TÜRK-ALMAN ÜNİVERSİTESİ
TÜRKISCH-DEUTSCHE UNIVERSITÄT

SİBER OLAYLARA MÜDAHALE POLİTİKASI

Revizyon Takibi:

Sıra No	Rev. No	Tarih	Hazırlayan	Revizyon Nedeni	Onaylayan	İmza
1						
2						
3						
4						

1. AMAÇ

Bu Politika, Türk-Alman Üniversitesinin Bilgi varlıklarının Gizlilik, Bütünlük ve Erişilebilirliğini bozabilecek bir Siber Olay Meydana gelmesi durumunda yapılması gereken kuralları tanımlamaktadır.

2. KAPSAM

Bu Politika, Türk-Alman Üniversitesi ile ilişkili Dijital Bilgi Varlıkları ve bu varlıklar ile ilişkili altyapı bileşenlerini kapsamaktadır.

3. SORUMLULUK

Bu politika ile ilgili gereklerin uygulanmasından SOME ekibi sorumludur.

4. UYGULAMA

4.1 Tanımlar

BİDB: Bilgi İşlem Daire Başkanlığı

SOME: Siber Olaylara Müdahale Ekipleri

Kurumsal SOME: Kurumunda bulunan siber güvenlik risklerini azaltan ve siber olay meydana geldiğinde görev tanımında yer alan çalışmaları yapan Kurumsal Siber Olaylara Müdahale Ekibini tanımlar.

Ağ Saldırı Tespit Cihazı (IPS -Intrusion Prevention System): Temel görevi; kötü niyetli aktiviteleri belirlemek, kötü niyetli saldırıları durdurmak ve saldırının türünü rapor etmek olan ağ güvenlik cihazıdır. IPS ağ trafiğini üzerinden geçirir; iyi niyetli trafiğin engellenmeden akmasına izin verirken, kötü niyetli ve istenmeyen trafiği engeller. Aslında IPS, iyi trafiğin performansını, ağı sürekli temizleyerek ve kullanım önceliği olan uygulamalara öncelik vererek, optimize eder.

DMZ (Demilitarized Zone): Farklı güvenlik seviyesi ile iç ve dış ağlardan ayrılmış ve dışarıdan erişilmesi gereken sunucuların bulunduğu güvenlik duvarı ortamıdır. Dışarıya açık olması sebebiyle erişim sınırlamaları güvenlik açısından oldukça önemlidir.

Güvenlik duvarı (Firewall): Yerel ağlar üzerindeki kaynakları diğer networkler üzerinden gelecek saldırılara karşı koruyan, iç ve dış ağlar arası ağ trafiğini tanımlanan kurallara göre denetleyen bir ağ geçidi cihazıdır.

NAT (Network Address Translation): Bir network içerisinde kullanılan bir IP adresinin başka bir network içerisinde bilinen başka bir IP adresine çevrilmesidir. Statik olarak lokal (sanal) bir IP adresini global (gerçek) bir IP adresine çevirme şeklinde olabileceği gibi lokal bir IP adresini dönüşümlü olarak üniversitenin sahip olduğu global IP havuzundan bir IP`ye çevirme şeklinde de uygulanabilir.

Phishing: Yemleme, yasadışı yollarla bir kişinin şifresini veya kredi kartı ayrıntılarını öğrenme. Sözcük, İngilizce password (şifre) ve phishing (balık avlamak) sözcüklerinin birleşmesiyle oluşturulmuş phishing ifadesinin Türkçe karşılığıdır. "Yemle" diye tanımlanan şifre avcıları, genelde

e-posta gibi yollarla kişilere ulaşır ve onların kredi kartı gibi ayrıntılarını sanki resmi bir kurummuş gibi ister. Bu "av" a karşılık veren kullanıcıların da hesapları, şifreleri vb. özel bilgileri çalınmaktadır. Örnek olarak; format açısından resmi bir banka konseptinde bir e-posta alınır ve bu e-postada şifre, kredi kartı numarası vb. bilgilerin verilmesi önerilir.

