1. GİRİŞ

OSTİM Teknik Üniversitesi bünyesinde yönetilen ağ cihazlarının güvenliğinin sağlanması, bilgisayar korsanlığı, bilgi çalma, yetkisiz erişim gibi birçok güvenliği tehlikeye düşürecek riskin önüne geçmek için gereklidir. Bu maksatla İBB "Ağ Cihazları Güvenlik Prosedürü" hazırlanmıştır. Bu prosedür doğrultusunda ağ cihazların güvenli yönetim ve işletimi sağlanmaktadır.

2. TANIMLAR VE KISALTMALAR

- **CCTV:** Kapalı Devre Televizyon Sistemi
- **VLAN:** Sanal Özel Ağ
- **ARP:** Address Resolution Protocol
- **DHCP:** Dynamic Host Configuration Protocol
- **ESSID:** Extended Service Set Identifier
- **FQHN:** Fully Qualified Hostnames
- **IP:** Internet Protocol
- **ISS:** İnternet Servis Sağlayıcı
- **LAN:** Local Area Network
- **VLAN:** Virtual Local Area Network
- **NPS:** Network Policy Server
- **RADIUS:** Remote Authentication Dial In User Service
- **UTP:** Unshielded Twisted Pair
- **VTP:** VLAN Trunking Protocol
- **LLDP:** Link Layer Discovery Protocol
- **SSID:** Service Set Identification
- **WPA:** Wi-Fi Protected Access
- **GD:** Güvenlik Duvarı
- Microsoft Azure Cloud Services

- **İzleme Yönetim Yazılımı:** Ağ cihazlarının sağlık durumlarının izlendiği, önceden belirlenen eşik değerlerinin altında/üstündeki değerlere göre alarm üreten uygulamalar.
- **Sistem Odası Envanter Uygulaması:** Sistem odasında bulunan tüm aktif/pasif ağ cihazları, sunucu yedekleme ünitesi vb. cihazların fiziksel konumunun/IP adreslerinin tutulduğu, Kurum bünyesinde kullanılan tüm IP bloklarının listelendiği ve yönetildiği, Yük Dengeleme ve NAT listelerinin tutulduğu uygulamadır. RackTables uygulaması bu sınıfa girer.
- **Patch Panel:** Ağ kabloların hepsinin toplandığı kabin ya da kabinetlerin içinde bütün kabloların toplandığı priz gruplarıdır.
- **Trunk Port:** Birden fazla VLAN'ı tek bir bağlantı hattı ile taşımaya olanak veren Ethernet trunking protokolünün devreye alındığı Ethernet anahtar portu.
- **Uplink/Downlink:** Ağ hiyerarşisinde, bir üst/alt aktif ağ cihazına olan bağlantı hattı.
- **Fail-Open**: Bir arıza durumunda trafiğin akmasını sağlama.

3. AMAÇ VE KAPSAM

Bu prosedürün hazırlanmasında ağ ve sistem yöneticilerine ağ cihazlarında ve işletim sistemlerinde uygulanabilecek güvenlik önlemlerinin belirtilmesi amaçlanmıştır. Yönetilen tüm ağ cihazları bu prosedürün kapsamındadır. İleriki tarihlerde gerek teknolojik değişimler gerekse sistem bileşen değişiklikleri çerçevesinde bu prosedür güncellenmelidir.

4. AĞ CİHAZLARI GÜVENLİK PROSEDÜRÜ

4.1 Genel İlkeler

• Kurum tarafından yerel alan ağı ile geniş alan ağı üzerinden verilen hizmetlerin kesintisiz bir şekilde verilebilmesini sağlayan birçok farklı cihaz vardır. Bu cihazların kurulumu, yapılandırılması ve yönetilmesi BYDB tarafından işbu dokümanda anlatıldığı şekilde yapılır.

• Kurum bünyesinde kullanılan IP adresleri tek bir merkezden yönetilir. Kurulum, bakım, yenileme ve benzeri faaliyetler için cihazlara IP adresi atanmadan önce işbu dokümandaki süreçler işletilir.

