1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesine Bilgi İşlem Daire Başkanlığı bünyesinde meydana gelecek bir olaydan sonra Bilgi İşlem operasyonlarını normal seyrine mümkün olan en kısa ve en efektif şekilde dönmesini sağlanmaktır.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı bünyesinde meydana gelecek tüm olayları kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı
- Sistem Yönetimi Birimi

4. TANIMLAR

Acil Durum Çalışanların, hastaların veya halkın yaralanma ve/veya ölümüne neden olan, ani gelişen olaylardır.

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 olaylar aşağıda yer almaktadır:

Yangın, Deprem, Patlama, Sel, Fırtına, Yıldırım düşmesi, Heyelan, Sabotaj/bombalama

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.

Felaket Kurtarma Merkezi: Olağanüstü bir durumda sistemlerin çalıştırılması ve İş sürekliliği kapsamında sistemin faaliyetlerinin yürütülmesi esnasında meydana gelecek acil ve beklenmedik bir durumda, bilgi işlem sistemlerinin çalıştırıldığı diğer Alternatif Çalışma Merkezidir.

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

5. UYGULAMA

5.1 Bilgi Güvenliği Olay Yönetimi

Acil ve Beklenmedik Durum Planında belirtilen tedbirlerin kısmen veya tamamen uygulanabilme Yetkililer tarafından verilecek karar ve talimat sonrasında, "Olağanüstü Durum İlanı" çalışanlara duyurulur. Ancak, hasarlı bir deprem olayı kendiliğinden "Olağanüstü Durum" sayılacak olup, ayrıca bir "Olağanüstü Durum İlanı" m gerektirmez.

"Olağanüstü Durum" halinde "Acil ve Beklenmedik Durum Planı" çerçevesinde alınması öngörülen tedbirler ile olağanüstü koşulların gerektirebileceği diğer önlemler, bu plan uyarınca oluşturulacak "Felaket Kurtarma Merkezi" tarafından uygulanır ve koordine edilir.

Plan kapsamındaki tedbirlerin ilgili sorumlu tarafından veya "Felaket Kurtarma Merkezi" tarafından kısmen veya tamamen devreye sokulması mümkündür.

5.2 Felaket Kurtarma Merkezi

Felaket Kurtarma Merkezi: Kurumda meydana gelen hasarlı bir deprem veya olağanüstü durum haberinin alındığı ilk andan itibaren veya bir "Olağanüstü Durum İlanında bir "Felaket Kurtarma Merkezi" oluşturulur.

5.3 Veri Kurtarma Görevleri

5.3.1.1 Bilişim Sistemleri Hasar ve Kayıp Tespit ile Ulaştırma Çalışmaları

Bir doğal afet veya maddi hasar yaratan olağanüstü durumda, "Felaket Kurtarma Merkezi" tarafından öncelikli olarak sistemlerin çalışabilir hale gelebilmesi için hizmet binasından sırası ile Yedek Sunucu, Taşınabilir Diskler, Sunucular, Bilişim sistemleri (PC, Monitör, Yazıcı) ve teknik ekipman (Ağ Anahtarlama elemanları, alt yapı sistemleri, fotokopi ve diğerleri) kurtarılarak "Felaket Kurtarma Merkezi" en az bir üye denetiminde ulaştırılır ve sistemler en kısa sürede çalışır hale getirilir.

Olağanüstü hallerde hizmet binasının hasar miktarının yüksek olması ve/veya binaya girişlerin engellenmesi durumunda eğer ilgili cihaz ve ekipmana ulaşılamazsa "Felaket Kurtarma Merkezi" nde sürekli olarak aktif durumda bulunan sunucu sistemi üzerinde bulunan son yedek ile birlikte LOKAL(yerel) olarak hizmete alınır.

"Felaket Kurtarma Merkezi" ne ulaştırılan bilişim sistemlerinin sayımları alınarak kayıt altına alınır ve kayıp/hasar tespitleri yapılarak iki üye tarafından imza altına alınır.

