DOĞAN ŞİRKETLER GRUBU HOLDİNG A.Ş.

SİBER OLAY MÜDAHALE PROSEDÜRÜ

Bu dokümanın güncel hali elektronik ortamda saklanmaktadır. Kağıt kopyanın güncelliği elektronik ortamda kontrol edilmelidir.

İÇİNDEKİLER

1. AMAÇ

Siber Olay Müdahale Prosedürü, bilgi güvenliği olaylarının belirlenmesine, olay sonrası inceleme / analiz / iletişim gibi hususlarda sürdürülecek esasların tanımlanmasına, bilgi güvenliğinden kaynaklanan olaylarda tehditin 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, Doğan Şirketler Grubu Holding A.Ş.'ye konsolide olan ve Yönetim yetki ve erkine haiz olunan Doğan Grubu firmalarında Doğan Holding Bilgi Güvenliği Politikası' na aykırı durum oluşturan ve Doğan Holding bilgi varlıkları ve bu bilgi varlıklarının bulunduğu kullanıcı, süreç ve sistemleri etkileyen tüm vakaları kapsamaktadır.

3. TANIM ve KISALTMALAR

Bu bölümde Prosedürde geçen özel terim ve deyimler, kavramlar, kısaltmalar kısaca açıklanmaktadır

3.1. Doğan Holding: Doğan Şirketler Grubu Holding A.Ş.'ni belirten tanımdır.

3.2. Doğan Grubu: Doğan Şirketler Grubu Holding A.Ş. ve bağlı ortaklık, iştirakleri, yönetimde %50'den fazla söz hakkı olan ve/veya yönetim erkine haiz olunan iş ortaklıklarıdır.

3.3. Yönetim Kurulu: Doğan Holding Yönetim Kurulu'nu ifade eder.

3.4. İcra Kurulu: Doğan Holding İcra Kurulu Başkanı ve Üyeleri'ni belirten tanımdır.

3.5. Siber Olay *(Vaka)*: Doğan Holding bilgi varlıklarının güvenliğine yönelik olarak gerçekleşen ve Bilgi Güvenliği Politikaları ile uyumsuzluk oluşturan durumlara, sistemlerde oluşabilecek beklenmeyen ve Doğan Holding'in 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

3.6. Bilgi Güvenliği Komitesi : Doğan Şirketler Grubu Holding A.Ş. Bilgi Güvenliği Komitesi'ni ifade eder.

3.7. Bilgi Güvenliği Yöneticisi: Doğan Şirketler Grubu Holding A.Ş. Bilgi Güvenliği Yöneticisi'ni *(CISO)* ifade eder.

3.8. Risk Yönetim Başkanlığı: Doğan Şirketler Grubu Holding A.Ş. Denetim ve Risk Yönetim Grup Başkanlığı'nı ifade eder.

3.9. Baş Hukuk Müşavirliği: Doğan Şirketler Grubu Holding A.Ş. Baş Hukuk Müşavirliği'ni ifade eder

4. ROLLER ve SORUMLULUKLAR

4.1 Yönetim Kurulu

Politika'ya, kural ve düzenlemelere uyulmaması durumunda bildirim, inceleme ve yaptırım mekanizmalarının belirlenmesi ve işletilmesinin üst gözetiminden sorumludur.

4.2 İcra Kurulu

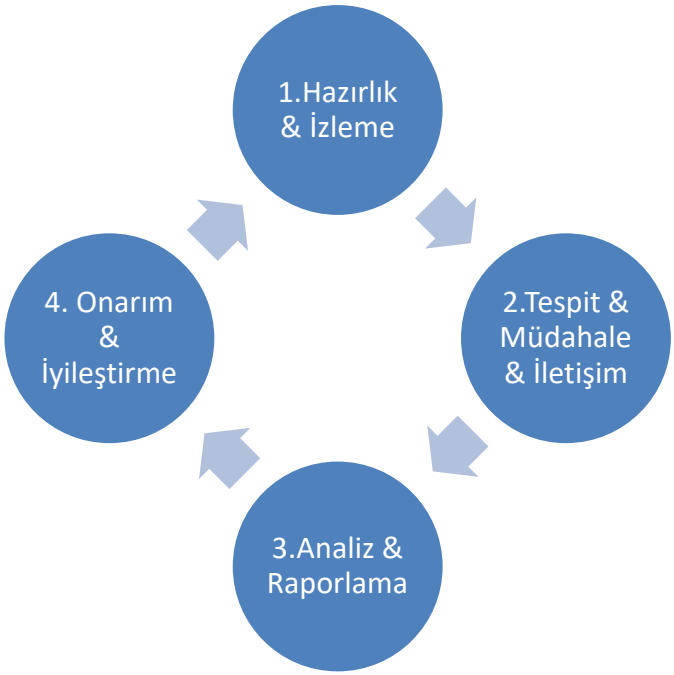
Politikanın oluşturulması, onaylanması, uygulanması ve gerektiğinde güncellenmesi konusunda yetkili onay mekanizmasıdır.

