

Doküman Kodu: BGT-1006

EXCHANGE SERVER 2003 GÜVENLİĞİ KILAVUZU

SÜRÜM 1.00

3 MART 2008

Hazırlayan: Doğan ESKİYÖRÜK

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak 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 güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman "Ulusal Bilgi Sistemleri Güvenlik Projesi" kapsamında hazırlanmış olup ihtiyaç sahiplerini bilgi sistemleri güvenliği 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 değişik ürünler/yapılandırmalar için farklılık gösterebilir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan değiştirilemez.

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. EXCHANGE SUNUCULARIN AĞ MİMARİSİNDE KONUMLANDIRILMASI.....	8
2.1 Ön Uç (Front-End) ve Arka Uç (Back-End) Sunucu Mimarisi ve Avantajları	8
2.1.1 Güvenlik.....	8
2.1.2 Tek isim alanı.....	8
2.1.3 SSL şifreleme yükünün dağıtılması	9
2.1.4 Ortak klasörlere erişim.....	9
2.1.5 Birden çok protokol desteği.....	9
2.2 Ağ Mimarileri	9
2.2.1 Ön uç ve arka uç sunucularının herhangi bir güvenlik duvarının arkasında bulunduğu yapı.....	9
2.2.2 Ön uç sunucusunun iki güvenlik duvarı arasında veya bir güvenlik duvarının farklı bir bacağında bulunduğu yapı.....	10
2.2.3 Ön uç ve Arka uç sunucularının Internet Security and Acceleration(ISA) Server arkasında bulunduğu ve sunulan servislerin ISA ile yayınlandığı yapı.....	11
2.3 Ön uç - Arka uç yapısında iletişim protokollerinin çalışması ve güvenliği	12
2.3.1 HTTP protokolü.....	12
2.3.2 IMAP, POP protokolleri	13
2.3.3 SMTP protokolü	14
3. EXCHANGE SUNUCULARIN ROLLERİNE GÖRE SIKILAŞTIRILMASI.....	15
3.1 Ön uç sunucularının sıkılaştırılması	15
3.1.1 Servislerin sıkılaştırılması.....	15
3.1.2 Kullanılacak protokoller için gerekli ayarlar	19
3.1.3 Dosya erişim kontrol listeleri.....	20
3.1.4 Posta kutusu ve ortak klasör depolarının kaldırılması	22
3.2 Arka uç sunucularının sıkılaştırılması	23

3.2.1 Servislerin sıkılaştırılması.....	23
3.2.2 Dosya erişim kontrol listelerinin ayarlanması	24
3.2.3 E-posta Mesajlarının Geriye Dönük Takip Edilmesi.....	25
3.2.4 E-posta Kutuları (Mailbox Store) Boyutunun Kısıtlanması	26
3.2.5 Ortak Klasör (Public Folders) Boyutunun Kısıtlanması.....	27
3.2.6 E-posta Relay (Nakil)	29
3.2.7 Protokoller için kimlik doğrulama mekanizmaları ve kayıt tutulması.....	31
4. İLETİŞİM GÜVENLİĞİ	34
4.1 Ön Uç ve Diğer Sunucular Arasındaki Trafiğin Güvenli Hale Getirilmesi.....	34
4.2 Sunucular ve İstemciler Arasındaki Trafiğin Güvenli Hale Getirilmesi	34
4.2.1 İstemci internet üzerinden OWA ile bağlandığında.....	35
4.2.2 İstemci kurum ağı içerisinden Outlook ile bağlandığında	38
4.2.3 İstemci internet üzerinden Outlook ile bağlandığında	38
5. EXCHANGE ORTAMININ GÜVENLİĞİ	40
5.1 Exchange organizasyonundaki gerekli güvenlik ayarları	40
5.1.1 İşletim sistemi, Exchange ve istemciler için yamalar uygulanmalıdır.	40
5.1.2 Exchange organizasyonunu ve/veya sunucularını yönetecek gruplar oluşturulmalıdır.	40
5.1.3 Gönderilen ve alınan e-postaların maksimum boyutu sınırlandırılmalıdır	41
5.1.4 En fazla alıcı sayısı kısıtlanmalıdır.	41
5.1.5 Otomatik mesajlara izin verilmemelidir.	42
5.1.6 E-postaların bütünlüğünü ve gizliliğini korumak için PKI kullanılabilir	43
5.2 İstenmeyen e-postaların (spam) önlenmesi	43
5.2.1 Bağlantı filtreleri (Connection Filtering).....	46
5.2.2 Alıcı filtreleri (Recipient Filtering).....	47
5.2.3 Gönderen filtreleri (Sender Filtering).....	48
5.2.4 Intelligent Message Filter (IMF).....	50
5.2.5 SMTP Bataklik Özelliği (Tar Pitting).....	51
5.3 Virüslerden korunma	52

1. GİRİŞ

E-posta sistemi kurumların haberleşmesini çok kolaylaştırmış ve iş yapış şekillerini değiştirmiştir. İş akışları, süreçlerin işleyişi ve haberleşme ihtiyaçlarında çok kritik roller oynayan bu sistemler kurumlar için büyük önem arz etmektedir. Bu sebeple e-posta sistemlerinin güvenliği ve sürekliliği çok önem taşımaktadır.

1.1 Amaç ve Kapsam

Bu rehber kurumlar için önemi çok artan e-posta sistemlerinin çalışmasını sağlayan yazılımlar içerisinde en popülerlerinden biri olan Exchange Server 2003 sistemine karşı olabilecek tehditleri ve sistemin nasıl güvenli hale getirileceğini anlatmaktadır.

1.2 Hedeflenen Kitle

Bu doküman Exchange sistemini güvenli hale getirmek isteyen sistem yöneticileri, bu sistemleri denetlemekle yükümlü olanlar ve güvenlikle ilgilenen diğer tüm BT çalışanları içindir.

1.3 Kısaltmalar

UEKAE	: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
SDDL	: Security Descriptor Definition Language
ACL	: Access Control List
POP	: Post Office Protocol
IMAP	: Internet Message Access Protocol
SSL	: Secure Sockets Layer
TLS	: Transport Layer Security
DMZ	: Demilitarized Zone
AH	: Authentication Header
ESP	: Encapsulating Security Payload
IPSec	: Internet Protocol Security
OWA	: Outlook Web Access

- SM** : Sertifikasyon Makamı
- MAPI** : Messaging Application Programming Interface
- NTLM** : New Technology LAN Manager
- RPC** : Remote Procedure Call
- RBL** : Real-time Block List
- IMF** : Intelligent Message Filter
- ESE** : Extensible Storage Engine

2. EXCHANGE SUNUCULARIN AĞ MİMARİSİNDE KONUMLANDIRILMASI

Exchange sunucu rolleri ön uç (front-end) ve arka uç (back-end) olarak ikiye ayrılır. Tüm kullanıcıların posta kutuları, ortak klasörler arka uç sunucusunda bulunurken ön uç sunucuları dış dünyayla iletişim kurma ve arka uç sunucularındaki kaynakların yerini belirleme görevini üstlenir. İnternette gelen ve kurum dışına gönderilecek e-postalar ön uç sunusundan geçerler. Böylece dış dünyayla iletişim kurun sunucu üzerinde kullanıcı bilgileri tutulmamış olur. Bu bölümde ön uç ve arka uç sunucu mimarisinin avantajları, en çok kullanılan yapılar ve bu mimarilerde kullanılan protokollerin güvenlik ayarları anlatılmaktadır.

2.1 Ön Uç (Front-End) ve Arka Uç (Back-End) Sunucu Mimarisi ve Avantajları

2.1.1 Güvenlik

Ön uç sunucusunu internet güvenlik duvarının arkasına koyduğunuzda erişim için tek bir nokta sağlanmış olur. Böylece güvenlik duvarı üzerinde birden fazla sunucuya internette erişim hakkı vermek gerekmez.

Ön uç sunucusu üzerinde kullanıcı bilgisi barındırmadığı için sunucunun ele geçirilmesi söz konusu olsa bile kullanıcı bilgisi kaybedilmez. Buna ek olarak ön uç sunucusu istekleri arka uç sunucusunu göndermeden önce isteği yapan için kimlik doğrulaması yapabilir. Bu şekilde arka uç sunucusuna ulaşan tüm isteklerin kimlik doğrulaması yapmış kullanıcılardan gelmesi sağlanır.

2.1.2 Tek isim alanı

Ön uç arka uç yapısının en önemli avantajlarından biri dışarıya (güvensiz ağa) tek bir isim uzayının açılmasına olanak sağlamasıdır. Böylece kullanıcılar posta kutularının veya erişmek istedikleri ortak klasörün hangi sunucu üzerinde tutulduğunu bilmek zorunda kalmazlar. Kullanıcılar tüm isteklerini ön uç sunucusuna gönderirler. İstedikleri kaynağın yerini bulmak ve kullanıcıyı buraya yönlendirmek ön uç sunucusunun görevidir. Bunun için ön uç sunucusu kullanılmadığında esneklik kaybolur ve yönetim zorlaşır. Ölçeklenebilirliği artırması ve SSL şifrelemesi için gerekli sertifika sayısını azaltması da diğer faydalarıdır.

2.1.3 SSL şifreleme yükünün dağıtılması

SSL trafiğini oluşturmak ve deşifre etmek sunucu için ciddi bir yük olabilir. İstemcilerle yapılan SSL trafiğini ön uç sunucusunun üstlenmesi arka uç sunucusunun yükünü hafifletecektir.

2.1.4 Ortak klasörlere erişim

Ön uç sunucusu olmadan kullanıcılar ortak klasörlerdeki iletilere cevap yazamazlar. Ayrıca ön uç sunucusu ortak klasörlerin hangi arka uç sunucularında tutulduğu bilgisini sorgulayıp kullanıcıları yönlendirir ve kullanıcıları sunuculara dağıtarak yük dağılımı(load balancing) yapar.

2.1.5 Birden çok protokol desteği

Exchange ön uç sunucuları HTTP, POP3, IMAP4 ve SMTP protokollerinin yanında RPC over HTTP' yi de destekler.

2.2 Ağ Mimarileri

2.2.1 Ön uç ve arka uç sunucularının herhangi bir güvenlik duvarının arkasında bulunduğu yapı

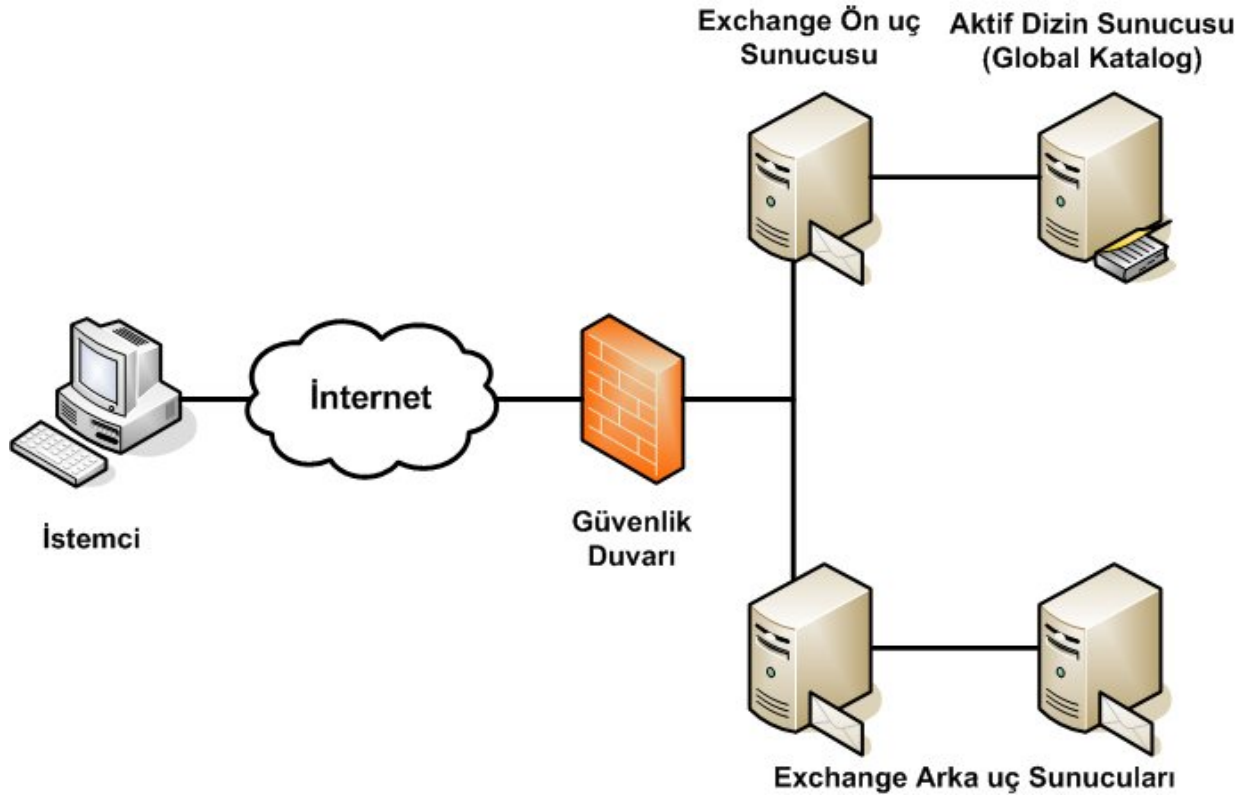
Bu senaryoda internet ve iç ağ arasında tek bir güvenlik duvarı bulunmaktadır. Verilen tüm hizmetlerim (POP, IMAP, HTTP) güvenliği için bu güvenlik duvarı kullanılmaktadır. Bu mimarinin ağ diyagramı Şekil 2.1'deki gibidir.