5.3.1.2 Bilgi Güvenliği / Operasyonel Olayları

Aşağıdakiler Bilgi Güvenliği Olayları ya da Operasyonel Olaylar olarak tanımlanır:

- Bilgi İşlem kaynaklarının bir saldırıya uğraması veya bir tehdidin oluşması
- Bilgi İşlem kaynaklarına yetkisiz bir erişim / izleme ya da değişiklik olması
- Bilgi İşlem kaynaklarının organizasyon/kuruluş politikalarına, yasa ve yönetmeliklere uygunsuz kullanımından ötürü, Bilgi İşlem kaynaklarının veya bilgilerinin gizlilik, bütünlük ve erişilebilirliğine zarar verilmesi

5.3.1.3 Bilgi Güvenliği Olayı Örnekleri:

- Başarılı ya da başarısız olarak sonuçlanan, içeriden ya da dışarıdan Bilgi İşlem sistemlerine veya verilerine yetkisiz erişim girişimleri
- Bilgi İşlem sistemlerinin veya altyapısının hizmet engelleme saldırılarına (denial of service (DoS)) uğraması ya da yetkisiz olarak devre dışı bırakılma
- Organizasyonun özel (gizli) verilerinin/belgelerinin kaybı
- Bölüm yöneticisinin bilgisi ya da onayı olmadan sistem donanımının, yazılım sürümünün ya da yazılımın değiştirilmesi
- Zararlı yazılım saldırıları (virüs, trojan vb.)
- Sosyal Mühendislik (Gizli bilginin kişiler yanıltılarak ele geçirilmesi, örn. sistem güvenlik şifreleri vb.);
- Dijital imza güncelleme hataları
- Sürekli olarak yanıltıcı uyarı mesajları (Örn. sürekli hatalı virüs uyarı mesajları alan birinin gerçek virüs mesajlarını dikkate almaması).

- Operasyonel Olay Örnekleri:
- Firewall donanım hataları
- Anti-virüs cihazlarının arızalanması

Problem/Vaka

Vaka; bir sistemde, ağda veya günlük operasyonlarda gözlenen veya gözlenebilen günlük olaylarda gözlemlenen ya da gözlemlenebilir durumdur. Karşılaşılan vaka, eğer Bilgi İşlem Sistemleri/altyapısı üzerinde olumsuz etkiye sahip ise ya da bir hadisenin otomatik olarak olumsuz bir etkiye sahip olduğu varsayılacak koşulları ifade eden, önceden kararlaştırılmış bir kriterden ötürü olumsuz olarak nitelendiriliyorsa "olay" (incident) olarak değerlendirilir. Bir vaka, olay yönetiminden sorumlu ekibi (SOME) tarafından analiz edildikten ve zararlı olarak değerlendirildikten sonra "olay" adını alır. Bir vaka zararsız olarak sınıflandırılmadıkça "şüpheli olay" olarak isimlendirilir.

5.4 Olay Müdahale Ekibi (IRT Incident Response Team)

Olay Müdahale Ekibi oluşan olaylara acil olarak müdahale etmeleri ve çözmeleri için kurulur. Olay Müdahale Ekibi potansiyel risklerin ve risklerin doğuracağı olaylara karşı proaktif kurallar koyar. Olaylar önceliğine ve etkisine göre seviyelere ayrılarak ele alınırlar.

Olay Müdahale Takım Üyeleri (Incident Response Team Members)

Bilgi İşlem bölümünde ağ ve güvenlik sorumluları aynı zamanda Olay Müdahale Takımı'nın üyeleridir. Takım üyelerinin, herhangi bir olay hakkında aksiyon almadan önce Bilgi Güvenliği Yöneticisi'nden detaylı bilgi almaları gerekir. Takım üyeleri aynı zamanda olayı bildiren kişiden detaylı bilgi almak için toplanır veya uygun iletişim kanalları ile iletişime geçer. Bilgi Güvenliği Yöneticisi ve Olay Müdahale Takım Üyeleri acil durumlarda kullanılacak bütün ilgili takım üyelerinin, tedarikçilerin ve hizmet sağlayıcıların vb. erişim bilgilerinin listesini tutar.