SMTP: Elektronik posta gönderme protokolü (Simple Mail Transfer Protocol), bir e-posta göndermek için sunucu ile istemci arasındaki iletişim şeklini belirleyen protokoldür. Farklı işletim sistemleri için geliştirilmiş e-posta protokolleri vardır. Bu protokollerinin SMTP'ye geçit yolu (gateway) vardır. SMTP, Aktarım Temsilcisi (Mail Transfer Agent, MTA) ve Kullanıcı Temsilcisi (Mail User Agent, MUA) yazılımları arasındaki iletişimi sağlar.

Antispam: Spam engellemeye yönelik yazılım.

Antivirüs: Virüs, worm vb. zararlı yazılımları engellemeye yönelik program.

White List: Uygulandığı cihazda herhangi bir denetleme ve engellemeye uğramaksızın geçişin sağlanması için hazırlanan liste.

Web Uygulama Güvenlik duvarı-WAF (Web Application Firewall): Sistem web trafiğinin HTTP/HTTPS/SOAP/XML-RPC/Web Servisleri üzerinde detaylı paket incelemesi yaparak anormal trafiği engellemeye yarayan teknolojidir.

Siber Olay: Bilişim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlal teşebbüsünde bulunulmasını.

İz Kaydı: Bilişim sistemlerinin işletilmesi esnasında veya siber olaya maruz kalması durumunda ürettiği kayıtları.

USOM: Temel görevleri, "Ulusal Siber Olaylara Müdahale Merkezinin Kuruluş, Görev ve Yetkilerine Dair Usul ve Esasların" da yer alan Ulusal Siber Olaylara Müdahale Merkezini ifade eder.

4.2 Ağ Güvenliği

• İç ağda oluşabilecek saldırı veya zararlı yazılımların oluşturduğu anormal faaliyetleri tespit etmek için "Ağ Saldırı ve Tespit Cihazı (IPS)" kullanılmaktadır. SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu;

• IPS (Ağ Saldırı Tespit Cihazı) üzerinde tanımlanan tüm kullanıcılar aşağıda anlatılan Sistem Güvenliği adımları uyarınca belirlenen şekilde açılacak, yetkilendirilecek ve şifrelenecektir.

• IPS konumlandırıldığı yerlerde Omurga cihazlarının önüne konumlandırılmıştır. Bu sayede tüm VLAN ler segmentasyon yapılarak cihazların Gbit portlarından VLAN ler arası trafiği de izleyecek şekilde konumlandırılmıştır. Bununla beraber Güvenlik Duvarı Cihazı üzerindeki IPS modülü ile Arka uçların trafiği izlenmektedir.

• Tüm VLAN lardan ve internetten gelen saldırılar veya internete ve iç ağa yönelik, içerden yapılan saldırılar high level (yüksek seviyede) olarak engellenmekte (block) ve tüm bu trafik ve IPS tarafından yapılan müdahaleler raporlanabilmektedir.

• IPS ağ tabanlı saldırı imzaları (signature) lisansları 3 yılda bir yenilenmeli ve IPS cihazı tüm yeni internet saldırılarına karşı hazır tutulmalıdır.

• IPS cihazları mevcut topolojiden farklı bir topolojiye taşındığında bunun sebebi bir raporla açıklanmalı ve yeni topolojinin sebepleri açıkça belirtilmelidir. Özellikle DMZ (Demilitarized Zone) bölgesinde tanımlanan sunucu ve cihazların raporlanması ve illegal trafiğin minimuma çekilmesine özen gösterilmelidir.

4.3 Sistem Güvenliği

• Üniversite dışından hem içerideki kullanqasıcılara hem de sunuculara gelebilecek saldırıları tespit etmek, engellemek ve sonrasında alınacak önlemler aşağıda yer alan "Güvenlik Duvarı Kullanım ve Kontrol" adımları uyarınca gerçekleştirilmektedir.

