

Doküman Kodu: BGT-1004

ZARARLI YAZILIMA KARŞI KORUNMA KILAVUZU

SÜRÜM 1.00

16 TEMMUZ 2007

Hazırlayan: Battal ÖZDEMİR

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Arařtırma Enstitüsü (UEKAE)'nün misyonu, "bilgi güvenliđi, haberleřme ve ileri elektronik alanlarında Türkiye'nin teknolojik bađımsızlıđını sađlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliđi, haberleřme ve ileri elektronik alanlarında yeni teknolojilerin geliřtirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulařılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliřtirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı arařtırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sađlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliđi konusunda bilinçlendirmeyi hedeflemektedir. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda bahsi geçen belirli ticari marka isimleri kendi özgün sahiplerine aittir. Burada anlatılanlar tamamen tavsiye niteliğinde olup deđişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu deđildir. Bu doküman UEKAE'nin izni olmadan deđiřtirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geen Ađ Güvenliđi personeline ve dokümanı gözden geirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Burak BAYOĐLU'na teşekkürü bor biliriz.

İÇİNDEKİLER

1. GİRİŞ.....	6
1.1 Amaç ve Kapsam	6
1.2 Hedeflenen Kitle	6
1.3 Kısaltmalar	6
2. ZARARLI KOD/YAZILIM TÜRLERİ	8
2.1 Virüs	8
2.1.1 Dosya Virüsleri.....	8
2.1.2 Boot Sector	9
2.1.3 Multipartite.....	9
2.1.4 Makro Virüsler	9
2.1.5 Betik Virüsler	10
2.2 Solucan (Worm)	10
2.2.1 Ağ Solucanları	10
2.2.2 E-posta Solucanları.....	10
2.2.3 Polimorfik Virüs ve Solucanlar	11
2.3 Truva Atı (Trojan Horse)	11
2.4 Zararlı Mobil Kodlar	12
2.5 Casus Yazılımlar	12
2.5.1 Arka Kapı (Backdoor).....	12
2.5.2 Keylogger	12
2.5.3 Rootkit	13
3. VIRÜS/ZARARLI YAZILIM KORUNMA YÖNTEMLERİ.....	14
3.1 Politika	14
3.2 Kullanıcı Eğitimi	15
3.3 Açıklık Yönetimi.....	16

3.4 Antivirüs Yazılımı.....	16
3.5 Virüs Temizleme / Acil Müdahale.....	18
3.5.1 Tanımlama Aşaması:.....	19
3.5.2 Engelleme Aşaması.....	24
3.5.3 Temizleme Aşaması.....	27
4. MERKEZİ ANTIVİRÜS KORUMASI.....	29
4.1 ZKY İmzalarının Güncelliği.....	31
4.2 Gerçek Zamanlı Virüs Koruma.....	31
4.3 Periyodik/İsteğe Bağlı Tarama.....	32
4.4 İzleme/ Raporlama/Uyarı Ayarları.....	32
5. EPOSTA ANTIVİRÜS KORUMASI.....	33
5.1 ZKY İmzalarının Güncelliği.....	33
5.2 ZKY Tarama.....	34
5.3 Eklenti Bloklama Kuralları.....	34
5.4 Başlık Bloklama Kuralları.....	34
5.5 İzleme/ Raporlama/Uyarı Ayarları.....	35

1. GİRİŞ

Kurumlarda BT ortamından kaynaklanan hizmet kesintileri, veri kayıpları, gizli bilgilerin istenmeyen kişilerin eline geçmesi vb. durumların ana sebeplerinden biri sistemlere bulaşan zararlı yazılımlardır. Bu sebeplerle zararlı yazılımlardan kaynaklanan tehditlerin farkında olmak, kullanıcıları bilinçlendirmek ve korunmak için gerekli önlemleri almak kritik önem taşımaktadır.

1.1 Amaç ve Kapsam

Bu dokümanda zararlı yazılımların türleri, korunma yöntemleri ve sisteme bulaşan zararlı yazılımlara nasıl müdahale edilmesi gerektiği konularında bilgi verilmektedir.

1.2 Hedeflenen Kitle

Bu doküman, kurumda kullanılacak virüs koruma yazılımlarının kurulumundan ve yönetiminden sorumlu olan sistem yöneticilerine ve zararlı kod/yazılım kaynaklı olaylara acil müdahalede bulunacak ekipte yer alacak kişilere yardımcı bilgiler sunmaktadır.

1.3 Kısaltmalar

UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ZKY	: Zararlı Kod ve Yazılım
STS	: Saldırı Tespit Sistemi
VLAN	: Virtual Local Area Network (Sanal Yerel Alan Ağı)
RAM	: Random Access Memory (Rasgele Erişimli Bellek)
TCP	: Transmission Control Protocol
UDP	: User Datagram Protocol
CPU	: Central Processing Unit (Merkezi İşlemci Birimi)
MBR	: Master Boot Record (Birincil Sabit Disk Alanı)

OS : Operating System (İşletim Sistemi)

2. ZARARLI KOD/YAZILIM TÜRLERİ

Bilgisayar ortamına kullanıcının bilgisi/onayı dışında aktarılmış, mevcut kullanıcı dosyaları, yazılım ve/veya işletim sisteminin bütünlüğünü, erişilebilirliğini, gizliliğini tehdit eden yetkisiz kod parçaları ve yazılımlar genel olarak zararlı kod/yazılım olarak isimlendirilmektedir. Yayılma yöntemine, yapısına ve amacına göre çeşitli türleri mevcuttur:

2.1 Virüs

Virüsler kendilerini dosyalara, programlara ya da bilgisayara kopyalayarak yayılmak üzere tasarlanmıştır. Örneğin Word dosyalarına eklenmiş kötü amaçlı makrolar diğer Word dosyalarına bulaşabilir, ya da bir boot sector virüsü disketten boot sektörüne kendini kopyalayarak işletim sisteminin açılmasını engelleyebilir. Virüsler bilgisayar kullanıcıyı rahatsız edecek mesajlar gösterebilir, dosyaları kullanılmaz hale getirebilir, kişisel bilgileri başkalarına gönderebilir ya da işletim sistemini çalışmaz hale getirebilir. Virüsler bir dosyanın açılması, bir programın çalıştırılması, boot sector virüs içeren bir disket/CD'nin bilgisayar açılırken takılı olması ya da e-postalara eklenmiş dosyaların açılması ile bilgisayara bulaşabilir. Virüsler antivirüs programları tarafın tespit edilmemek için değişik karıştırma, şifreleme, değişme vb. yöntemleri kullanmaktadır.

2.1.1 Dosya Virüsleri

Word, Excel veya oyun programları gibi çalıştırılabilir programlara kendilerini eklerler. Bir programa bulaştıktan sonra diğer programlara bulaşabilirler. Jerusalem ve Cascade virüsleri bu tür virüslere örnektir.

2.1.2 Boot Sector

Boot sector virüsleri sabit diskin master boot record (MBR), boot sector kısımlarını ya da floppy disket, CD, flash disk gibi taşınabilir medyalarla bulaşırlar. Boot sektör sabit disk sürücünün başlangıç kısmında bulunan ve disk / drive yapısı hakkında bilgileri içeren kısımdır. Açılış sektörü bilgisayar üzerine kurulu işletim sisteminin başlatılabilmesi için gerekli programları içerir. MBR disk üzerinde özel bir bölgede bulunur, bilgisayar BIOS boot programının yer bilgisini tutar ve çalıştırma komutunu içerir. Sistem açılışı esnasında taşınabilir disk takılı konumda ise sisteme boot sector virüsleri bulaşabilir (Taşınabilir diskte boot sector virüsü olması durumunda). Boot sector virüsleri sistemi çalışmaz konuma getirebilir. Belirtileri sistem açılışında görülen hata mesajları ya da sistemin açılmaması olabilir. Form, Michelangelo ve Stoned boot sector virüslerine örnektir.

2.1.3 Multipartite

Boot sektör ve File Infector virüslerinin özelliklerini taşır. Flip ve Invader bu tür virüslere örnektir

2.1.4 Makro Virüsler

Makro virüsler en yaygın ve etkili virüs türüdür. Bu tür virüsler kendilerini makro (kompleks, tekrarlanan işlemleri otomatize eden betikler) kullanımına izin veren Word, Excel vb. programların açtığı dokümanlara kopyalarlar. Makro virüsler bu tür programların makro programlama dili yeteneklerini kullanarak yayılırlar ve programlandıkları işlevi gerçekleştirirler. Bir makro virüs bulaştığında ilgili programın yeni dokümanlar oluştururken ya da mevcut dokümanları açarken kullandığı taslak doküman (template) virüslü hale gelir. Concept, Marker, ve Melissa virüsleri bilinen makro virüslere örnektir.