Avantajları:

- Ucuz ve kurulumu nispeten daha kolay olması
- Tüm servisler aynı ağda olduğu için özel ayar gerektirmemesi

Dezavantajları:

- Kademeli güvenlik anlayışından (defense in depth) uzak olması
- Güvenlik duvarının doğru ayarlanmaması durumunda tüm ağın risk altında kalması



Şekil 2.1 – Ön uç ve arka uç sunucularının herhangi bir güvenlik duvarının arkasında bulunduğu yapı

2.2.2 Ön uç sunucusunun iki güvenlik duvarı arasında veya bir güvenlik duvarının farklı bir bacağına bulunduğu yapı

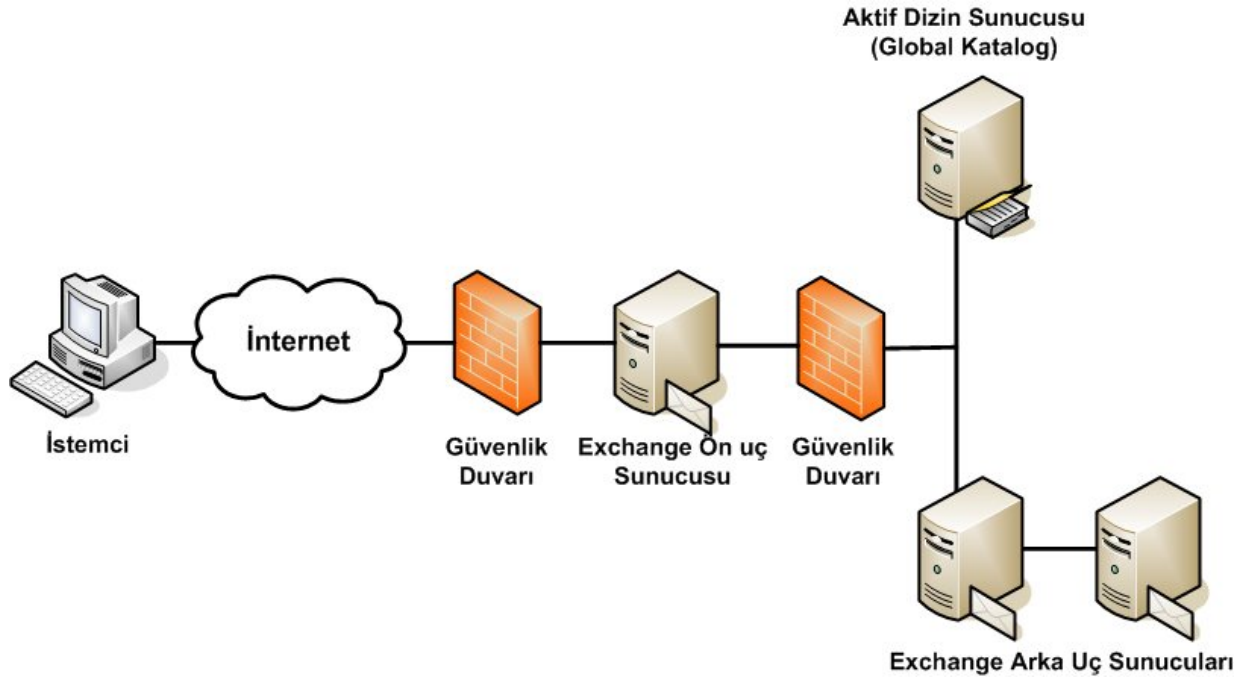
Bu senaryoda kurum ön uç sunucusunu DMZ bölgesine yerleştirir. Böylece internet üzerinden gelen istekler doğrudan iç ağa gönderilmez. Ön uç sunucusu gelen istekleri değerlendirdikten sonra gerekli arka uç ve aktif dizin sunucularıyla haberleşir. Bu mimarinin ağ diyagramı Şekil 2.2'deki gibidir.

Avantajları:

- Kademeli güvenlik anlayışına uygundur. Yani saldırgan ön uç sunucusu ele geçirdiğinde direk olarak iç ağa erişim elde etmez.

Dezavantajları:

- Ön uç sunucu çalışmak için pek çok servise ihtiyaç duyduğundan (DNS, AD) ikinci güvenlik duvarı üzerinde çok sayıda port açılması gerekmektedir.
- DMZ ve iç ağ arasında RPC iletişimi gerektirdiğinden ayarlanması daha zordur.



Şekil 2.2 – Ön uç sunucusunun iki güvenlik duvarı arasında bulunduğu yapı

2.2.3 Ön uç ve Arka uç sunucularının Internet Security and Acceleration (ISA) Server arkasında bulunduğu ve sunulan servislerin ISA ile yayınlandığı yapı

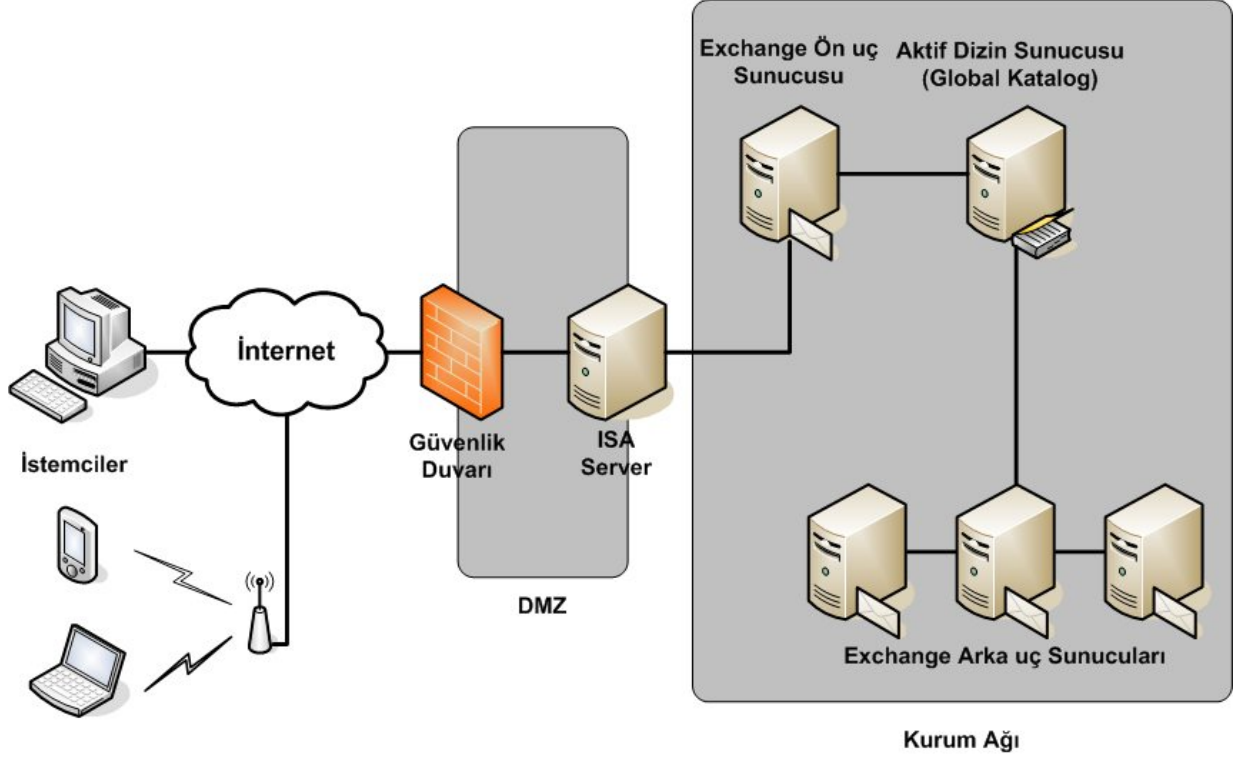
Bu senaryoda gelişmiş güvenlik duvarı internet güvenlik duvarı ile iç ağ güvenlik duvarı arasına yerleştirilmiştir. Hem ön uç hem de ara uç sunucuları bu güvenlik duvarının arkasındadır. Bu yapılandırma hem dışarıdan gelebilecek kötü niyetli kullanıcıları iç ağdan ayırdığı hem de uygulama bazında protokol filtrelemesi yaptığı için incelenen yapılar arasında en güvenli olanıdır. Burada sunucu sayısını azaltmak için gelişmiş güvenlik duvarı internet güvenlik duvarı olarak kullanılabilir.

Avantajları:

- Gelişmiş güvenlik duvarlarının izinsiz giriş engelleme, trafik inceleme ve saldırılarda sistem yöneticilerini uyarma gibi ekstra özellikleri bulunur.
- IP ve port bazında filtreleme yapılabilir.
- Kullanıcı, grup, uygulama, tarih ve zaman bazlı erişim kontrolleri uygulanabilir.
- Tüm sunucular aynı ağda olduğu için DMZ bölgesinden iç ağa RPC trafiği için izin ayarlamak gerekmez

Dezavantajları:

- Sunucu ve yazılım sayısı arttığı için maliyeti yüksektir
- Diğer mimarilere göre daha çok yönetsel yük getirir.



Şekil 2.3 – Ön uç ve Arka uç sunucularının ISA Server arkasında bulunduğu yapı

2.3 Ön uç - Arka uç yapısında iletişim protokollerinin çalışması ve güvenliği

Ön uç sunucularının genel görevi gelen istekleri arka uç sunucularına iletmek olsa da bu işlem her protokol için farklı şekilde gerçekleştirilir. Bu bölümde ön uç sunucusunun verebileceği HTTP, POP, IMAP ve SMTP hizmetlerinin nasıl çalıştığı ve güvenlik için neler yapılması gerektiği anlatılmaktadır.

2.3.1 HTTP protokolü

E-posta servislerine erişim için HTTP kullanıldığında, ön uç arka uç yapısında iki yerde kimlik doğrulama yapmak gerekir. Birincisi istemci ile ön uç sunucusu arasında, diğeri ise ön uç ve arka uç sunucuları arasındadır.

İstemci ile ön uç sunucusu arasında kimlik doğrulama:

İstemciler ön uç sunucusuna kimlik bilgilerini yollarken iki yöntem kullanabilirler. Yöntemlerden biri temel (basic) kimlik doğrulamadır. Bu HTTP tanımında belirtilen ve oldukça zayıf şifreleme kullanan bir metottur. Kullanılabilecek diğer bir metot ise form tabanlı kimlik doğrulamadır. Burada kullanıcı bilgilerini girip kimlik doğrulamayı yaptıktan sonra bir çerez (cookie) kullanılır. Ama yine de ilk kimlik doğrulama işleminde şifre ağ üzerinden açık olarak gider. Bu yüzden hangi yöntem kullanılırsa kullanılsın SSL kullanılarak iletişim şifrelenmelidir.

Ön uç ve arka uç sunucuları arasında kimlik doğrulama:

Sunucular arası kimlik doğrulamada da temel kimlik doğrulama kullanılabilir fakat yine bilgiler ağ üzerinde şifrelenmeden dolaşacaktır. Bu durumda IPSec kullanılması tavsiye edilir. Sunucular arasında kullanılan diğer bir yöntem ise entegre (integrated) kimlik doğrulamadır. Burada sunucular kimlik doğrulama için Kerberos ve NTLM kullanırlar. Önce Kerberos denir, başarılı olmazsa NTLM kullanılır. NTLM de kullanılamıyorsa temel kimlik doğrulama metodu geçerli olur. Kimlik doğrulama için bu yöntem kullanıldığında Kerberos veya en az NTLMv2 kullanılmalıdır.

2.3.2 IMAP, POP protokolleri

İstemcilerin e-posta erişimi için POP veya IMAP kullanmaları durumunda gerçekleşen işlemler HTTP erişiminden çok farklı değildir. POP veya IMAP istemcileri erişmek istedikleri posta kutusunu ve kimlik bilgilerini ön uç sunucusuna gönderir. Ön uç sunucusu aktif dizin sorguları ile kimlik doğrulaması yapar, istenen posta kutusunun hangi arka uç sunucusunda tutulduğunu öğrenir ve istemciden gelen istekleri bu sunucuya yönlendirir.

POP ve IMAP protokolleri kullanıldığında istemciler kullanıcı bilgilerini açık olarak gönderirler bunun için SSL kullanılması gereklidir.

2.3.3 SMTP protokolü

POP ve IMAP protokolleri sadece kullanıcıların e-posta alması için kullanılır. EĖer kullanıcılar internet üzerinden geldiklerinde e-postalarını almak için bu protokolleri kullanıyorlarsa e-posta göndermek için ön uç sunucusunda SMTP kullanmak gerekir. Kullanıcıların dış etki alanlarına e-posta göndermeleri için ön uç sunucusu SMTP relay (nakil) yapacak şekilde ayarlanmalıdır. EĖer gerekli önlem alınmazsa sunucu üzerinden istenmeyen e-posta (spam) gönderilebilir. Bunun için anonim nakle (anonymous relay) tüm IP adreslerinde izin verilmemelidir. Ayrıca TLS ile SMTP oturumu şifrelenmeli ve kullanıcı bilgilerinin açık gitmesi engellenmelidir.

3. EXCHANGE SUNUCULARIN ROLLERİNE GÖRE SIKILAŞTIRILMASI

Sunucuların doğru yapılandırılması kadar sunucuların sıkılaştırılması yani güvenlik açığı oluşturabilecek yapılandırmalara izin verilmemesi de çok önemlidir. Ön uç ve arka uç sunucularının görevleri farklı olduğu için yapılacak sıkılaştırmalar da farklıdır. Bu bölümde sunucunun kurulduğu işletim sistemi sıkılaştırmalarına en olarak Exchange sunucular üzerinde rollerine göre hangi sıkılaştırmaların yapılacağı anlatılmaktadır.

3.1 Ön uç sunucularının sıkılaştırılması

3.1.1 Servislerin sıkılaştırılması

3.1.1.1 Gerekli servisler ve başlama tipleri

Microsoft Exchange Server 2003 yazılımı ile birlikte sunucu üzerine birçok yeni servis yüklenmektedir. Ön uç sunucusu görevini yapabilmek için bu servislerin hepsine ihtiyaç duymaz. Tablo 3.1 ön sunucular için gerekli servisleri, bunların başlama tiplerini ve servislere neden ihtiyaç duyulduğunu veya duyulmadığını göstermektedir. Burada mail almak için hiçbir protokol etkin değildir. Bunun sebebi sunucuyu ilk kurulumda olabildiğince sıkıştırmaktır. Daha sonra kullanılacak protokoller için gerekli servisleri ve başlama tipleri verilecektir. Ayrıca sebep sütununda verilen açıklamada belirtilen servislere/yazılımlara ihtiyaç duyulursa bu servisler de otomatik olarak çalıştırılmalıdır.

Servis İsmi	Başlama tipi	Sebeup
Microsoft Exchange IMAP4	Devre dışı	Sunucu IMAP4 için yapılandırılmamış
Microsoft Exchange Information Store	Devre dışı	Posta kutularına ve ortak klasörlere erişim için gerekli
Microsoft Exchange POP3	Devre dışı	Sunucu POP3 için yapılandırılmamış
Microsoft Search	Devre dışı	Exchange sunucunun çalışması için gerekli değil
Microsoft Exchange Event	Devre dışı	Sadece Exchange 5.5 ile geriye dönük uyumluluk için gerekli

Servis İsmi	Başlama tipi	Sebep
Microsoft Exchange Site Replication Service	Devre dışı	Sadece Exchange 5.5 ile geriye dönük uyumluluk için gerekli
Microsoft Exchange Management	Otomatik	Mesaj izleme ve Exchange Server Best Practices Analyzer (ExBPA) için gerekli
Windows Management Instrumentation	Otomatik	Microsoft Exchange yönetimi için gerekli
Microsoft Exchange MTA Stacks	Devre dışı	X.400 konektörleri kullanıldığında veya geriye dönük uyumluluk için gerekli
Microsoft Exchange System Attendant	Devre dışı	Exchange bakımı ve bazı diğer görevler için gerekli
Microsoft Exchange Routing Engine	Devre dışı	Exchange sunucular arasında mesaj iletimini koordine etmek için gerekli
IPSEC Policy Agent	Otomatik	Sunucu üzerinde IPsec politikası uygulamak için gerekli
IIS Admin Service	Devre dışı	HTTP, SMTP ve Exchange routing engine servisleri için gerekli
NTLM Security Support Provider	Otomatik	System Attendant servisi için gerekli
Simple Mail Transfer Protocol (SMTP)	Devre dışı	Exchange mesaj iletimi için gerekli
World Wide Web Publishing Service	Devre dışı	Outlook Web Access ve Outlook Mobile Access için gerekli
Network News Transport Protocol (NNTP)	Devre dışı	Exchange kurulumu ve haber grupları için gerekli
Remote Registry	Otomatik	Exchange kurulumu ve uzaktan yönetim için gerekli

Tablo 3.1 – Ön uç sunucular için servisler ve başlama tipleri

Servislerin bu şekilde yapılandırılması ön uç sunucusunun yapması gerekenler için yeterlidir fakat bu yapılandırma sonucu bazı özellikler kullanılamaz hale gelir. Kapatılan bazı önemli servisler ve kaybedilen özellikler şu şekildedir.

