaylar için senaryolar oluşturmuş, bu tür durumlarda alınacak aksiyonları belirlemiştir. Olağanüstü Durum'un ilan sonrasında personel ve yönetim kadrosuna gerekli bilgilendirmeler yapılır. İş Kurtarma Ekipleri görevli oldukları kritik iş süreçleri için hazırlanan kurtarma planlarını uygular ve mevcut durumu düzenli olarak raporlar. Acil Durum Ekipleri ise olaya müdahale eder.

7.2. İŞ KURTARMA STRATEJİLERİ

- Öncelikli süreçlerin ve sistemlerin tespiti için tüm iş birimleri ile yapılan iş etki analizlerinin sonucunda belirlenen geri kazanım öncelikleri (RTO) ve veri kurtarma hedefleri (RPO) kullanılır. Sistem Odası içerisindeki sistemler felaket durumunları için hazırlanır.
- Geri kazanım öncelikleri ve veri kurtarma hedefleri 5 ayrı zaman dilimine yayılır:
  - 0-6 saat,
  - 6 saat-12 saat,
  - 12 saat-24 saat,
  - 24 saat-48 saat,
  - 48 saat üstü.
- Veri kurtarma hedefi 12 saate kadar olan sistemler Yüksek Öncelikli olarak değerlendirilmektedir. Yüksek öncelikli olarak belirlenen sistemlerin kurtarılmasına önem verilir.
- İş kurtarma faaliyetleri temel olarak aşağıdaki 2 yöntemden birisi ile yapılır:
  - İşlemlerin manuel olarak devam ettirilmesi (çalışma alanından bağımsız olarak)
  - Sistem Odası'nda bulunan yedek sunucular aracılığıyla faaliyetlerin devam ettirilmesi

İdari Birimler bina bağımsız çalışabildiği için ilk aşamada, Merkeze VPN ile uzaktan erişim sağlayarak iş sistemlerini kullanabilirler.

Uygulamalara uzaktan bağlantı hakkı verilebilecek (Merkez bağlantısı ihtiyacı duyan tüm kullanıcılar) personel (çalışmalarını bireysel olarak devam ettirebilecek) belirlenir, gerekli bilgilendirmeler yapılır, ilgili altyapı ve kaynaklar hazırlanır.

7.3. ACİL DURUM SENARYOLARI:

a) Siber olayların yangın, su / elektrik kesintisi gibi farklı felaketlere sebep olması / tetiklemesi:

Bu gibi durumlarda, “ACİL DURUM EYLEM PLAN”ları uygulanır.

b) Siber olaylar; yangın, su / elektrik kesintisi; deprem vb. felaketlerde BT Kesintisi:

- Teknoloji altyapısında oluşabilecek kesinti riskleri değerlendirilerek, altyapı bileşenleri bu riskleri minimize edecek şekilde tasarlanmalıdır.
- Şirketlerin interneti farklı pop noktalarından olacak şekilde yedeklenmelidir. Farklı bir ISP kullanması altyapı uygunluğunda tavsiye edilmektedir.
- Network güvenliğini sağlamak için firewall, merkezi yönetilen lisanslı antivirüs programı kullanılmalıdır.
- Şirket dahilindeki teknolojik ihtiyaçları karşılamak amacıyla konumlandırılan sunucuların sanallaştırma teknolojisi kullanılarak yedeklilik sağlayacak şekilde konfigüre edilmelidir. Sistemler yedeklilik ilkesiyle tasarlanmış olmasına ek olarak, servis sağlayıcı firmalarla gerekli seviyelerde ürün destek anlaşması yapılmalıdır. Sistemlerde herhangi bir donanım arızası oluşması durumunda ürünler şirketin iş sürekliliği planına uygun koşullarda değiştirilerek, süreklilik sağlanabilmelidir.
- Kurumun BT sistemlerinin kesintiye uğraması durumunda, tekrar kullanılabilir duruma gelmesi için gereken zaman ve maliyetler ile tekrar kullanılabilir duruma gelemeyecek olan varlıkların/kaynakların belirlenmesi önerilir.
- Eğer kesinti uzun süreli ise durum ilgili birimlere iletilir ve belirlenecek lokasyonda çalışmalara devam edilir.

- Kesinti durumu sadece yerinde çalışmayı engelleyecek durumda ise kullanıcılar internet erişiminin olduğu herhangi bir yerde Kurum tarafından tahsis edilmiş dizüstü bilgisayarlara kurulu VPN bağlantısı ile bilgi sistemleri altyapısına erişebilir.