2.1.5 Betik Virüsler

Makro virüslere benzerdirler, temel farkları makro virüsler belli bir program tarafından kullanılan betiklerden oluşurken, betik virüsleri işletim sistemi tarafından çalıştırılan servislerin çalıştırabildiği betiklerden oluşur. Örneğin Windows Scripting Host servisi VBScript'le yazılan betikleri çalıştırmaktadır. Bu tür virüslere örnekler First ve Love Stages virüsleridir.

2.2 Solucan (Worm)

Worm'lar bir dosyaya bulaşmak için host programa ihtiyaç duymayan zararlı kodlara verilen isimdir. Solucanlar yayılmak için kullanıcının dosyayı açmasına ihtiyaç duymadan yayılabilirler. Bu nedenle tüm sisteme kısa sürede yayılma olanağına sahiptirler. Solucanlar bilinen açıklıkları (işletim sistemi, uygulama açıklıkları) ya da konfigürasyon hatalarını (güvenlik önlemi alınmamış paylaşımlar gibi) kullanırlar. Sistem ya da ağ kaynaklarını tüketmek ya da sisteme izinsiz giriş için arka kapılar oluşturmak amacıyla kullanılırlar. İki çeşit solucan bulunmaktadır:

2.2.1 Ağ Solucanları

İşletim sisteminin/uygulamaların ağ servislerinde bulunan açıklıkları kullanarak yayılırlar. Solucan bir sisteme bulaştıktan sonra aynı servisi kullanan diğer sistemleri tarar ve bu sistemlere bulaşmaya çalışır. Kullanıcının yapacağı işlemlere bağımlı olmadığı için diğer zararlı kod/yazılımlara göre daha hızlı yayılırlar. Sasser ve Witty bu tür solucanlara örnektir.

2.2.2 E-posta Solucanları

E-posta ile yayılan virüslere benzerler, fakat e-posta solucanları bulaştıktan sonra sistemde kayıtlı e-posta adreslerini arar ve kopyalarını bu adreslere gönderir. Bu tür solucanlar e-posta sunumcusunun servis dışı kalmasına sebep olabilir veya ağ performansını düşürebilir. Beagle, Mydoom ve Netsky bu tür solucanlara örnektir.

2.2.3 Polimorfik Virüs ve Solucanlar

Polimorfik kod genel olarak, çalışan yazılımın aynı tutulmasına karşılık her kopyada farklı görüntüye sahip yazılım olarak tanımlanmaktadır. Benzer olarak polimorfik solucan, her solucan kopyasında farklı bir örüntüye sahip olan solucandır. Bu sebeple polimorfik solucanların basit örüntü tanıma yöntemleriyle başarılı şekilde tespit edilmesi mümkün değildir. Öte taraftan her polimorfik solucan örneğinde aynı olan kod parçaları da bulunmaktadır. Polimorfik virüs ve solucanlar günümüzde tespit edilmesi en zor zararlı yazılım türleri arasındadır. AdmMutate, Clet gibi polimorfik kod üretme motorlarının virüs koruma yazılımları tarafından tanınmaya başlamasıyla beraber yavaşlamış gibi görünse de saldırı uzmanları tarafından geliştirilmiş özel polimorfik kod üretme motorları halen büyük bir tehdittir.

2.3 Truva Atı (Trojan Horse)

Eğlenceli ya da faydalı bir program gibi gözükten, ancak maksadı hedef sisteme zarar vermek olan programlardır. Truva atları virüs ve solucanların aksine yayılma özelliğine sahip değildir ve kullanıcı tarafından faydalı olduğu düşünülerek bilgisayara kurulur. Truva atları kurulduğunda mevcut sistem dosyalarını değiştirebilir, kendi dosyalarını oluşturabilir, saldırganı arka kapı (backdoor) açabilir, kullanıcının kişisel bilgilerini toplayabilir. Truva atlarının varlığı antivirüs/spyware türü programlarla tespit edilmekle beraber, bilgisayarın CPU, RAM ya da ağ kullanımındaki beklenmedik değişiklikler Truva atının varlığına işaretler. Truva atlarına şu örnekler verilebilir:

- Sistemde kullanılan şifreleri toplayan bir oyun programı.
- Prosesleri listelemek için kullanılan programın zararlı programların listelenmesini engellemesi
- Erişim kontrol programının şifreleri saldırgan için saklaması
- Sözlük olduğu sanılan programın sistem dosyalarını silmesi vb.

SubSeven, Back Orifice ve Optix Pro bilinen truva atlarına birkaç örnektir.

2.4 Zararlı Mobil Kodlar

Mobil kod, uzaktaki bir bilgisayardan ağ üzerinden gönderilen, gönderildiği bilgisayarda kullanıcının müdahalesine gerek kalmaksızın çalıştırılabilen kodlara verilen isimdir. Değişik işletim sistemlerinde ve birçok uygulama üzerinde çalıştırılabilmektedirler. Saldırganlar tarafından yazılan zararlı mobil kodlar sistemlere doğrudan saldırmak dışında, virüs, solucan, truva atı vb. zararlı kod/yazılım yüklemek için de kullanılırlar. Virüs ve solucanlardan farklı olarak sistem/ağ üzerinde yayılmazlar veya dosyalara bulaşmazlar. Sistemlere, mobil kodlara verilen varsayılan hakları kullanarak saldırırlar. Mobil kodlar için kullanılan popüler programlama dilleri Java, ActiveX, JavaScript ve VBScript'tir. En çok bilinen mobil kod Nimda'dır, JavaScript kullanılmıştır.

2.5 Casus Yazılımlar

2.5.1 Arka Kapı (Backdoor)

Arka kapı, belli bir TCP ya da UDP portundan gelecek saldırı amaçlı komutlar için dinleme yapan zararlı programlara verilen isimdir. Arka kapılar çoğunlukla istemci/sunumcu yapısında çalışmaktadır. Sunumcu bileşeni saldırılan bilgisayara yüklenmekte, istemci bileşeni ise saldırganın uzaktaki bilgisayarından çalıştırılarak sunumcuya bağlanılmaktadır. Bağlantı sonucunda saldırgan saldırılan bilgisayar üzerinde belli ölçülerde kontrol elde edebilmektedir: dosya transferi, şifrelerin ele geçirilmesi, istenilen komutların çalıştırılması (Uzaktan Yönetim Amaçlı araçlar: SubSeven, Back Orifice, ve NetBus), başka bilgisayarlara, sistemlere devre dışı bırakma saldırıları yapabilme (*Zombies* ya da *Bot* olarak da adlandırılırlar, Trinoo ve Tribe Flood Network) vb.

2.5.2 Keylogger

Keylogger kullanıcının klavyede dokunduğu tuşları kaydeden programlara verilen isimdir. Bu tür programlar aracılığıyla yazılan e-postalar, kullanılan kullanıcı isimleri/şifreleri, hazırlanan dokümanlar, kredi kartı bilgileri vb. kritik bilgiler gizlice kaydedilir ve saldırgan tarafından e-posta, dosya transferi vb. yollarla elde edilebilir. KeySnatch, Spyster ve KeyLogger Pro keylogger programlarına örnektir.

2.5.3 Rootkit

İřletim sistemi dosyalarını deęiřtirerek sistemin saldırganın amacı doęrultusunda alıřmasını saęlayan dosyalar toplamına verilen isimdir. Rootkit tarafından sistem üzerinde yapılan deęiřiklikler ile rootkitin varlıęının tespiti zorlařtırılır. Örneęin rootkite ait dosyaların ya da ilgili proseslerin listelenmesi engellenir. Rootkitler sisteme arka kapı, keylogger gibi saldırı araçları kurulması için kullanılabilir. LRK5, Knark, Adore ve Hacker Defender rootkitlere örnektir.

