Revizyon İzleme Tablosu		
Rev. No	**Rev. Tarihi**	**Açıklama**
01	27.05.2022	Talimat uygulama maddelerinde güncelleme yapıldı.
02	18.10.2022	Referanslar düzenlendi.

1. AMAÇ

Kurumumuzda virüslere karşı korunmak için ilgili kuralları belirlemektir.

2. SORUMLULUKLAR

Bu talimatın uygulanmasından tüm kullanıcılar sorumludur.

3. UYGULAMA

3.1. Antivirüs Yazılımı Özellikleri

Merkezi yönetim yazılımının şu özelliklere sahip olması gerekir:

- Virüs tanımlamalarını merkezi olarak güncelleyebilme
- Periyodik tarama yapabilme, isteğe bağlı tarama yapabilme ve sürekli (dosya oluşturulduğunda, kopyalandığında, okunduğunda, değiştirildiğinde vb.) tarama yapabilme özelliğine sahip olmalıdır.
- Antivirüs istemcilerinin durumlarının izlenmesi (bağlantı durumu, antivirüs servisinin durumu, virüs tanımlarının güncelliği, virüs bulundu uyarısı, tarama motorunun ve yazılımın verisyonu bilgisi, IP bilgisi vb.) ekranı bulunmalıdır.
- Antivirüs yazılımlarının üreteceği kayıtlara erişim ve virüs yayılması konusunda sistemden rapor alınabilmelidir.
- Kuruma özel paket halinde alınan antivirüs yönetim programının, kullanıcıların sade olarak kullanabileceği şekilde kurulumunun yapılmış olması gerekmektedir.
- Paket programın ayarlarının (güncelleme, periyodik tarama) yapılmış halde teslim edilmesi gerekmektedir.

3.1.1. Konfigürasyon / Yönetim

Merkezi antivirüs yapısının kurulum işlemi sonrasında, sunucular ve kullanıcı bilgisayarları üzerlerinde çalışan uygulamalara, maruz kaldıkları tehditlere, zorunlu ise taramalarda kapsam dışı tutulması gereken dosya dizinlere, periyodik taramaların zamanına vb. farklı politika uygulanma ihtiyaçlarına göre yapılmalıdır. Örneğin; kullanıcı bilgisayarlarında periyodik taramalar hafta içi öğle arasında yapılırken sunucularda hafta sonu yapılabilir vb.

3.1.2. İmzaların Güncelliği

Antivirüs yazılımının başarılı olabilmesi için imza güncellemelerinin zamanında yüklenmesi sağlanmalıdır. Tavsiye edilen güncelleme periyodu günlüktür. Fakat bazı acil virüs saldırısı durumlarında daha kısa aralıklarla güncelleme yapılabilmesi gerekmektedir.

3.1.3. Gerçek Zamanlı Virüs Koruma

Gerçek zamanlı virüs koruma tarama ayarlarında; müdahale yöntemi, virüs bulunduğunda temizleme, karantinaya alma ya da silme işlemlerinden biri tercih edilmiş olmalıdır.

3.1.4. Periyodik / İsteğe Bağlı Tarama

Periyodik taramalar için tavsiye edilen periyot kritik bileşenler için günlük, daha az kritik bileşenler için ise haftalıktır. Periyodik tarama zamanı seçilirken, bileşenlerin açık olduğu ve tarama sonucu oluşacak performans kaybının etkisinin en az hissedileceği zamanların seçilmesine dikkat edilmelidir. Tarama işlemlerini kullanıcıların durduramaması sağlanmalıdır.

3.1.5. İzleme / Raporlama / Uyarı Ayarları

Mümkün olan tüm bileşenlere antivirüs yazılımının kurulması ve ayarların yukarıda belirtildiği şekilde yapılması virüslere karşı güvenlik mekanizmasının oluşturulmasını sağlamaktadır. Bileşenlerin durumu uygun şekilde takip edilmezse:

- Antivirüs yazılımı kaldırılan / servisi durdurulan / ayarları değiştirilen / antivirüs yazılımı hiç kurulmamış bileşenler fark edilmeyebilir.
- Antivirüs yazılımının temizlemekte başarısız olduğu ya da antivirüs yazılımını etkisiz hale getiren virüsler zamanında fark edilmeyebilir.
- Virüslerin yoğun olarak bulaştığı bileşenler ve bulaşma yöntemleri fark edilemez ve önlem alınamayabilir.
- Virüs tanımlamaları güncel olmayan antivirüs yazılımları belirlenemeyebilir.

