****

**Sistem Yönetimi ve Bilgi Güvenliği Dairesi Başkanlığı**

**WINDOWS SIKILAŞTIRMA(HARDENING) KONTROL LİSTESİ V.1.0**

**HAZIRLAYAN**

Cihan Mehmet DOĞAN

(Sızma Testi Uzmanı)

**18.12.2019**

**İçindekiler**

[ÖZET 3](#_Toc27560692)

[Windows Sıkılaştırma (Hardening) Kontrol Listesi 4](#_Toc27560693)

# ÖZET

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

Windows 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.

## Windows Sıkılaştırma (Hardening) Kontrol Listesi

|  |  |  |  |
| --- | --- | --- | --- |
| **No** | **Windows Sıkılaştırma (Hardening) Kontrol Listesi** | **Yapıldı** | **Yapılmadı** |
| **1** | Destek verilmesi durdurulan Windows işletim sistemleri kullanılmalıdır ve eskiler yenileri ile güncellenmelidir. |  |  |
| **2** | Bilgisayar/Sunucu başlangıcında yetkisiz değişiklikleri önlemek için BIOS alanına parola getirilmelidir. |  |  |
| **3** | Otomatik güncelleştirmeler belirli aralıklarla kontrol edilerek gerekli testlerden sonra güncellemeler yapılmalıdır |  |  |
| **4** | Güncellemeler ve güvenlik yamaları için SSCM ya da WSUS kullanılmalıdır. |  |  |
| **5** | Hiyerarşiyi takip edecek listeler oluşturulmalıdır (Excel, vb.) |  |  |
| **6** | Sunucuların/bilgisayarların yönetimi için kurulumdan sonra Active Directory üzerine dahil edilmelidir. |  |  |
| **7** | Sunucular arasında iletişim kurulacaksa IPsec gibi VPN teknolojileri kullanılmalıdır. |  |  |
| **8** | Parola güvenliğini sağlamak amacı ile 180 günde bir parola değiştirmeye zorlanmalıdır. |  |  |
| **9** | Parola uzunluklarını minimum 12 karakter olacak şekilde ayarlayın |  |  |
| **10** | Sunucularda 15 dakikada 5 kez geçersiz parola denemesi yapılırsa hesabı devre dışı bırakılmalıdır. |  |  |
| **11** | Bilgisayarların giriş loglarını (Logon Event) belirli aralıklarla takip edilmelidir. |  |  |
| **12** | Sunucular/bilgisayarlar üzerinde kullanılan 3.parti yazılımların güvenlik güncelleştirmelerini mutlaka gerçekleştirilmelidir. |  |  |
| **13** | Ataklara karşı koymak için sunuculara/bilgisayarlara lisanslı bir antivirüs(ücretsiz olan Windows Defender) kurulmalıdır. |  |  |
| **14** | Sistemde yüklü olan antivirüs uygulaması ile belirli aralıklarla tarama işlemi gerçekleştirilmelidir |  |  |
| **15** | Sistemde log tutmayı aktif hale getirilmelidir.(kritik suncular vb.) |  |  |
| **16** | Güvenlik duvarı kullanımına özen gösterilmelidir, ihtiyacınız olmasa bile güvenlik duvarını açılmalıdır. |  |  |
| **17** | Kullanılmayan portlara erişimleri kalıcı olarak kapatılmalıdır. |  |  |
| **18** | RDP bağlantısı yapılacaksa mutlaka dışarıdan SSL-VPN üzerinden erişime izin verilmelidir. |  |  |
| **19** | Sunucunun dışarı bağlantısı (RDP, SSH, SMB) olmamalıdır. Uzak masaüstü bağlantılarında IPSEC gibi VPN teknolojileri kullanın |  |  |
| **20** | Sunucuda kullanılmayan bütün özellikleri devre dışı bırakın (yazıcı sunucusu, yazıcı paylaşımı, dosya paylaşımı) |  |  |
| **21** | Sunuculardaki kimlik avı saldırılarına karşı korumak için sunucudaki gereksiz tüm e-posta istemcilerini kaldırılmalıdır. |  |  |
| **22** | Kullanıcı hesap denetimini etkinleştirin ve kuralları operatörlere göre düzenlenmelidir |  |  |
| **23** | Web sunucusu üzerinde kullanılacak bütün web sitelerinde TLS kullanımına özen gösterilmelidir. |  |  |
| **24** | Yedekleme için en az iki DNS sunucusu ve komut isteminden nslookup kullanarak çift onay ad çözümlemesi yapılandırılmalıdır. |  |  |
