İÇİNDEKİLER

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

1 Amaç

Bu politikanın amacı, ESOGÜ BİDB'nin kendisinin ve hizmet verdiği fakülte ve yüksekokulların, laboratuvarların, sosyal tesislerin ve diğer ilgili bağlı birimlerin ortak olarak kullandığı ve ESOGÜ fiziksel çerçevesi içerisinde konumlanmış ağ sistemleri ve ağ ekipmanlarının ISO 27001 standart kapsamında bilgi ve iletişim altyapılarının gizlilik, bütünlük, erişilebilirlik ve sürekliliğinin sağlanması amacıyla ağ yönetiminde uyulması gereken ve işletilen minimum standartları tanımlamaktır.

2 Kapsam

ESOGÜ bünyesinde kullanılan tüm ağ cihazları ve bunların yönetimi bu politika kapsamındadır.

3 Tanımlar ve Kısaltmalar

ESOGÜ: Eskişehir Osmangazi Üniversitesi
BİDB: Bilgi İşlem Daire Başkanlığı
BGYS: Bilgi Güvenliği Yönetim Sistemi
ISO: International Organization for Standardization / Uluslararası Standartlar Örgütü
VPN: Virtual Private Network / Sanal Özel Ağ
IDS: Intrusion Detection System / saldırı tespit sistemi
UTP: Unshielded Twisted Pair / Korumasız Bükümlü Kablo
IP: Internet Protocol / İnternet Protokolü
VLAN: Virtual Local Area Network / Sanal Yerel Alan Ağı
DMZ: Demilitarized Zone / Sivil Bölge
DoS/DDoS: Denial Of Service- Servis Hizmet Reddi / Distributed Denial of Service- Dağıtılmış Hizmet Reddi
NAC: Network Access Control (Ağ Erişim Kontrolü)
EBYS: Elektronik Belge Yönetim Sistemi
DHCP: Dynamic Host Configuration Protocol / Dinamik Ana Bilgisayar Yapılandırma Protokolü
MAC: Media Access Control / Ortam Erişim Kontrolü (Cihazın fiziksel adresi)
DNS: Domain Name System / Alan Adı Sistemi
FIREWALL: Güvenlik Duvarı

4 Sorumlular

Bu politikanın oluşturulmasından Bilgi Güvenliği Birimi sorumludur. Bu süreçte BGYS Yöneticisi ile beraber çalışmak Ağ Donanım Yönetim birimi, Sunucu ve İnternet Sistemleri birimi sorumluluğundadır. Politikanın uygulanmasından Ağ Donanım Yönetim birimi, Sunucu ve İnternet Sistemleri birimi ekibi sorumludur.

5 Kurallar

ESOGÜ bünyesinde bulunan bilgi işlem merkezinde çeşitli ağ cihazları bulunmaktadır. Kullanılan bu ağ cihazlarının yönetiminin BGYS kapsamında uygun ve periyodik kontrol edilebilir bir şekilde yapılması sağlanmaktadır.
Ağ ekipmanı yönetimi için sorumlulukların ve prosedürlerin tanımlanması, ağlar ve bilgisayar faaliyetleri arasındaki görevlerin ayrılması, transit ve birbirine bağlı sistemlerdeki (örneğin VPN) verileri korumak için kriptografik çözümlerin kullanılması, kimlik doğrulama ve ağa bağlı kaynakların erişimini ve kullanımını kısıtlamak için kullanılan diğer yollar, izleme ve günlüğe kaydetme (örn. bir Saldırı Tespit Sistemi - IDS kullanarak) gibi genel kontroller seti uygulanmaktadır.
ESOGÜ bünyesinde ağ sistemlerinin yönetimi, ağ ekibi içerisinde geliştirilen ağ yönetim yazılımı üzerinden gerçekleştirilmektedir (NAC(network Access control)-libre yazılımı ile).
Ağ yönetimi konusunda belirli bir kural ve güvenlik çerçevesi oluşturulmuş. Personeller ağ yönetimine tehdit oluşturabilecek konularda duyarlı ve farkındadır.

Bütün yönlendirici ve anahtarlar minimum aşağıdaki konfigürasyon standartlarına sahiptir.

- Erişim listeleri belirlenmiştir.
- Kara liste veya beyaz liste kullanılarak varlıkların ağ erişimleri sınırlandırılmıştır.
- Network cihazlarının yönetim ağı son kullanıcı cihazlarından yalıtılması sağlanmıştır.
- Cihazlar üzerinde kullanılmayan ve güvenlik riskli servisler kapatılmıştır.
- ESOGÜ bünyesinde bulunan kabinetler, aktif cihazlar, UTP ve fiber optik aktarma kabloları, cihazların portları uygun ve anlaşılır bir şekilde etiketlenmiştir.

Ağ yönetiminde uyulması gereken minimum kurallar aşağıdaki standartlara sahip olması gerekir;

- Yönetimi ve işletmesi yapılacak ağın kapsamı tanımlanmış.

