****

**Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı**

**MAC-OSX SIKILAŞTIRMA(HARDENING) KONTROL LİSTESİ V.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**18.12.2019**

**İçindekiler**

[ÖZET 2](#_Toc27560477)

[1) Mac-Osx Sıkılaştırma (Hardening) Kontrol Listesi 3](#_Toc27560478)

#

# ÖZET

Bu dokümanda Siber Olaylara Müdahale Ekibi tarafından hazırlanmış olan Mac-OSX işletim sistemine güvenli kontrol listesi yer almaktadır.

Mac-OSX işletim sistemi kurulumlarında ve kurulumdan sonra sistemin/sunucunun daha güvenlik olması için kontrol listesi yer almaktadır. Bu önlemler sisteminize gerçekleştirilebilecek dış ve iç saldırılara karşı korunmasında gereken en önemli bileşenlerden biri durumundadır.

##

## Mac-Osx Sıkılaştırma (Hardening) Kontrol Listesi

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **MAC-OSX Sıkılaştırma (Hardening) Kontrol Listesi** | **Yapıldı** | **Yapılmadı** |
| **1** | Mümkün olan en güncel işletim sistemini kullanmayı tercih edilmelidir. |  |  |
| **2** | Sistemin çalışacağı network’ün VLAN’lar aracılığı ile ayrılmış olduğuna dikkat edilmelidir. |  |  |
| **3** | Mac-Osx disk güvenliği için full disk şifrelemesinde kullanılan FaileVault etkin hale getirilmelidir. |  |  |
| **4** | Apple Güvenlik Duvarı açık hale getirilmelidir. |  |  |
| **5** | Firmware için gereken parola korumalarını aktif edilmelidir. |  |  |
| **6** | Bilgisayar kurulduktan sonra güncellemeler 2 ayda bir düzenli aralıklarla kontrol edilerek ilgili güncellemeler yapılmalıdır. |  |  |
| **7** | Zaman senkronizasyonu için NTP kullandığınızdan emin olunmalıdır. |  |  |
| **8** | Sistem üzerinde olay günlüklerini aktif edilmelidir. |  |  |
| **9** | Yönetici hesapları için karmaşık parolalar oluşturulmalıdır. |  |  |
| **10** | Kullanılmayan hizmetler ve kullanıcı hesaplarını kalıcı olarak devre dışı bırakılmalıdır. |  |  |
| **11** | Ana bilgisayarda çalışan hizmetlere bağlantıyı yetkili kullanıcılara sınırlanmalıdır. |  |  |
| **12** | Bonjour servisi kapalı tutulmalıdır. Paylaşılan müzik kütüphanelerini, AirPort Express ve Apple TV gibi işlemler kullanılacağı zaman Bonjour servisi açılmalıdır.  |  |  |
| **13** | Her biri için bir yönetici hesabı ve standart bir kullanıcı hesabı oluşturulmalıdır. |  |  |
| **14** | Otomatik oturum açmayı devre dışı bırakılmalıdır. |  |  |
| **15** | En az 10 karakter olacak şekilde bir parola politikaları belirlenmelidir. |  |  |
| **16** | /home dizini için güvenlik politikaları belirleyin |  |  |
| **17** | Spotlight’ın gizli klasörleri ve yedekleme birimlerini aramasını engellenmelidir. |  |  |
| **18** | Sistem hesaplarının bütünlük denetimini, grup üyelikleri ve bunların ilişkili ayrıcalıklarını etkinleştirilmelidir. (Karşılaşabilecek sorunlara karşı test edilmelidir) |  |  |
| **19** | Kullanılacak olan servislerde mutlaka TLS aktifleştirilmelidir |  |  |
| **20** | Web sunucusu kullanılacaksa TLS aktifleştirilmelidir. |  |  |
| **21** | SSH bağlantılarında root kullanıcı kullanılmamalıdır. |  |  |
| **22** | Sunucu dışarı açılacaksa SSH servisi kapatılmalıdır. SSH bağlantısı SSL-VPN üzerinden sağlanmalıdır. |  |  |
| **23** | Gereksiz bütün uygulamaları sistemden kalıcı olarak kaldırılmalıdır. |  |  |
| **24** | İşletim sistemi destekliyorsa, kritik çalışma ortamları için bütünlük kontrolünü etkinleştirin (3. parti yazılımlar aracılığı ile) |  |  |
| **25** | Lisanslı Antivirüs yazılımları kullanılmalıdır. |  |  |
| **26** | Lisanslı Antivirüs yazılımı ile işletim sistemi belirli aralıklarla taratılmalıdır. |  |  |
| **27** | Güvenli bir web bağlantı için Firefox tercih edilmelidir. Zararlı bağlantıları ve güvenli erişim için No Script + HTTPS Everywhere eklentileri kullanılmalıdır. |  |  |
| **28** | Otomatik oturum kilitleme özelliklerini kullanılmalıdır. |  |  |
| **29** | Veri sızdırmalarını engellemek adına .DS\_Store oluşturulmasının önüne geçilmelidir. |  |  |
| **30** | Mümkünse sistemi Active Directory veya LDAP’a dahil edilmelidir. |  |  |
| **31** | Mutlaka belirli aralıklarla yedek alındığından emin olunmalıdır. |  |  |
| **32** | Yedekleme için şifreleme algoritmalarını kullanılmalıdır. (PGP vb) |  |  |