| **25** | Sunucunun, istediğiniz adla birlikte DNS’de geçerli bir A kaydının yanı sıra geriye doğru aramalar için bir PTR kaydının olduğundan emin olunmalıdır. |  |  |
| **26** | Sunucuda eğer IPv6 kullanılmayacaksa interface üzerinden kalıcı olarak devre dışı bırakılmalıdır. |  |  |
| **27** | İhtiyacınız olan her şeyin kurulu olduğundan emin olunmalıdır. |  |  |
| **28** | İhtiyacınız olmayan her şeyi kaldırın. Bu şekilde sunucunun/bilgisayarın saldırı yüzeyini gereksiz yere arttırmamış olur. |  |  |
| **29** | Sunucuda/bilgisayarda varsayılan olarak yüklü gelen gereksiz uygulamaları kaldırın |  |  |
| **30** | Windows oturum açmalarını ve kerberos güvenliğine dayalı çeşitli diğer işlevler tamamen aksayacağından dolayı NTP kullanımına özen gösterilmelidir. |  |  |
| **31** | Powershell ve SSH gibi diğer uzaktan erişim mekanizmaları eğer kullanılacaksa sadece SSL-VPN üzerinden kullanılacak şekilde ayarlanmalıdır. |  |  |
| **32** | Şifrelenmemiş protokoller kullanılmamalıdır (Telnet, FTP) |  |  |
| **33** | Mümkünse dosya yükleme işlemlerini FTP yerine SFTP üzerinden gerçekleştirilmelidir. |  |  |
| **34** | 2003, 2005 ve 2008 gibi eski sürümlerde bulunan servisleri özellikle kontrol edin, gerekli olmayanları kapatın. Kullanılacak uygulama varsa ağdan izole edilerek çalıştırılmalıdır. |  |  |
| **35** | Bilgisayar yeniden başlatma gibi durumlar için önemli servisleri otomatik olarak başlayacak şekilde ayarlanmalıdır. |  |  |
| **36** | Kurtarma konsoluna otomatik yönetimsel oturum açmayı devre dışı bırakılmalıdır. |  |  |
| **37** | Alternatif medyadan izinsiz olarak önyükleme yapılmasını önlemek için aygıt önyükleme sırasını yapılandırılmalıdır. |  |  |
| **38** | Misafir hesaplarını devre dışı bırakılmalıdır. |  |  |
| **39** | “everyone” olarak geçen izinleri gerekmedikçe asla kullanılmamalıdır. |  |  |
| **40** | Anonim SID ve Ad çeviri özelliğini devre dışı bırakılmalıdır. |  |  |
| **41** | Kullanılmayan kullanıcı hesaplarını belirlenip devre dışı bırakılmalıdır veya silinmelidir. |  |  |
| **42** | Sunucuda Ncacn\_ip\_tcp deaktif edilmelidir. |  |  |
| **43** | TCP/IP üzerinden NetBIOS’u devre dışı bırakılmalıdır. |  |  |
| **44** | Herhangi bir paylaşımın anonim olarak yetkisiz erişilmesine izin verilmemelidir. |  |  |
| **45** | Yerel Sistemin NTLM için bilgisayar kimliğini kullanmasına izin verilmelidir. |  |  |
| **46** | Ağda daha güvenli bir bağlantı için LAN Manager kimlik doğrulama seviyesini sadece NTLMv2’ye izin vermek ve LM ile NTLM’yi reddetmek için ayarlanmalıdır. |  |  |
| **47** | NTFS veya BitLocker ile yerleşik dosya şifrelemesini etkinleştirilmelidir. |  |  |
| **48** | Kurulacak işletim sistemleri lisanslı olmalıdır. Windows Server 2016/2012/2008/2003 lisans anahtarlarınızı mutlaka girilmelidir. |  |  |
| **49** | Windows XP/Vista/7/8/8.1/Server 2003 işletim sistemlerine Microsoft'un desteği kalktığı için kurumda Windows 10 ve Server 2016/2019 kullanılmalıdır. |  |  |
| **50** | Gereksiz tüm yürütülebilir dosyaları ve kayıt defteri aracılığı ile kaldırılmalıdır. |  |  |
| **51** | Fiziksel sunucu güvenliğinizi mutlaka tamamlayın (kabin ve sistem odası güvenliği) |  |  |
| **52** | Son kullanıcılar Teamviewer ve Anydesk gibi uzaktan bağlantı programları kurulması engellenmelidir. |  |  |