4.2 IP Adres Havuzu Yönetimi

• Kurum bünyesinde kullanılan tüm IP adresleri tek merkezden yönetilir. IP adres havuzunun yönetimi BYDB tarafından yapılır.

• Kullanıcı IP adresleri merkezi DHCP sunucu üzerinden otomatik olarak dağıtılır. Merkezi DHCP sunucusunun yönetimi Bilgi Yönetim Daire Başkanlığı tarafından yapılır.

• Sunucu, ağ ve güvenlik cihazları, IP adresi kullanan altyapı cihazlarının (iklimlendirme kontrol ünitesi, ortam izleme ünitesi vb.) IP adresleri ilgili cihazdan Bilgi Yönetim Daire Başkanlığı tarafından cihaza statik olarak tanımlanır.

• Güvenlik duvarı üzerinden kural yazılacak IP adresleri için DHCP üzerinde rezervasyon yapılır.

• Statik olarak tanımlanan IP adresleri elle veya otomatik olarak Bilgi Yönetim Daire Başkanlığı tarafından girilir.

• Statik IP adresi isteği, oluşturulan bir değişiklik ile tetiklenir. Değişiklik isteği onaylandıktan sonra kullanılacak IP adresleri, kaydedilir ve isteği yapan birime iletilir.

4.3 Ağ Uygulamaları Yönetimi

• Ağ cihazları ile ilgili bilgiler Ruijie Cloud ile kayıt altına alınmaktadır.

• Ağ cihazlarının yapılandırma dosyalarının yedekleri İzleme Yönetim Yazılımı üzerinde tutulur; güncellemeler İzleme Yönetim Yazılımı üzerinden izlenir.

5.4. Ağ Cihazları Kurulumu ve Yönetimi

• Ağ cihazlarını birbirine, sunucu ve aktif cihazları ağ cihazlarına bağlamak için fabrikasyon UTP/Fiber kablolar kullanılır. Cihazlar arasındaki bağlantılar patch paneller üzerinden yapılır.

• Ağ cihazlarının yönetimi Bilgi Yönetim Daire Başkanlığı tarafından yapılır.

• Ağ cihazlarının yönetimi, cihaz üzerinde varsa yerleşik bulunan adanmış yönetim portları üzerinden yok ise omurga anahtara erişebilen trunk portu üzerinden yapılır. Bu durumlar dışında, cihaz üzerinde kullanılabilir ilk port yönetim portu olarak tanımlanır.

• Ağ cihazlarının yönetimi için SSH v2 kullanılmaktadır. Komut satırının yetersiz olduğu durumlarda HTTPS protokolü devreye alınır.

• Ağ cihazlarının yönetim ara yüzlerine sadece belirli IP adreslerinin (Ağ Yönetim Ekibinin kullandığı bilgisayarların IP adresleri ile izleme sunucularının IP adresleri) erişimine izin verilir.

• Ağ cihazları yönetimi için izole bir VLAN ve bu VLAN'a özgü bir IP bloğu kullanılır. Bu VLAN'a sadece Bilgi Yönetim Daire Başkanlığı erişmesini sağlayacak şekilde güvenlik duvarı üzerinden erişim kısıtlanır.

• Yönlendirme yapmayan ağ cihazları üzerinde IP adresi üzerinden yönetilir.

• Ağ cihazları üzerinde planlanmamış herhangi bir değişiklik yapılmaz.

• Ağ cihazları üzerinde planlı bir değişiklik yapılmadan önce yapılandırma dosyası yedeği alınır.

• Yeni bir ağ cihazı devreye alınmadan önce aşağıdaki adımlar gerçekleştirilir:

◦ Cihazın fiziksel muayenesi yapılır.

◦ Cihazın üzerindeki yapılandırma dosyası yedeklenir ve tamamen silinir.

◦ Cihaz üzerine üretici firma tarafından sağlanan ve Kurum tarafından kullanılan en güncel işletim sistemi kurulur ve yazılımsal muayenesi yapılır.

◦ Yapılandırma şablon dosyası ağ cihazı üzerine yüklenir ve gerekli özelleştirmeler yapılır.

