Siber Olaylara Müdahale Prosedürü

DOKÜMAN NUMARASI	PR.16
REVİZYON NUMARASI	00
REVİZYON TARİHİ	-
YAYIN TARİHİ	26.10.2022
TASNİF	Hizmete Özel
HAZIRLAYAN	
KONTROL EDEN	
ONAYLAYAN	

1. AMAÇ

Bu prosedürün amacı**;** Pamukkale Üniversitesi Bilgi İşlem Daire Başkanlığı karşılaştığı herhangi bir siber olayda yapılacak çalışmaları tanımlamayı amaçlamaktadır.

2. KAPSAM

BGYS DD.01 Bilgi Güvenliği Yönetim Sistemleri Kapsamı ve Sınırları dokümanında belirtilen gibidir.

3. SORUMLULAR

Bu prosedürün uygulanmasından Pamukkale Üniversitesi Bilgi İşlem Daire Başkanlığı SOME Ekibi sorumludur.

4. KISALTMALAR & TANIMLAR

BGYS **:** Bilgi Güvenliği Yönetim Sistemi
SOME Ekibi **:** Siber Olaylara Müdahale Ekibi

5. UYGULAMA

5.1. SOME Ekibi

Pamukkale Üniversitesi Bilgi İşlem Daire Başkanlığı siber olaylara müdahale için bir SOME Ekibi mevcuttur. Bu ekip 11 Kasım 2013 Tarihli ve 28818 Sayılı Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliği kapsamındaki görevleri yürütür.

Kurumsal SOME İletişim Bilgileri Formu ile USOM'a bildirilen ekibe ait güncel bilgiler https://sip.usom.gov.tr/#/some/detay/1110 sekmesinde yer alır.

5.2. Siber Olaya Müdahale

5.2.1 Riskin Tanımı

Siber saldırılar nedeniyle sistemlere izinsiz girişler, yetkili kullanıcıların sistemlere erişememesi ve giriş yapamaması, tüm bilişim sistemlerindeki verilerin bütünlüğünün ve gizliliğinin bozulmasıdır.

5.2.2 SOME Ekibi Müdahalesi

a) Ekip Lideri (Bilgi İşlem Daire Başkanı):

I. Yetkili kurumlar, ekip üyeleri ve diğer kaynaklardan gelen bilgileri siber saldırı açısından değerlendirip ekibi göreve çağırır.
II. Siber saldırı ile ilgili acil durum faaliyet planını yönetir.

b) Ekip Üyesi (Sistem Yöneticileri):

I. Sunucu ve depolama ortamlarına olan etkiyi kontrol eder.
II. Tespit ettiği etkiyle ilgili SOME Ekip Liderini bilgilendirir.

III. Gelen direktifler doğrultusunda gerekli önlemleri alır.

c) Ekip Üyesi (Yazılım Teknolojileri Şube Müdürü):

I. Etkiyi kontrol eder.
II. Ekip Liderini bilgilendirir.

d) Ekip Üyesi (Ağ ve Güvenlik Yöneticileri):

I. Ekip Liderini bilgilendirir.
II. Ulaknet üzerinden alınan internet trafiğinin yönü güvenlik duvarı üzerinde yönlendirme metrik ayarı yapılarak DDOS korumalı yedek internet hattı üzerine yönlendirilir.
III. Alınan DDOS hizmeti kapsamında servis sağlayıcı ile görüşülerek atak hakkında bilgi alınır.
IV. Saldırı kaynak IP'lerinden kurum ağına erişimler güvenlik sistemlerinde kesilecek şekilde tanımlamalar yapılır.
V. Saldırı tipine göre gerekli durumlarda tüm kullanıcılar için, internet trafiğinde kısıtlamalara gidilir.
VI. Anlık olarak yada periyodik raporlar şeklinde veri trafiği izlenir.
VII. Veri trafiğinde görülen şüpheli durumlara karşı güvenlik sistemlerinde gerekli tanımlamalar yapılır.
VIII. Gerekli önlemlerin atağı engelleyeceğinden emin olunduktan sonra internet yönü Ulaknet üzerine geri alınır.