- **Microsoft Exchange POP3, Microsoft Exchange IMAP4**

İstemciler POP3 ve IMAP4 kullanmıyorlarsa bu servisler kapatılmalıdır. Bu işlem yerel olarak veya grup politikası ile yapılabilir fakat servisleri kapamadan önce ortamda bu protokollere ihtiyaç duyan özel yazılımlar olmadığından emin olunmalıdır.

- **Simple Mail Transfer Protocol (SMTP)**

Ön uç sunucunun SMTP hizmeti vermesi gerekmez. Bu servis IMAP veya POP kullanan istemciler e-posta göndereceğinde veya ön uç sunucusu SMTP geçidi(gateway) olarak kullanılacağı zaman gereklidir.

- **Microsoft Exchange System Attendant**

Bu servis ön uç sunucusunda yapılandırma değişiklikleri yapılacağı zaman gereklidir. Her zaman çalışmasına gerek yoktur. Ayrıca virüs tarama araçları için bu servis gerekli olabilir.

- **Microsoft Exchange Information Store**

Ön uç sunucusunda posta saklanmadığı için bu servis kapatılmalıdır. Fakat sunucu SMTP geçidi olarak kullanılıyorsa, virüs taramaları ve ortak klasör iletilerinin yönlendirilmesi için servis gereklidir.

3.1.1.2 Gerekli servislerin erişim denetim listeleri

Servislerin başlamış veya durmuş olması kadar hangi kullanıcıların servislerin ayarlarını değiştirme yetkisine sahip olduğu da önemlidir. Ön uç sunucusunda Exchange ile ilgili servislerin listesi şu şekildedir.

- Microsoft Exchange Event (MSEExchangeES)
- Microsoft Exchange IMAP4 (IMAP4Svc)
- Microsoft Exchange Information Store (MSEExchangeIS)
- Microsoft Exchange Management (MSEExchangeMGMT)
- Microsoft Exchange MTA Stacks (MSEExchangeMTA)

- Microsoft Exchange Routing Engine (RESvc)
- Microsoft Exchange Site Replication Service (MSEExchangeSRS)
- Microsoft Exchange System Attendant (MSEExchangeSA)
- Microsoft Search (MSSEARCH)
- Microsoft Exchange POP3 (POP3Svc)
- Microsoft Exchange IMAP4 (IMAP4Svc)
- World Wide Web Publishing Service(W3Svc)
- IIS Admin Service(IISAdmin)
- Simple Mail Transfer Protocol (SMTPSvc)
- Network News Transfer Protocol (NNTPSvc)
- HTTP SSL(HTTPFilter)
- Cluster Service (ClusSvc)
- Distributed Transaction Coordinator (MSDTC)
- Windows Management Instrumentation (Winmgmt)
- IPSEC Services (PolicyAgent)
- Remote Registry (RemoteRegistry)

Bu servislere verilmesi gereken haklar ise şu şekildedir:

- Authenticated Users – Read
- System – Full Control
- Builtin Administrators – Full Control

MSDTC servisi için yukarıdakilere ek olarak Network Services – Write and Special Permissions hakkı gerekir. (Tam olarak READ_CONTROL, READ_PROPERTY, CREATE_CHILD, DELETE_CHILD, LIST_CHILDREN, SELF_WRITE, LIST_OBJECT, hakları verilir, WRITE_PROPERTY, DELETE_TREE, CONTROL_ACCESS hakları verilmez.)

Ayrıca servislerin ayarlarını değiştirmeye çalışan kullanıcılar kayıt altına alınmalıdır. Bunun için servisler üzerinde kayıt tutma ayarları etkin hale getirilmelidir. Servislere yapılacak başarılı veya başarısız tüm erişimlerin kaydını tutmak ve daha sonra bu kayıtları incelemek için çok fazla kaynak gerekebilir. Bu gibi durumlarda en azından başarısız erişimlerin kayıtları tutulmalıdır (Audit : Everyone – Failure).

Bu ayarları yapmak için aktif izin grup ilkeleri kullanılabilir. Servislerle ilgili ayarlar “*Computer Configuration > Windows Settings > Security Settings > System Services*” yolu izlenerek yapılabilir.

Servis sıkılaştırmaları için grup ilkelerinin yanı sıra güvenlik şablonları da (security template) kullanılabilir. Bu güvenlik şablonları içerisinde SDDL kullanılarak servisler için erişim denetim listeleri ve kayıt tutma ayarları yapılabilir. Microsoft System Attendant servisi için örnek bir güvenlik şablonu aşağıda verilmiştir. Ayrıca SDDL ile ilgili daha detaylı bilgi <http://msdn2.microsoft.com/en-us/library/aa379567.aspx> adresinden alınabilir.

```
; (c) Microsoft Corporation 1997-2004
;
; Security Configuration Template for Security Configuration Editor

[Version]
signature="$CHICAGO$"
Revision=1

[Service General Setting]
"MSExchangeSA",4,"D:AR(A;CCLCSWLOCRRCC;AU)(A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;
;BA)(A;CCDCLCSWRPWPDTLOCRSDRCWDWO;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;
;WD)"
```

3.1.2 Kullanılacak protokoller için gerekli ayarlar

Ön uç sunucu üzerinde e-posta almak veya göndermek için HTTP, POP3, IMAP4, SMTP gibi ilave protokoller kullanmak istenirse Tablo 3.2’de verilen servisler belirtilen başlama tipleriyle açılmalıdır.

Protokol	Servisin ismi	Başlama tipi
HTTP	IIS Admin Service	Otomatik
	World Wide Web Publishing Service	Otomatik
	HTTP SSL	Manüel
POP3 / IMAP4	IIS Admin Service	Otomatik
	Microsoft Exchange POP3/IMAP4	Otomatik
SMTP	Simple Mail Transport Protocol	Otomatik
	Microsoft Exchange POP3	Otomatik
	Microsoft Exchange Information Store	Otomatik
	Microsoft Exchange System Attendant	Otomatik
	Microsoft Exchange MTA Stacks	Manüel
	Microsoft Exchange Routing Engine	Otomatik

Tablo 3.2 – Ön uç sunucusunda kullanılacak diğer protokoller için gerekli servisler ve başlama tipleri

3.1.3 Dosya erişim kontrol listeleri

Exchange kurulumu ile gelen yeni klasörlerin erişim denetim listelerinin varsayılan olarak yeterince güvenli değildir. Bu klasörlere verilen haklarda bazı değişiklikler yapmak gereklidir. Fakat burada dikkat edilmesi gerek şey yukarıdan uygulanan hakların alt dizinlerdeki hakları da etkileyeceğidir. Bazı hakların tüm alt dizinlere uygulanması sorun yaratabilir. Verilmesi gereken haklar ve bu hakların hangi alt dizinlere uygulanacağı Tablo 3.3'te verilmiştir.

Dizin	Eski ACL	Yeni ACL	Alt dizinlere uygulansın mı?
%systemdrive%\inetpub\mailroot	Everyone: <ul style="list-style-type: none">• Full Access	Administrators: <ul style="list-style-type: none">• Full Access Local System: <ul style="list-style-type: none">• Full Access	Evet
%systemdrive%\inetpub\nttpfile\	Everyone: <ul style="list-style-type: none">• Full Access	Administrators: <ul style="list-style-type: none">• Full Access Local System: <ul style="list-style-type: none">• Full Access	Evet

Dizin	Eski ACL	Yeni ACL	Alt dizinlere uygulanır mı?
%systemdrive%\inetpub\wwwroot	Everyone: <ul style="list-style-type: none">• Full Access	Everyone: <ul style="list-style-type: none">• Full Access	Evet
%ProgramFiles%\exchange\bin	Administrators: <ul style="list-style-type: none">• Full Access Users: <ul style="list-style-type: none">• Read• Read & Execute Server Operators: <ul style="list-style-type: none">• Modify• Read & Execute• List Folder Contents• Read• Write•	Administrators: <ul style="list-style-type: none">• Full Access Local System: <ul style="list-style-type: none">• Full Access Server Operators: <ul style="list-style-type: none">• Modify• Read & Execute• List Folder Contents• Read• Write CREATOR OWNER: <ul style="list-style-type: none">• Full Access (Sub Folders and Files Only)	ADDRESS, OMA, BIN, EXCHWEB ve RES dizinleri dışındaki tüm alt dizinlere

Dizin	Eski ACL	Yeni ACL	Alt dizinlere uygulansın mı?
%ProgramFiles%\exchsrvr \\OMA ADDRESS \\BIN \\EXCHWEB \\RES	Administrators: <ul style="list-style-type: none">• Full Access Users: <ul style="list-style-type: none">• Read• Read & Execute• List Folder Contents Server Operators: <ul style="list-style-type: none">• Modify• Read & Execute• List Folder Contents• Read• Write	Administrators: <ul style="list-style-type: none">• Full Access Local System: <ul style="list-style-type: none">• Full Access Users: <ul style="list-style-type: none">• Read• Read & Execute• List Folder Contents Server Operators: <ul style="list-style-type: none">• Modify• Read & Execute• List Folder Contents• Read• Write CREATOR OWNER: <ul style="list-style-type: none">• Full Control (Sub Folders and Files Only)	Evet

Tablo 3.3 – Ön uç sunucular için önemli Exchange dizinleri ve gerekli haklar

3.1.4 Posta kutusu ve ortak klasör depolarının kaldırılması

Ön uç sunucusunun görevi kendisine gelen istekleri arka uç sunucusuna iletmek olduğu için posta kutusu veya ortak klasör depolarına ihtiyaç duymaz. Bu depolar arka uç sunucusu tarafından yönetilir. Eğer sunucu üzerinde SMTP protokolü çalışmıyorsa bu depolar kaldırılmalıdır veya “*dismount*” edilmelidir. Bunun için aşağıdaki yol izlenebilir.

Administrative Groups → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → %Depolama Ünitesi Grubu (Storage Group) Adı% → *Depolama Ünitesi Adı%* → Sağ klik → *Delete / Dismount store*

3.2 Arka uç sunucularının sıkılaştırılması

3.2.1 Servislerin sıkılaştırılması

3.2.1.1 Gerekli servisler ve başlama tipleri

Ön uç sunucularda olduğu gibi arka uç sunucular üzerinde çalışan servislerin de sıkılaştırılması gereklidir. Arka uç sunucular üzerinde kullanıcı posta kutuları ve ortak klasörler gibi değişik hizmetler bulunduğu için ön uç sunuculara göre bazı ekstra servislerin çalışması gerekmektedir. Gerekli tüm servisler ve bu servislerin başlama tipleri Tablo 3.4'te verilmiştir.

Servis İsmi	Başlama tipi	Sebeup
Microsoft Exchange IMAP4	Devre dışı	Sunucu IMAP4 için yapılandırılmamış
Microsoft Exchange Information Store	Otomatik	Posta kutularına ve ortak klasörlere erişim için gerekli
Microsoft Exchange POP3	Devre dışı	Sunucu POP3 için yapılandırılmamış
Microsoft Search	Devre dışı	Exchange sunucunun çalışması için gerekli değil
Microsoft Exchange Event	Devre dışı	Sadece Exchange 5.5 ile geriye dönük uyumluluk için gerekli
Microsoft Exchange Site Replication Service	Devre dışı	Sadece Exchange 5.5 ile geriye dönük uyumluluk için gerekli
Microsoft Exchange Management	Otomatik	Mesaj izleme ve Exchange Server Best Practices Analyzer (ExBPA) için gerekli
Windows Management Instrumentation	Otomatik	Microsoft Exchange yönetimi için gerekli
Microsoft Exchange MTA Stacks	Otomatik	X.400 konektörleri kullanıldığında veya geriye dönük uyumluluk için gerekli
Microsoft Exchange System Attendant	Otomatik	Exchange bakımı ve bazı diğer görevler için gerekli
Microsoft Exchange Routing Engine	Otomatik	Exchange sunucular arasında mesaj iletimini koordine etmek için gerekli

Servis İsmi	Başlama tipi	Sebeup
IPSEC Policy Agent	Otomatik	Sunucu üzerinde IPSec politikası uygulamak için gerekli
IIS Admin Service	Otomatik	HTTP, SMTP ve Exchange routing engine servisleri için gerekli
NTLM Security Support Provider	Otomatik	System Attendant servisi için gerekli
Simple Mail Transfer Protocol (SMTP)	Otomatik	Exchange mesaj iletimi için gerekli
World Wide Web Publishing Service	Otomatik	Outlook Web Access ve Outlook Mobile Access için gerekli
HTTP SSL	Manüel	World Wide Web Publishing Service ihtiyaç duyduğunda otomatik çalışır
Network News Transport Protocol (NNTP)	Devre dışı	Exchange kurulumu ve haber grupları için gerekli
Remote Registry	Otomatik	Exchange kurulumu ve uzaktan yönetim için gerekli

Tablo 3.4 – Arka uç sunucular için servisler ve başlama tipleri

3.2.1.2 Gerekli servislerin erişim denetim listeleri

Arka uç sunucular için gerekli servislerin erişim denetim listeleri ve kayıt tutma ayarları bölüm 3.1.1.2’de ön uç sunucular için verilenler ile aynıdır. Tablo 3.4’te belirtilen tüm servisler için

- Authenticated Users – Read
- System – Full Control
- Builtin Administrators – Full Control

hakları verilmelidir ve en az başarısız erişimlerin kaydı tutulmalıdır.

3.2.2 Dosya erişim kontrol listelerinin ayarlanması

Arka uç sunucularındaki Exchange dosyalarının erişim kontrol listeleri Tablo 3.3’te verildiği gibi ayarlanmalıdır.