5.5 Problem/ Olay Yönetimi Süreci

Oluşan olaylar (güvenlik / Operasyonel) ile Kurum bünyesinde oluşan problemleri ayrıştırmak için bir süreç geliştirilmiştir. Bu süreç olaylar ve problemlerin organizasyon operasyonlarının normal seyri sırasında nasıl işleneceği hakkında detayları verir. Bilgi İşlem Bölümü günlük operasyonlarını nasıl gerçekleştirdiğine dair detaylı prosedürler oluşturur.

Problem / Vaka Bildirimi

Organizasyon içerisinde oluşan problemler, Kurum problem yönetimi sürecinde belirtildiği gibi, kullanıcı tarafından Bilgi İşlem personeline iletilir ya da OTRS uygulamasına karşılaşılan problemle ilgili kayıt açılır. Bilgi Güvenliği Yöneticisi bir olaya neden olabilecek vakaları tanımlamak için aşağıdaki önlemlerden birini ya da daha fazlasının uygulanmasını sağlar:

- Bütün kritik bilgi sistemi altyapısında denetim izi (log) tutulması ve bunların takip edilmesi.
- Tespit edici kontroller; örnek olarak dosya bütünlüklerinin izlenmesi, kritik dosya sistemlerinde MD5 şifreleme algoritmasının kullanılması.
- Bilgi İşlem Bölümü tarafından tespit edilen Problem / Vaka, tipine göre ilgili Olay Müdahale Ekibi üyesine bildirilir.
- Her durumda, vakadan ilk haberdar olan Olay Müdahale Ekibi üyesi vaka/olay tipine uygun şekilde ekibin diğer ekip üyelerine de durumu bildirir ve onları da sürece dâhil eder.
- Güvenlik değerlendirmeleri olası zayıflıkları proaktif olarak sunabilir. Bu nedenle, risk ve güvenlik değerlendirmelerinin sonuçları Olay Müdahale Ekibi ile paylaşılır.
- Bilişim sistemlerini ve hizmetlerini kullanan bütün çalışanlardan, üçüncü parti çalışanlardan ve taşeronlardan, sistemlerde veya hizmetlerde karşılaştıkları veya fark ettikleri zayıflıkları Olay Müdahale Ekibi yetkilisine bildirmeleri istenir.
- Vaka/Olayın çözümünde görev alan Olay Müdahale Ekibi üyelerinin sayısı olayın tipine göre asgari seviyede tutulabilir.

Aşağıda örnek olaylar ve bu olayların çözülmesi için bulunması gereken (asgari olarak) Olay Müdahale Ekibi üyeleri verilmiştir.

Anti-virüs ve Firewall güvenlik olayları – Sistem Uzmanı ve Bilgi Güvenliği Yöneticisi;

Web-Sunucusu güvenlik olayları – Sistem ve Yazılım Uzmanı ve Bilgi Güvenliği Yöneticisi;

Sistem operasyon problemleri – Sistem Birimi

Ağ operasyon problemleri – Network Uzmanı

Güvenlik açıklıkları – Network Destek Uzmanı, Sistem ve Son Kullanıcı Destek Uzmanı ve/veya ilgili sistemin yöneticisi ve Bilgi Güvenliği Yöneticisi

5.6 Problem / Vaka gözden geçirme ve analizleri

Bilgi İşlem Personeli tarafından gözden geçirilerek günlük operasyon problemi veya güvenlik vakası olarak ayrıştırılır. Örnek problemler:

- Bilgi İşlem – Satın Alma
- Mobile
- Network/Donanım
- Satın Alma
- Web Sunucuları

Eğer bir tespit edilen vaka bir olay ise bu konu Olay Müdahale Ekibi'ne daha derin inceleme yapılması için yönlendirilir.