3. VİRÜS/ZARARLI YAZILIM KORUNMA YÖNTEMLERİ

3.1 Politika

Öncelikle kurumun zararlı kod ve yazılımlardan korunmak için yazılmış bir politikasının olması gerekmektedir. Politika, kullanıcıların ve BT personelinin zararlı kod/yazılımlar konusunda bilinçli konuma getirilmesi, açıklıkların kapatılması, tehditlerin engellenmesi konularında yönlendirici/yol gösterici temel teşkil edecek kuralları içermelidir. Aksi durumda zararlı kod/programların sisteme zarar vermesini engellemek için kurum genelinde alınacak önlemler etkili ve sürekli olmayacaktır. Politika değişik çözümlerin uygulanmasına olanak sağlayacak şekilde genel ifadeler içermeli, aynı zamanda kapsam ve içerik olarak anlaşılır ve uygulanabilir olmalıdır. Politika aşağıda belirtilen maddeleri içerebilir, fakat bu maddelerle sınırlı değildir ve tüm maddeleri içermesi zorunlu değildir:

- Sistem üzerinde çalışan antivirüs programının ağa giren ve ağdan çıkan tüm trafiği taraması sağlanmalıdır.
- Kurumun bilgi işlem kaynakları sadece iş amaçlı kullanılmalıdır. Kişisel kullanımlar zararlı kod/yazılımların sisteme bulaşmasının başlıca sebebidir, kaçınılmalıdır.
- Kurum dışından getirilen disket/CD/flash disk/hafıza kartları/mp3 player/taşınabilir hard disk vb. medyalar kullanılmadan önce zararlı kod/program taramasından geçirilmelidir.
- E-posta eklenti dosyaları öncelikle hard diske kaydedilmeli, taranmalı ve sonrasında açılmalıdır.
- Belli uzantılara (exe, com, dll, vbs vb.) sahip dosyalar e-posta eklentisi olarak gönderilememelidir, Zararlı kod/program yayılması tespit edildiğinde e-posta eklentilerinde geçici süre ile ek kısıtlamalara gidilebilir (örneğin doc uzantılı dosyalar)
- Mesajlaşma, masaüstü arama motoru, dosya paylaşma vb. programlar zararlı kod/programların yayılmasına yardımcı oldukları için iş amaçlı olmadıkça kullanımları engellenmelidir.
- Kullanılmayan servisler/programlar zararlı kodlar/programlar tarafından kullanılan açıklıklar içerebilir, bu sebeple kullanımları/kurulumları engellenmelidir.
- Yönetici haklarının kullanıcılar tarafından kullanılması önlenmelidir. Bu sayede zararlı kod/yazılımlar sisteme bulaştığında verecekleri zararlar sınırlandırılabilir.

- İşletim sistemi ve uygulamalara ait güncellemeler ve yamalar zamanında yapılarak sistemde bilinen açıklıkların bulunması önlenmelidir.
- Taşınabilir medyanın zararlı kod/yazılım bulaşma riski yüksek olan sistemler üzerinde kullanımı engellenmelidir.
- Sistem bileşeninin kullanım amacına (dosya sunumcu, vekil (Proxy) sunumcu, E-posta sunumcu, kişisel bilgisayar), konumuna (ağ geçidi(gateway), frontend sunumcu vb.) ve gücüne (Sunumcu, PC, PDA vb.) bağlı olarak ne tür önleyici yazılımlar kurulacağı (örnek: antivirüs, spyware detection, removal utilities), konfigürasyon parametreleri (tarama periyodu, tarama kapsamı, güncelleme yöntemi, zamanı vb.) belirlenmelidir.
- Diğer ağlara/İnternete erişim sadece kurum tarafından onaylanmış ve güvenliği sağlanmış yollardan yapılmalıdır. Kurum dışı kablosuz erişim, dial-up, GPRS vb. erişimlere izin verilmemelidir.
- Güvenlik duvarı kurallarında yapılacak değişiklikler gerekli onay sürecinden geçmelidir.
- Sistemde kullanılması gerekli mobil kodlar belirlenmeli, gereksiz olanlar engellenmelidir.
- Mobil cihazların sistemin hangi bölümlerinde hangi güvenlik önlemleri ile kullanılabileceği tanımlanmalıdır.

3.2 Kullanıcı Eğitimi

Sistem kullanıcılarının zararlı kod/yazılımların sisteme giriş, yayılma ve sisteme zarar verme yöntemleri ile bunlardan korunma yolları konusunda bilinçlendirilmeleri gerekmektedir. Kullanıcılar şu hususlarda bilgilendirilmelidirler:

- Şüpheli e-postalar ve eklenti dosyalar açılmamalıdır.
- Şüpheli web tarayıcı popup pencerelerine tıklanmamalıdır.
- Zararlı kod/yazılım içermesi muhtemel sitelere girilmemelidir.
- Bilinmeyen fakat zararlı kod/yazılım olması muhtemel .bat, .com, .exe, .pif, .vbs vb. uzantılı dosyalar açılmamalıdır.
- Antivirüs, spyware tespit, zararlı kod kaldırma, güvenlik duvarı vb. güvenlik yazılımlarının çalışması engellenmemelidir.

- Yönetici yetkilerine sahip hesaplar günlük işlerde (web gezintisi, kişisel e-posta kullanımı, geliştirme faaliyetleri vb.) kullanılmamalıdır.
- Güvenilmeyen sitelerden programlar indirilmemeli/çalıştırılmamalıdır.

3.3 Açıklık Yönetimi

Zararlı kod/programlar sıklıkla işletim sistemi, uygulamalar ya da servislerde bulunan açıklıkları kullanarak sistemlere zarar verirler. Bu sebeple açıklık yönetiminin nasıl yapılacağı prosedürlerle tanımlanmalı ve uygulanması sağlanmalıdır.

- Sistem bileşenlerinde ortaya çıkabilecek açıklıkların takibi:
 - İlgili e-posta gruplarına üyelik
 - Üretici firma web siteleri
 - Açıklıkların, güncel tehditlerin duyurulduğu güvenlik web sitelerinin takibi
 - vb.
- Açıklıkların kapatılması:
 - Güncellemelerin, yamaların gecikmeden yapılması
 - Kullanılmayan servislerin kapatılması
 - Güvenlik sıkılaştırması, zayıflığa yol açan konfigürasyonun değiştirilmesi
 - Kurulumla gelen kullanıcı ismi ve şifrelerin değiştirilmesi
 - Zorunlu olmayan paylaşımların kapatılması
 - Kullanıcı haklarının işlerini yapması için yeterli olan en düşük seviyede tutulması
 - vb.
- Periyodik açıklık taramaları

3.4 Antivirüs Yazılımı

Antivirüs yazılımları zararlı kod/yazılımlardan korunmak için kullanılan teknik kontrol mekanizmalarının en etkinidir. Antivirüs yazılımı işletim sistemini, uygulamaları ya da dosyaları hedef alan tehditlere karşı koruma sağlar. Antivirüs yazılımları genel olarak:

- Kritik sistem bileşenlerinin sistem açılışında taranması (İşletim sistemi başlatma dosyaları, boot record dosyaları, dll dosyaları vb.)
- Sistem aktivitelerinin şüpheli durumları tespit amacıyla gerçek zamanlı izlenmesi
- E-postaların ve eklenti dosyalarının alma ve gönderme aşamalarında taranması
- Kopyalanan/açılan/değiştirilen dosyaların taranması (on-access taraması)
- Mevcut dosyaların genel virüs taramasından geçirilmesi (periyodik/isteğe bağlı (on-demand) virüs taramaları)

- Virüslü dosyaların temizlenmesi / karantinaya alınması / silinmesi
- Virüslü programların çalışmasının engellenmesi
- Virüs olaylarının raporlanması
- Virüslerin yayılmasını önlemek amacıyla servislerin, portların kapatılabilmesi (tüm antivirüs ürünlerinde bu seçenek bulunmamaktadır)

Antivirüs yazılımlarının zararlı kod/yazılımları tespit etmek için kullandığı ana yöntem, her bir zararlı kod/yazılımın belirli karakteristik özelliklerini içeren imzalarla, taranan bileşenleri ve/veya sistem aktivitelerini karşılaştırma yöntemidir. İmza ile karşılaştırma yöntemi sadece bilinen türlerdeki virüsleri tespit etmekte kullanılabilir. Yeni ortaya çıkan ya da sürekli yapısını değiştirmek üzere programlanmış zararlı kodları tespit edebilmek için antivirüs yazılımları *heuristic tekniklerini* kullanmaktadırlar. Heuristic teknik ile taranacak dosyaların karakteristik özellikleri dikkate alınır. Dosyaların içinde şüpheli kod dizileri aranır, ya da dosyalar sanal makine (virtual machine) üzerinde çalıştırılarak normal dışı aktivitelere sebep olup olmadığı incelenir. Fakat heuristic tekniklerin dezavantajları da vardır. Hatalı tespit (false positive) 'ler yaparak temiz dosyaların kullanımını engelleyebilir. Bu sebeple birçok antivirüs yazılımı varsayılan ayarlarında heuristic tarama seviyesi düşük ya da orta seviye seçili olarak kurulmaktadır. Bu durumda da zararlı kod/yazılımların tespit edilememesi riski (false negative) ortaya çıkmaktadır. Bu noktada yanlış uyarılarla normal kullanımın aksaması, sistem yöneticilerinin zaman kaybı ile yeni çıkmış (imzası oluşturulmamış, ancak heuristic tekniklerle tespit edilebilecek) zararlı kod/yazılımların tespit edilememesi sonucu doğabilecek riskler dikkate alınarak heuristic koruma seviyesi belirlenmelidir.