5.2.3 İntikal Planlaması

Mesai saatleri içinde tüm ekip üyeleri Pamukkale Üniversitesi Rektörlüğü Bilgi İşlem Daire Başkanlığı adresinde bulunurlar. Bu adres dışında iseler mevcut imkanları kullanarak bu adrese gelmelidirler;

Saldırı **mesai saatleri dışında** gerçekleşmiş ise ekip aşağıdaki adrese kendi imkanları ile 1 saat içerisinde ulaşmalıdır.

5.2.4 Müdahale Şekli, Zaman Planlaması ve Raporlama

MESAİ SAATLERİ İÇİNDE

0-1 SAAT AKSİYONLARI

- Ekip lideri ya da saldırıyı ilk öğrenen tüm ekibe haber verir.
- Tüm ekip üyeleri sorumlusu olduğu sistemlere erişimleri (fiziksel ya da sanal) kontrol eder.
- Tüm ekip üyeleri saldırının etkileri konusunda Ekip Liderini bilgilendirir.

1-3 SAAT AKSİYONLARI (TÜM EKİP ÜYELERİ EŞ ZAMANLI)

SİSTEM YÖNETİCİLERİ

- Sunucu ve depolama ortamlarına olan etkiyi kontrol eder.
- Tespit ettiği etkiyle ilgili SOME Ekip Liderini bilgilendirir.
- Gelen direktifler doğrultusunda gerekli önlemleri alır.

YAZILIM TEKNOLOJİLERİ ŞUBE MÜDÜRÜ

- Sorumlusu olduğu sistem, yazılım ve cihazlara olan etkiyi kontrol eder.
- Tespit ettiği etkiyle ilgili SOME Ekip Liderini bilgilendirir.
- Gelen direktifler doğrultusunda gerekli önlemleri alır.

AĞ ve SİBER GÜVENLİK YÖNETİCİLERİ

- Alınan DDOS hizmeti kapsamında servis sağlayıcı ile görüşülerek ataklar kontrol edilir
- Saldırı kaynak IP'lerinden kurum ağına erişimler güvenlik sistemlerinde kesilecek şekilde tanımlamalar yapılır.
- Saldırı tipine göre gerekli durumlarda tüm kullanıcılar için, internet trafiğinde kısıtlamalara gidilir.
- Anlık olarak yada periyodik raporlar şeklinde veri trafiği izlenir.
- Veri trafiğinde görülen şüpheli durumlara karşı güvenlik sistemlerinde gerekli tanımlamalar yapılır.

3-6 SAAT AKSİYONLARI

TÜM EKİP ÜYELERİ

- Sorumlusu oldukları tüm sistem ve cihazlarda son kontrolleri yaparlar.
- Ekip Lideri son durum hakkında bilgilendirilir.
- Kısıtlanan erişimler kontrollü biçimde açılır.

EKİP LİDERİ

- Saldırıya ilişkin son kontrolleri gerçekleştirir.
- Siber saldırı sonrasında saldırıya ilişkin "SİBER OLAY DEĞERLENDİRME FORMU" USOM'a iletilir.

MESAİ SAATLERİ DIŞINDA

0-1 SAAT AKSİYONLARI

TÜM EKİP ÜYELERİ

Saldırıya ilişkin bilgiyi aldıktan sonra bu bilgiyi ekip üyeleri ile paylaşırlar.

Aşağıdaki adrese kendi imkanları ile 1 saat içerisinde ulaşmalıdır.

Pamukkale Üniversitesi Rektörlüğü Bilgi İşlem Daire Başkanlığı Pamukkale/DENİZLİ

1-3 SAAT AKSİYONLARI

(TÜM EKİP ÜYELERİ EŞ ZAMANLI)

SİSTEM YÖNETİCİLERİ

Sunucu ve depolama ortamlarına olan etkiyi kontrol eder.

Tespit ettiği etkiyle ilgili SOME Ekip Liderini bilgilendirir.

Gelen direktifler doğrultusunda gerekli önlemleri alır.