5.7 Olayların Sınıflandırılması ve Raporlanması

Bilgi Güvenliği Yöneticisi olayları aşağıdaki tabloya göre sınıflandırır. Bilgi Güvenliği Yöneticisi bu sınıflandırmayı, olayı bildiren kişiden aldığı bilgiye istinaden yapar. Bilgi Güvenliği Yöneticisi olayın etki ve önceliğine göre Olay Müdahale Ekibi oluşturur. Raporlama yapılacak kişiler ve bu kişilerin erişim bilgileri ilgili tüm kişilerin gerek gördüğü durumlarda ulaşabileceği ortamlarda bulunur.

Olaylar, olası iş etkisine ve kabul edilebilir en uzun kesinti süresine göre sınıflandırılır.

Olayların Sınıflandırılması				
Etki Önem Seviyesi	**Etki Alanı**	**Çözüm Süresi**	**Raporlama**	**Örnekler**
Yıkıcı Etki (Seviye 3)	Tüm Tesisin Etkilenmesi	3 saat	Daire Başkanı	Veri Merkezi, Sunucu odası ve / veya çok sayıda süreç / işlem için uzun vadeli tehdit; tüm büro uygulamalarının veya veritabanı raporlarının teslim edilmesine gecikmeye neden olan kesinti; çok gizli bilgilerin yetkisiz olarak açıklanması. Uzun süreli internet kesintisi, yangın vs.
Yüksek Etki (Seviye 2)	Bir ya da Daha Çok Sürecin Etkilenmesi	6 saat	Bilgi Güvenliği Yöneticisi / Bilgi İşlem Yöneticisi	Virüs tehdidi, faaliyetlerin kısmen etkilenmesi (operasyonların % 30'a kadar etkilenmesi), gizli bilgilerin yetkisiz olarak açıklanması
Orta Seviye Etki (Seviye 1)	Operasyonların Kısmen Etkilenmesi	8 saat	Bilgi Güvenliği Yöneticisi / Bilgi İşlem Yöneticisi	Uygulamanın bir bölümünün çalışmaması, ofis iletişiminin bozulması, toplu (batch) işlem ile ilgili sorunlar, iç uygulamaların çalışmaması vb.
Az ya da Etkisiz	Operasyonların etkilenmemesi	24 saat	Bilgi Güvenliği Yöneticisi / Bilgi İşlem Yöneticisi	Kuyruktan başkasının kartı ile geçiş, talep edilmemiş erişim kartları, planlanmış bakım görevleri, vb
Beklenen Raporlama / Tepki Süresi – Acil				

Raporlama: Raporlama hiyerarşisi aşağıdaki şekildedir:

Seviye 1 –Bilgi Güvenliği Yöneticisi/ Bilgi İşlem Yöneticisi

Seviye 2 – Bilgi Güvenliği Yöneticisi/ Bilgi İşlem Yöneticisi

Seviye 3 – Daire Başkanı

Uygun seviyeden üyeler tarafından raporlama yapılacaktır.

5.8 Olayın Araştırılması

Oluşan güvenlik vakası, sadece bir vaka mı yoksa olay mı olduğunun anlaşılması için Bilgi Güvenliği Yöneticisi tarafından incelenir. Olay analiz edilir ve eğer mümkün ise iş üzerine etkisi de belirlenir. Eğer mümkün ise olaya sebep olan olayın güvenlik olayı mı yoksa Operasyonel olay mı olduğunun ayrımı için incelenir. Olay üst yönetime, örneğin Bilgi İşlem

Yöneticisi, Bilgi Güvenliği Yöneticisi ve Bilgi İşlem destek ve ağ yöneticisine raporlanır. Bilgi İşlem Yöneticisi, Bilgi İşlem destek ve ağ personeli ve Bilgi Güvenliği Yöneticisi olayın tipini "Operasyonel" veya "Güvenlik" ve olayın derecesini "Yüksek", "Orta" veya "Düşük" olarak belirler. Olayın derecesi olayın iş üzerine etkisi ile ölçülür. Asgaride aşağıdaki kriterler bir olayın "Operasyonel Olay" olarak tanımlanması için kullanılabilir:

- Güvenlik ve ağ cihazlarındaki donanım problemleri
- Bilgi İşlem ve güvenlik takımcılarınca yapılan uygun olmayan konfigürasyonlar

Operasyonel olaylar yüksek/orta/düşük olarak önceliklendirilir. Aşağıdakiler Operasyonel olaylara örnektir:

Operasyonel Olaylar – Yüksek

- Donanım problemlerinden ötürü oluşan firewall hataları
- Sunucu arızaları
- Canlı sistem veritabanlarındaki hatalar
- İnternet bağlantı, MPLS, VPN bağlantı hataları

Operasyonel Olaylar – Orta

- IDS/IPS/İçerik filtreleme cihazlarındaki donanımsal arızalar
- E-posta bağlantı cihazlarının arızalanması
- Dış ortam ve DMZ cihazlarının arızaları
- **Operasyonel Olaylar – Düşük**
- Sunucunun 1 cluster'ında hata oluşması
- Uygulama bölgesindeki Switch/Router arızaları

Güvenlik olayları Yüksek / Orta / Düşük olarak derecelendirilmelidir. Aşağıda güvenlik olaylarına örnekler verilmiştir:

Güvenlik Olayı - Yüksek

- İnternetten gelen korsan saldırılardan ötürü internet router'larının hatalı çalışması
- Web sunucusunun arızalanması
- Başarılı korsan (hack) saldırılarından ötürü uygulama sunucularının hatalı çalışması
- Başarılı korsan (hack) saldırılarından ötürü e-posta bağlantı cihazlarının hatalı çalışması
- Virüs ve solucan saldırıları
- Ağ ve konfigürasyon cihazlarının yapılandırılmalarının yetkisiz olarak değiştirilmesi
- Ağ ve konfigürasyon cihazlarında onaysız olarak kullanıcı oluşturulması
- Kullanıcı ve yüklenicilerin doğrulanan güvenlik ihlalleri gerçekleştirmeleri

Güvenlik Olayı - Orta

- Internet üzerinden sürekli olarak aktif portların denenmesi
- İnternet üzerinden web sayfalarına yapılan tahrip teşebbüsleri ve saldırıları
- Web sunucusu üzerindeki web sayfalarının yetkisiz olarak değiştirilmesi
- Uygulama sunucularına yönelik saldırılar
- Çok sayıda kullanıcının virüs ve Spam posta aldığını bildirmesi
- İnternet üzerinden mesajlaşmayı sağlayan sosyal haberleşme uygulamalarının izinsiz şekilde kurulması
- Organizasyon ağından ya da dışarıdan kaynaklara izinsiz olarak erişim girişimleri

- İzinsiz ve yetkisiz olarak canlı ortam uygulama sistemlerinde değişiklik yapılması
- Yazılımların izinsiz olarak kurulması

Güvenlik Olayı - Düşük

- Internet üzerinden web sunucusu ve e-posta bağdaştırıcıları ile sistemlerin sürekli olmamak kaidesi ile taranması veya ping atılması
- 10'dan az kullanıcının virüs ve Spam- mail şikâyetinde bulunması
- 3'ten fazla hatalı şifre girilmesi sebebiyle hesap kilitlenmesi
- Sistem konsollarının korunmaması
- Anti-virüs yazılımının bulunmaması

5.9 Olaylara Müdahale ve Çözüm

Güvenlik Olayının tipine ve etkisine göre uygun çözüm uygulanır. Bilgi Güvenliği Olayının maliyeti, çözüm uygulanmadan önce belirlenir ve gözlemlenir.