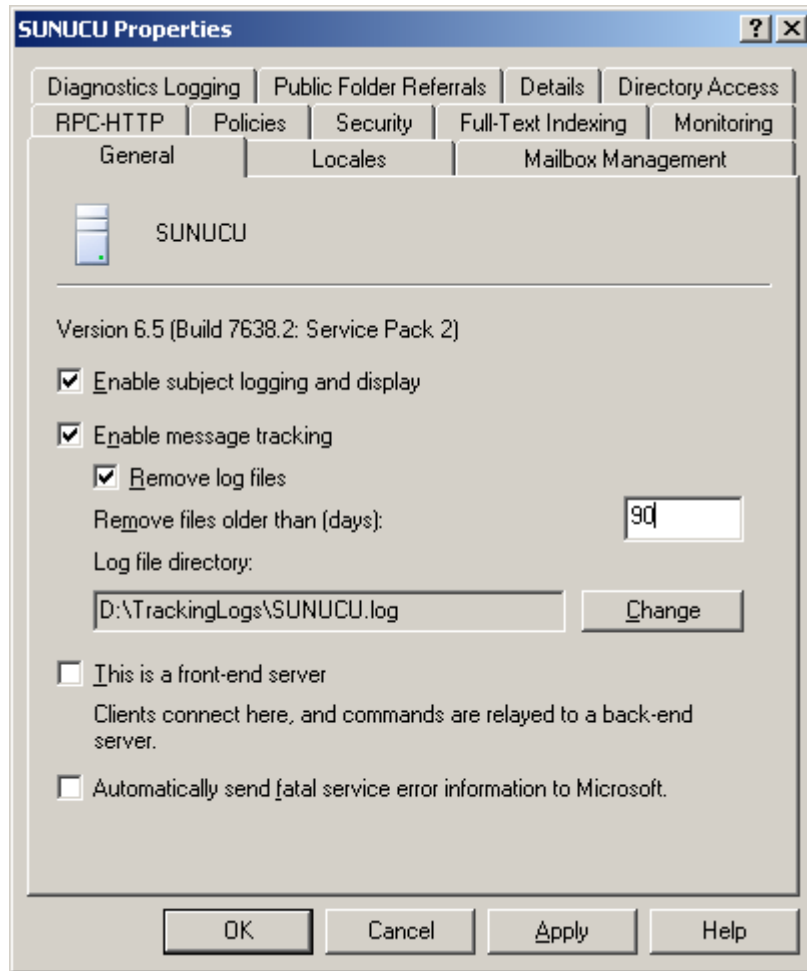
3.2.3 E-posta Mesajlarının Geriye Dönük Takip Edilmesi

Exchange organizasyonu içerisinde gönderilen veya alınan iletilerin takip edilmesi gerekir. Mesaj takibi hem gerektiğinde geriye dönük iz takibi yapılabilmesi için hem de kullanıcıların iletilerinin son durumunu belirlemem için önemlidir. Bunun için Exchange yazılımının mesaj izleme özelliği açılmalı ve gönderen, alıcı, e-posta sunucu, zaman aralığı ve konu bazında arama yapabilecek şekilde e-posta mesajlarının olay kayıtları tutulmalıdır. Mesaj izleme özelliğini açmak için

1. Mesaj izleme özelliği etkin hale getirilmelidir. (Enable Message Tracking)
2. E-posta konularının kayıtlarının tutulmalıdır (Enable subject logging and display)

Bu ayarlar aşağıdaki menü yolu izlenerek yapılabilir (Şekil 3.1):

Administrative Groups → %Yönetimsel Grup Adı% → Servers → %Sunucu Adı% → Properties → General



Şekil 3.1 – Exchange mesaj izleme özelliği

Exchange mesaj izleme kayıtları bir text dosyası formatında kaydedilir ve mesaj izleme etkin hale getirildiğinde yöneticilerin görebileceği bir paylaşım içerisinde saklanır. Bu kayıtlar e-postalarla ilgili bilgiler içerdiğinden korunmalıdır ve yapılan erişimler denetlenmelidir. Bu kayıtlar mümkünse işletim sisteminden ve Exchange yazılımından farklı bir sabit disk bölümünde tutulmalıdır. Bunun için Şekil 3.1’de görülen “*Log file directory*” bölümüne dosyanın bulunacağı yol girilmelidir.

Ayrıca bu kayıtlarının yedekleme planı bulunmalı ve düzenli olarak yedekleri alınmalıdır. Kayıtların saklandığı yerden silinme periyodu da yedekleme periyoduna uygun şekilde belirlenmelidir (*Remove log files older than X days*).

3.2.4 E-posta Kutuları (Mailbox Store) Boyutunun Kısıtlanması

Kullanıcıların tüm bilgileri posta kutuları içerisinde tutulur. Eğer kullanıcılar hiçbir zaman posta kutularını temizlemezlerse dosyaların disk üzerinde kapladığı yer gittikçe büyür. Bu durumda sunucunun servislerini hatta işletim sistemini çalıştırmak için yeri kalmayabilir ve bütünlüğünü bozabilir. Kullanıcı sayısının fazla olduğu kurumlarda disk alanı problemi daha da büyük olabilir. Bunun için posta kutusu boyutları kısıtlanmalıdır.

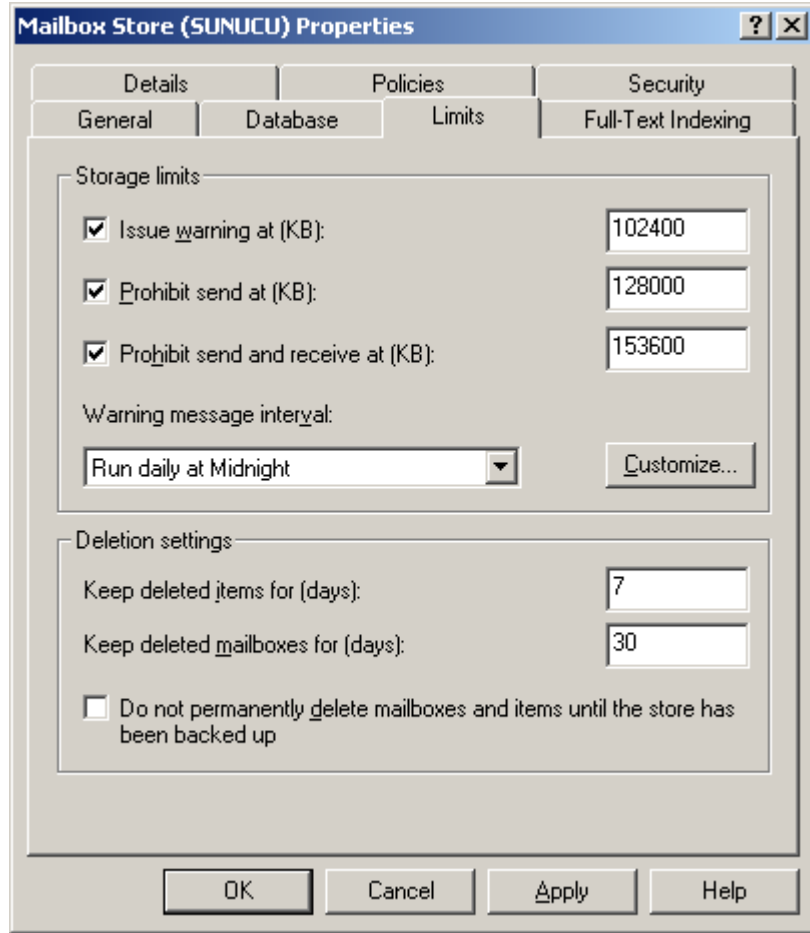
Sunucu üzerinde kullanıcı e-posta kutularının boyutunu kısıtlamak için üç seçenek vardır. Aşağıda verilen bu üç seçenek mevcut kullanıcı sayısı, boş disk alanı ve gelecekteki büyüme planları göz önüne alınarak uygun şekilde ayarlanmalıdır..

- E-posta kutusu boyutu bir üst limite geldiğinde kullanıcının otomatik olarak uyarılmalıdır. (Issue warning at (KB))
- E-posta kutusu boyutu bir üst limite geldiğinde kullanıcının e-posta göndermesinin engellenmelidir. (Prohibit send at (KB))
- E-posta kutusu boyutu bir üst limite geldiğinde kullanıcının e-posta göndermesinin ve almasının engellenmelidir. (Prohibit send and receive at (KB))

Belirtilen limitler aşağıdaki menü yolu izlenerek uygulanabilir.

Administrative Groups → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → %Depolama Ünitesi Grubu (Storage Group) Adı% → % E-posta Kutusu Depolama Ünitesi Adı% → *Properties* → *Limits*

Örneğin Şekil 3.2’deki örnekte limitler sırasıyla 100MB, 125MB ve 150MB olarak belirlenmiştir.



Şekil 3.2 – E-posta kutularının boyutlarının kısıtlanması

3.2.5 Ortak Klasör (Public Folders) Boyutunun Kısıtlanması

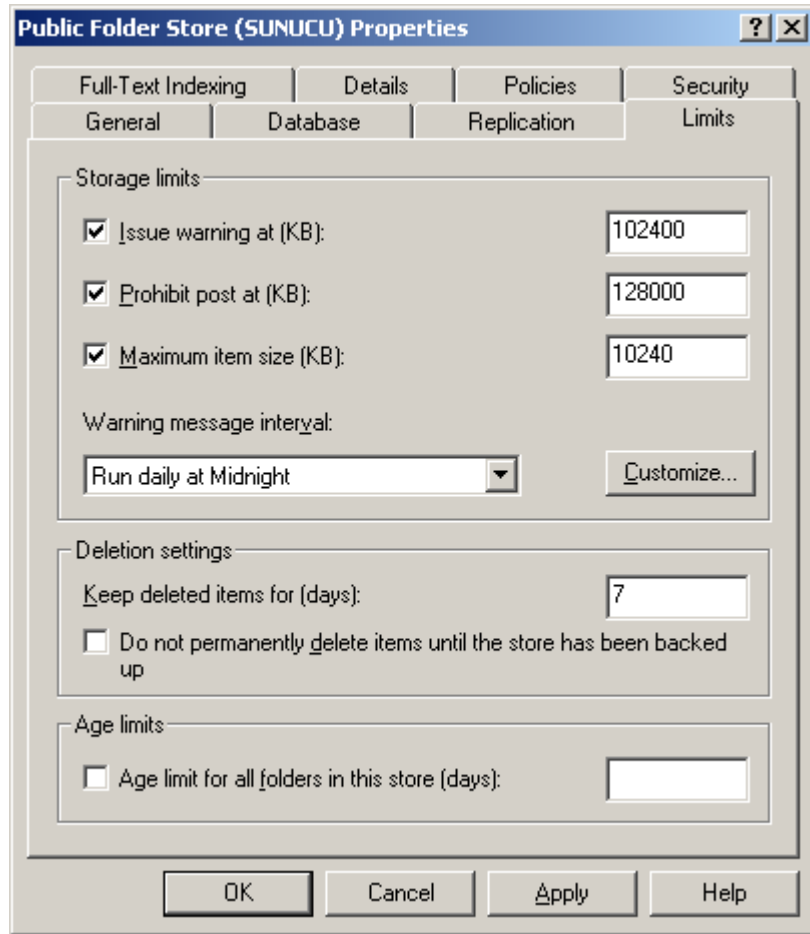
Ortak klasörler kullanıcılarına e-posta dosya, takvim bilgisi vb. bilgilerini paylaşma imkanı sağlar. E-posta kutularında olduğu gibi boş disk alanı sorunu ortak klasörler için de geçerlidir. Ortak klasörlerin boyutunun çok artması sunucunun diskinde yer kalmamasına ve böylece servislerin ve işletim sisteminin çalışmamasına neden olabilir. Bu riski engellemek için ortak klasörlerin boyutları üzerinde aşağıdaki kısıtlanmalar uygulanmalıdır.

- Ortak klasör boyutu bir üst limite geldiğinde kullanıcının otomatik olarak uyarılmalıdır. (Issue warning at (KB))
- E-posta kutusu boyutu bir üst limite geldiğinde kullanıcının ileti göndermesinin engellenmelidir. (Prohibit send at (KB))
- Ortak klasörlere koyulabilecek dosyaların boyutu için bir üst limit belirlenmelidir. (Maximum item size (KB))

Bu ayarlar aşağıdaki menü yolu izlenerek yapılabilir.

Administrative Groups → *%Yönetimsel Grup Adı%* → *Servers* → *%Sunucu Adı%* → *%Depolama Ünitesi Grubu (Storage Group) Adı%* → *% Ortak Klasör Depolama Ünitesi Adı%* → *Properties* → *Limits*

Örneğin Şekil 3.3'deki örnekte limitler sırasıyla 100MB, 125MB ve 10MB olarak belirlenmiştir.



Şekil 3.3 – Ortak klasör boyutlarının kısıtlanması

3.2.6 E-posta Relay (Nakil)

Relay, sunucunun sahip olmadığı bir DNS etki alanından diğer bir etki alanına göndermek üzere e-posta kabul etmesidir. Örneğin kurumunuzun alan adı *kurum.com* olsun. Exchange sunucunuza kimlik doğrulaması yapmadan *kullanıcı@test.com* adresinden *kullanıcı@deneme.com* adresine gönderilmek üzere bir e-posta geldi. Eğer Exchange sunucunuz nakil işlemine izin veriyorsa gelen e-posta kabul edilir ve deneme.com etki alanının posta sunucusuna iletmeye çalışılır. Eğer sunucuda gerekli önlemler alınmazsa sunucu istenmeyen mesaj (spam) gönderimi için açık bir nokta haline gelebilir. Bu durumun devam etmesi durumunda gönderilen istenmeyen mesajlar yüzünden sunucunuz/etki alanınız gerçek zamanlı kara listelere (real time block list) girebilir ve kurumunuz internet üzerinden e-posta gönderemez hale gelebilir.

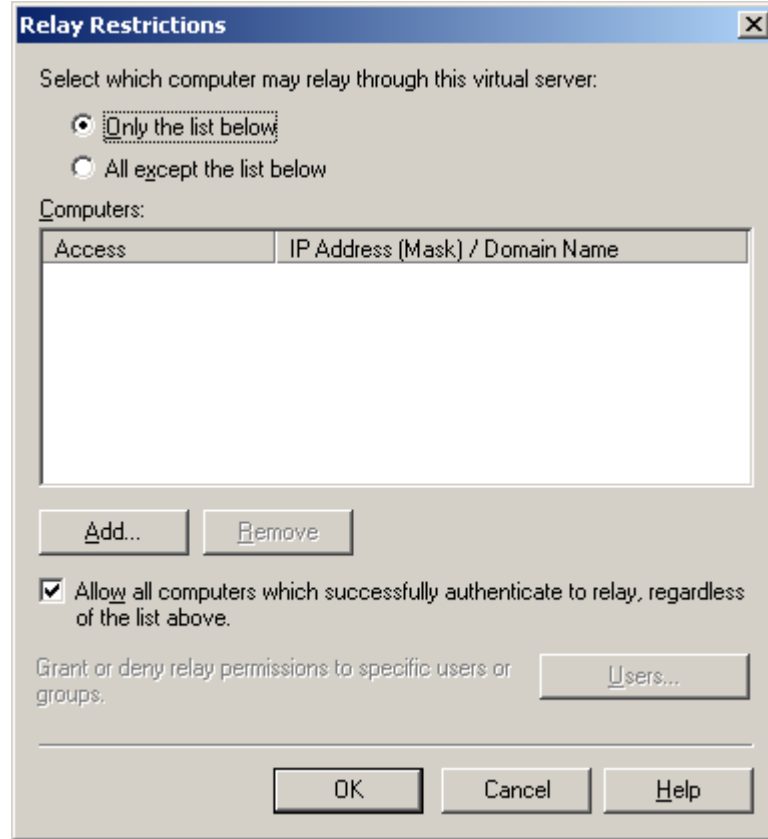
SMTP nakil işlemi bazı durumlarda gerekli olabilir. Örneğin sunucunuz başka etki alanları için e-posta kabul edeceği zaman, istemcileriniz POP3 veya IMAP4 kullanıyorsa e-posta gönderebilmeleri için veya kurumunuzda kullandığınız uygulamalar uyarı veya başka nedenlerle SMTP kullanıyor ve kimlik doğrulaması yapamıyorsa nakil özelliğini açmak gerekebilir. Bu gibi durumlarda SMTP nakil işlemi güvenli hale getirmek gerekir. Bunun için alınması gereken önlemler şunlardır.

