1. AMAÇ

Bu prosedürün amacı; Bursa Uludağ Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde kullanılan tüm bilgi sistemlerinin (sunucu, ağ cihazı, güvenlik cihazı, yazılım, veri tabanı vb.) güvenli, standartlara uygun, kontrol edilebilir ve izlenebilir şekilde yapılandırılmasını, yapılandırma değişikliklerinin yönetilmesini ve yetkisiz değişiklik risklerinin azaltılmasını sağlamaktır.

2. KAPSAM

Bu prosedür; kurumun sahip olduğu veya hizmet olarak aldığı tüm sunucu, ağ cihazı, güvenlik cihazı, veri tabanı, sanallaştırma platformu, işletim sistemi ve uygulama yapılandırmalarını kapsar.

3. TANIMLAR

Konfigürasyon: Bir bilgi sisteminin çalışmasını sağlayan ayarların, parametrelerin ve bileşenlerin bütünü.
Güvenli Yapılandırma: Cihaz veya sistemin saldırı yüzeyini azaltacak şekilde en iyi güvenlik uygulamalarına göre yapılandırılması.
Yetkili Personel: Sistem, ağ veya güvenlik yapılandırması yapma yetkisi olan personel.

4. SORUMLULUKLAR

Sistem Yönetimi Ekibi: Sunucu ve işletim sistemi konfigürasyonlarını yönetir.
Ağ Yönetim Ekibi: Ağ cihazlarının konfigürasyonlarını yönetir.
Siber Güvenlik Ekibi: Güvenlik konfigürasyon standartlarını belirler.
Yazılım Ekibi: Uygulama konfigürasyonlarını yönetir.
BGYS Yönetim Temsilcisi: Uyumun sürdürülebilirliğini sağlar.

5. UYGULAMA

5.1. Güvenli Yapılandırma Standarlarını Oluşturulması

5.1.1. Her cihaz tipi için güvenli yapılandırma standartları hazırlanır (ör. Windows sunucu güvenlik rehberi, switch konfigürasyon standardı, firewall politikaları).
5.1.2. Standartlar yılda en az bir kez gözden geçirilir.
5.1.3. Yeni cihazlar kurulumdan önce bu standartlara uygun hale getirilir.

5.2. Konfigürasyonların Dökümantasyonu

5.2.1. Her cihazın güncel konfigürasyonu kurumsal depolama alanında saklanır.
5.2.2. Konfigürasyon yedekleri cihaz tipine göre belirlenen periyotta (haftalık/aylık/yıllık) alınır.
5.2.3. Her konfigürasyon dosyası; cihaz adı, lokasyon, tarih, sürüm bilgilerini içerir.
5.2.4. Yapılandırma dosyaları şifreli olarak saklanır.

5.3. Yapılandırma Değişikliklerinin Yönetimi

5.3.1. Her değişiklik Değişiklik Yönetimi Prosedürü'ne uygun olarak kayıt altına alınır.
5.3.2. Planlanmamış/acil değişikliklerde işlem sonrasında mutlaka kayıt açılır.
5.3.3. Hiçbir çalışan kendi başına onaysız değişiklik yapamaz.
5.3.4. Değişiklik sonrası test yapılmadan sistem canlıya alınamaz.

5.4. Yetkilendirme Kontrolü

5.4.1. Konfigürasyon yapma yetkisi sadece ilgili yöneticiler tarafından verilen personele tanımlanır.
5.4.2. Yönetim arayüzlerine erişim IP kısıtlamaları ile sınırlandırılır.

5.4.3. Tüm yönetim işlemleri loglanır ve loglar izlenir.

5.5. **Güvenli Konfügürasyon Gereklilikleri**

Aşağıdaki maddeler tüm sistemler için zorunludur:

5.5.1. Gereksiz servisler devre dışı bırakılır.
5.5.2. Varsayılan şifreler değiştirilir.
5.5.3. Güçlü parola politikası uygulanır.
5.5.4. Yönetim arayüzlerine yalnızca yetkili IP'lerden erişim sağlanır.
5.5.5. Güncel yamalar düzenli uygulanır.
5.5.6. Loglama açık ve merkezi log sunucusuna yönlendirilmiş olmalıdır.
5.5.7. Yönetim bağlantıları (SSH, HTTPS vb.) şifreli yapılır.
5.5.8. Eski ve kullanılmayan hesaplar kapatılır.

5.6. **Otomatik Zafiyet ve Konfigürasyon Denetimleri**

5.6.1. Zafiyet taramaları en az yılda bir gerçekleştirilir.
5.6.2. Konfigürasyon uyumluluk taramaları (CIS benchmark vb.) yılda bir yapılır.
5.6.3. Tespit edilen kritik bulgular en geç 30 gün içinde giderilir.

5.7. **Acil Durumda Yapılandırma Değişikliği**

5.7.1. Kritik servis kesintisinde acil konfigürasyon yapılabilir.
5.7.2. İşlem sonrası mutlaka kayıt oluşturulur ve standart değişiklik sürecine sonradan dahil edilir.

5.8. **Konfigürasyonların Saklanması**

5.8.1. Konfigürasyon yedekleri en az 1 yıl saklanır.
5.8.2. Yedekler şifreli olarak korunur.
5.8.3. Güvenli bir depolama alanında tutulur.

6. KAYITLAR

Aşağıdaki kayıtlar bu prosedüre göre tutulur:

6.1. Konfigürasyon değişiklik kayıtları
6.2. Konfigürasyon dosyaları
6.3. Yedekleme kayıtları
6.4. Güvenli yapılandırma kontrol listeleri
6.5. Zafiyet tarama raporları

8. REFERANSLAR

ISO/IEC 27001:2022

- **A.8.8 Güvenli Yapılandırma**
- **A.8.9 Konfigürasyon Yönetimi**
- **A.5.23 Değişiklik Yönetimi**

BGYS Politikası
Değişiklik Yönetimi Prosedürü