4.3 Bilgi Sistemleri Departmanı

Prosedürün işletilmesinden sorumludur; olay bildirimlerine ilişkin tüm iş birimlerinin desteğini beklemektedir.

5. UYGULAMA ESASLARI

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



5.1. Hazırlık&İzleme

- **<u>Siber Olay Müdahale & Kriz Komitesi'nin Kurulması:</u>** Her iki oluşum da 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 yanında, 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 Kriz Komitesi'nin kimlerden oluşturulacağı Şirket Üst Yönetimi tarafınca belirlenir. Kriz Komitesi üyeleri, kriz süresince kendi rollerine ilişkin yedeklerini de belirleyip Komite'ye bildirirler.

  Kriz Komitesi, 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 Doğan Holding IT departmanı ile paylaşılacaktır.

  BT personelinin aşağıdaki içeriklerideki eğitimleri alması zorunlu olup; müdahale ekibinin farklı departmandan olması halinde alınması önerilmekle birlikte; zorunlu değildir.

Temel Yetenek	**Eğitimler**
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 Olay 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.

- **<u>Sızma Testi ve Denetim Çalışmaları:</u>**

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.

- **İç ağda yer alan bileşenlerde bulunabilecek zafiyetlerin taranması**
- **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**
- 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 müdale ekibi; üstünde zafiyet bulunduğu tespit edilen varlıklar için başta bilgi işlem birimi olmak üzere kurumun ilgili birimleri ile işbirliği 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 Derecesi"ndeki riskleri DOHOL İcra Kurulu'na da sunar.

d) 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 müdale 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 simulasyonu 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.

5.2. Tespit&Müdahale& İletişim

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 farkedildiğinde kurumun tüm sistemleri ile internet ağı yalıtılmalıdır.
- Olası saldırı durumunda mutlka surette DOHOL Bilgi Güvenliği Yönetimi bilgilendirilmeli ve gerekirse aşağıdaki aksiyonların alınmasına yönelik DOHOL 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 Olayı' nın 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 DOHOL 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 Doğan Holding'e olan 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 Doğan Holding' e verdiği veya vereceği zararlar göz önüne alınarak aşağıda belirtilen uygun kategorideki önem derecesi belirlenir.

ÖNEM DERECESİ:

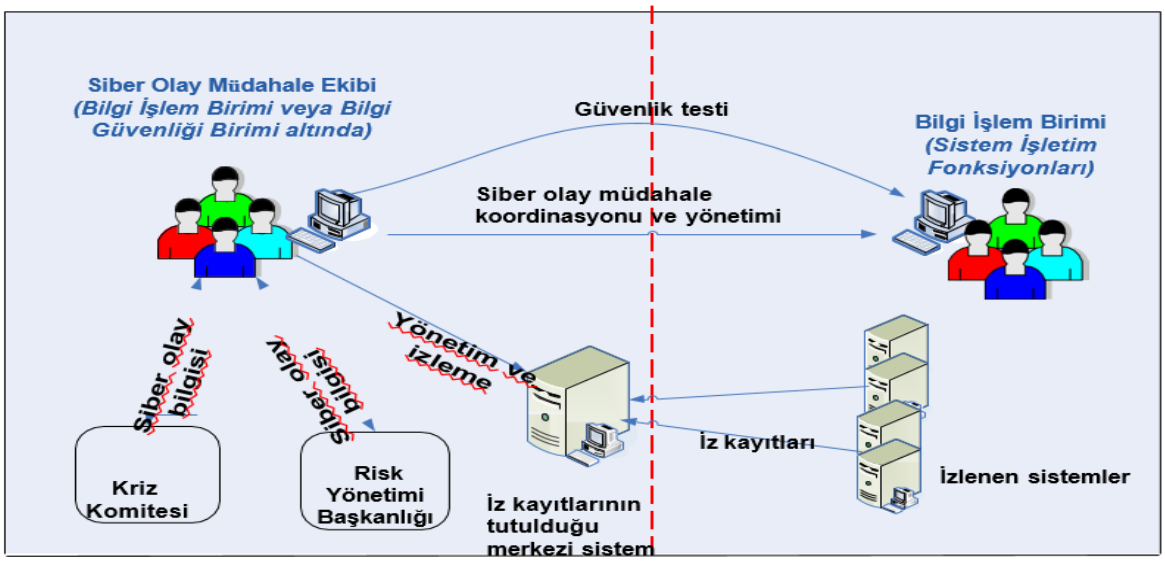
Yüksek [Y]: Acil olarak BS müdürü ve Bilgi Güvenliği Komitesi'ne raporlanmalı.
Orta [O]: Acil olarak BS müdürüne raporlanmalı. Düzenli olarak Bilgi Güvenliği Komitesi'ne raporlanmalı
Düşük [D]: Sadece BS Müdürüne raporlanmalı. Düzenli olarak Bilgi Güvenliği Komitesi'ne raporlanmalı

	Kritik veri kaybı	Kritik olmayan veri kaybı	1 günden az operasyon durması	1 günden fazla operasyon durması	Veri bütünlüğünün bozulması	Gizli bilgilerin açığa çıkması
Doğal Afetler (deprem, yangın vb.)	Y	D	O	Y	Y	Y
Hack, mail spoof, fishing saldırıları	Y	O	O	Y	O	Y
Eski çalışan saldırıları	Y	O	O	Y	O	Y
Mevcut çalışanların yetkisiz erişimleri	Y	D	O	O	O	Y
3.parti firmalardan yetkisiz erişim	Y	Y	Y	Y	Y	Y
Teknik sorunlar (donanımsal ve yazılımsal)	Y	D	D	O	D	-
Virus saldırıları	Y	D	O	Y	O	Y
Sistem odası kaynaklı sorunlar	O	D	D	O	D	-
Veri hırsızlığı	Y	O	O	Y	Y	Y

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.