1. Sadece kimlik doğrulaması yapmış istemcilerin nakil yapmasına izin vermek
Administrative Groups → *%Yönetimsel Grup Adı%* → *Servers* → *%Sunucu Adı%* → *Protocols* → *SMTP* → *%SMTP Sanal sunucu Adı%* → *Properties* → *Access* → *Relay* yolundan “*Allow all computers which successfully authenticate to relay, regardless of the list below*” seçeneği işaretlenerek bu ayar etkinleştirilebilir (Şekil 3.4).
2. Nakil yapabilecek bilgisayarları, IP adreslerini ve/veya etki alanlarını kısıtlamak

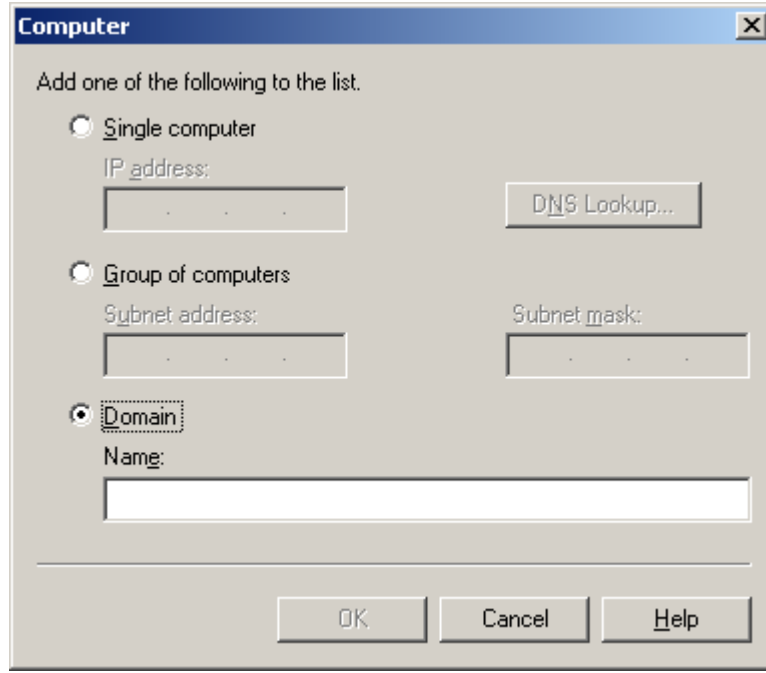
Bu kısıtlamalar 1 numaralı adımda verilen yol izlenip “*Add*” tuşuna basılarak yapılabilir. Buraya IP, IP bloğu veya etki alanı adı girilebilir (Şekil 3.5). Buraya girilen değerler Şekil 3.4’deki “*Select which computer may relay through this virtual server*” Seçeneğine verilen cevaba göre değerlendirilir. “*Only the list below*” seçilirse listedeki bilgisayarlar nakil işlemi gerçekleştirebilir. Eğer “*All except the list below*” seçilirse listedeki bilgisayarlar dışındaki tüm bilgisayarlar nakil yapabilir. Buraya nakil yapması gereken bilgisayarlar girilmeli, diğer bilgisayarların nakil yapmasına izin verilmemelidir.

3. Belirli etki alanlarına yapılacak nakil işlemleri için farklı SMTP konektörler kullanmak
4. Gelen ve giden e-postalar için sertifikalar ile 128 bitlik TLS şifrelemesi kullanmak.

SMTP trafiği şifresiz bir trafiktir. Eğer sunucuya gelen haberleşme dinlenirse mesaj içeriği ve kimlik bilgileri ortaya çıkabilir. Bunun için SMTP haberleşmesi şifrelenmelidir.



Şekil 3.4 – E-posta relay kısıtlamaları



Şekil 3.5 – E-posta relay için istisna ekleme ayarları

3.2.7 Protokoller için kimlik doğrulama mekanizmaları ve kayıt tutulması

Microsoft Exchange Server sisteminde kullanılabilen protokoller olan SMTP, POP3, IMAP4 ve NNTP için kullanılacak 4 farklı kimlik doğrulama mekanizması mevcuttur.

1. Anonim (SMTP ve NNTP için geçerli) kimlik doğrulama

Anonim kimlik doğrulamada karşı tarafa kimlik bilgisi gönderilmez. İnternet üzerinde posta sunucular genellikle anonim SMTP kullanırlar.

2. Temel (Basic) kimlik doğrulama

Temel kimlik doğrulamada kimlik bilgileri Base64 kodlama ile kodlanarak iletilir. Fakat bu kodlama yöntemi çok basit bir kodlamadır ve kırılması çok çok kolaydır. Zaten temel kimlik doğrulama aktif hale getirildiğinde şifrelerin açık gideceğine dair bir uyarı mesajı görülür.

3. SSL/TLS ile şifrelenmiş temel kimlik doğrulama

Temel kimlik doğrulamada kullanılan şifreleme çok zayıf olduğu için iletişim SSL veya TLS kullanarak şifrelenebilir.

4. Bütünleşmiş (integrated) Windows kimlik doğrulama

Bu yöntem Windows'un bütünleşmiş kimlik doğrulama yöntemidir. Kerberos veya NTLM yöntemi kullanılır. Kimlik doğrulama için bu yöntem kullanıldığında Kerberos veya en az NTLMv2 kullanılmalıdır.

Yukarıdaki kimlik doğrulama mekanizmaları kullanılırken dikkat edilmesi gerekenler şunlardır:

- Sadece Windows 2000/2003 etki alanı kullanıcıların bulunduğu ve/veya kapalı sistemlerde (dışarıdan e-posta kabul etmeyen) sadece “*Integrated Windows Authentication*” yönteminin etkin olması, diğer yöntemlerin devre dışı bırakılması gereklidir.
- “*Basic Authentication*” yöntemi etkin ise oturum bilgisinin korunması için TLS kullanımı zorunlu kılınmalıdır (Require TLS encryption). Aksi takdirde etki alanı kullanıcıları kimlik doğrulama bilgileri ağda açık şekilde dolaşır ve ağı dinleyen kişiler tarafından ele geçirilebilir.

Kimlik doğrulama ayarları aşağıdaki menü yolu izlenerek yapılabilir.

Administrative Groups → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → *Protocols* → %Protokol Adı% → %Sanal Sunucu Adı% → *Properties* → *Access* → *Authentication*

Geriye dönük takip yapılabilmesi için kullanılan tüm protokoller için kayıt tutulmalıdır. Ayrıca bu kayıtların işletim sisteminden farklı bir disk bölmesine kaydedilmelidir ve düzenli olarak yedekleri alınmalıdır. Kayıt tutma ayarları

- **SMTP için:** *Administrative Groups* → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → *Protocols* → *SMTP* → %SMTP Sanal Sunucu Adı% → *Properties* → *General* → *Enable Logging*
- **POP3 için:** *Administrative Groups* → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → *Diagnostic Logging* → *POP3Svc*
- **IMAP4 için:** *Administrative Groups* → %Yönetimsel Grup Adı% → *Servers* → %Sunucu Adı% → *Diagnostic Logging* → *POP3Svc*

- **NNTP için:** *Administrative Groups* → *%Yönetimsel Grup Adı%* → *Servers* → *%Sunucu Adı%* → *Protocols* → *NNTP* → *%NNTP Sanal Sunucu Adı%* → *Properties* → *General* → *Enable Logging*

yolları ile ayarlanabilir. SMTP ve NNTP kayıtları tekst tabanlı dosyalarda tutulur fakat POP3 ve IMAP4 kayıtları Windows kayıt günlüğüne (Event Log) düşer. Yedekleme işlemleri planlanırken buna dikkat edilmelidir.

4. İLETİŞİM GÜVENLİĞİ

Exchange e-posta sistemi Exchange sunucunun yanı sıra diğer aktif dizin sunucularını, kullanıcı bilgisayarlarını ve kullanıcıların kullandıkları e-posta istemcilerini içerir. Bunun için sadece Exchange sunucuların güvenli hale getirilmesi e-posta sisteminin güvenli hale getirilmesi için yeterli değildir. Exchange sunucunun hem diğer sunucularla hem de istemcilerle gerçekleştirdiği haberleşme güvenli hale getirilmelidir.

4.1 Ön Uç ve Diğer Sunucular Arasındaki Trafiğin Güvenli Hale Getirilmesi

Sunucular arasındaki trafik düşünüldüğünde en kritik haberleşme Exchange ön uç sunucusu ile diğer sunucular arasında gerçekleşir. Bunun nedeni ön uç sunucusunun herkesin erişebildiği DMZ bölgesinde olması ve iç ağdaki sunucularla haberleşmesidir. Exchange ön uç sunucusunun; Exchange arka uç sunucusu, etki alanı kontrolcüsü ve global katalog sunucusu ile iletişim ihtiyacı vardır. Bu iletişimi güvenli hale getirmek için sunucular arasındaki trafik IP Security (IPSec) kullanılarak şifrelenmelidir.

IPSec ile sunucular arasında aktarılan verinin hem bütünlüğü hem gizliliği korunabilir. Authentication Header (AH) bütünlüğü, Encapsulating Security Payload (ESP) ise gizliliği korumak için kullanılır.

Authentication Header verinin bütünlüğünü sağlar. IP paketine bir sağlama toplamı (checksum) eklenerek paketin istenen kaynaktan geldiği ve yol boyunca bütünlüğünün bozulmadığı garanti edilir. AH port 51'i kullanır. Encapsulating Security Payload ise IP paketinin tamamını şifreler ve port 50 üzerinden çalışır.

Güvenlik açısından AH için Message Digest 5 (MD5) yerine SHA1, ESP için ise Data Encryption Standard(DES) yerine 3DES kullanılmalıdır.

IPSec protokolünün detayları bu rehberin kapsamının dışındadır.

4.2 Sunucular ve İstemciler Arasındaki Trafiğin Güvenli Hale Getirilmesi

Sunucular ve istemciler arasındaki trafiğin güvenli hale getirilmesi en az sunucuların sıklaştırılması kadar önemlidir. Çünkü içeriğini korumak istediğimiz e-posta istemci bilgisayarında oluşturulur ve işlemler için gerekli kimlik bilgileri istemciden gönderilir.

Bu bölümde istemcinin Exchange sunucuya erişmesi için en sık kullanılan üç yöntem ele alınmıştır.

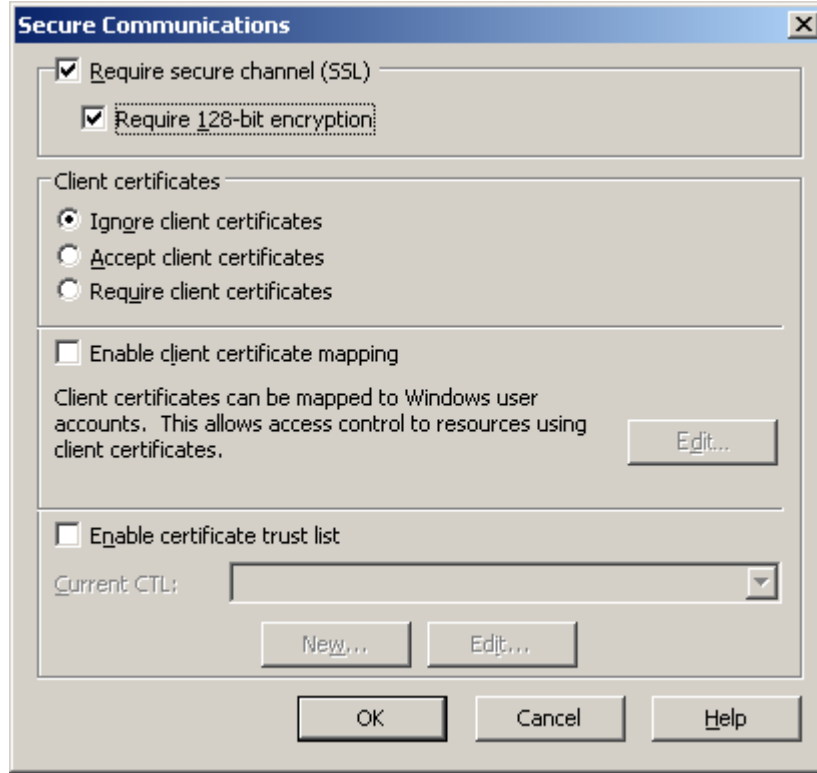
4.2.1 İstemci internet üzerinden OWA ile bağlandığında

Kullanıcılar e-posta ve ortak izin işlemleri için Exchange sunucusuyla gelen a web arayüzünü yani OWA'yı (Outlook Web Access) kullanabilirler. Bunun için kullanıcı tarayıcısına adres olarak ilgili sunucunun web adresine yazar, kimlik bilgilerini girdikten sonra sisteme giriş yapar. Burada hem kimlik bilgilerinin açık gönderilmemesi, hem de mesaj alıp verirken mesaj içeriğinin açığa çıkmaması için şifreleme kullanmak gereklidir.

İstemcilerin Outlook Web Access(OWA) ile erişimde SSL kullanımı etkin ve zorunlu olmalıdır. Ayrıca en az 128 bit şifreleme kullanılmalıdır. aksi takdirde kullanıcıların etki alanı kullanıcı adları ve parolaları internet üzerinde açık olarak dolaşır. SSL için kullanılacak sertifika üçüncü parti bir sertifikasyon makamından (SM) veya kurum içinde kurulan yerel bir sertifika makamından alınabilir. Eğer sertifikamızı imzalayan sertifika makamı, işletim sisteminde tanımlı güvenilen kök sertifika makamları arasında değilse, sertifikayı kullandığımızda istemci yazılımı bu sertifikayı imzalayan makama güvenmediğini belirtecektir. Bundan kurtulmak için sertifika sunucunuzun kök sertifikasını tüm istemcilere güvenilir kök SM sertifikası olarak yüklemeniz gerekir.

SSL kullanımının zorunlu kılınması için aşağıdaki yol izlenerek Şekil 4.1'deli ilk iki ayar olan *“Require secure channel (SSL)”* ve *“Require 128-bit encryption”* işaretlenmelidir.