Antivirüs yazılımının kurulu olması bir bilgisayarın zararlı kod/yazılımlara karşı güçlü bir korumaya sahip olduğunu göstermez. Başarılı sonuç için:

- Antivirüs yazılımı ağ giriş-çıkış noktalarına (güvenlik duvarı, e-posta sunucusu, uzaktan erişim sunucusu vb.), sunuculara, kullanıcı bilgisayarlarına, dizüstü bilgisayarlar ve PDA'lere işletim sistemleri kurulduktan hemen sonra yüklenmelidir..
- Antivirüs yazılımlarının ağ bileşenlerinde kurulu ve çalışır konumda olduğu merkezi olarak izlenmelidir. Kullanıcıların programı kaldırmalarına izin verilmiyor olmalıdır.
- Antivirüs yazılımının etkin çalışması gerekli ayarlar sistem yöneticisi tarafından yapılmış olmalı ve kullanıcılar tarafından değiştirilememelidir. Örneğin gerçek zamanlı koruma her zaman açık olmalı, periyodik taramalar durdurulamamalı, güncellemeler engellenememelidir.

- Virüs tanımları / arama motoru güncellemeleri zamanında yapılmalıdır.
- Virüs ya da diğer zararlı yazılım saldırılarının zamanında tespiti için uyarı mekanizmasının (e-posta ile sistem yöneticisinin otomatik olarak bilgilendirilmesi vb.) ayarlanmış olması gerekmektedir.
- Ağ giriş noktalarında kullanılan antivirüs yazılımı ile kullanıcı bilgisayarları ve sunucu makinelerinde kullanılan antivirüs yazılımının farklı olması tercih edilmelidir. Antivirüs yazılım üretici firmaların virüs tespit başarımları sabit değildir. www.avcomperatives.org dan yayınlanan bağımsız antivirüs yazılım karşılaştırma raporlarının bir çoğundan görülebileceği gibi antivirüs yazılımlarının başarımları zamanla ve virüsten virüse değişiklik göstermektedir. Farklı antivirüs yazılımlarının farklı sistem noktalarında kullanımı, bir antivirüs yazılımının sayıflığının sistemi büyük zararlara uğratması riskini azaltacaktır.

3.5 Virüs Temizleme / Acil Müdahale

Bağımsız araştırmalara göre gelişmiş antivirüs yazılımları zararlı kod/yazılımları %90'ın üzerinde başarı oranı ile tespit edebilmekte ve gerekli işlemleri yapmaktadırlar (Temizlemek, karantinaya almak, yayılmalarını önlemek gibi) [1]. Fakat bazı durumlarda antivirüs yazılımları virüslerin tespitinde, temizlenmesinde ya da yayılmasının engellenmesinde yetersiz kalabilmektedir. Bu tür durumlarda karşılaşılan sorunlar:

- Veri kaybı/çalınma/değiştirme vb.
- Sistem performansında düşüşler
- Sistemlerin çalışmaması
- Sistem kaynaklarının yetkisiz kullanımı
- vb.

Bu ve benzeri durumlarda zararın önlenmesi/azaltılması için acil müdahale de uzman bir ekibin müdahalesine ihtiyaç duyulmaktadır. Acil müdahale ekibinde yer alacak elemanların sahip olması gereken özellikler şunlardır:

- Zararlı Kod/ Yazılım Yayılma Yöntemleri: Farklı zararlı kod/yazılım türleri farklı yöntemlerle yayılmaktadır (Örnek: virüs bulaşmış program çalıştırıldığında, e-posta eklentileri ile, ağ paylaşımları ile, programlara gömülü olarak vb.). Yapılacak müdahalenin doğru noktalara yapılması ve etkin olması için ilgili zararlı kod/yazılımın yayılma yöntemleri konusunda yeterli bilgi sahibi olmak zorunludur.

- Zararlı Kod/ Yazılım Tespit Araçları: Tespit işlemi yaygın olarak antivirüs yazılımı, ağ veya bilgisayar tabanlı saldırı tespit yazılımları, spyware tespit yazılımları ve benzeri araçlarla yapılmaktadır. Acil müdahale ekibi elemanlarının kurum ağında bulunan tespit amaçlı araçlarının kullanımı konusunda bilgi sahibi olması gerekmektedir.
- Bilgisayar Adli Analiz: Acil müdahale ekip elemanlarından en az bir kişinin bilgisayar adli analiz (computer forensics) için kullanılan araçların kullanımı konusunda bilgi sahibi olması gerekmektedir. Bu tür bir uzmanlığa çok ciddi analiz gerektiren rootkitlerin tespiti gibi durumlarda için ihtiyaç duyulacaktır.
- BT Alanında Tecrübe: ZYK'ların potansiyel etkisinin analiz edilmesi, yayılmasının önlenmesi, temizlenmesi ve kayıp verilerin geri döndürülmesi aşamalarında uygun adımların atılması için acil müdahale ekibi elemanlarının BT Alanında tecrübeli olmaları gerekmektedir.
- Programlama Yeteneği: Betik ve makro dilleri konusunda bilgi sahibi olmak yeni çıkan ZYK'ların davranışları ve etkileri konusunda tahminlerde bulunmaya ve uygun önlemleri almaya yardımcı olacaktır.

Acil müdahale sırasında izlenmesi gereken adımlar:

- Tanımlama Aşaması: ZKY'nin tespit ve analizi
- Engelleme Aşaması: Zararlı kod / yazılım bulunan bileşenlerin izolasyonu / yayılmanın engellenmesi / temizlenmesi
- Temizleme Aşaması: Oluşan kayıp / sorunların giderilmesi

3.5.1 Tanımlama Aşaması:

Sisteme bulaşan ZKY'nin tanımlanması ve kritikliğinin belirlenmesi büyük önem taşımaktadır. Aşağıda bir sisteme ZKY bulaştığında sıklıkla karşılaşılan durumlar sıralanmıştır:

- Kullanıcıların internet ve yerel alan ağında düşük hızlardan, RAM/ CPU kullanımının yüksek seviyelerde bulunmasından, sabit disk erişimindeki yavaşlıktan ve bilgisayarın yavaş açılıyor olmasından dolayı yaptığı şikayetler.
- Antivirüs yazılımının solucan tespit etmesi ve uyarı vermesi
- Dosya isimlerinde alışılmadık karakterler görülmesi

- Kayıt tutma ayarlarının değiştirilmesine dair bir kayıt görülmesi
- Web Sunucusunun çalışmaz hale gelmesi
- Web browser kullanılmaya çalışıldığında bilgisayarın yeniden başlatılması
- E-Posta yöneticisinin çok sayıda şüpheli içerikli geri dönmüş e-posta tespit etmesi
- Çok sayıda bilgisayarda antivirüs ve güvenlik duvarı yazılımlarının kapatılmış olması
- Ağ yöneticisinin ağ trafik yapısında normal dışı aktiviteler tespit etmesi
- Vb.

Bu durumlardan herhangi biri ile karşılaşıldığında ZKY'nin varlığından şüphelenmek akılcı bir yaklaşım olsa da, sistemlerde yaşanabilecek sorunlar aynı zamanda yanlış konfigürasyon, yazılımda bulunan kodlama sorunu ya da donanımsal bir sorun da olabilir. Bu sebeple doğru tespitlerin yapılabilmesi için sistemde bulunan güvenlik bileşenleri ya da ZKY'lerin yayılmak/bilgi kaçırmak/komut almak için kullandığı/geçtiği bileşenlerden kayıtlar veya kullanıcılardan/ağ/sistem sorumlularından gelecek geri bildirimlerin değerlendirilmesi kritik önem taşımaktadır. ZKY tespiti için şu bileşenler incelenmelidir:

- Antivirüs ve STS yazılımlarının uyarı mesajları / kayıtları, antivirüs yazılımından alınabilecek sistem durum raporları
- Güvenlik duvarı ve yönlendirici kayıtları (Bloklanmış trafik bilgisi)
- E-posta sunumcusu ya da ağ tabanlı STS'den e-posta header, ya da eklenti dosya bilgileri,
- Ağ trafiğini kaydeden Sniffer kayıtları, Ağ analiz araçlarının kaydettiği ZYK'lara ait ağ trafiği

Tablo 3.1'de [2] çeşitli uyarı ya da belirtilerin ne tür ZYK'lardan kaynaklanmış olabileceğine dair bilgi verilmektedir:

Uyarı /Belirti	ZKY Türü						Saldırı Aracı Türü				
	Multipartite Virüs	Makro Virüs	Ağ Servisi Soluncanı	E-posta Soluncanı	Trojan Atı	Zararlı Mobil Kod	Backdoor	Keylogger	Rootkit	Zararlı Browser Plug-In	E-Posta Gönderici
Güvenlik Araçları											
Antivirüs Uyarıları	X	X	X	X	X	X	X	X	X	X	X
Spyware Uyarıları					X	X				X	
Ağ-Tabanlı Saldırı Önleme Uyarıları			X	X			X				
Bileşen Tabanlı STS dosya değişik uyarıları					X				X		
Güvenlik Duvarı ve Yönlendirici Kayıtları			X				X				
Gözlenen İstemci Aktiviteleri											
İşletim Sistemi (OS) Boot Edemiyor	X								X		
OS Boot Ederken Hata Mesajı	X								X		
OS Sıklıkla Göçüyor		X	X		X		X		X		
Programlar yavaş başlıyor/çalışıyor ya da hiç çalışmıyor.	X	X	X		X				X	X	
OS başlatılırken bilinmeyen prosesler çalışıyor					X		X	X			X
Çalışması beklenmeyen portlar açık							X				
Ani olarak e-posta gönderim ve alımında yükseliş		X		X					X		
Word/Excel vb. dosyaları çalıştıran programların kalıp dosyalarında değişiklikler		X									

Uyarı /Belirti	ZKY Türü						Saldırı Aracı Türü				
	Multiparitate Virüs	Makro Virüs	Ağ Servisi Soluncanı	Eposta Solucanı	Trojan Atı	Zararlı Mobil Kod	Backdoor	Keylogger	Rootkit	Zararlı Browser Plug-In	E-Posta Gönderici
Web tarayıcısı konfigürasyonunda değişiklikler (değiştirilmiş varsayılan giriş sayfası vb.)						X				X	
Dosyalar silinmiş/ değiştirilmiş/açılmıyor	X	X			X				X		
Ekranda beklenmeyen mesajlar/pencereler/grafikler		X				X			X		X
Beklenmeyen diyalog kutuları izin talep ediyor.						X				X	
Gözlenen Ağ Aktiviteleri											
Normalin üstünde ağ kaynaklarının kullanımı			X	X			X				X
Port taramaları, açıklık içerebilecek servislere başarısız bağlantı girişimleri			X				X				
Bilinmeyen ağ dışı sistemlere bağlantılar			X		X	X	X	X	X	X	X

Tablo 3.1 – ZKY Tespit Tablosu

Bir kurumda ZKY kaynaklı olduğu düşünülen bir olayla karşılaşıldığında, öncelikle antivirüs sorumlusunun ZKY'nin türünü tanımlaması gerekmektedir. Sistemi/ilgili bileşenleri incelemeli, antivirüs firmalarının ZKY veritabanlarında tarama yapılmalı, BT güvenlik sitelerinde benzer olaylar araştırılmalı ve eğer ZKY olmadığına karar verilirse asıl sorunun çözümü için ağ/sistem/uygulama yöneticisi uyarılmalıdır.

Sistemde karşılaşılan ZKY daha önceden tanımlanmış ise, antivirüs yazılımının web sayfasından erişilen ZKY veritabanında şu bilgiler bulunacaktır:

- ZKY türü (virüs, solucan, Trojan atı vb.)
- Hedeflediği port ve servisler
- Kullandığı açıklıklar
- E-posta başlık, eklenti ismi, eklenti büyüklüğü, eposta içeriği
- Hangi işletim sistemlerinin, uygulamaların etkilendiği
- ZKY'nin nasıl sisteme/bileşene bulaştığı (Açıklık, yanlış konfigürasyon vb.)
- ZKY bulaştıktan sonra sistemi nasıl etkilediği (değiştirdiği/sildiği dosyalar, değiştirdiği konfigürasyon, açtığı backdoor portları vb.)
- ZKY'nin sistemden nasıl temizleneceği

Önceden tanımlanmamış ZKY durumunda ise olay müdahale ekibinin inceleme yapması ve uygun önlemleri belirlemesi gerekecektir. Bu işlem mevcut sistem üzerinde ya da ZKY ayrı bir test sistemine taşınarak yapılabilir (ZKY, ZKY içeren bileşen ya da disk imajı alınarak test sistemine aktarılabilir). ZKY analiz işlemi için yardımcı araçlara ihtiyaç duyulabilir. Araçlar taşınabilir medyada tutulmalıdır. Bu araçlar:

- ZKY'nin tanımlanması için antivirüs, spyware tespit ve temizleme araçları
- Çalışan prosesleri listeleyen bir araç
- Ağ bağlantılarını görüntüleyen bir araç
- Vb.

Araçların ZKY'lerden etkilenmemesi ve değiştirilememesi sağlanmalıdır. Bunun için örneğin floppy diskler ve USB flash diskler yazma korumalı yapılmalı, CD'ler kapatılmış (finalized) olmalıdır. Bu araçları kullanmaktaki amaç sistemde bulunan ZKY'lerin kurulu olan antivirüs, spyware türü programların çalışmasını engellemiş olma durumunda ZKY tespit işlemini gerçekleştirebilmektir.

ZKY tanımlandıktan sonraki aşama olay müdahale işleminin aciliyetinin belirlenmesidir. Örneğin solucan türü ZKY'ler oldukça hızlı yayılırlar ve birkaç saat içinde sisteme önemli zararlar verebilirler, bu sebeple acil müdahaleye ihtiyaç duyulmaktadır. Fakat Truva atı türü ZKY'ler yayılma yeteneğine sahip değildirler, bunlara müdahale önceliği Truva atı bulaşan bileşenin taşıdığı verilerin kritikliğine göre belirlenmelidir. Bu sebeple her kurumun ZKY olaylarında müdahalenin aciliyetini belirlemek için kriterler oluşturması gereklidir:

- ZKY sisteme nasıl girdi, ne tür veri gönderme yöntemi kullanıyor?
- ZKY türü nedir?
- ZKY tarafından bileşene ne tür saldırı araçları yerleştirilmiş?
- ZKY hangi bileşenleri/ ağları etkiliyor, etkileme yöntemi nedir?

- ZKY'nin etkisi müdahale edilmezse ne kadar zamanda artacak?

ZKY türü belirlendikten sonra hangi ağ bileşenlerine ZKY'nin bulaştığının belirlenmesi zahmetli ve zaman alıcı bir işlem olabilir. Bileşenlerin belirlenmesinde uygulanabilecek yöntemler aşağıda belirtilmiştir

- Antivirüs, STS, Spyware türü yazılımların kayıtlarının incelenmesi. Eğer belirtilen araçlar ZKY bulaşan bileşenleri belirleyebiliyorsa bu işlem kısa sürede tanımlanmış olur.
- ZKY'lerin bileşenler üzerinde yaptığı karakteristik değişiklikleri kontrol eden login script kullanarak,
- Ağ tabanlı saldırı tespit sistemine benzer karakteristikleri içeren imza oluşturarak
- Paket dinleme yazılımları ile dinleme yapılıp, ZKY'nin karakteristik özellikleri aranarak (Bağlanılmak istenen bir IP vb.).
- Port taramaları yapmak, eğer ZKY belli bir porttan backdoor oluşturuyorsa tespit işleminde yardımcı olacaktır.

Burada dikkat edilmesi gereken husus, yukarıdaki yöntemlerin kapalı konumdaki ya da ağ bağlantısı kesilmiş bileşenleri kontrol edemeyeceğidir. Bileşen tespit işlemi müdahale işlemi süresince belli aralıklarla tekrarlanmalı, yukarıdaki yöntemler yetersiz kaldığında bileşenlere giderek direk kontroller yapılmalıdır.

3.5.2 Engelleme Aşaması

ZKY tanımlandıktan sonra yapılması gereken işlem ilgili ZKY'nin sistemde yayılmasının durdurulması ve sisteme daha fazla zarar vermesinin engellenmesidir. Yayılma eğilimi göstermeyen ZKY'lere müdahale kısmen daha kolaydır: ilgili bileşenin ağ bağlantısı koparılır veya kapatılır ve böylece ilk müdahale aşaması (engelleme) tamamlanmış olur. Fakat yayılma eğilimi gösteren ZKY'lere müdahale için kurumların bir strateji geliştirmiş olmaları gerekmektedir: Böylece ilk müdahalenin mümkün olduğunca çabuk yapılması sağlanarak sistemin ZKY'lerden göreceği zarar sınırlandırılabilir ve sistem geri döndürme işleminin en kısa zamanda tamamlanması sağlanabilir.

