

# İşletmeler için Örnek Antivirüs Politikası

Hazırlayan: Burç Yıldırım (burc@olimpos-IT.com)

## Amaç

Bu politika <işletme adı>nın virus, kurt, truva atı, spyware gibi kötü niyetli yazılımlardan korunmasını, bilişim kaynaklarının bu tip istenmeyen yazılımlarla kullanılmamasını amaçlamaktadır.

## İlgililer

<işletme adı> tüm çalışanları

## Tanım

Kötü Niyetli Yazılım (KNY): İşgücü veya veri kaybına sebep olabilecek, virüs, kurt, truva atı, spyware gibi, her tür yazılım. Politika metni içerisinde KNY olarak anılacaktır.

## Sorumluluklar

### Bilgi İşlem Departmanı:

- Merkezi kontrol sağlayan bir antivirüs uygulaması kullanır, uygulamanın sık ve düzenli aralıklarla yenildiği kontrol edilir.
  - Sistemler ağa bağlandığında, antivirüs uygulamasının kurulu olup olmadığı kontrol edilir ve virüs imzaları yenilenir.
  - Sistemler periyodik taramalardan geçirilir.
  - Kullanıcıların antivirüs uygulamasını kaldırması veya devre dışı bırakmaması için şifre koruması sağlanır.
  - Kayıtlar merkezi tutulur ve belirlenen düzeylerdeki uyarı mesajları, e-posta yoluyla ilgili bilgi işlem personeline ulaşır.

- E-Posta Sunucusu üzerinde;
  - İleti eklerini filtrelendir. (Ek 1)
  - Hem gelen iletilerin, hem de giden iletilerin KNY kontrolünü yapılır.
  - KNY içeren iletiler ve içeriği kontrol edilemeyen ileti ekleri silinir, iletinin kaynağı uyarılır. (Ek 2) KNY içeren iletiler eğer işletme içi kaynaklıysa, ilgili personele uyarı mesajı yollanılır ve kaynak sistem için KNY temizleme prosedürü uygulamaya konulur. (Ek 5)
  - İletilerin belirlenen sayıdan fazla alıcıya gitmesine engel olunur.
- Güvenilir ağ dışına çıkış/giriş:
  - Tüm trafik denetlenir, içeri veya dışarı doğru trafikte bir uyarı üretildiği takdirde ilgili personel e-posta yoluyla uyarılır.
  - İşletme çalışma prensipleri dışında hizmet veren içerikli siteler (Ek 3) filtrelendir.
- İhtiyaç duyulmayan sistemlerde disket sürücü, CDROM, modem benzeri dışardan kontrolsüz veri transferine izin verebilecek üniteler iptal edilir.
- İşletim Sistemi ve uygulamaların güvenlik yamaları düzenli olarak yapılır, ve bu yamaların uygulanmasının ardından sistem dosyalarının veri bütünlük uygulaması yardımıyla imzası alınır ve arşivlenir.
- Kullanıcılar yeni KNYlerden haberdar edilir. (Ek 4)
- KNY bulaşmış sistem temizleme prosedürüne sokulur. (Ek 5)

## **Kullanıcılar:**

- Şüpheli, güvenilmez veya bilinmeyen kaynaklardan gelen e-posta iletilerini açmayın, bunları hem "Gelen Kutusu"ndan hem de "Çöp Kutusu"ndan silin.
- Spam, zincir veya yönlendirilmiş iletileri asla başka kişilere yönlendirmeyin, bu tip iletileri hemen silin.
- Asla bilinmeyen veya güvenilmeyen kaynaktan dosya çekmeyin.
- İşiniz gerektirmedikçe, diskinizi okuma/yazma haklarıyla paylaşma açmayın.
- Kullandığınız sistemde şüpheli bir durum oluşursa ilgili personeli bilgilendirin.
- Kullandığınız sistemde KNY olduğuna dair bir uyarı alırsanız ilgili personeli derhal uyarın.

## İrtibat

Antivirüs merkezi yönetim sorumlusu

Ad/Soyad	
E-posta adresi	
Dahili Hat	
Mobil Telefon	

E-posta antivirüs sorumlusu

Ad/Soyad	
E-posta adresi	
Dahili Hat	
Mobil Telefon	

Güvenilir Ağ Dışı Trafik antivirüs sorumlusu

Ad/Soyad	
E-posta adresi	
Dahili Hat	
Mobil Telefon	

KNY içeren sistem sorumlusu

Ad/Soyad	
E-posta adresi	
Dahili Hat	
Mobil Telefon	

İşletim Sistemi ve uygulamalar güvenlik yamaları sorumlusu

Ad/Soyad	
E-posta adresi	
Dahili Hat	
Mobil Telefon	

### Ek 1:

Filtrelenen ileti ekleri soyadları.

bat	bin	com	dll	exe
fla	hta	inf	ini	js
jse	lnk	msi	ocx	pif
reg	scr	shs	swf	sys
url	vb	vba	vbs	wsc
wsf	wsh			

### Ek 2:

Virüs içeren ileti kaynağına gönderilen uyarı mesajı formu.

Kime: kullanıcı@<kaynak>

Konu: Tarafınızdan yollanan e-posta iletisi KNY içermektedir. / The message you have sent is infected.

İçerik: kullanıcı@<kaynak> tarafından yollanan e-posta iletisi <virüs adı> içermektedir. İleti silinmiş olup, alıcıya iletilmemiştir. / The message that was sent by [kullanıcı@<kaynak>](mailto:kullanıcı@<kaynak>) is infected by <virüs adı>. Subject message is deleted and is not transmitted to receiver.

### Ek 3:

Filtrelenecek site içeriği:

İrkçılık / Düşmanlık

Cinsel içerik

İllegal uygulama dağıtımı

### Ek 4:

Kullanıcı KNY bilgilendirme formu

Konu: KNY uyarısı <virüs adı>

İçerik: KNY yayılma şekli, tanınma sağlayacak özellikleri, verebileceği zararlar, bulaştığı sistemde yarattığı anormallikler.

## Ek 5:

KNY bulaşan sistemin temizlenme prosedürü.

- KNY bulaşmış sistemin ağ bağlantısını derhal kesin.
- Sistemi kontrollü ortamda çalıştırarak KNYyi tanımlamaya çalışın.
- Eğer KNYyi tanımlayabiliyorsanız, antivirüs yazılımı üreticinizin gösterdiği yolu izleyerek sistemi temizleyin, veri bütünlük uygulaması yardımıyla sistem dosyalarının dijital imzasını alın ve sistemi test ortamına aktarın.
- Eğer KNYyi tanımlayamıyorsanız, KNYnin bir örneğini antivirüs yazılım üreticinizin ilgili irtibatına yollayın, KNYnin sistemde yarattığı değişiklikleri ve KNYnin davranışlarını belirleyin. Bu belirtiler KNYnin temizlenebilmesi için yol gösterici olabilir. Sistem dosyalarının değişiklere karşı kontrol edilmesi için daha önce arşivlenen dijital imzalar kullanılır.
- Test ortamında sistemin günlük işleyişinin gerçekleşmesini sağlayın, sistemi beklenmeyen anormallikler için kontrol altında tutun. Sistem dosyalarının veri bütünlüğünü kontrol edin, sistemin ağ trafiğini izleyin. Test ortamını istemci sistemler için XX saat, sunumcu sistemler için XX saattir.