7.4. PLANIN GÜNCELLENMESİ

İş Sürekliliği Planları; Kurum tarafından yıllık olarak, Kurum faaliyetleri ile organizasyonel yapıdaki değişiklikler dikkate alınarak gözden geçirilir ve gerekli değişiklikler gerçekleştirilir. Güncellemeler, iş birimleri temsilcilerinin geri bildirimlerinden yararlanılarak Bilgi Güvenliği Yöneticisi koordinasyonunda yapılır ve şirket Yönetim Kurulu tarafından onaylanır. Güncelleme süreci tamamlandıktan sonra ilgili personel ve birimlerin haberdar olması sağlanır. Planın güncellenmesinde aşağıdaki kriterler dikkate alınır:

- Geliştirilen yeni ürün ve hizmetler,
- Mevcut oran, hizmet ve iş süreçlerinde gerçekleştirilen değişiklikler,
- Ürün, hizmet ve iş süreçlerinde gerçekleştirilen değişiklikler nedeniyle ortaya çıkan yeni ekipman ve altyapı ihtiyaçları,
- Çalışma yerlerindeki altyapı değişiklikleri,
- Planda yer alan personelin transferi, işten ayrılması, terfisi, adres/telefon değişikliği ya da Kurum organizasyon değişiklikleri, ilgili dokümanlarda ya da belgelerde meydana gelen değişiklikler,
- Hizmet alınan üçüncü tarafların, alınan hizmetlerin veya süreçlerin değişmesi,

İş Sürekliliği Planı ve bu planı tamamlayan diğer tüm alt plan ve prosedürlerin yürütülmesi Yönetim Kurulu'nun yetki verdiği Bilgi Güvenliği Ekibi sorumluluğundadır.

8. DÖKÜMANIN YAYINLANMASI VE SAKLANMASI

İşbu Prosedür basılı kağıt ve elektronik ortamda olmak üzere iki farklı ortamda saklanır. Kurum portalında dokümanların güncel versiyonu yer alır. Islak imzalı nüshalar Mali ve İdari İşler, kontrollü kopyalar Hukuk Müşavirliği tarafından saklanır ve gerektiğinde Bölüm Yöneticisinin yazılı onayı ile Hukuk Müşavirliği'nce imha edilir.

9. GÜNCELLEME PERİYODU

İşbu Prosedür en az yılda bir kez gözden geçirilir ve ihtiyaç halinde Dokümantasyon Yönetimi Prosedüründe belirlenen esaslar dahilinde güncellenir.

10. YÜRÜRLÜK

İşbu politika yayınlandığı tarihte yürürlüğe girer.

11.EKLER

EK – 1 Siber Olay Müdahale Ekibi İletişim Formu

Ek – 2 Bilgi Güvenliği Vaka/Olay Analiz Raporu

Ek-1: Siber Olay Müdahale Ekibi İletişim Formu (*) İşareti - Zorunlu Alanları

SİBER OLAY MÜDAHALE EKİBİ İLETİŞİM BİLGİLERİ FORMU					
Kurum Adı*					Tarih:
SOME Takımı 7/24 İletişim Bilgileri*		Telefon	Cep telefonu	Kurumsal e-posta	
Hizmet aldığı ISS*					
ISS'ten almış olduğu güvenlik hizmetleri*		DDOS	Diğer:		
Hangi tür Güvenlik Cihazları kullanılıyor		IPS	WAF	FW	Diğer:
Kurum IP Adres Aralığı					
Müdahale Ekibi Personelinin*	**Adı Soyadı**	**Ünvanı**	**Telefonu**	**Cep telefonu**	**Kurumsal e-posta adresi**
İzlenmesi Talep Edilen Sistemlerin	**Alan Adı**	**IP Adresi**	**Açıklama**		

EK-2 **Bilgi Güvenliği Vaka/Olay Analiz Raporu**

Olay ID	Olay/Vaka Tanımı	Olayın Yaşandığı Tarih	Olayın Tespit Tarihi	Nedeni	Türü	Analiz	Sonuç	Olayın Etkisi	Etkilenen Birimler	Aksiyonlar	Tamamlanacak Adımlar	Değerlendirme/ Tavsiyeler

HAZIRLANMASI VEYA REVİZE EDİLMESİ					
Doküman Referans No	**Açıklama**	**Ad Soyad-Unvan**	**Bölüm**	**Revize Edilen Madde**	**Hazırlanma / Revize Tarih**
202512-bg10					10.12.2025

ONAY ve YÜRÜRLÜK			
Doküman Referans No	**Makam**	**Onay / Karar Tarihi-No**	**Yürürlük Tarihi**
202512-bg10	Yönetim Kurulu		12.12.2025