Engelleme aşamasında dikkate alınması gereken önemli bir hususta bir ZKY'nin ağ üzerinde yayılmasının engellenmesi, o ZKY'nin sisteme vereceği zararın engellendiği anlamına gelmeyebilir. Yayılması engellendikten sonra da dosyaları, uygulamaları, OS bileşenlerini silmeye ya da onlara bulaşmaya devam edebilir. Ayrıca bazı tür ZKY'ler bulaştıkları bileşenin ağ bağlantısı kesildiğinde ya da başka türlü engelleme önlemleri alındığında ek zararlar vermek üzere tasarlanmıştır. Örneğin bir ZKY uzak bir bilgisayara periyodik olarak bağlantı kurmakta, bağlantı sağlanamadığında ise hard disk üzerindeki dosyaların üzerine yazmak için ayarlanmış olabilir. Bu sebeple olaya müdahale eden acil müdahale elemanı ZKY'nin verebileceği zararları dikkate alarak hareket etmeli, gerektiği zaman ZKY temizleme işlemine engelleme aşamasından hemen sonra başlamalıdır.

Engelleme işlemi gerçekleştirilirken ilgili bileşenin kurum için kritikliği dikkate alınmalıdır. Bu kritik bileşenlere müdahale için stratejiler ve prosedürler geliştirilmelidir. Örneğin e-ticarette uğraşan bir kurumun web sunumcusunun bağlantısının koparılması, ZKY'nin engellenmesi için kabul edilemez olabilir. Bu durumda alternatif engelleme yöntemleri kullanılmalıdır (belli portların kapatılması, servislerin durdurulması vb.).

Engelleme metotları 4 temel kategori içinde ele alınabilir:

- **Kullanıcı katılımı:** ZKY'nin çok sayıda bileşene yayıldığı ve merkezi müdahalenin mümkün olmadığı durumlarda etkin bir yöntemdir. Kullanıcılara, ZKY'nin varlığını nasıl tespit edecekleri, olması durumunda ne tür işlemler yapmaları gerektiğini bildirilir (Örneğin yardım masasını aramak, ağ bağlantısını koparmak, bilgisayarı kapatmak, antivirüs tanımlarını güncellemek, virüs taraması yapmak, temizleme araçlarını çalıştırmak vb.). Kullanıcı katılımı ZKY'nin engellenmesi ve temizlenmesi aşamalarında etkin bir yöntem olmakla beraber, tüm kullanıcılara talimatların iletilmesi ya da tüm kullanıcıların talimatları uygulaması sağlanamayabilir. Bu sebeple kurumun sadece kullanıcı katılımına güvenmesinin ağır sonuçları olabilir.

- **Otomatik Tespit ve Engelleme:** Antivirüs, Spyware, STS, E-Posta filtreleme araçları ZKY'lerin engellenmesinde kullanılan otomatik yöntemlerdir. Yeni çıkmış ZKY'nın tespitinde yetersiz kalındığında yapılacak güncellemelerle tehdidin engellenmesi mümkün olabilmektedir. Fakat bazı durumlarda engelleme için kullanılan araçlarda ZKY'lerden zarar görmekte ve kullanılamaz hale gelebilmektedir. Böyle durumlar için alternatif engelleyici araçların sistemde kullanılabilir durumda tutulması kritik önem taşımaktadır. Örneğin antivirüs servisi bir solucan tarafından durdurulmuş olabilir. Bu durumda solucan e-posta yoluyla yayılıyor ise e-posta filtreleme yapabilen (başlık, eklenti ya da içeriğe göre) bir e-posta sunucu güvenlik yazılımı ile solucan yayılması engellenebilir. Ağ tabanlı ya da bileşen tabanlı saldırı önleme sistemleri (SÖS) yapılacak güncelleme ve ayarlar ZKY'lerin yayılmasını durdurabilir. Ağ tabanlı SÖS tek ya da az sayıda bileşende kurulu olacağı için güncellenmesi de daha hızlı ve kolayca yapılabilir.
- **Servislerin geçici durdurulması:** Bazı ZKY'ler sistemde yıkıcı etkiye bulunuyor olabilirler. Yoğun e-posta ya da dosya transfer trafiği yaratarak bazı uygulamaların çalışmaz hale getirilmesi vb. durumlar görülebilir. Bu tür durumlarda engelleme işlemi ZKY'nin kullandığı servislerin kapatılması, güvenlik duvarı üzerinden ilgili servisin kullandığı portların kapatılması, e-posta listelerinin kullanımının engellenmesi vb. yöntemlerle yapılabilir. Bu yöntemlerin kullanımındaki amaç sistemin engelleme aşamasında sistemin zarar gören kısımlarını engellemek, diğer servislerin mümkün olduğunca çalışmaya devam etmelerini sağlamaktır. Engelleme işlemleri uygulama(servislerin kapatılması) ya da ağ seviyesinde(TCP/UDP portlarının güvenlik duvarı ya da ağ geçitleri üzerinde engellenmesi) yapılabilir. Servislerin durdurulması sistem yöneticileri için kolay ve hızlı şekilde uygulanabilir bir çözümdür. Bu yöntemin dikkat edilmesi gereken kısmı hangi servislerin kapatılması gerektiğinin belirlenmesi ve bir servisin kapatılması durumunda etkilenecek diğer servislerin biliniyor olmasıdır. Bu sebeple kurumda kullanılan servislerin bağımlılıkları, hangi servislerin hangi uygulamalar tarafından kullanıldığı ve hangi portları kullandıkları önceden dökümanite edilmiş olmalıdır.

- **Belli türdeki ağ bağlantılarının engellenmesi:** ZKY'lerin belli portları kullanarak yayıldığı, uzak sistemlere bağlanıp veri transferi yaptığı, toolkit yüklediği ya da komutlar aldığı durumlarda ilgili IP'lere erişimin ya da portların kullanımının güvenlik duvarı üzerinden engellenmesi olayın kontrol altına alınana kadar engellenmesinde etkin bir çözümdür. Bir başka çözüm de müdahale edilecek ağ bileşeninin ağ bağlantısının fiziksel olarak engellenmesidir. Alternatif olarak henüz ZKY bulaşmamış bileşenlerin ağ bağlantıları engellenerek bunların zarar görmesi de engellenebilir. Proaktif önlem olarak sunucuların ve istemcilerin farklı ağ segmentlerine alınması, ya da bileşenlerin ağa dahil edilmeden Ağa Giriş Kontrol Sunucusu tarafından bileşen üzerinde antivirüs yazılımının çalışıp çalışmadığı, virüs tanımlarının güncelliği, güvenlik duvarının durumu, OS güncellemelerinin yapılıp yapılmadığı vb. kontrol edilerek ağa kabul edilmesi ya da karantina VLAN'ına alınmasına karar verilebilir (Network Access Control).

3.5.3 Temizleme Aşaması

ZKY'nın tespit edilip yayılması ve sisteme zarar vermesi önlendikten sonraki aşama ZKY'nın sistemden tümüyle temizlenmesidir. Temizleme aşaması aynı zamanda ZKY'nın sisteme girmesine sebep olmuş olan ilgili açıklığın (OS güncelleme eksikliği, güvenlik kontrolü yapılmayan ağ paylaşımları, gereksiz servisler vb.) kapatılması işlemini de içermektedir. Engelleme aşamasında kullanılan yöntem, temizleme aşamasında kullanılabilecek yöntemleri de belirlemektedir. Örneğin ağ bağlantısı kesilmiş bir bileşenin temizlenmesi işlemi uzaktan yapılamaz, fakat eğer bileşen ayrı bir VLAN'a alınmış ise temizleme için kullanılacak sunucu aynı VLAN'a alınarak uzaktan temizleme işlemi gerçekleştirilebilir.

Temizleme işlemlerinde yaygın olarak kullanılan araçlar antivirüs, spyware tespit ve temizleme yazılımları, yama yönetimi yazılımı vb. olarak sayılabilir. Bir bileşende uzaktan ZKY taraması başlatmak gibi otomatik temizleme yöntemleri, yerel olarak CD'den başlatılacak temizleme aracı kullanmaktan daha etkili ve kolay bir yöntemdir, fakat bazı durumlarda otomatik yöntemler etkisiz kalabilir. Örneğin sistem kaynaklarını tüketen ve diğer ağ bileşenlerine zarar vermeye çalışan ZKY'lerle karşılaşıldığında ilgili bileşenin ağ bağlantısı kapatılmak zorundadır. Bu durumda otomatik yöntemlerin kullanılması mümkün değildir ve yerel olarak temizleme işlemi gerçekleştirilmelidir. Yerel müdahalenin gerektiği ve ZKY bulaşan bileşen sayısının fazla olduğu durumlarda kullanıcı katılımı gerekli olabilmektedir. Kullanıcılara gönderilecek talimat ve temizleme araçları ile temizleme işlemi daha kısa sürede gerçekleştirilebilir.