Internet Information Services (IIS) Manager → %SunucuAdı% → Web sites → Default Web Site → Exchnage → Properties → Directory Security → Secure Communications → Edit



Şekil 4.1 – SSL ayarları

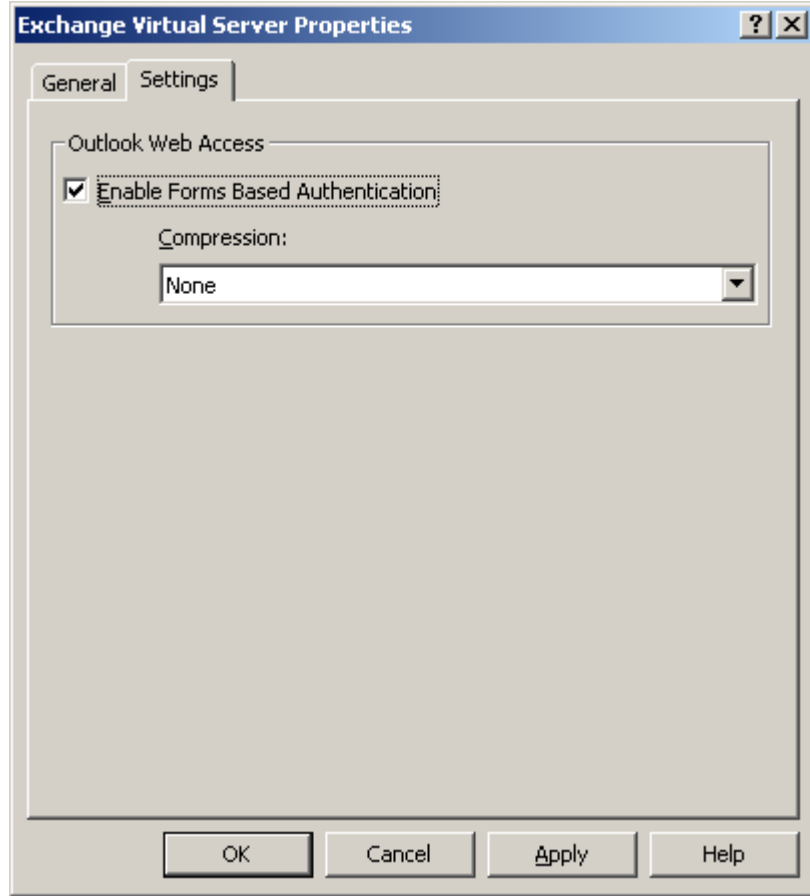
Form tabanlı kimlik doğrulama kullanılması güvenlik açısından tercih edilmesi gereken bir yöntemdir. Bunun nedeni kimlik bilgilerinin tarayıcıda değil bir çerez (cookie) içerisinde saklanmasıdır. Bu sayede tarayıcı kapatıldığında oturum da kapatılmış olur. Ayrıca bir süre etkinlik görülmezse de oturumun kapanması ayarlanabilir. Bu süre aşağıdaki kütük değerleri(DWORD tipinde) değiştirilerek ayarlanabilir. Bu değerler dakika cinsindedir.

HKLM\System\CurrentControlSet\Services\MSExchangeWEB\OWA\TrustedClientTimeout

HKLM\System\CurrentControlSet\Services\MSExchangeWEB\OWA\PublicClientTimeout

Form tabanlı kimlik doğrulamayı etkin hale getirmek için aşağıdaki yol izlenerek Şekil 4.2'deki "Enable Forms Based Authentication" kutusu işaretlenmelidir.

Administrative Groups → %Yönetimsel Grup Adı% → Servers → %Sunucu Adı% → Protocols → HTTP → %HTTP Sanal Sunucu Adı% → Properties → Settings



Şekil 4.2 – Form tabanlı kimlik doğrulamanın aktif hale getirilmesi

OWA ile internet üzerinden e-postalarını okuması için tarayıcılarından bir adres girmeleri gerekir (örneğin onucsunucu.kurum.com/exchange). Bu adresi daha kolay hale getirmek mümkündür. Bunun için DNS sunucuda herkesin kolayca hatırlayabileceği bir kayıt yaratılır (eposta.kurum.com) ve bu kayıt ön uç sunucuna yönlendirilir. Daha sonra ön uç sunucusunda Internet Information Services(IIS) ayarlarında bu sunucuya gelen http isteklerinin bir alttaki dizine yönlendirilmesini sağlayan ayar yapılır ve bu alt dizin '/exchange' olarak belirtilir. Bu sayede kullanıcılar eposta.kurum.com adresine girdiğinde otomatik olarak onucsunucusu.kurum.com/exchange adresine yönlendirilirler. Ayarlar ile ilgili ayrıntılı bilgi <http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3ClientAccGuide/0061a99a-d963-477a-96f8-46207a8c8776.mspx> adresinden alınabilir. Ayrıca aynı işlem http isteklerini https'e yönlendirmek için de kullanılabilir. Bu şekilde sunucuya güvensiz bağlanmaya çalışan kullanıcılar güvenli bağlantıya otomatik olarak aktarılmış olur.

Özet olarak internet üzerinden OWA kullanıldığında güvenlik ile ilgili dikkat edilmesi gereken en önemli konular şunlardır:

- SSL etkin hale getirilmelidir.
- 128 bitlik SSL kullanılmalıdır.
- Sunucuya güvensiz (SSL olmadan) erişim engellenmelidir.
- Form tabanlı kimlik doğrulama etkin olmalıdır.

4.2.2 İstemci kurum ağı içerisinde Outlook ile bağlandığında

Kurum ağı içerisinde e-posta alıp göndermek için en çok kullanılan yazılımlardan biri Microsoft Outlook yazılımıdır. Outlook bir MAPI istemcidir ve Exchange sunucusuyla iletişim için RPC kullanır. Güvenlik açısından RPC trafiği şifrelenmelidir. RPC trafiğinin şifrelenmesi için Outlook 2003'te:

Tools → E-mail Accounts → %Kullandığınız Exchange Hesabı% → Change → More Settings → Security → Encrypt data between Microsoft Outlook and Microsoft Exchange Server

Outlook 2002'de

Tools → Accounts → %Kullandığınız Exchange Hesabı% → Change → More Settings → Advanced → Encrypt information when using network

ayarları etkin hale getirilmelidir.

Ayrıca aynı sekmelerden kimlik doğrulama metotları da değiştirilebilir. Kimlik doğrulama seçeneği olarak Kerberos ve NTLM mevcuttur. Her zaman olduğu gibi kimlik doğrulama için NTLM kullanılacaksa NTLMv2 kullanılması gerekli ayarlarla zorunlu kılınmalıdır.

4.2.3 İstemci internet üzerinden Outlook ile bağlandığında

Bir önceki bölümde belirtildiği gibi Outlook Exchange sunucusuyla haberleşmek için RPC kullanmaktadır. Bu durum Outlook istemcilerinin internet üzerinden kullanılmasını zorlaştırmaktadır. Microsoft Outlook istemcisinin internette de kullanılabilmesi için "RPC over HTTP" protokolünü geliştirmiştir. Bu sayede tüm RPC istekleri HTTP üzerinden Exchange ön uç sunucuya aktarılmaktadır.

RPC over HTTP kullanıldığı zaman kullanılacak iki kimlik doğrulama metodu vardır

- Password Authentication (NTLM)

- Basic Password Authentication

Güvenlik açısından NTLM kullanılmalıdır ve sadece SSL ile bağlantı yapılmalıdır. Ayrıca karşılıklı olarak kimlik doğrulama yapılarak oturum açılmalıdır. Bu ayarlar şu şekilde yapılır:

Tools → Accounts → %Kullandığınız Exchange Hesabı% → Change → More Settings → Connection → Connect to my Exchange mailbox using http

Tools → Accounts → %Kullandığınız Exchange Hesabı% → Change → More Settings → Connection → Exchange proxy settings → Connect with SSL only ve Mutually authenticate the session when connecting with SSL

Bu ayarların yapılmış olması yeterli değildir. Kullanıcıların bu ayarları değiştirmesi de engellenmelidir. Aksi takdirde kullanıcı veya kullanıcı haklarıyla çalışan başka bir program bu ayarları değiştirip haberleşmeyi güvensiz hale getirebilir. Bu işlem grup politikası ile veya bir kütük ayarıyla yapılabilir.

1. Grup politikası ile yapmak için aşağıdaki ayar yapılmalıdır:

User Configuration → Administrative Templates → Microsoft Office Outlook 2003 → Tools → E-Mail Accounts → Exchange over the Internet User Interface → Hidden

2. Kütük(Registry) ayarı ile yapmak için aşağıdaki değer yaratılmalıdır:

HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\11.0\Outlook\RPC

Değer ismi: EnableRPCTunnelingUI

Değer tipi: DWORD

5. EXCHANGE ORTAMININ GÜVENLİĞİ

Sunucuların sıkılaştırılmasından bağımsız olarak tüm Exchange organizasyonunda etkin olacak bazı güvenlik önlemleri alınmalıdır. Ayrıca istenmeyen e-postalar (spam) ve e-posta virüsleri güvenlik açısından en büyük tehditlerdir. Bu bölümde istenmeyen e-postaları ve virüsler engellemek için yapılması gerekenler de anlatılmaktadır

5.1 Exchange organizasyonundaki gerekli güvenlik ayarları

Sunucuların yapılandırılması ve iletişim güvenliği dışında Exchange ortamının güvenliği için Exchange organizasyonunda bazı ayarlar yapılmalıdır.

5.1.1 İşletim sistemi, Exchange ve istemciler için yamalar uygulanmalıdır.

Tüm sistemlerde açıklıklar çıkabilir. Önemli olan bulunan açıklıkları kapatacak yamaların kısa sürede çıkarılması ve uygulanmasıdır. Bunun için Exchange yazılımının ve üzerinde koştuğu işletim sisteminin yamaları tam olmalıdır. Eksik yamaların bulunması ve indirilmesi işlemi için Microsoft'un geliştirdiği Microsoft Baseline Security Analyzer (MBSA), Microsoft Update (MU) veya Windows Server Update Services (WSUS) kullanılabilir.

5.1.2 Exchange organizasyonunu ve/veya sunucularını yönetecek gruplar oluşturulmalıdır.

Exchange sistemi pek çok farklı seviye için (organizasyon, sunucu, posta kutusu deposu vs.) yetkilendirmeye izin vermektedir. “Exchange full administrator”, “Exchange view only administrator” gibi önceden belirlenmiş yetkilendirme seviyeleri bulunduğu gibi her nesne üzerinde aktif dizin kullanıcı veya grupları ile de yetki ayarlamak mümkündür. Yetkisiz yöneticiler sistem bütünlüğünün bozulmasına neden olabilir. Ayrıca görevlerin ayrımı ilkesine uyulmamasından dolayı yetkisiz işlemlerin yapılması da olasıdır.

Exchange System Manager da güvenlik sekmesinin gözükmemesi için kütüğe aşağıdaki değer eklenmelidir

HKCU\Software\Microsoft\Exchange\ExAdmin

Değer adı ve tipi: ShowSecurityPage DWORD

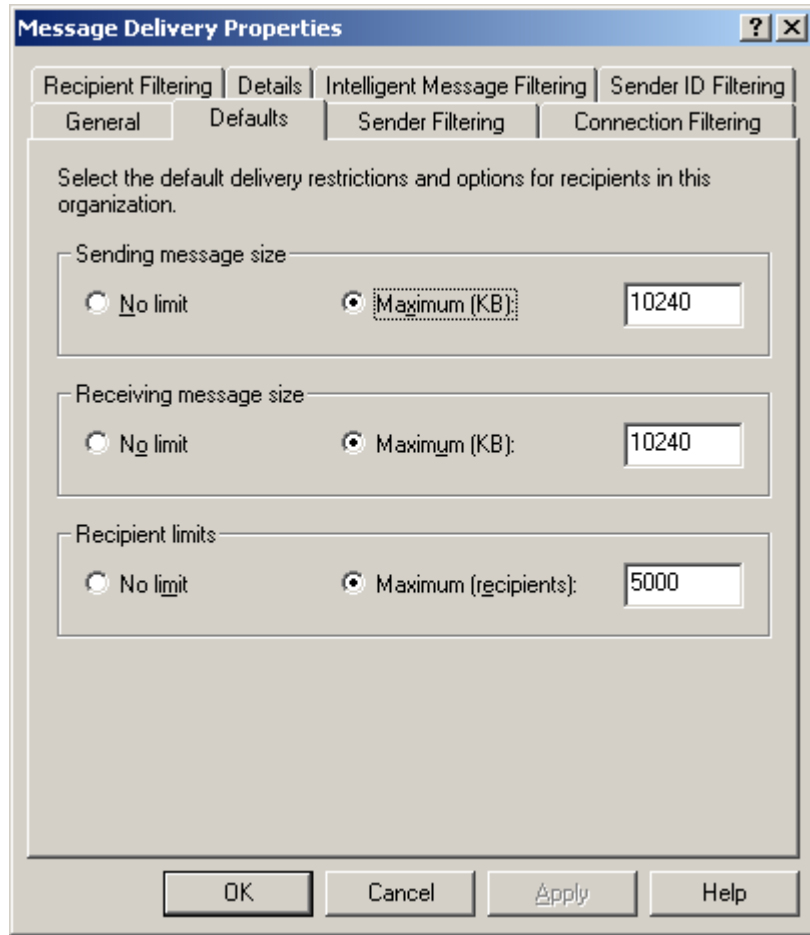
Değeri: 1

5.1.3 Gönderilen ve alınan e-postaların maksimum boyutu sınırlandırılmalıdır.

Kullanıcılarının gönderebileceği ve alabileceği e-posta mesajlarının boyutları için uygun bir üst limit belirlenmelidir. Aksi takdirde posta kutularını barından diskler dolabilir ve sistem çalışmaz hale gelebilir. Bu ayar aşağıdaki menü yolu izlenerek yapılabilir (Şekil 5.1).

Global Settings → Message Delivery → Properties → Defaults → Sending Message Size

Global Settings → Message Delivery → Properties → Defaults → Receiving Message Size



Şekil 5.1 – Organizasyonda geçerli mesaj limitleri

5.1.4 En fazla alıcı sayısı kısıtlanmalıdır.

Bir e-posta mesajının dağıtılacağı en fazla alıcı sayısı için uygun bir üst limit belirlenmelidir. Bu istenmeyen posta gönderen kişilerin engellenmesi için önemlidir. Bu ayar aşağıdaki menü yolu izlenerek yapılabilir (Şekil 5.1).

Global Settings → Message Delivery → Properties → Defaults → Recipient limits

5.1.5 Otomatik mesajlara izin verilmemelidir.

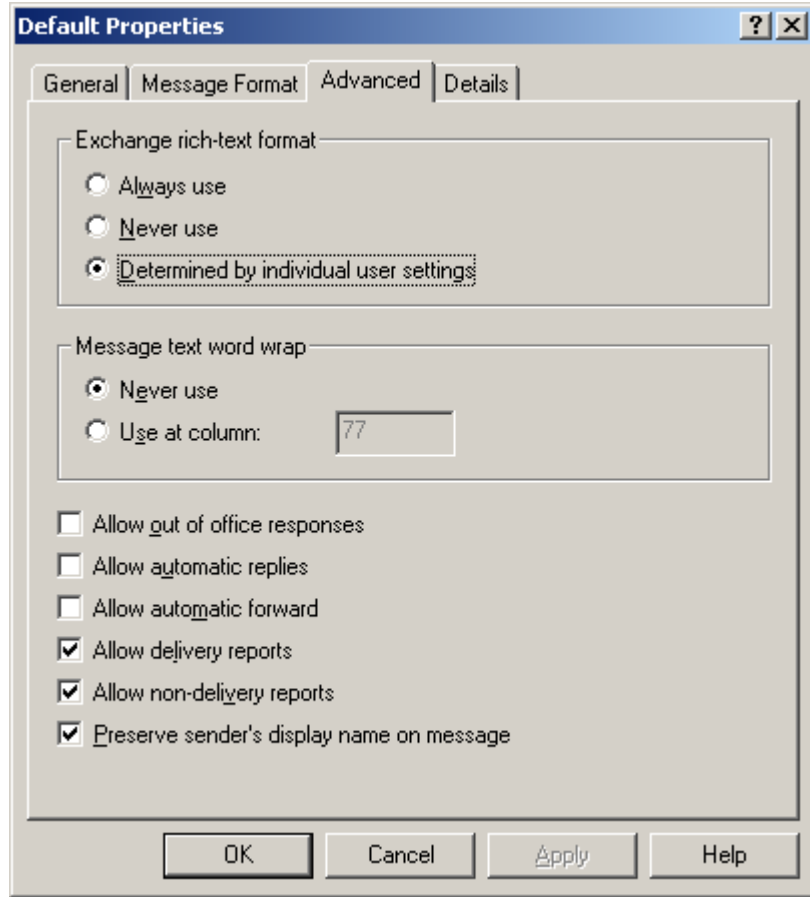
Kullanıcıların bilinçsiz otomatik mesaj belirlemesi durumunda yetkisiz kişilere fazladan bilgi aktarılabilir (Görev dağılımı, bağlantı noktası vs.), otomatikleştirilmiş programlar kullanılarak gereksiz e-posta trafiği oluşturulabilir. Bunu engellemek için:

- Ofis Dışı (Out of Office) özelliğinin devre dışı olması gereklidir.
- Otomatik Cevaplar (Automatic Replies) özelliğinin devre dışı olması gereklidir.
- Otomatik Yönlendirme (Automatic Forward) özelliğinin devre dışı olması gereklidir.