◦ Cihazın adı, IP adresi, fiziksel konumu vb. bilgileri İzleme Yönetim Yazılımına girilir.

• Ağ cihazları üzerinde uplink / downlink portları ile sunucu ve diğer ağ cihazlarının bağlı olduğu portlara o cihaz ile ilgili tanımlayıcı bilgi cihaz konfigürasyonuna girilir.

• Ağ cihazları üzerinde güvenlik nedeniyle kullanılmayan protokoller (VTP vb.) ile kullanılmayan özellikler devre dışı bırakılır.

• CDP ve LLDP gibi protokoller sadece başka bir ağ cihazına bağlanan portlarda etkinleştirilir diğer portlarda devre dışı bırakılır.

5.5. Omurga Ağ Cihazlarında Güvenlik Fiziksel Güvenlik

• OSTİM Teknik Üniversitesi bünyesinde kullanılan omurga anahtarlama cihazları fiziksel güvenlik önlemleri alınmış, erişim denetimi uygulanan sistem odalarında yerleştirilmiştir.

• Omurga anahtarlama cihazları dışında ofislere dağıtım için kullanılan anahtarlama cihazları kolay erişilemeyecek yerlerde, mümkün olduğu yerlerde ise kamera ile izlenebilen / kaydedilebilen yerlerde konumlandırılmıştır.

• Tüm ikinci katman (Layer 2) anahtarlama cihazları yönetilebilen cihazlardan seçilmeli. Hub benzeri yönetilemeyen ağ cihazları kullanılmamaktadır.

Ağlarda Ayrım

• OSTİM Teknik Üniversitesi bünyesinde lokasyon bazında ikinci katman ayrımı VLAN ile yapılmaktadır.

• Özel amaçlı VLAN'lar arasında geçişler erişim denetimi altında tutulmalı doğrudan yönlendirme yapılmamalıdır. Default VLAN1 kapatılmalı, varsayılan VLAN olarak başka VLAN kullanılmaktadır.

• Canlı sistemler, test sistemleri geliştirme ortamları, iş istasyonları farklı VLAN'larda hizmet vermektedir.

• Yerel ağda oluşturulan her bir VLAN için bir IP bloğu tanımlanır. Bu blok 255 IP'lik (C class) bir subnet'ten daha büyük olamaz. Bu VLAN'lar güvenlik gereksinimlerine bağlı olarak güvenlik duvarında ya da omurga ethernet anahtar üzerinde (veya omurga ethernet anahtar görevi yapan ethernet anahtar üzerinde) sonlandırılmıştır.

• Bir VLAN içerisinde birden fazla ağ geçidi kullanılmamaktadır.

İkinci Katman Güvenliği

• Gerek performans gerekse güvenlik sebebiyle uygun yerlerde ikinci katman erişim denetimi uygulanmalıdır. Bunun için portlara bağlantı sayısına limit koymak amacıyla port güvenliği uygulanmaktadır.

• IP ataması otomatik sistemler aracılığı ile DHCP sunucularla yapılmaktadır. Kasıtlı veya kasıtsız IP adresi atamalarının önüne geçmek için uygun seviyedeki ağ cihazlarında DHCP yayınım sunucusu (DHCP relay server) yapılandırması yapılmaktadır.

• Yetkisiz DHCP sunucuların engellenmesi için DHCP Snooping yapılmalıdır. Ayrıca Mac/IP aldatmaları için IP Source Guard konfigürasyonu uygulanmaktadır.

• Kullanılmayan portlar kapatılmalıdır.

Yetkilendirme ve Kimlik Doğrulama

• Ağ cihazlarına yönetim maksatlı erişimlerde kimlik doğrulama uygulanmalıdır.

• Üretici firmanın ilk yapılandırmasında kullanılan kullanıcı adı ve parolalar mutlak değiştirilmeli, özelleştirilmelidir.

Servis Güvenliği

• Ağ cihazlarında kullanılmayan servisler kapatılmıştır.