- Ağ topolojisi çıkartılmış. Topolojide anahtarlar, yönlendirme vb. unsurlar görsel olarak gösterilmiştir. Ağ topolojisi güvenli bir şekilde muhafaza edilmektedir. Ağ cihazlarının güncel yapılandırma bilgileri saklanmakta ve güncel sürümü kullanılmaktadır.
- Bilgisayar ağının işletme sorumluluğu ve bilgisayar sistemlerinin bakım/işletme sorumluluğu birbirinden ayrılmış durumdadır.
- İş sürekliliğini sağlamak için bilgisayar ağı yedeklenmesi ve sürekli olarak izlenmektedir.
- Erişime izin verilen ağlar, servisler ve yetkilendirme metotları çok iyi tanımlanmış ve kontrol altında tutulmaktadır
- Ağ üzerinde kullanıcıların erişeceği/erişebileceği gereksiz servisler kısıtlanmıştır.
- Uygulamaların gerektirdiği port tanımları sadece gerekli olan ağ ve güvenlik cihazlarında yapılmakta olup. Diğer gereksiz kısımlarda kapalı ve kısıtlıdır.
- İzin verilen kaynak ve hedef ağlar arası iletişimi sağlayan cihazları aktif olarak kontrol eden teknik önlemler alınmıştır.
- Güvenlik duvarlarında kullanılmayan servisler, portlar kapalı ve IP'lere kontrollü erişim izni verilmektedir.
- Ağ yönetimi konusunda yetkisiz kişiler müdahale etmemelidir. Yetkililerin görev ve sorumlulukları belirlenmiş ve yedekli bir yapı oluşturulmuştur.
- Ağ üzerinde pasif ve/veya aktif izleme ve günlüğü kaydetme sistemi mevcut ve alarmlar, anormallikler takip edilmektedir.
- Bilgisayar ağlarının ve bağlı sistemlerin iş sürekliliğini sağlamak için düzenli denetimler ve güncellemeler uygulanmaktadır.
- Erişimine izin verilen ağlar, ağ servisleri ve ilgili yetkilendirme yöntemleri belirlenmiş ve yetkisiz erişimle ilgili tedbirler alınmıştır.
- Gerek görülen uygulamalar için, portların belirli uygulama servislerine veya güvenli ağ geçitlerine otomatik olarak bağlanması sağlanmaktadır.
- Sınırsız ağ dolaşımı engellenmiştir. Ağ servisleri, varsayılan durumda erişimi engelleyecek şekilde olup, ihtiyaçlara göre serbest bırakılmaktadır.
- Harici ağlar üzerindeki kullanıcıları belirli uygulama servislerine veya güvenli ağ geçitlerine bağlanmaya zorlayıcı teknik önlemler alınmıştır.
- İzin verilen kaynak ve hedef ağlar arası iletişimi aktif olarak kontrol eden güvenlik duvarı gibi ağ cihazları yoluyla önlemler alınmış ve kayıtlar tutulmaktadır.

- Ağ erişimi VPN, VLAN gibi ayrı mantıksal alanlar oluşturularak sınırlandırılmıştır. Kurum kullanıcılarının bilgisayarlarının bulunduğu ağ, sunucuların bulunduğu ağ, DMZ ağı birbirlerinden ayrılmalı ve ağlar arasında geçiş güvenlik sunucuları (firewall) üzerinden sağlanmaktadır.
- Uzaktan teşhis ve müdahale için kullanılacak portların güvenliği sağlanmaktadır
- Bilgisayar ağına bağlı bütün makinelerde kurulum ve yapılandırma parametreleri, ESOGÜ BİDB güvenlik politika ve standartlarıyla uyum sağlanmıştır.
- Sistem tasarımı ve geliştirilmesi yapılırken ESOGÜ BİDB tarafından onaylanmış olan ağ ara yüzü ve protokolleri kullanılmaktadır.
- İnternet trafiği, İnternet Erişim ve Kullanım Politikası ve ilgili standartlarda anlatıldığı şekilde izlenebilmektedir.
- Bilgisayar ağındaki adresler, ağa ait yapılandırma ve diğer tasarım bilgileri 3. şahıs ve sistemlerin ulaşamayacağı şekilde saklanmaktadır.
- Ağ cihazları görevler dışında başka bir amaç için kullanılamaz.
- Ağ cihazları yapılandırılması Ağ Yöneticisi tarafından veya Ağ Yöneticisinin denetiminde/bilgisinde yapılmakta ve değiştirilmektedir.
- Ağ dokümantasyonu hazırlanmalı ve ağ cihazlarının güncel yapılandırma bilgileri gizli ortamlarda saklanmaktadır.
- ESOGÜ ağı üzerinden diğer iç ağlara veya internete bağlanacak olan tüm kullanıcıların Net yetki merkezi kimlik doğrulama sistemi üzerinden kullanıcı adı ve şifreleri ile giriş yapmaları sağlanmaktadır.
-
- Kurumun internete açık hizmetleri için olası DoS/DDoS saldırılarına karşı servis dışı kalmasını önlemek, iş sürekliliğini sağlamak amacıyla en az aşağıdaki önlemler alınmalıdır. (Güvenlik ürünleri üzerinde DoS/DDoS saldırılarına özel konfigürasyonların yapılması DDoS engelleme sistemlerinin sınırları ve yeteneklerinin düzenli aralıklarla test edilmesi ve sürekli iyileştirilmesi/güncellenmesi DDoS koruma için bir servis sağlayıcıdan hizmet temin edilmiş ise; servis sağlayıcıdan yukarıdaki şartlara göre hizmet verildiğine dair taahhüt alınması, tedarik şartname ve sözleşmelerinde bu hususların belirtilmesi)

