MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

AĞ GÜVENLİĞİ YÖNETİMİ PROSEDÜRÜ

İçindekiler

1 Amaç

Bu dokümanın amacı, kuruluş ağındaki bilgi ve destekleyici bilgi işleme olanaklarının korunmasını sağlamaktır.

2 Kapsam

Bu doküman Bilgi Güvenliği Kapsamı dokümanında belirtilen ağ ve destekleyici bilgi sistemlerini kapsamaktadır.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi
SNMP	Ağ cihazlarında yönetimsel bilgi alışverişinin sağlanması için oluşturulmuş bir uygulama katmanı protokolü
VLAN	Sanal yerel alan ağı anlamına gelen VLAN, yerel ağ içerisinde çalışma grupları oluşturmak, yerel ağı anahtarlarla bölmektir
IP	Ağ üzerinden veri alışverişi yapmak için kullandıkları adres
SNMP Community	SNMP yetkilendirme bilgileri
SSH	Güvenli veri iletimi için kriptografik ağ protokolüdür
Firmware	Donanımın kendisinden beklenen işlevleri yerine getirebilmesi için kullandığı yazılımlara verilen addır

UPS	Kesintisiz güç kaynağı

5 İşlem Detayı

5.1 Ağ Güvenliği Mimarisi

Ağ güvenliği için ilk önce doğru mimari oluşturulmalıdır. Ağlar erişim ihtiyaçlarına göre ayrılmalı ve ayırılan ağlar üzerinden gerektiği kadar erişim yetkileri tanımlanmalıdır.

Ağ blokları tasarlanırken bu ağda erişilecek varlıklara kimler erişecek, varlıklar üzerinde ne tür bilgiler olacak ve bu bilgilerin önem ve gizlilik dereceleri gibi konular göz önünde bulundurulmalıdır. Buna göre ek güvenlik önlemleri (Saldırı tespit ve önleme sistemleri, fiziksel olarak ayrılmış ağlar vb.) alınmalıdır.

Kimlik doğruluma yöntemleri kullanılmalı servis sağlayıcıların ve kullanılan cihazların yetenekleri ve bağlantı kapasitesi gereksinimleri analiz edilerek planlama yapılmalıdır.

5.2 Ağ Altyapısı İlkeleri

Kurumun ağ altyapısı ilkeleri en az yılda bir kez olmak üzere gözden geçirilmeli ve gerekli olan değişiklikler yapılmalıdır.

1. Ağ alt yapısı yönetimi onaylanmış prosedür ve talimatlara göre yapılır.
2. Ağlar için operasyonel sorumluluklar görevlerin ayrılığı ilkesine göre belirlenir.
3. Network içerisinde ayrı VLAN yapıları olması zorunludur. Kritik sistemler ve kullanıcı bilgisayarları aynı VLAN (ağ segmentleri) üzerinde bulundurulmaz.
4. VLAN'lar arası trafik, erişim ihtiyacına uygun olarak, gerektiği kadar ilkesine göre tanımlanır.
5. Halka açık ağlar için özel kontroller uygulanmalıdır. "Bilgi Sistemlerinin Güvenlik Gereksinimleri Prosedürü" ile açıklanmıştır.
6. Dış IP bloğunda internete doğrudan açık sunucular bulundurulmaz. Kontrollü şekilde izinler tanımlanmalıdır.
7. Kullanıcıların hizmet aldığı sunuculara kurum iç ağından tam erişim izni verilmemelidir.
8. Ağ hareketleri izlenir ve kayıt altına alınır.
9. Kurum ağı içerisinde erişim yönetimi sadece gerekli olan sunuculara sadece gerekli olan portlarla sağlanacak şekilde tasarlanır.