• Kullanılan servislerin güvenli sürümleri kullanılmaktadır. Güncelleme

• Ağ cihazlarında üretici firmanın yayımladığı güvenlik açıklıkları ile ilgili tüm güncel sürümler yüklüdür.

• Güvenlik ile ilgili olmayan güncel sürümlerin yüklenmesi kümülâtif olarak yapılabilir. Yönetim Güvenliği

• Ağ cihazlarının yönetimi güvenli kanallardan yapılmalı yapılandırma bilgilerinin şifreli olarak gitmesi için https, ssl, ssh gibi şifreli kanallar kullanılarak yönetim gerçekleştirilmektedir.

• Telnet, http gibi açık veri kanalları ile yönetim yapılmamalı, kapatılması mümkün olan ağ cihazlarında kapatılmıştır.

• Tüm yönetici eylemleri loglanmaktadır.

Yönlendirme ve Üçüncü Katman Güvenliği

• Yönlendirme cihazlarında kullanılan protokol (RIP, OFPF, IS-IS) çerçevesinde güvenli sürümleri kullanılmaktadır. (Ör: RIP v2:)

• İzlenebilirliğin sağlanması için, yönetimden sorumlu birden fazla kişinin olması durumunda uygun olan cihazlarda her yönetici için ayrı bir kullanıcı adı kullanılmaktadır.

5.6. Kablosuz Ağ Güvenliği SSID Yayınımı

• OSTİM Teknik Üniversitesi bünyesinde kullanılan kablosuz erişim noktalarında tek bir SSID kullanılmaktadır.

• Gereksiz yayınımın önüne geçmek için erişim noktalarının konumları mümkün olduğunca bina merkezine yakın seçilmiştir.

• Gerekli durumlarda SSID isimlendirmesi, OSTİM Teknik Üniversitesi ile bağdaştırılmayacak şekilde yapılmıştır. Yetkilendirme ve Kimlik Doğrulama

• Kimlik doğrulama için etki alanı verileri kullanılmalı, etki alanı parolası ile kimlik doğrulama gerçekleştirilmiştir. Yönetim Güvenliği

• Uygun erişim noktalarında şifreli kanallar üzerinden yönetim gerçekleştirilmelidir. http, telnet gibi açık iletişim yapılan kanallardan yönetim gerçekleştirilmemektedir.

• Takip edilebilirliğin sağlanması için, yönetimden sorumlu birden fazla kişinin olması durumunda uygun olan cihazlarda her yönetici için ayrı bir kullanıcı adı kullanılmaktadır.

• Tüm yönetici eylemleri loglanmaktadır.

Ağlarda Ayrım

• Uygun erişim noktalarında VLAN tabanlı çoklu SSID kullanılmaktadır.

• Bunlardan biri misafir internet erişimi için kullanılırken diğeri kurumsal amaçlı kullanılmaktadır.

• Bu kontrol donanım bağımlı olası sebebiyle tüm erişim noktalarında uygulanması zorunlu değildir. Uygun erişim noktalarında uygulanabilmektedir.

5.7. Santral ve Telefon Sistemi Güvenliği

• Kullanılan santral yazılım güvenlik güncellemeleri en kısa zamanda uygulanmaktadır.

• Kullanılan IP telefonlara erişim için kimlik doğrulama uygulanmaktadır.

5.8. Güvenlik Ürünleri Konfigürasyonu Temel Gereksinimleri

Güvenlik duvarı, saldırı tespit ve engelleme sistemleri ve içerik kontrolcüleri üzerinde alınabilecek önlemler bu bölümde sıralanmıştır.

5.8.1. Güvenlik Duvarı

• OSTİM Teknik Üniversitesi bünyesinde, ağlar arasındaki erişimi ve güvenliği kontrol etmek amacıyla merkezi Güvenlik Duvarı (F/W) kullanılır.

• F/W'nin yönetimi Güvenlik Yönetim Ekibi tarafından yapılır ve yapılacak değişikler kayıt altına alınır.

• Merkezi yönetim sunucusunda, güvenlik duvarlarında çalışan yapılandırma dosyaları tutulur.

