Aşağıda bilgilerini vermiş olduğum sunucu ile ilgili tanımlamaların “Ege Üniversitesi Sunucu Güvenlik Politikası” na bağlı kalarak, tarafınızca yapılmasını talep ederim.

|  |
| --- |
| Birim Sorumlusu |
| Adı Soyadı |
| İmza |

|  |  |
| --- | --- |
| **Sunucu Adı :** |  |
| **Ip Adresi :** |  |
| **Açılması İstenilen Portlar(80, 22… vb.) :** |  |
| **Mac Adresi (Ethernet) :** |  |
| **Projenin Amacı :** |  |
| **Yer (Fiziksel Konum) :** |  |
| **Sorumlular (Admin Şifresine Sahip Olanlar) :** |  |
| **Telefon ve E-mail :** |  |
| **Donanım :** |  |
| **İşletim Sistemi :** |  |
| **Kullanıcı Sınıfı :** |  |
| **Lokal Kullanıcı Sayısı :** |  |
| **Tahmini Üniversite Dışı Kullanıcı Sayısı :** |  |
| **Sunucu Üzerinde Bulunan Güvenlik Yazılımları :** |  |
| **NYG Bünyesinde Güvenlik Uygulamalarından Yararlanmak İsteniliyor mu? :** |  |
| **Ek Açıklamalar :** |  |

\* Birim Sorumlusu: Bölüm/fakülte için Dekan ve Enstitü ve Araştırma Merkezleri için Müdür, Yüksekokullar için Yüksek Okul Müdürü, Meslek Yüksek Okulları için Meslek Yüksek Okulu Müdürü, İdari Birimler için Daire Başkanı, Kulüpler için Kulüpler Birliği Başkanlığı, seminer vb bilimsel etkinlikler için Koordinatör.

**SUNUCU GÜVENLİK POLİTİKASI**

**Politikanın Amacı**

Bu politikanın amacı Ege Üniversitesi’nin sahip olduğu sunucularının temel güvenlik konfigürasyonları için standartları belirlemektir. Bu politikanın etkili uygulanmasıyla, Ege Üniversitesi bünyesindeki sunuculara ve teknolojiye yetkisiz erişimler minimize edilecektir.

**Sunucu Yöneticilerinin Sorumlulukları**

Kurum bünyesindeki bütün dahili sunucuların yönetiminden, yetkilendirilmiş sistem yöneticileri sorumludur. Sunucu konfigürasyonları sadece bu gruptaki kişiler tarafından yapılacaktır.

1. Birimin sahip olduğu bütün sunucular E.Ü. BİDB Ağ Grubu sunucu yönetim sistemine kayıt olmalıdır.
2. Server (sunucu) olarak kullanılmak istenen makineler ve kullanıcıları hakkında son sayfadaki bilgiler resmi yazının ekinde bize iletilmelidir.

**Konfigürasyon Kuralları**

1. Kullanılmayan servisler ve uygulamalar kapatılmalıdır.
2. Servislere erişimler sistem yöneticileri tarafından 6 (altı) ay boyunca loglanacak ve erişim kontrol metotlarıyla koruma sağlanacaktır.
3. Sunucular üzerinde yapılacak değişiklikler yönetim kuralları çerçevesinde bir onay ve test mekanizmasından geçirildikten sonra uygulanmalıdır.
4. Sistem yöneticileri gerekli olmadığı durumlar dışında "Administrator" ve "root" gibi genel kullanıcı hesapları kullanmamalı, gerekli yetkilerin verildiği kendi kullanıcı hesaplarını kullanmalıdır. Genel yönetici hesapları yeniden adlandırılmalar. Gerekli olduğunda, önce kendi hesapları ile log-on olup, daha sonra genel yönetici hesaplarına geçiş yapmalıdırlar.
5. Ayrıcalıklı bağlantılar teknik olarak güvenli kanal (SSH veya SSL IPSec VPN gibi şifrelenmiş ağ) üzerinden yapılmalıdır.
6. Sunucular fiziksel olarak korunmuş sistem odalarında bulunmalıdır.
7. Sunuculara ait bağlantılar normal kullanıcı hatlarına asla takılmamalıdır. Sunucu vlan’larının tanımlı olduğu portlardan bağlantı sağlanmalıdır.
8. Kurulan sunucular web hizmeti verecekse, sunucu üzerinde mutlaka web uygulama güvenlik duvarı kurulmalıdır veya BİDB Ağ Grubu’ndan bu hizmetin temini için istekte bulunulmalıdır.

ı) Sunucu olarak çalıştırılacak bilgisayarlar üzerinde kesinlikle kişisel işlemler yapılmamalı ve kullanım politikasına aykırı bir kullanıma olanak verilmemelidir.

Sunucu üzerinde barındırılacak materyal kesinlikle 5651 sayılı yasa :

*(****Erişimin engellenmesi kararı ve yerine getirilmesi)***

***MADDE 8-*** *(1) İnternet ortamında yapılan ve içeriği aşağıdaki suçları oluşturduğu husu- sunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak erişimin engellenmesine karar ve- rilir:*

* 1. *26/9/2004 tarihli ve 5237 sayılı Türk Ceza Kanununda yer alan;*
     1. *İntihara yönlendirme (madde 84),*
     2. *Çocukların cinsel istismarı (madde 103, birinci fıkra),*
     3. *Uyuşturucu veya uyarıcı madde kullanılmasını kolaylaştırma (madde 190),*
     4. *Sağlık için tehlikeli madde temini (madde 194),*
     5. *Müstehcenlik (madde 226),*
     6. *Fuhuş (madde 227),*
     7. *Kumar oynanması için yer ve imkân sağlama (madde 228), suçları.)*

çerçevesinde belirtilen içeriklere sahip olmalıdır. Aksi durumlarda sunucunun internet üzerinden erişimi BİDB Ağ Grubu çalışanları tarafından kesilecektir.

1. Sunucular kesinlikle hack ve benzeri girişimler için kullanılmamalıdır. Bu duruma uymayan sunuculara erişim anında kapatılacaktır.
2. Sunucular üzerinde kesinlikle ticari amaç güden yazılımlar kurulmamalıdır.
3. Bu politikanın içeriği [http://internet.ege.edu.tr](http://internet.ege.edu.tr/) adresinde yayınlandığı tarihten itibaren bütün sunucular için geçerli olacaktır.
   1. **Gözlemleme**

Kritik sistemlerde oluşan bütün güvenlikle ilgili olaylar loglanmalıdır ve aşağıdaki şekilde saklanmalıdır.

* + - Bütün güvenlikle ilgili loglara online olarak minimum 180 gün süreyle erişilebilmelidir.
    - Loglar sunucu üzerinde tutulmalarının yanında ayrı bir sunucuda daha tutulmalıdır.
    - Sunucu üzerinde herhangi bir zararlı yazılım (malware, spyware, hack programları, warez programları, vb.) çalıştırılmamalıdır.

**YUKARIDAKİ SÖZLEŞMEYİ OKUDUM, KABUL EDİYORUM.**

|  |  |
| --- | --- |
| **Unvanı :** |  |
| **Ad Soyad :** |  |
| **İmza :** |  |