Bu ayarlar aşağıdaki menü yolu izlenerek yapılabilir (Şekil 5.2).

Global Settings → Internet Message Formats → Default → Properties → Advanced

Fakat bu risklere rağmen kurumun bu özelliklere ihtiyacı olabilir. Bu durumda riskin bilinmesi ve dokümente edilmesi gerekir.



Şekil 5.2 – Otomatik mesaj ayarları

5.1.6 E-postaların bütünlüğünü ve gizliliğini korumak için PKI kullanılabilir.

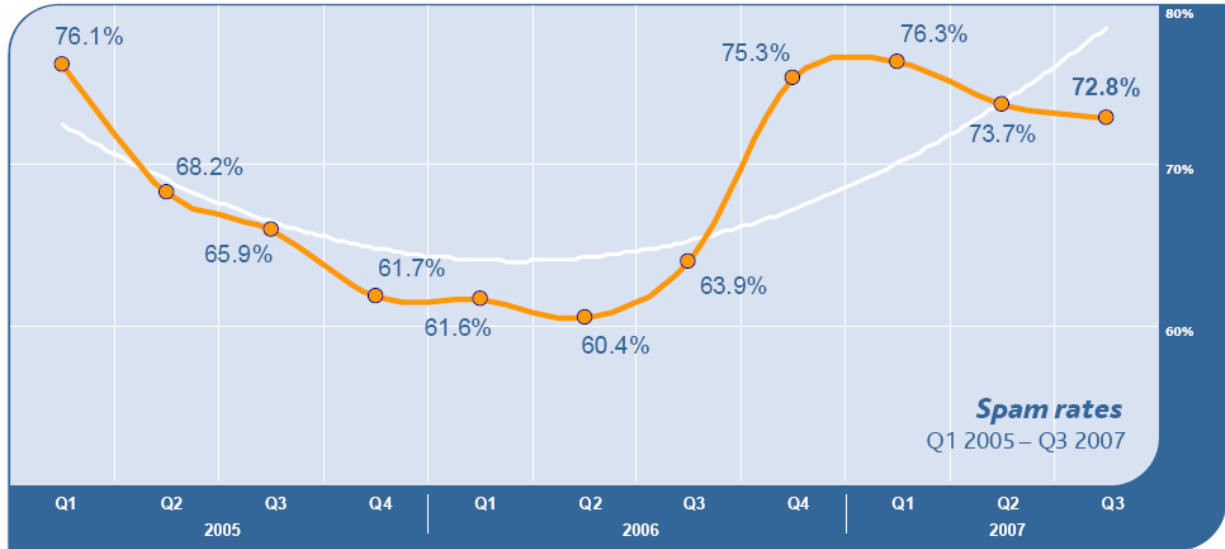
E-posta mesajı içeriğinin iletim sırasında değişmesi veya yetkisiz kullanıcılar tarafından okunabilmesi kuruluşlarda büyük sorunlar yaratabilir. Bunun için PKI kullanılmalıdır. PKI konusunun detayları bu rehberin kapsamı dışındadır.

5.2 İstenmeyen e-postaların (spam) önlenmesi

Spam yani istenmeyen e-postalar herkesin posta kutusuna gelen, genellikle bir şeyler pazarlamaya veya zararlı yazılımları yaymaya çalışan e-postalardır. İstenmeyen e-postaların yol açtığı bazı zararlar şu şekildedir:

- Virüslerin ve phishing saldırılarının yayılmasını sağlar
- Sistem kaynaklarının boşa kullanılmasına neden olur
- İş gücü kaybı yaratır
- Kurumun markasına/itibarına zarar verebilir.

MessageLabs firmasının “[MessageLabs Intelligence: September 2007 A Downpour of Virus & Phishing Activity, In the Wake of a Storm Worm Surge](#)” isimli raporuna göre 2007 yılının üçüncü çeyreğinde ortalama olarak her 100 e-postanın 73 tanesi istenmeyen e-postadır. Aynı rapordan alınan ve 2005 yılından bu yana istenmeyen e-posta oranlarını veren grafik Şekil 5.3’de verilmiştir.



Şekil 5.3 – MessageLabs firmasının istatistiklerine göre yıllara göre istenmeyen e-posta(spam) oranı

Exchange Server 2003 istenmeyen e-postalarla mücadelede kendi başına pek yeterli olmayabilir ve üçüncü parti yazılımlar kullanmak gerekebilir. Buna rağmen istenmeyen e-postalarla mücadele etmek için Exchange Server 2003 yazılımıyla birlikte birçok araç gelmektedir. Burada bu araçlar anlatılmakta üçüncü parti yazılımlar anlatılmamaktadır.

İstenmeyen e-postalarla mücadele iki fazda gerçekleşir:

1. Mesaj kullanıcının posta kutusuna ulaşmadan yapılabilecekler.

- Alıcı filtreleri (Recipient Filtering)
- Gönderen filtreleri (Sender Filtering)
- Bağlantı filtreleri (Connection Filtering)
- Intelligent Message Filter (IMF)
- SMTP Bataklık Özelliği (Tar Pitting)

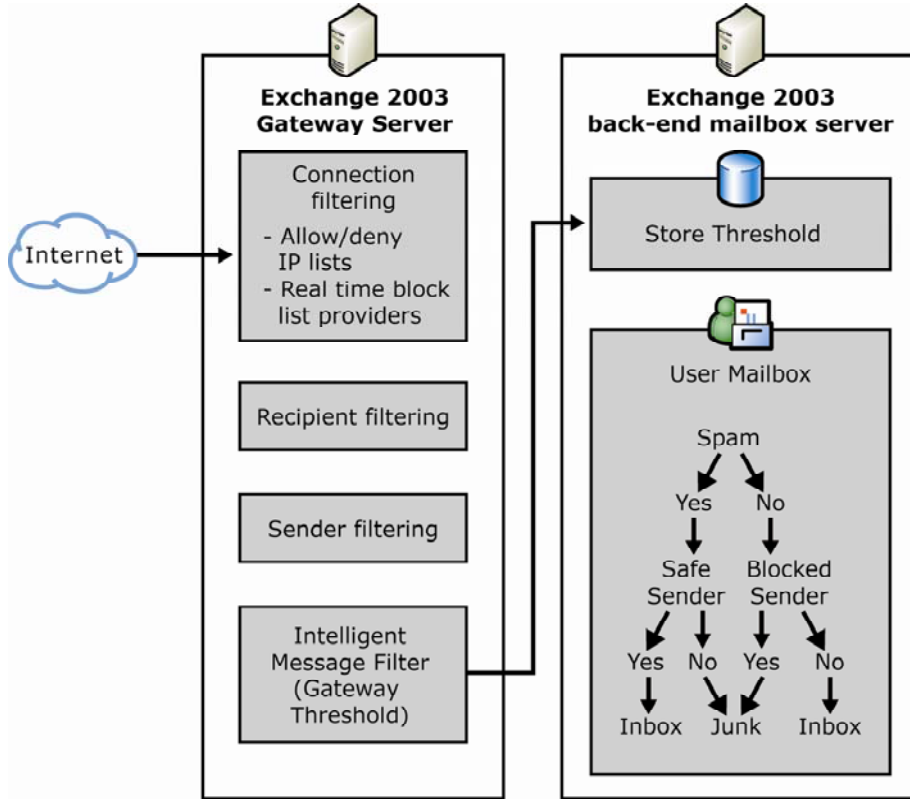
- E-posta Kimlik doğrulaması ve Sender ID
2. Mesaj kullanıcının posta kutusuna ulaştıktan sonra yapılabilecekler:
 - Outlook 2003 veya OWA ile spam olduğu düşünülen e-postaların otomatik olarak işlenmesi

Bir SMTP bağlantısında Exchange sunucu aşağıdaki ölçütlere göre bağlantı filtrelerini uygular. Bahsi geçen filtreler ileride detaylı olarak anlatılacaktır.

1. Global accept listesi incelenir. IP adresi bu listede ise mesaj kabul edilir ve başka herhangi bir filtre (bağlantı, alıcı, gönderen) uygulanmaz.
2. Global deny listesi incelenir. IP adresi bu listede ise mesaj reddedilir ve başka herhangi bir filtre (bağlantı, alıcı, gönderen) uygulanmaz.
3. Ayarlanmış real-time block listeleri kontrol edilir. Gönderenin IP adresi listedeyse mesaj kabul edilmez.
4. Gönderenin adresi (MAIL FROM komutu ile belirtilen) ile gönderen filtreleri karşılaştırılır.
5. Alıcı filtreleri kontrol edilir.
6. Gönderenin çözümlenmiş adresi gönderen filtreleri ile karşılaştırılır.
7. Mesaj bu aşamalardan geçebilirse Intelligent Message Filter uygulanır. Bu işlem sonucunda mesajın Spam Confidence Seviyesi (SCL) belirlenen değerden yüksekse mesaja uygun işlem uygulanır (kabul edilmez, arşivlenir vs). Belirlenen değerden düşükse mesaj kullanıcın posta kutusuna iletilir.

Bu noktadan sonra kullanıcı tarafında alınmış önlemler devreye girer. Kullanıcı Outlook 2003 veya Exchange 2003 OWA kullanıyorsa mesajın sunucu tarafından belirlenen SCL derecesi kullanıcının belirlediği derece ile karşılaştırılır. Mesajın derecesi düşükse ve gönderen blocked sender olarak tanımlanmamışsa veya mesajın seviyesi yüksek olduğu halde gönderen safe sender olarak belirlenmişse mesaj gelen kutusuna atılır. Aksi takdirde istenmeyen posta klasörüne koyulur.

Yukarı anlatılan adımların hepsi Şekil 5.4'te görsel olarak verilmiştir. Exchange sunucuda gerçekleşecek tüm filtreleme işlemleri ve bu filtrelerin nasıl ayarlanacağı bundan sonraki başlıklarda ele alınmaktadır.



Şekil 5.4 – Exchange sunucuya gelen bir mesajın uygulanan filtreler

5.2.1 Bağlantı filtreleri (Connection Filtering)

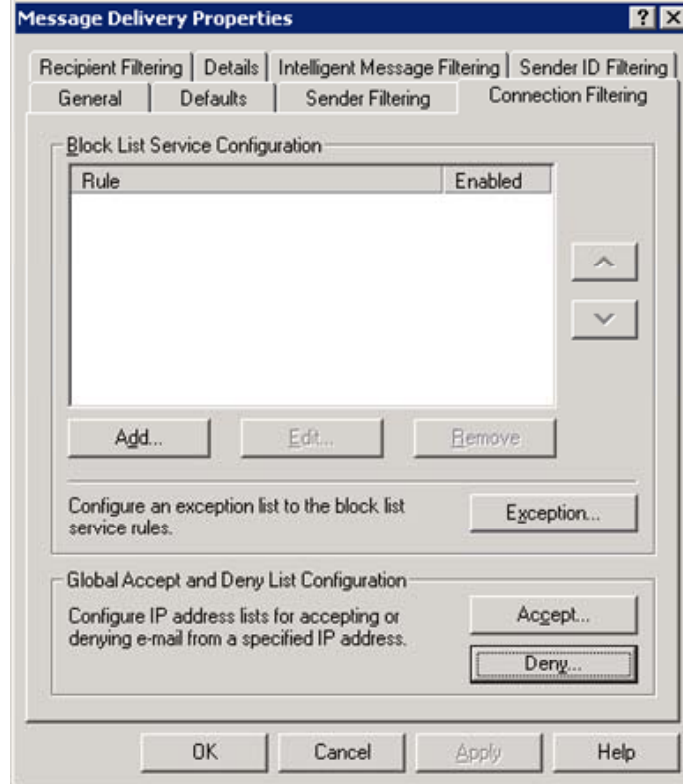
Bağlantı filtreleri ile:

1. Global kabul ve red listeleri (Global Accept, Global Deny) oluşturulabilir.

Global kabul ve red listeleri bir e-posta geldiğinde uygulanan ilk filtrelerdir. Kabul listesindeki gönderenlerden/etki alanlarından gelen e-postalara başka herhangi bir filtre uygulanmaz ve kabul edilir. Aynı şekilde ret listesindeki gönderenlerden/etki alanlarından gelen e-postalar başka işlem uygulanmadan reddedilir.

2. Kullanılacak Real-Time Block (RBL) listeleri tanımlanabilir.

RBL'ler gerçek zamanlı olarak istenmeyen e-posta gönderen IP adreslerinin listesini tutan DNS sunumcularıdır. E-posta gönderen bilgisayarın IP adresi bu listelere sorulur. Yapılan DNS sorgusunda IP adresi bulunursa RBL sağlayıcısı belirli bir kod döner (127.0.0.x gibi). Bu durumda gönderilen posta spam olarak varsayılır ve kabul edilmez. Eğer sorgulanan IP adresi DNS de bulunmuyorsa mesaj kabul edilir.



Şekil 5.5 – Bağlantı filtreleri ayarları

Bağlantı filtrelerini ayarlamak için aşağıdaki yol izlenebilir. Buradan yapılabilecek ayarlar Şekil 5.5’de görülmektedir.

Exchange System Manager → *%Exchange Organizasyonu%* → *Global Settings* → *Message Delivery* → *Properties* → *ConnectionFiltering*

5.2.2 Alıcı filtreleri (Recipient Filtering)

Alıcı filtreleri ile:

1. Belirli kullanıcılara e-posta gönderilmesi engellenebilir.

Buradaki listeye e-posta alması istenmeyen kullanıcılar eklenebilir. E-posta gönderimi için SMTP bağlantısı gerçekleşip karşı sunucu “RCPT TO:” komutunu gönderdiğinde bu filtre sorgulanır. Belirtilen kullanıcı bu listedeyse mesaj kabul edilmez.

2. Aktif dizinde bulunmayan kullanıcılara e-posta gönderilmesi engellenebilir.

Bu değer (*Filter recipients who are not in the Directory*) etkinken alıcının etki alanı adı doğru olsa bile kullanıcın dizinde kayıtlı olup olmadığı kontrol edilir. Eğer kullanıcı dizinde kayıtlı değilse mesaj kabul edilmez.



Şekil 5.6 – Alıcı filtreleri ayarları

Alıcı filtrelerini ayarlamak için aşağıdaki yol izlenebilir. Buradan yapılabilecek ayarlar Şekil 5.6’da görülmektedir.