• F/W'de IP ve Port bazlı kurallar yazılır.

• F/W yedekleri merkezi yönetim sunucusu üzerinden haftalık olarak alınır.

• F/W ara yüzüne sadece yönetici IP'leri erişebilir.

• F/W firmware güncellemeleri kesinti yaşanmaması için daha önceden belirlenen bir tarihte sırası ile ve kontrollü bir şekilde yapılır.

Sistem Güncelliği

• Güvenlik duvarlarında üretici firmanın yayımladığı güvenlik açıklıkları ile ilgili tüm yamalar yüklü olmalıdır.

• Güvenlik ile ilgili olmayan yamaların yüklenmesi kümülâtif olarak yapılabilir. Servis Güvenliği • Güvenlik duvarında yönetim arayüzü haricinde hiçbir arayüzü üzerinde açık bir servis bulunmamaktadır.

Kural Tablosu

• Güvenlik duvarı kural tablosu olabildiğince sade tutulmaktadır.

• Benzer kurallar gruplandırılmıştır.

• Uygun kurallarda, kuralların geçerlilik tarihi zamanı ayarlanmıştır.

Yönetim Güvenliği

• Tüm güvenlik duvarları için şifreli kanallar üzerinden yönetim gerçekleştirilmelidir. Http, telnet gibi açık iletişim yapılan kanallardan yönetim gerçekleştirilmemektedir.

• Takip edilebilirliğin sağlanması için, yönetimden sorumlu birden fazla kişinin olması durumunda her yönetici için ayrı bir kullanıcı adı kullanılmaktadır.

• Tüm yönetici eylemleri loglanmaktadır.

Kural Tablosu Güvenliği

• Saldırıların tespiti ve engellenmesi için kullanılan cihaz ve sistemlerde saldırı imza kayıtlarının güncelliği sağlanmaktadır.

• Mümkün olacak en güvenli durum için canlı güncelleme yapılandırmasının yapılması manuel müdahaleye gerek kalmaksızın imza güncellemesi yapılması için gerekli yapılandırma yapılmaktadır.

Yönetim Güvenliği

• Tüm saldırı tespit ve engelleme sistemleri için şifreli kanallar üzerinden yönetim gerçekleştirilmelidir. Http, telnet gibi açık iletişim yapılan kanallardan yönetim gerçekleştirilmemektedir.

• Takip edilebilirliğin sağlanması için, yönetimden sorumlu birden fazla kişinin olması durumunda her yönetici için ayrı bir kullanıcı adı kullanılmaktadır.

• Tüm yönetici eylemleri loglanmaktadır.

4.3.1 İçerik Filtreleme Sistemleri

Filtre kuralları

• İçerik filtrele kural listesi güncel tutulmaktadır.

• Erişilmesinde kanunen veya kurumsal politika gereği sakınca görülen internet kaynaklarına erişim mutlak engellenmektedir.

Yönetim Güvenliği

• Takip edilebilirliğin sağlanması için, yönetimden sorumlu birden fazla kişinin olması durumunda her yönetici için ayrı bir kullanıcı adı kullanılmaktadır.

• Tüm yönetici eylemleri loglanmaktadır.

5.REVİZYON GEÇMİŞİ

Revizyon No	Tarih	Açıklama
01	07.11.2024	Entegre Kalite Yönetim Sisteminde kalite yönetiminde zorluklar ile karşılaşılması sebebiyle ISO 9001 Kalite Yönetim Sistemi (KYS) ve ISO 27001 Bilgi Güvenliği Yönetim Sisteminin (BGYS) ve dokümanlarının ayrılması ve ayrı ayrı takip edilmeleri kabul edilmiştir. Bu sebeple doküman kodlamalarında revizyon yapılmıştır.

Hazırlayan	Kontrol Eden	Onaylayan
İlknur ALŞAHİN Kalite Birimi	Kenan IŞIK Kalite Koordinatörü	Prof.Dr. Murat Ali YÜLEK Rektör
E-imzalıdır/paraflıdır	E-imzalıdır	E-imzalıdır