Ağ bağlantı istekleri aşağıdaki şekilde yapılmalıdır.

- Ağ üzerinde yapılan istekler prosedürde belirlenen kurallar çerçevesinde yapılmaktadır.
- Yapılan ağ istekleri servis masası üzerinden istek oluşturarak yapılmaktadır.

- Dışarıdan yapılan ağ istekleri ise web sitesinde yayınlanan formlar doldurularak veya EBYS veya servis masası üzerinden istekler ile kayıt altına alınmaktadır.

IP Kullanımı aşağıdaki şekilde yapılmalıdır.

- **Yetkisiz Kullanım Yasağı:** Kurum ağındaki IP adresi dağıtımı için yalnızca Bilgi İşlem Daire Başkanlığı yetkilidir. Kullanıcılar, kendilerine tahsis edilen IP adreslerini izinsiz değiştiremez, manuel (statik) IP tanımlayamaz veya başka bir kullanıcı/cihaz ile paylaşamaz.
- **Tahsis ve Kayıt:** Tüm IP talepleri resmi bir talep süreciyle **destek.ogu.edu.tr** üzerinden yapılmalı; IP adresinin hangi cihaz (MAC adresi) ve hangi kullanıcı için ayrıldığı, ilgili envanter listesinde güncel tutulmalıdır.
- **Kullanım Amacı:** Tahsis edilen IP adresleri yalnızca iş tanımlarına uygun cihazlarda kullanılabilir. Kişisel cihazların ağa dahil edilmesi ve bu cihazlara IP tanımlanması, ilgili birimin onayı ile gerçekleştirilir.
- **Dinamik IP Önceliği:** Standart kullanıcı cihazları için DHCP (Dinamik Ana Bilgisayar Yapılandırma Protokolü) kullanımı esastır. Manuel (statik) IP, yalnızca sunucular, ağ yazıcıları ve özel ağ donanımları gibi zorunlu durumlar için atanır. EBYS üzerinden resmi yazı ile talep edilir.

İşten Ayrılan Personel ve IP Kayıtlarının Silinmesi

- **İlişik Kesme Süreci:** İşten ayrılan personelin üzerine kayıtlı olan tüm statik IP adresleri, DHCP rezervasyonları ve DNS kayıtları, personelin son çalışma gününde Bilgi İşlem birimi tarafından iptal edilerek boşa çıkarılır.
- **Erişim Yetkilerinin Kaldırılması:** IP adresine bağlı olarak tanımlanmış özel güvenlik duvarı (Firewall) kuralları, VPN erişim izinleri ve VLAN geçiş yetkileri, personelin ayrılış bildirimiyle eş zamanlı olarak pasif hale getirilir.

6 Yaptırım

Bu politikanın ihlal edilmesi durumunda BGYS yöneticisi tarafından gerekli personel desteği de alınarak ihlal nedeni incelenir. İhlal kasıtsız olup personelin eğitim vb. bir eksikliğinden kaynaklanıyorsa problemin kaynağını oluşturan eksikliği kapatmak için çalışma yapılır. Personel BGYS Yöneticisi tarafından e-posta üzerinden yazılı olarak uyarılır.
Eğer ihlal işleminin kasıtlı olduğu anlaşılırsa veya kasıtsız olan ihlaller 3'ten fazla tekrar ederse 657 sayılı devlet memurları kanunu ve Üniversite resmi yazısıyla belirtilen ilave yaptırımlar gereğince personel hakkında işlem yapılır.

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI

Tüm çalışanlar, güvenlik ihlali olaylarını ve bu politikanın ihlallerini, Olay İhlal Yönetimi Prosedüründe tanımlanan şekilde en kısa sürede bildirme sorumluluğundadır.

7 İlgili Dokümanlar

PR.12- OLAY İHLAL YÖNETİM PROSEDÜRÜ

Hazırlayan	Kontrol Eden	Onaylayan
BİLGİ GÜVENLİĞİ BİRİMİ	BİDB ŞUBE MÜDÜRÜ	BİDB DAİRE BAŞKANI