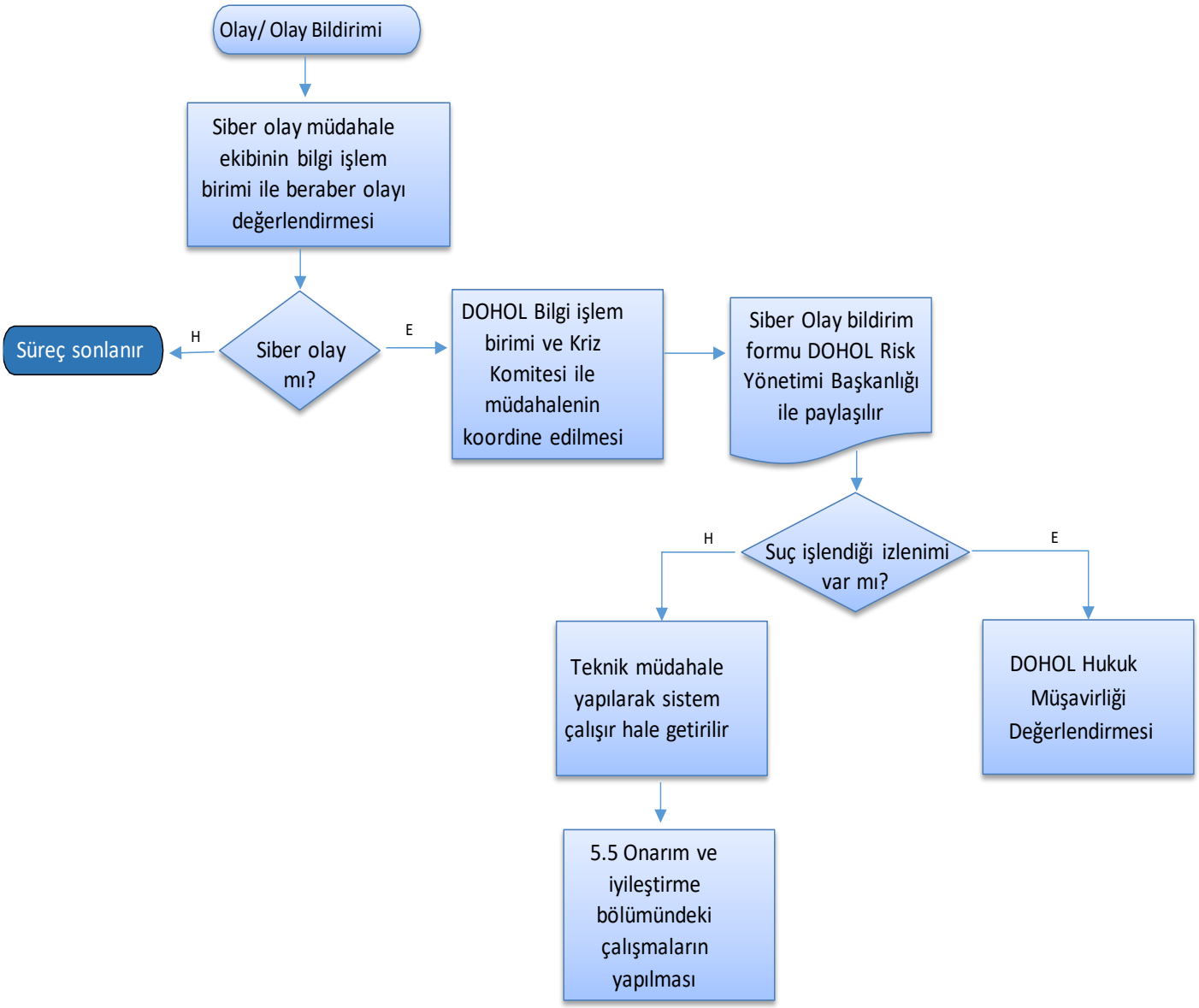


5.3. Analiz ve Raporlama

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

Siber Olay Müdahale Akış Diyagramı



5.4. İletişim

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
- Risk Yönetimi Başkanlığı
- Şirket 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 Derecesi"*ndeki vakıalarda, yukarıdaki organlar harici, Şirket ve DOHOL'ün 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 Derecesi"*ndeki 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 ile beraber Baş Hukuk Müşavirliği 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 Derecesi"*ndeki 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 DOHOL 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.

5.5. Onarım ve İyileştirme

- 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 DOHOL İcra Kurulu bilgisine sunulur.

6. ACİL DURUM EYLEM PLANI

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

6.1. Olması 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.

6.2. İş Kurtarma Stratejileri

- 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.

6.3. Acil durum senaryoları:

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 antivirus 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 belirlencek 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.

6.4. Planın Güncellenmesi

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.

7. 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 Baş Hukuk Müşavirliği tarafından saklanır ve gerektiğinde Bölüm Yöneticisinin yazılı onayı ile Baş Hukuk Müşavirliği'nce imha edilir.

8. GÜNCELLEME PERİYODU

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

9. YÜRÜRLÜK

İşbu politika yayınlandığında yürürlüğe girer.

10. 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

(*) **işareti zorunlu alanları belirtmektedir.**

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 güvenlikhizmetleri*		DDOS	Diğer:		
Hangi tür Güvenlik Cihazlarıkullanılıyor		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

DOKÜMAN KÜNYESİ

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

KATKIDA BULUNULMASI				
Doküman Referans No	**Ad Soyad-Unvan**	**Katkıda Bulunan Bölüm**	**Gözden Geçirilen Sayfa/Madde**	**Tarih**

ONAY ve YÜRÜRLÜK			
Doküman Referans No	**Makam**	**Onay / Karar Tarihi-No**	**Yürürlük Tarihi**

ONAY MAKAMI

Adı Soyadı

Unvan Doğan Holding İcra Kurulu

İmza