Bazı ZKY olaylarında temizleme işlemi işletim sistemin yeniden kurulması, güvenli hale getirilmesini ve kaybedilen verilerin önceki temiz yedeklerden döndürülmesini içerebilir. Fakat bu yöntem klasik temizleme yöntemlerine göre daha fazla zaman ve kaynak tüketici olduğu için mümkün olduğu kadar son çare olarak görülmelidir. İşletim sistemi ve standart programların bulunduğu bilgisayar imajları bu işlemi hızlandırabilir. Yeniden kurulumu gerektiren durumlara örnekler şunlardır:

- Saldırganlar bileşene yönetici seviyesinde erişim hakkı elde etmiş,
- Yetkilendirme işleminden geçmeden bir backdoor ya da solucan tarafından açılmış paylaşımlarla sisteme sınırsız erişim mümkün,
- Sistem dosyaları Truva atı, Arka kapı, Rootkit veya benzer saldırı araçları ile değiştirilmiş,
- ZKY temizlendikten sonra da işletim sistemi beklendiği gibi çalışmıyor, verdiği zararlar geri döndürülemez seviyede
- ZKY'yi temizle yöntemi bilinmiyor

ZKY'ın yukarıda belirtilen karakteristikleri taşımadığı durumlarda temizleme işleme güncel virüs veritabanı yüklenmiş antivirüs yazılımı, spyware temizleme araçları, ilgili ZKY için yazılmış temizleme araçları (Antivirüs üreticilerinin web sayfalarından indirilebilir) ya da BT güvenlik sitelerinde bulunabilecek talimatların elle uygulanması yolu ile temizlenebilirler. Temizleme işlemiyle birlikte ilgili açıklık ta kapatılmalıdır.

Temizleme işlemi çoğunlukla günler, haftalar sürebilen uzun süreli bir aşamadır. Bu aşamada ZKY bulaşmış bileşenleri tespit etme işlemine devam edilmelidir. İlgili bileşenlerin sayısında görülen azalma uygulanan temizle yönteminin etkinliğinin göstergesi olacaktır. Aksi takdirde alternatif temizleme yöntemleri denenmelidir.

4. MERKEZİ ANTİVİRÜS KORUMASI

Sistemin güvenliğinin sağlanması amacıyla, antivirüs yazılımlarının zararlı yazılımları tespit edip engelleyebilecek şekilde yapılandırılmaları ve yönetilmeleri gerekmektedir. Çok sayıda sunumcu ve kullanıcı bilgisayarının olduğu kurumlarda bu işlemlerin her bir bilgisayar üzerinde ayrı ayrı yapılması mümkün değildir. Merkezi antivirüs yönetimi yapılmayan kurumlarda, tüm konfigürasyonlar doğru olarak yapılsa da, aşağıda belirtilen riskler mevcuttur:

- Yapılan ayarlar kullanıcılar tarafından değiştirilerek yazılımın etkin çalışması engellenebilir
- Antivirüs servisleri durdurulabilir
- Antivirüs yazılımı kaldırılabilir
- Antivirüs kurulu olmayan bilgisayarlar fark edilmeyebilir
- Virüs tanımlarının güncellenmesi aksayabilir
- Sisteme yapılan virüs saldırılarının antivirüs yöneticisi tarafından çabukla analiz edilip müdahale edilmesi mümkün olmayabilir.
- vb.

Yazılım Özellikleri: Bu sebeplerle merkezi olarak yönetilen bir antivirüs yapısı olmayan kurumların merkezi yapıya geçmeleri kritik önemdedir. Merkezi yönetim yazılımının şu özelliklerinin olması beklenmelidir:

- Uzaktan kurulum
- Kullanıcıların yapılan ayarları değiştirmesini, servisleri durdurmasını, programı kaldırmasını önleme kabiliyeti
- Virüs tanımlarının merkezi olarak güncelleyebilme
- Periyodik tarama ayarları
- İsteğe bağlı tarama yapabilme
- Sürekli (dosya yaratıldığında, kopyalandığında, okunduğunda, değiştirildiğinde vb.) tarama ayarları

- Antivirüs istemcilerin statülerinin izlenmesi (baęlantı durumu, antivirüs servisinin durumu, virüs tanımlarının güncellięi, virüs bulundu uyarısı, tarama motorunun ve yazılımın versiyon bilgisi, IP bilgisi vb.)
- Antivirüs yazılımlarının üreteceęi kayıtlara erişim
- Virüs yayılması konularında antivirüs yöneticisini bilgilendirecek e-posta, anlık mesaj vb. uyarı mekanizmaları
- Raporlama özellięi

Kurulum Aşaması: Merkezi antivirüs yapısı kurulurken aę topolojisi ve farklı aę bölümleri arasındaki hatların hızları dikkate alınmalıdır. Tek merkezi antivirüs yönetim sunucusu kurulumu yerine, farklı aę bölümlerinde (uzak ofislerde) yardımcı antivirüs sunumcuları kurulmalı, bu sunumcular merkezi antivirüs yönetim sunucusuna baęlanıp konfigürasyonları, virüs tanım dosyalarını, tarama motoru güncellemelerini almalıdır. Yoęun antivirüs trafięinin oluřtuęu anlardaki ihtiyaçları karřılamak için gerekli ise merkezi antivirüs sunucusu için İkili/Yedekli bir yapı kurulumu saęlanmalıdır. Mümkün olması durumunda ikili/yedekli yapıda çalışacak sunumcular için farklı işletim sistemi kullanımı tercih edilmelidir, böylece iki sunumcunun da benzer açıklıklar sonucunda devre dıřı kalması önlenecektir.

Konfigürasyon/Yönetim: Merkezi antivirüs yapısının kurulum işleminin sonrasında, sunucular ve kullanıcı bilgisayarları üzerlerinde çalışan uygulamalara, maruz kaldıkları tehditlere, zorunlu ise taramalarda kapsam dıřı tutulması gereken dosya/dizinlere, periyodik taramaların zamanına vb. farklı politika uygulanma ihtiyaçlarına göre gruplandırılmalı ve konfigürasyonları gruplara göre yapılmalıdır. Örneęin üzerinde Microft Exchange kurulu olan bir sunucuda *Exchsrvr\Mdbdata* dizini tarama kapsamı dıřında tutulmalıdır, ya da kullanıcı bilgisayarlarında periyodik taramalar hafta içi öęle arasında yapılırken sunumcularda hafta sonu yapılabilir vb.

4.1 ZKY İmzalarının Güncelliği

Antivirüs yazılımlarının zararlı kod/yazılımları tespit etmek için kullandığı ana yöntem, her bir zararlı kod/yazılımın belirli karakteristik özelliklerini içeren imzalarla, taranan bileşenleri ve/veya sistem aktivitelerini karşılaştırma yöntemidir. Bu yöntemin başarılı olabilmesi için sisteme bulaşan zararlı kod/yazılımı tespit için gerekli imzanın antivirüs yazılımına yüklenmesi gerekmektedir. Antivirüs yazılım üreticileri bir virüs ortaya çıkarıldıktan 1-2 saat sonra imzasını oluşturup yayımlayabilmektedirler. Ayrıca çoğunlukla günlük olarak imza paketlerini yayımlamaktadırlar. Antivirüs yazılımının başarılı olabilmesi için imza güncellemelerinin zamanında yüklenmesi sağlanmalıdır. Tavsiye edilen güncelleme periyodu gündüzdür. Fakat bazı acil ZKY saldırısı durumlarında daha kısa aralıklarla güncelleme yapılması gerekebilmektedir.

İnternet bağlantısı olan bilgisayarlarda güncellemeler yayımlandıktan kısa süre sonra ilgili güncelleme dosyası otomatik olarak çekilebilmektedir. İnternet bağlantısı olmayan sistemlerde ise güncellemeler, internetten çekilen güncelleme dosyasının taşınabilir medya ile merkezi yönetim sunucusuna aktarılması ile yapılmaktadır. Yukarıda belirtilen 2 durumda da güncellemelerin sadece antivirüs sunucusu üzerinden istemcilere dağıtılması yoluyla yapılmalıdır. İstemcilerin her birinin internetten güncelleme yapmak üzere ayarlanması, ağ kaynaklarının gereksiz kullanımına sebep olacaktır.