Exchange System Manager → *%Exchange Organizasyonu%* → *Global Settings* → *Message Delivery* → *Properties* → *Recipient Filtering*

5.2.3 Gönderen filtreleri (Sender Filtering)

Gönderen filtreleri ile:

1. Belirli kullanıcıların veya etki alanlarının e-posta göndermesi engellenebilir.

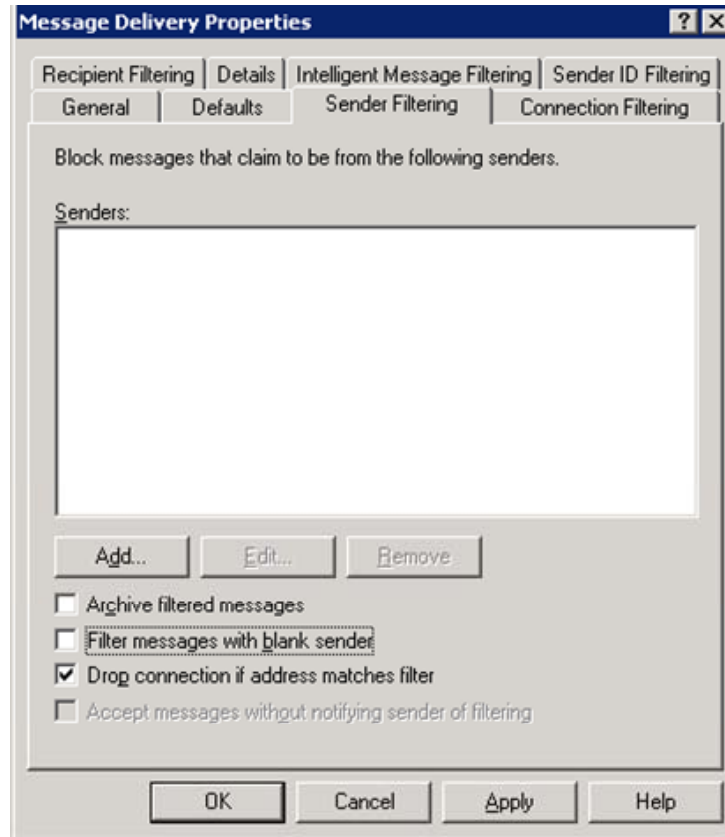
Bunun için filtreler kısmına engellenmek istenen adresler veya etki alanları girilir. Seçilen seçeneğe göre mesajlar kabul edilmez veya daha sonra gözden geçirilmek üzere ayrı bir yerde saklanır.

2. Gönderen kısmı boş olan e-postaların gönderilmesi engellenebilir.

SMTP bağlantısı sırasında “MAIL FROM:” komutunda gönderen adresi belirtilmezse mesaj filtrelenir.

3. Engellenen mesajlar daha sonra incelemek için arşivlenebilir. (*Accept messages without notifying sender of filtering*)

Bu seçenek işaretli ise Exchange sunucu mesaj gönderene mesajın filtrelendiğine dair bir hata mesaj vermez fakat mesajı gönderilen kişiye de iletmez. Daha sonra incelenmek için mesaj saklanır. Exchange sunucu filtrelenen mesajları düşürecek şekilde yapılandırılmışsa (*Drop connection if address matches filter*) bu seçenek işaretlenemez.



Şekil 5.7 – Gönderen filtreleri ayarları

Gönderen filtrelerini ayarlamak için aşağıdaki yol izlenebilir. Buradan yapılabilecek ayarlar Şekil 5.7’de görülmektedir.

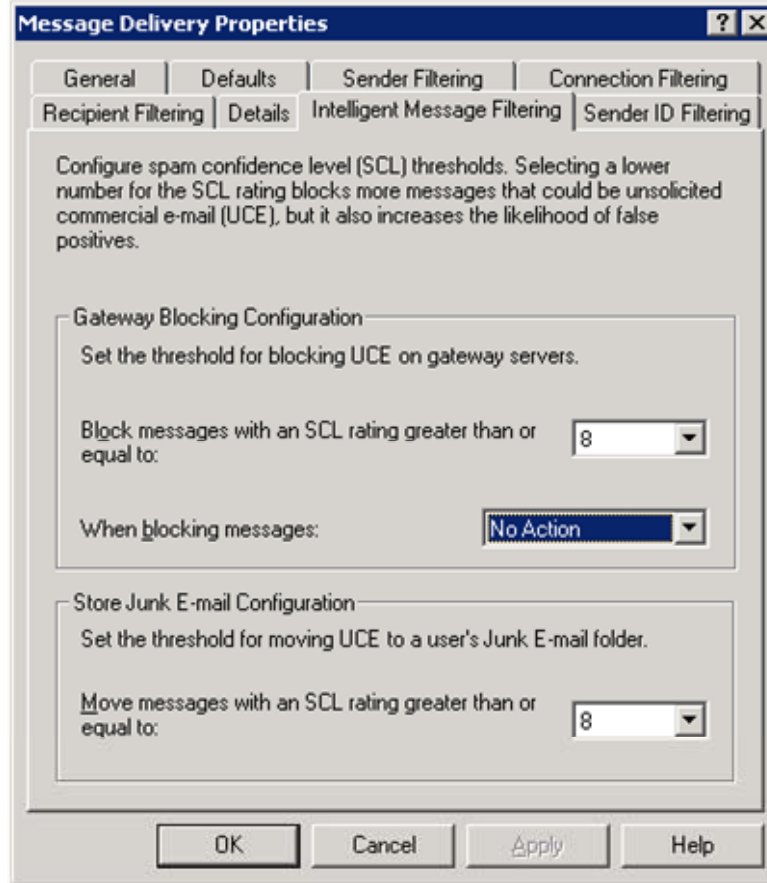
Exchange System Manager → *%Exchange Organizasyonu%* → *Global Settings* → *Message Delivery* → *Properties* → *Sender Filtering*

5.2.4 Intelligent Message Filter (IMF)

IMF gelen e-postanın içeriğini değerlendirip mesajın SPAM olma olasılığını değerlendirir ve bu olasılığa göre mesaja bir spam confidence level (SCL) atar. “-1” ile “9” arasında onbir adet SCL seviyesi bulunur.

- “-1” seviyesi Microsoft tarafından iç mesajlaşmada kullanılır ve içeride gerçekleşen mesajlaşmanın spam olarak algılanmasını engeller.
- “0” SCL seviyesine sahip e-postalar spam değildir.
- “1” – “9” arasındaki seviyeler mesajın spam olma olasılığını gösterir. Seviye ne kadar büyükse mesajın spam olma olasılığı da o kadar fazladır.

Exchange sunucuda IMF ayarlarında iki eşik seviyesi belirlenir. Sunucunun eşik seviyesini aşan mesajlar direk olarak engellenir. Kullanıcılar için belirlenen eşik seviyesini geçen mesajlar ise kullanıcının istenmeyen mesajlar dizinine aktarılır. Bu iki eşik değeri Şekil 5.8’de görülen “*Gateway Blocking Configuration*” ve “*Store Junk E-mail Configuration*” bölümlerinde ayarlanabilir.



Şekil 5.8 – Intelligent Message Filtre ayarları

IMF ayarları aşağıdaki yol izlenerek yapılabilir.

Exchange System Manager → *%Exchange Organizasyonu%* → *Global Settings* → *Message Delivery* → *Properties* → *Intelligent Message Filtering*

5.2.5 SMTP Bataklık Özelliği (Tar Pitting)

SMTP bataklık özelliği, belirli SMTP iletişimlerine bilerek bir gecikme eklemektir. Kullanıcının gönderdiği bir e-postaya 1-2 saniye gecikme eklemek kullanıcıyı etkilemez fakat aynı anda milyonlarca e-posta göndermek isteyen biri için bu işlem çok vakit kaybına sebep olur. Böylece otomatik olarak istenmeyen posta gönderenlerin bu işlemi gerçekleştirmesi çok uzun sürer.

Bu özellik SMTP protokolü 5.x.x hata kodları içeren tüm yanıtları yavaşlatarak çalışır ve sadece anonim bağlantılara uygulanır. Ayrıca bataklık özelliği alıcı filtresi ile birlikte uygulanmalıdır.

Bataklık özelliği, bir kayıt defteri anahtarı ayarlanarak etkinleştirilebilir ve yapılandırılabilir. Değer ondalık olarak girilmelidir ve geciktirme süresini saniye cinsinden belirler. Bu değer eklendikten sonra etkin olması için SMTP servisi tekrar başlatılmalıdır.

Anahtar adı:

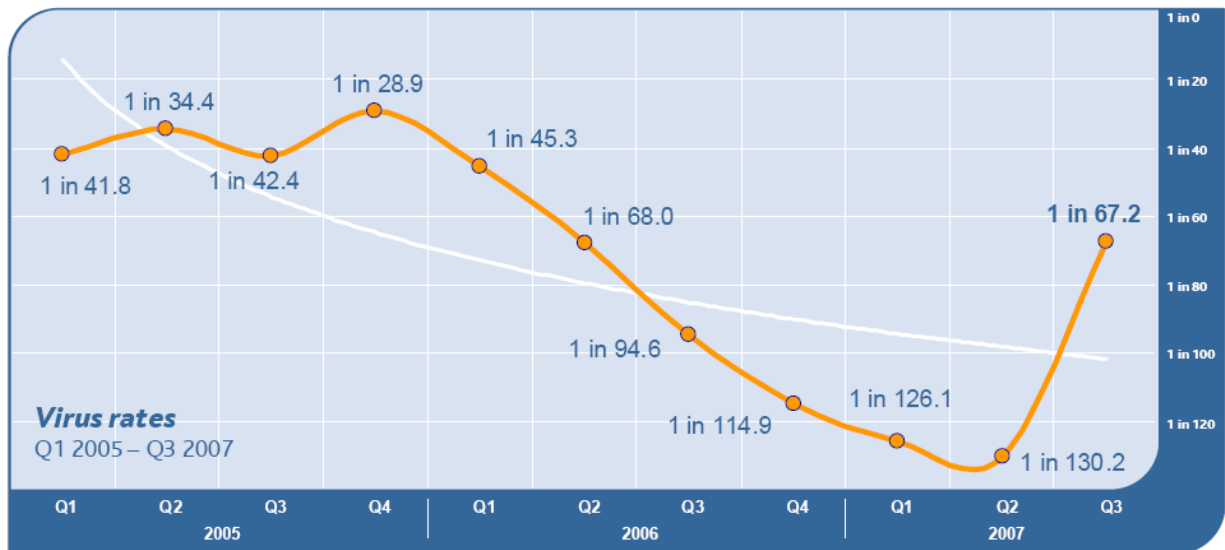
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SMTPSVC\Parameters

Değer ismi: TarpitTime

Değer tiği: DWORD

5.3 Virüslerden korunma

Virüslerin yayılmasını kolaylaştıran en önemli yollardan biri e-postalardır. Saldırganlar e-postalara ilgi çekici başlıklar ve güzel vaatler yazarak kullanıcıların virüslü dosyaları açmalarını sağlarlar. MessageLabs firmasının "[MessageLabs Intelligence: September 2007 A Downpour of Virus & Phishing Activity, In the Wake of a Storm Worm Surge](#)" isimli raporuna göre 2007 yılının üçüncü çeyreğinde ortalama olarak her 67 e-postanın bir tanesinde virüs bulunmaktadır. Aynı rapordan alınan ve 2005 yılından bu yana virüs oranlarını veren grafik Şekil 5.9'da verilmiştir.



Şekil 5.9 – MessageLabs firmasının istatistiklerine göre yıllara göre virüslü e-posta oranı

E-posta virüslerini engellemenin en iyi yolu mesajlaşma sisteminin her noktasında anti-virüs çözümleri kullanmaktır. Böylece kademeli bir şekilde mesaj kurum ağına girip kullanıcının e-posta istemcisinde açılana kadar her nokta virüs taramasından geçirilmiş olur. Örneğin virüs ve zararlı yazılımlara karşı taramalar güvenlik duvarında, SMTP geçidi seviyesinde, posta kutularının bulunduğu Exchange sunucularında ve kullanıcı bilgisayarlarında yapılabilir.

Elbette bu yaklaşımın dezavantajları da mevcuttur. Her noktada virüs taraması yapabilmek için değişik yazılımlara donanımlara ve bu yazılım ve donanımları yönetecek ve takip edecek personele ihtiyaç vardır.

Exchange Server 2003 ile kullanılacak anti-virüs yazılım çeşitleri şu şekilde sıralanabilir.

1. Dosya seviyesindeki tarayıcılar (file-level)

Bu tür tarayıcılar istendiği zaman (on-demand) veya sürekli olarak (memory-resident) dosyalar üzerinde virüs taraması gerçekleştirirler. Bu tip tarayıcılar dosyaları tararken dosyayı kilitleyebilir veya karantinaya alabilir. Exchange kayıt veya veritabanı dosyalarının kilitlemesi Exchange sistemini çalışmaz hale getirebilir. Bu yüzden Exchange Server üzerinde dosya seviyesinde tarama yapan bir anti-virüs yazılımı kullanılması tavsiye edilmez. Ayrıca bu tip programlar Melissa virüsü gibi virüsleri de bulamazlar çünkü bu tip virüsler dosya yerine başka şeyler kullanırlar (örneğin word makroları).

2. MAPI tarayıcıları

Bu tip tarayıcılar posta kutularına MAPI oturumu açarlar ve mevcut mesajları tararlar. Dosya seviyesinde çalışan tarayıcılara göre avantajları Exchange için kritik dosyaları kilitlememesi ve dosya tabanlı olmayan virüsleri yakalayabilmesidir. Dezavantajları ise gönderilen mesajları tarayamaması ve bir mesajı birden çok kez taramasıdır.

3. Virüs tarayan API tarayıcıları (Virüs scanning API scanners)

Bu tip tarayıcılar Exchange Server ile entegre çalışırlar. Örneğin virüslü mesajları silip gönderen kişiye bilgi verebilirler, istemcilerin kullanması için mesaja virüs durumunu belirten eklemeler yapabilirler vs.

4. Extensible Storage Engine (ESE) tabanlı tarayıcılar

ESE tabanlı tarayıcılar information store ile ESE arasında bir arayüz kullanırlar ve Microsoft tarafından desteklenmemektedir. Bu tip anti-virüs yazılımlarının kullanımı veritabanına zarar verebilir veya bilgi kaybına neden olabilir. Bu yazılımlar ese.dll dosyasının ismini değiştirip kendi ese.dll dosyalarını kullanırlar.

Ayrıntılı bilgi <http://support.microsoft.com/kb/823166> adresinden alınabilir.

Zararlı yazılımlara karşı korunmayla ilgili olarak UEKAE BGT-1004 Zararlı Yazılıma Karşı Korunma Kılavuzu'ndan faydalanılabilir.

KAYNAKÇA

- [1] MessageLabs Intelligence: September 2007 “A Downpour of Virus & Phishing Activity, In the Wake of a Storm Worm Surge”
- [2] Exchange Server 2003 and Exchange 2000 Server Front-End and Back-End Topology, Joey Masterson, Andrew Moss, www.microsoft.com/exchange/library
- [3] Secure Messaging with Microsoft Exchange Server 2003, Paul Robichaux
- [4] Microsoft Exchange Server 2003 Message Security Guide, Exchange Server Documentation Team
- [5] Microsoft Exchange Server 2003 Security Hardening Guide, Exchange Server Documentation Team