Sonuç olarak sistem geciken müdahale sebebiyle zarar görebilir. Bu sebeplerle merkezi antivirüs yazılımı üzerinde bileşenlerin durumları (virüs bulaşmış, virüs tanımı güncel değil, ulaşılamıyor vb.) düzenli olarak kontrol edilmeli, çok sayıda bileşenin olduğu durumlarda raporlama özelliği kullanılarak müdahale gereken bileşenler belirlenmeli, sisteme bulaşan virüsler hakkında detaylı bilgiler alınmalıdır. Ayrıca birçok merkezi antivirüs yazılımında bulunan e-posta ile uyarı sistemi devreye sokularak antivirüs sistemi yöneticisinin acil durumlara tepkisi hızlandırılmalıdır.

3.2. E-Posta Antivirüs Koruması

3.2.1. Virüs Tarama

E-posta ile bulaşan virüsler çoğunlukla eklenti dosyalarla gelmektedir. Bazı virüsler herhangi bir eklenti olmadan da bulaşabilmektedirler. Virüs tarama ayarları bütün eklenti dosyalar ve e-posta içeriği taranacak şekilde yapılması gerekmektedir. Ayrıca yapılacak ayarla sıkıştırılmış eklenti dosyalarının da taranması sağlanmalıdır. E-posta antivirüs yazılımı seçilirken, yazılımın e-postaları posta kutusuna düşmeden tarama yapma yeteneği olması beklenmektedir. Tarama yapılmamış e-postaların sırada bekletilmesi ve tarama sonrasında kullanıcının erişebilmesi sağlanmalıdır.

3.2.2. Eklenti Bloklama Kuralları

E-posta antivirüs sunucusu virüs taramasını mevcut virüs imzalarına göre yapmaktadır. Bu çalışma yöntemi dolayısıyla henüz tanımlanmamış virüslerin e-posta yoluyla yayılmaya

devam etmesi mümkündür. Bu sebeple virüs içerebilecek dosya türlerinin bloklanması etkin bir önleyici çözüm olarak düşünülmektedir.

Bloklanması önerilen uzantılar şunlardır: .asd, .asf, .asx, .bas, .bat, .chm, cmd, .com, .dll, .exe, .hlp, .hta, .hto, .js, .jse, .link, .lnk, .pif, .reg, .scr, .vb, .vbe, .vbs, .wsf, .wsh, ve .wsc. Burada verilen liste virüs taşıyabilecek dosya türlerinin tamamını kapsayamayabilir. Antivirüs yöneticileri tecrübelerinden ve BT güvenlik sitelerinde yayınlanan uyarılardan yararlanarak tehdit oluşturabilecek uzantıları bloklama listesine eklemelidir. Ayrıca e-posta eklenti dosyaları yoluyla yayılan bir virüs saldırısı durumunda geçici süreliğine bazı dosya türlerinin bloklanması acil müdahalenin engelleme aşamasında etkin bir çözüm olarak kullanılabilir.

3.2.3. Başlık Bloklama Kuralları

Virüsler e-posta yoluyla yayılırken kullandıkları, dikkat çekme amacı taşıyan başlıklar (Para, cinsel içerikli ifadeler, iş teklifi vb. kelimeler içeren başlıklar) kullanabilmektedir. E-posta antivirüs yazılımlarında bu tür başlıklarda kullanılan anahtar kelimeleri içeren listeler bulunmaktadır. Antivirüs yöneticisinin mevcut anahtar kelimeleri içeren başlık bloklamayı aktif hale getirmesi, gerekli görüldüğünde listeyi güncellemesi tavsiye edilmektedir.

4. REFERANSLAR

- Antivirüs Politikası BGYS.PLT.04
- Zararlı Yazılımlara Karşı Korunma Politikası BGYS.PLT.20