Hizmet Engelleme Saldırıları (Denial of service attacks):

- Atağın yapıldığı IP adresinin belirlenmesi ve dış firewall üzerinde bu IP adresinin durdurulmasını sağlayacak konfigürasyonun yapılması
- Internet Servis Sağlayıcısına bu IP adresinin engellenmesi isteğinin bildirilmesi

Virüsler ve Solucanlar

- Virüsten etkilenen sistemin ağdan çıkartılması
- Sistem üzerindeki anti-virüs imzalarının güncellenmesi ve cihazların hem işletim seviyesinde hem de mümkün ise BIOS seviyesinde (Boot Level) taranması
- Tedarikçi tarafında ki sistemlerin virüs ve solucan içermediğine dair taranması
- Solucan saldırılarının hangi port üzerinden yapıldığının bulunması ve bu port'un tedarikçi tarafında bulunup bütün firewall'larda engellenmesi
- Anti Virüs sistemlerinin sürekli olarak güncel tutulmasının sağlanması
- Organizasyon içerisindeki bütün kullanıcılara; bilinmeyen kaynaklardan gelen e-postaların ve belirli tiplerdeki, başlıklardaki, içeriklerdeki ve eklentili e-postaların açılmaması gerektiğine yönelik e-postalar gönderilmesi ve kullanıcıların uyarılması

Sunucu / Sistemlerin İş Göremez Hale Getirilmesi

- Sistemin ağdan çıkarılması
- Web sunucusu üzerindeki denetim izi dosyalarının alınıp hangi adresten girişimlerin olduğunun bulunması
- IDS/IPS ve dış firewall üzerindeki denetim izi dosyalarının kontrol edilmesi
- Web sunucusu üzerinde açıklık var mı gibi sunucu bazlı olarak zafiyet değerlendirmelerinin yapılması

- Canlı ortam uygulama sunucusunda dosya izinlerinin kontrol edilmesi ve sunucu bazlı zafiyet değerlendirmesinin yapılması
- Sistem üzerindeki tüm dosya yetkilerinin ve kullanıcı yetkilerinin kontrol edilmesi
- Internet üzerinden belirli kaynaklar için kısıtlama yapılarak sızma testlerinin yapılması
- Sistemi tekrar ağa bağlayıp, sistemin internet kullanıcılarının erişimine açılması

Ek Çözüm Önlemleri

Çözülemeyen bir olayla karşılaşıldığında, Güvenlik Kurulu'nun onayının alınmasının ardından, mevcutsa uygun bir alternatif çözüm uygulanır.

Olaya verilecek tepki güvenlik ve ağ cihazlarının konfigürasyonunda değişiklik yapılmasını gerektiriyor ise, değişiklikler ayrı ayrı hem önerilen değişiklik yönetimi sürecine hem de konfigürasyon yönetimi sürecine uygun olarak gerçekleştirilir.

Olayın, Kurum ekibi tarafından çözülememesi durumunda tedarikçi firma ile irtibata geçilir.

Olay çözümlenir ve Bilgi İşlem altyapısı normal çalışır durumuna getirilir.

Olay Dokümantasyonu

- Olay, güvenlik olayı mı yoksa Operasyonel olay mı olduğunun anlaşılması için açık bir şekilde dokümante edilir. Olay takip formu da ek olarak bu rapora eklenir.
- Tüm olaylar için Yardım Masası aracında kayıt açılır ve olay takibi için gerekli bilgiler (olayın önem derecesi, olayı raporlayan kişi ve çözümünde rol alan kişiler, olayın tanımı ve uygulanan çözüm ve olayın tanımlanması ve çözümü için ihtiyaç duyulan zaman) bu araca girilir.
- Yardım Masası aracı üzerinden aylık olay raporu çekilir.
- Olay yönetimi prosedüründe belirtildiği üzere, olaylar güvenlik kurulu ve yönetim kurulu toplantılarında sunulur.
- Benzer olayların meydana gelmesi durumunda olay veritabanı çözüm kılavuzu olarak kullanılır.
- Olay dokümantasyonu, izlenilen sürecin incelenmesine ve yargı aşamasında politika ve prosedürlere uyulup uyulmadığının kontrol edilmesine imkân verecek şekilde kanıt niteliğindeki çeşitli belgelerle desteklenir.

6. İLGİLİ DOKÜMAN

- Ağ Güvenliği Politikası
- Yedekleme ve Kurtarma Prosedürü
- Erişim Kontrolü Prosedürü
- Şifreleme Sistemleri Prosedürü