YAZILIM TEKNOLOJİLERİ ŞUBE MÜDÜRÜ

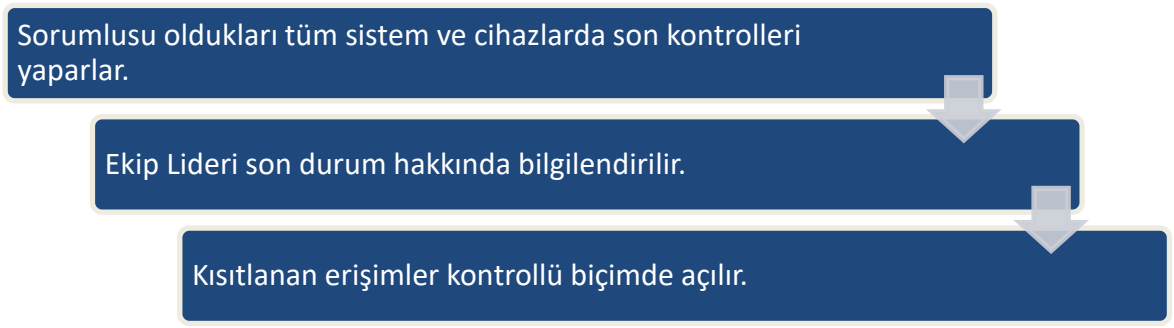
- Sorumlusu olduğu sistem, yazılım ve cihazlara olan etkiyi kontrol eder.
- Tespit ettiği etkiyle ilgili SOME Ekip Liderini bilgilendirir.
- Gelen direktifler doğrultusunda gerekli önlemleri alır.

AĞ ve SİBER GÜVENLİK YÖNETİCİLERİ

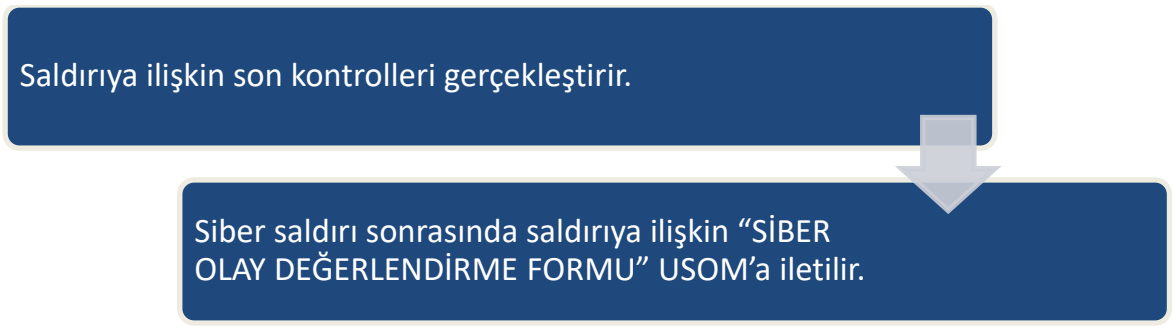
- Alınan DDOS hizmeti kapsamında servis sağlayıcı ile görüşülerek ataklar kontrol edilir
- Saldırı kaynak IP'lerinden kurum ağına erişimler güvenlik sistemlerinde kesilecek şekilde tanımlamalar yapılır.
- Saldırı tipine göre gerekli durumlarda tüm kullanıcılar için, internet trafiğinde kısıtlamalara gidilir.
- Anlık olarak yada periyodik raporlar şeklinde veri trafiği izlenir.
- Veri trafiğinde görülen şüpheli durumlara karşı güvenlik sistemlerinde gerekli tanımlamalar yapılır.

3-6 SAAT AKSİYONLARI

TÜM EKİP ÜYELERİ



EKİP LİDERİ



Not: Siber saldırının devam etmesi durumunda e-posta ve internet erişimi kontrolü sağlanabilir.

5.2.5 Gerek Olması Durumunda Kurtarma Faaliyetlerinin Planlaması

Siber saldırı sonrasında insan hayatını tehdit eden koşulların oluşmayacağı öngörülmektedir.

6. DAYANAK

ISO 27001:2013 Bilgi Güvenliği Yönetim Sistemi PR.11 İhlal Olayı Yönetimi Prosedürü