10. Ağ altyapı cihazlarında kimlik doğrulama açık olacaktır. Anahtarlama cihazında kimlik doğrulama; cihaza yönetimsel veya denetimsel erişim söz konusu olduğu zaman kişinin doğru kişi olup olmadığının kontrolü sağlanacaktır.
11. Ağ altyapı cihazlarındaki SNMP community adları varsayılan olarak gelen public ve private değerleri değiştirilir.
12. Ağ altyapı cihazlarında kullanılmayan servisler kapatılır. Aktif servisler sürekli kontrol edilerek işlem görmediğinde kapatılır.
13. Ağ altyapısında cihazlar için firmware'leri kararlı çalışan güncel sürümleri bulundurulur.
14. Ağ altyapısında cihazların firmware ve konfigürasyonlarının yedeği alınır.
15. Ağ altyapı cihazlarına fiziksel erişim ile (konsol bağlantısı ile) veya uzaktan erişim (telnet, web, ssl, ssh üzerinden, yönetim yazılımı veya SNMP ile) bağlantıları için kimlik kontrolü yapılır.
16. Ağ altyapı cihazlarının şifreleri varsayılan olarak gelen değerlerden değiştirilecek ve güçlü şifreler konularak yetkisi olmayan kişilerin bilmemesi sağlanmalıdır.
17. Ağ altyapı cihazlarının bulunduğu ortamlar toz, sıcaklık nem gibi ortamlardan korunmalı, düzenli olarak temizlenmelidir.
18. Ağ alt yapısı aktif dizin üyesi olmayan bilgisayar ve ağ bağlantı yeteneği olan her tür donanım mevcut ağ içerisine girmesi engellenmeli, kurallar belirlenerek uygunluk onayı ile geçiş sağlanmalıdır.
19. Kablosuz iletişim ile ilgili gereklilikler aşağıda belirtilmiştir:
    a. Ağ erişim kontrol yazılımı ile kullanıcı kimlik doğrulama kullanılmalıdır.
    b. Varsayılan SSID isimleri kullanılmamalıdır. SSID yayan bilgisi içerisinde kurumla ilgili bilgi olmamalıdır.
    c. Radyo dalgalarının binanın dışına taşmamasına özen gösterilmelidir. Bunun için çift yönlü antenler kullanılarak radyo sinyallerinin çalışma alanında yoğunlaşması sağlanmalıdır.

5.3 Ağ Yönetimi Prosedürleri

1. Ağ cihazları jeneratör veya yedek UPS ile güç kaynağı açısından yedekli çalışması zorunludur.

2. Kurumda en az iki kişinin ağ servisini oluşturan bileşenlerin güvenliği ve işletimi konusunda bilgi sahibi olacak şekilde gerekli düzenlemeler yapılır.
3. Kurum anahtarlama cihazları yüksek erişilebilirlik gereksinimlerini karşılayacak şeklide dizayn edilir. Bu cihazlarda yapılacak herhangi bir işlemde sistemin aksamaması için konfigürasyonlar ve denemeler "İşletim Prosedürleri ve Sorumlulukları Prosedürü" değişiklik yönetimi başlığına göre yapılmalıdır.
4. Ağ trafiği düzenli olarak izlenir ve ölçülür.
5. Kurum ağına direkt kablo takarak erişim engellenir.
6. Aktif cihazlarda yapılandırma portları yetkisiz erişimlere karşı parola ile korunmalı veya kapatılmalıdır.
7. Tüm ağ (Firewall, IPS, Ana omurga ve Aktif cihazlar) yönetimi ve yapılanması Bilgi İşlem tarafından yürütülür.
8. Ağ erişim yönetimi iç ve dış erişimler olarak ayrı ayrı takip edilir ve düzenlenir.
9. İnternet çıkışları güvenlik duvarı ile yönetilmektedir.
10. Dış bağlantılar SSL VPN ile yapılır.
11. 3. Taraflar dış bağlantı talepleri "Uzaktan Çalışma Politikası" 'na göre yapılır.
12. Her bir yönlendirici ve anahtar aşağıdaki uyarı yazısına sahip olmalıdır:

    "Bu cihaza yetkisiz erişimler yasaklanmıştır. Bu cihaza erişim ve yapılandırma için yasal hakkınız olmak zorundadır. Bu cihaz üzerinde işletilen her komut loglanabilir, bu politikaya uymamak disiplin kuruluna sevk ile sonuçlanabilir veya yasal yaptırım olabilir."

5.4 Güvenlik Duvarı Esasları

1. Güvenlik duvarı üzerindeki yapılandırmalar sadece uzman ve konu ile bilgili Bilgi İşlem yetkili personeli tarafından yapılır.
2. Güvenlik duvarı üzerinde ANY (her taraftan) TO ANY (her tarafa) açık kurallar tanımlanmaz.
3. Mümkün olduğunca yazılan kurallar servis tabanlı açılır.
4. Kritik sistemlere erişimlerde erişen ip ve servis güvenlik duvarı kuralları üzerinden kısıtlanır.
5. Kritik sistemlere olan erişimler mutlaka kayıt altına alınarak başka bir ortam da saklanır.

6. Güvenlik duvarı üzerinde tanımlanan servisler, sunucular veya gruplar mutlaka ismi anlaşılabilir şekilde isimlendirilir.
7. Yeni kural eklenirken, mutlaka ekleme sebebi, kimin tarafından eklendiği ve kural içeriği kayıt altına alınır.
8. Yeni yazılacak kurallar da mutlaka paketin gidiş ve dönüşü göz önünde bulundurularak güvenlik şartlarına uygun olarak yazılır.
9. Güvenlik duvarı kayıtlarının saklandığı sistem sadece yetkili kişiler tarafından erişilecek şekilde yetkilendirilir.
10. Güvenlik duvarı SNMP adı mutlaka public veya private gibi varsayılan değerlerden farklı olmalıdır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					