İmza güncellemelerine ek olarak antivirüs yazılımları için tarama motoru güncellemeleri ve yamalar da yayımlanmaktadır. Bunların da e-posta listeleri üzerinden takip edilmesi ve istemcilere zamanında ve mümkünse merkezi olarak yüklenmeleri gerekmektedir.

4.2 Gerçek Zamanlı Virüs Koruma

Antivirüs programları ZKY'leri iki farklı yolla tespit edebilmektedir: gerçek zamanlı tarama ve periyodik/isteğe bağlı taramalar. Gerçek zamanlı koruma bilgisayara ZKY'nin girişini engellemeyi amaçlamaktadır. Gerçek zamanlı koruma ile işletim sisteminin erişime izin verdiği tüm dosyalar erişim işleminin öncesinde mevcut imzalar/heuristic teknikler kullanılarak antivirüs tarama motoru tarafından taranmaktadır. Antivirüs yazılımları çeşitli ayar seçenekleri sunmaktadır:

- Tarama kapsamı:
 - Dosya erişim metoduna göre: Seçenekler: Açma, Okuma, Değiştirme, Kopyalama, Hepsi vb., Tavsiye Edilen: Hepsi,

- Dosya türüne göre: Seçenekler: Çeşitli dosya uzantıları girilebilir, Tavsiye Edilen: Hepsi
 - Taranacak birimler/dizinler: Seçenekler: CDROM, Floopy, Ağ Bağlantıları, C:\Windows vb., Tavsiye Edilen: Hepsi,
 - İstisnalar: Tavsiye Edilen: Çeşitli uygulamalar bazı dizinlerin tarama kapsamı dışında tutulmasını gerektiriyor olabilir (Microsoft Exchange vb.), bu tür zorunlu durumlar dışında istisna tanımlanmamalıdır. İstisna tanımlamaları periyodik olarak kontrol edilmelidir.
- Müdahale Yöntemi: ZKY bulunduğu temizleme, karantinaya alma ya da silme işlemlerinden biri tercih edilmiş olmalıdır.

4.3 Periyodik/İsteğe Bağlı Tarama

Periyodik tarama sisteme girerken tespit edilememiş ZKY'lerin bulunup temizlenmesini, isteğe bağlı tarama ise ZKY olayı gerçekleştikten sonra sistemdeki tüm ya da bazı dosyaların, ZKY'nın sistemden tümüyle temizlenebilmesi için taranması işlemidir. 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.

4.4 İzleme/ Raporlama/Uyarı Ayarları

Mümkün olan tüm bileşenlere antivirüs yazılımının kurulması ve ayarların yukarıda belirtildiği şekilde yapılması ZKY'lere 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 ZKY'ler zamanında fark edilmeyebilir,
- ZKY'lerin yoğun olarak bulaştığı bileşenler ve bulaşma yöntemleri fark edilemez ve önlem alınamayabilir,
- Virüs tanımları güncel olmayan antivirüs yazılımları belirlenemeyebilir,

Sonuç olarak sistem geciken müdahale sebebiyle zarar görebilir. Bu sebeplerle merkezi antivirüs yazılımı üzerinde bileşenlerin durumları (ZKY 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 ZKY'ler hakkında detaylı bilgiler alınmalıdır. Ayrıca birçok merkezi antivirüs yönetim yazılımında bulunan e-posta ya da anlık mesajla uyarı sistemi devreye sokularak antivirüs sistemi yöneticisinin acil durumlara tepkisi hızlandırılmalıdır..

5. EPOSTA ANTİVİRÜS KORUMASI

ZKY'lerin sistemlere bulaşmak için en sık kullandıkları yollardan biri e-posta mesajlarıdır [3]. E-posta mesajlarıyla gelen eklentiler, yanıltıcı linkler ve e-posta okuyucuların zayıflıklarını kullanan ZKY'lere sıklıkla karşılaşılmaktadır. Bu sebeple e-posta sunumcularına ulaşan e-posta mesajlarının ZKY taramalarından geçirilmesi, ZKY'lerin sisteme girmeden engellenmesini sağlayacağı için kritik önem taşımaktadır. E-posta antivirüs güvenlik çözümleri iki farklı türde ele alınabilir:

- E-posta sunucusu üzerine kurulan antivirüs/spam filtreleme yazılımı
- E-posta ağ geçidi (SMTP gateway) olarak görev yapan antivirüs/spam filtreleme yazılımı

SMTP ağ geçidi kullanımı durumunda ilgili sunucunun IP'sinin kuruma hizmet veren internet servis sağlayıcıya DNS MX kaydının güncellenmesi için bildirilmesi gerekmektedir. Böylece kuruma gönderilen e-posta mesajları ilk olarak SMTP ağ geçidi üzerinden geçecektir.

E-Posta antivirüs ürünleri günümüzde spam filtreleme hizmeti de sunmaktadırlar. Spam şöyle tanımlanmaktadır [4]: İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacıyla yöneliktir. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken mali yük büyük ölçüde mesajın alıcıları veya taşıyıcı, servis sağlayıcı kurumlar tarafından karşılanmak zorunda kalınır.

5.1 ZKY İmzalarının Güncelliği

Bölüm 4.1'de anlatılan hususlar E-Posta antivirüs yazılımı ZKY imzalarının güncellenmesi için de geçerlidir.

5.2 ZKY Tarama

E-posta ile bulařan ZKY'ler çoğunlukla eklenti dosyalarla gelmektedir. Bazı ZKY'ler herhangi bir eklenti olmadan da bulařabilmektedirler. ZKY tarama ayarları bütün eklenti dosyalar ve e-posta içeriđi taranacak şekilde yapılması gerekmektedir. Ayrıca yapılacak ayarla sıkıřtırılmıř eklenti dosyalarının da taranması sađlanmalıdır.

E-posta antivirüs yazılımı sečilirken, yazılımın e-postaları posta kutusuna düřmeden tarama yapma yeteneđi olması beklenmektedir. Tarama yapılmamıř e-postaların sırada bekletilmesi ve tarama sonrasında kullanıcının eriřebilmesi sađlanmalıdır.

Ek olarak periyodik tarama ile e-posta sunucusunda önceden tespit edilememiř ZKY'lerin temizlenmesi sađlanmalıdır. Örneđin periyodik tarama sıklıđı haftalık olabilir.

5.3 Eklenti Bloklama Kuralları

E-posta antivirüs sunumcusu ZKY taramasını mevcut ZKY imzalarına göre yapmaktadır. Bu çalışma yöntemi dolayısıyla henüz tanımlanmamıř ZKY'lerin e-posta yoluyla yayılmaya devam etmesi mümkündür. Bu sebeple ZKY içerebilecek dosya türlerinin bloklanması etkin bir önleyici çözüm olarak düşünölmektedir. Bloklanması önerilen uzantılar řunlardır: .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 ZKY taşıyabilecek dosya türlerinin tamamını kapsamayabilir. Antivirüs yöneticileri tecrübelerinden ve BT güvenlik sitelerinde yayınlanan uyarılardan yararlanarak tehdit oluşturabilecek uzantıları bloklama listesine eklemelidir. Ayrıca e-posta eklenti dosyaları yoluyla yayılan bir ZKY saldırısı durumunda geçici süreliđine bazı dosya türlerinin bloklanması acil müdahalenin engelleme aşamasında etkin bir çözüm olarak kullanılabilir.

5.4 Başlık Bloklama Kuralları

ZKY'ler e-posta yoluyla yayılırken kullandıkları, dikkat çekme amacı taşıyan başlıklar (Para, seks, 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 göröldüğünde listeyi güncellemesi tavsiye edilmektedir.

5.5 İzleme/ Raporlama/Uyarı Ayarları

Bir e-posta ZKY, istenmeyen uzantılı eklentili ya da başlığı sebebiyle bloklandığında güvenlik sebebiyle antivirüs yöneticisi, e-posta kaybının yol açabileceği iş kayıplarını önlemek amacıyla da gönderici ve alıcıların bilgilendirilmesi önem taşımaktadır. Dışarıdan gönderilen e-posta mesajlarında ise muhtemel dış saldırganlara bilgi verilmemesi amacıyla göndericiye geri bildirim yapılmaması tercih edilebilir.

KAYNAKÇA

- [1.] Independent Comparatives of Anti-virus Software: <http://www.av-comparatives.org/>
- [2.] Peter Mell, Karen Kent, Joseph Nusbaum, “Guide to Malware Incident Prevention and Handling“, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-83, Kasım 2005
- [3.] A Practical Guide to Enterprise Antivirus and Malware Prevention, Jay Martin August 17, 2001, SANS Institute 2001 Reading Room
- [4.] www.spam.org.tr/nedir.html