• Güvenlik Duvarı üzerinde içeriden dışarıya doğru, sıkça kullanılan portlar (http, https, FTP, DNS vb.) haricindeki portlar, ağ güvenliğini tehdit eden trafiğe neden oldukları için kapalı tutulur.

• Güvenlik duvarı üzerinde istenen port açma, NAT yapma gibi işlem talepleri BİDB' ne resmi yazıyla bildirilir.

• Kişisel uygulamalar için port açma veya NAT yapma benzeri istekler, BİDB tarafından uygun bulunduktan sonra düzenlenir.

4.4 DMZ Bölgesi

• DMZ bölgesinde, tüm üniversite tarafından kullanılan ve kritik iş süreçlerine sahip sunucular (web, e-posta, öğrenci ve personel otomasyon vb.) tutulur.

• DMZ bölgesinde tutulan sunuculara sağlanacak erişimlerin kararı sistem yönetimi ve uygulamaların sorumluları ile koordinasyon sonucunda verilir.

Güvenlik duvarının sağlıklı çalışmasının temini için cihaza ait yönetim yazılımları ve ara yüzler vasıtasıyla sürekli kontrolü ve takibi sağlanır.

• NAT dönüşüm logları "5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" gereği 6 ay süre ile tutulmaktadır.

• Hiçbir şekilde güvenlik duvarı üzerinde İÜ Bilgi Güvenliğini ihlal edecek istekler kabul edilmez.

4.5 Web Güvenliği

• Üniversite dışından web sayfalarına ve sunucularına gelebilecek saldırıları tespit etmek, engellemek ve sonrasında alınacak önlemler için "Web Uygulama Güvenlik Duvarı" kullanılmaktadır.

• WAF cihazı web sunucuları önüne bridge modda yerleştirilerek trafiği üzerinden geçirmesi ve incelemesini sağlanır. Network tabanlı IPS benzeri bulunduğu konum üzerinden geçen tüm trafiği inline olarak alır, inceler ve duruma göre bloklama yapar. SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu;

• Cihazın yönetimi web ara yüzünden gerçekleştirir.

• Farklı web uygulamalarına göre farklı profiller oluşturur.

• Oluşturulan profillere göre kurallar (policy) yazar.

• Cihaz ile ilgili gelen şikâyetleri inceler, web ara yüzünde gerekli konfigürasyonlar yapar.

• Engellenmesi gerekmeyen ancak güvenlik sisteminin engellediği (false positive) düşünülen durumlarda bir hata kodu oluşturarak daha önceden tasarlanmış bir web ara yüzünde kullanıcıya gösterilmesi sağlanır.

• Bir link vasıtasıyla bu hata kodunun e-posta yoluyla BİDB 'ne iletilmesi sağlanır.

• Bu sayfada yer alan hata kodu ile engellenen isteği loglardan bulur inceler. • İsteğin inceleme sonrası normal bir istek olduğunu tespit ederse cihazın aynı işlemi ve tepkiyi tekrarlamaması için ayar (deploy) yapar.

4.6 SOME Olay Yönetimi

• "Siber Olaylara Müdahale Ekiplerinin Kuruluş, Görev ve Çalışmalarına Dair Usul ve Esaslar Hakkında Tebliğ" kapsamında Kurumsal SOME kurma yükümlülüğü olan kurumların faydalanması amacıyla Kurumsal SOME Kurulum ve Yönetim Rehberi hazırlanmıştır.

• Bu rehber Kurumsal SOME'lerin kurum organizasyonu içerisindeki yerini, kapasite planlamasını, personelin niteliklerini (eğitim düzeyi ve tecrübe), alması gereken eğitimleri, bu personelin siber olay öncesi, esnası ve sonrasında yapması gereken çalışmaları, kurum içi/kurum dışı paydaşlarla iletişim esaslarını içermektedir.

• Kurumda herhangi bir siber olay gerçekleştiğinde ve sonrasında yapılacaklar ile ilgili adımlar aşağıda belirtilmiştir.

• SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu olay müdahale esnasında bilişim sistemlerine yetkisiz erişim yapılmaması için gerekli tedbirleri alır, aldırır.

• SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu acil durum koordinasyonunu sağlar. Bilgilendirme onun kanalıyla sağlanır.

• SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu saldırı konularının özelliğine göre ilgili kişilere ulaşır.

• Kurulun verdiği bilgiyi üst makama iletir.

• İlgili kişiler durumun aciliyeti ve önemine göre Daire Başkanlığı'na gelir.

• Siber olay müdahale akışı içinde suç unsuruna rastlanması halinde savcılık, kolluk makamı vb. makamlara haber verilmesi hem kanuni yükümlülüğün yerine getirilmesi hem de ulusal siber güvenlik kapsamında caydırıcılığın sağlanması açısından önem arz etmektedir. Sistemlerin, uygulamaların, kullanıcı işlemlerinin ve bilgi sistem ağındaki veri akışının iz kayıtları Log Yönetim mekanizmalarıyla tutulur. Bu iz kayıtları ile işlemi gerçekleştiren kişi belirlenebilir (accountability),

yetkisiz erişimler belirlenebilir (unauthorized), anormal işlemler belirlenebilir (abnormal) ve iz kayıtları kullanılarak performansa (sistemlerdeki olası sorunlar iz kayıtları ile önceden belirlenebilir) dair izleme yapılabilir.

• Saldırı Türlerine Göre Alınacak Aksiyonlar

• Ağ Saldırısı

♣ Switch, omurga, firewall vb. ağ elemanlarına yapılan saldırılar. SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu Ağ ve Kablolama Birimi Sorumlusu ile hareket ederek saldırıyı kesmek üzere çalışma başlatır.

• Sistem Saldırısı

♣ Sunuculara yapılan saldırı durumunda, SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu Sistem Sunucu Birimi Sorumlusu ile hareket ederek sorun tespiti ve çözümü için çalışma başlatır.

• Web Saldırısı

♣ Web siteleri üzerinden yapılan saldırılar durumunda, SOME (Siber Olaylara Müdahale Ekibi) Birim Sorumlusu Web ve Yazılım Destek Birimi Sorumlusu ile ortak hareket ederek tespiti ve çözümü sağlar.

• Saldırı Tespit Çözüm Adımları

• Tespit,

• Önleyici faaliyet

• Çözüm

• Delillerin toplanması

♣ Çözüme geçmeden önce sistemin yedeği alınır.

♣ Çözüm sağlandıktan sonra iz kayıtları (loglar) incelenir.

• Analizi

• Siber Olay Sonrası

• Kurumda bir siber olay gerçekleştikten ve olaya müdahale edildikten sonra; zaman geçirmeden olaya neden olan açıklık belirlenir ve çıkarılan dersler “Siber Olay Değerlendirme Formu (BGYS-FRM.01)” doldurularak kayıt altına alınır.

• Ağ ve Sistem Güvenlik Sorumlusu siber olay ile ilgili bilgileri USOM tarafından belirlenen kriterlere uygun şekilde “Siber Olay Değerlendirme Formu (BGYS-FRM.01)”nu doldurarak USOM’a gönderir ve kayıt altına alır.

• Olayla ilgili olarak gerçekleştirilebilecek düzeltici/önleyici faaliyetlere ilişkin öneriler kurum yönetimine arz edilir.

• Yaşanan siber olayların türleri, miktarları ve maliyetleri ölçülüp izlenir.

• Yaşanan siber olaya ilişkin iş ve işlemlerin detaylı bir şekilde anlatıldığı siber olay müdahale raporu hazırlanır, üst yönetim, USOM ve varsa bağlı olduğu Sektörel SOME'ye iletilir.

5. YAPTIRIM

Bu politikaya uygun olarak çalışmayan personel hakkında ilgili personel kanununun hükümleri uygulanır.

6. İLGİLİ DOKÜMANLAR

• TAU-FRM.01 Siber Olay Değerlendirme Formu