Microsoft Business Solutions

Navision Security Hardening Guide

Yayımlanma Tarihi: Ekim 2004

Microsoft

İçindekiler

Giriş

Microsoft® Windows®, seçkin standartlara dayalı güvenlik sağlar. En geniş anlamda, güvenlik işlemlerinizi planlama ve değerlendirme aşamasında önemlidir. Örneğin, bir bilgisayar mahzene kilitlenebilir ve yalnızca bir sistem yöneticisi tarafından erişilmesi sağlanabilir. Bu bilgisayar güvenli olabilir ancak başka herhangi bir bilgisayara bağlı olmadığından yararlı değildir. Bir ağı, kullanılabilirliğinden ödün vermeden nasıl mümkün olduğunca güvenli yapabileceğiniz konusunda düşünmeniz gerekir.

Çoğu kuruluş dışarıdan gelen ataklarla ilgili planlar yapar ve güvenlik duvarları oluşturur, ancak birçok şirket, kötü niyetli bir kullanıcı güvenlik duvarının içine bir kez girdikten sonra söz konusu olan güvenlik açığını nasıl kapatabilecekleri konusunda düşünmez. Kullanıcıların işlerini güvenli bir şekilde yapmak için çok fazla yordam ve adım uygulamaları gerekmiyorsa, müşterinizin ortamındaki güvenlik önlemleri iyi çalışacak demektir. Kullanıcılar için güvenlik ilkelerini gerçekleştirmek mümkün olduğunca kolay olmalıdır, yoksa işlerini yapmak için daha az güvenli yollar bulma eğiliminde olurlar.

Navision yüklemelerinin büyüklükleri büyük ölçüde değişiklik gösterebileceğinden, her müşterinin gereksinimlerini dikkatli bir şekilde göz önünde bulundurmak ve güvenliğin etkinliğini söz konusu olabilecek maliyetlerle karşılaştırmak önemlidir. Müşterinizin güvenilir danışmanı olarak, değerlendirme yeteneğinizi en iyi şekilde kullanın ve müşterinin sonuç olarak ilgili yordamları uygulamaya son vermesine neden olabilecek bir yük oluşturmadan güvenlik gereksinimlerini karşılayacak bir güvenlik ilkesi önerin.

Navision Güvenliği En iyi Yöntemler

Aşağıdaki genel kurallar, Navision ortamının güvenliğini artırmaya yardımcı olabilir:

- Navision Database Server'ı bir hizmet olarak çalıştırmak veya sunucuyu başlattığınızda *installasservice* komut satırı parametresini kullanmak isterseniz, hizmetin NT Authority\Network Service hesabı olarak çalışıyor olmasını sağlamanız gerekir. NT Authority\Network Service hesabı yalnızca Windows™ XP ve Windows Server™ 2003'te bulunur. Windows 2000 Server çalıştırıyorsanız, hizmet için en az ayrıcalığa sahip bir hesap oluşturmanız gerekir, yoksa hizmete bir Yerel Sistem hesabı atanır. Bu hesabın normal Kullanıcılar hesabıyla aynı ayrıcalıklara sahip olması veya etki alanında veya yerel bilgisayarda yönetici olmayan bir etki alanı hesabı olması gerekir.

  Kullanıcıların veritabanına bağlanmalarını sağlamak için, NT Authority\Network Service hesabına veya sunucunun çalıştırdığı kullanıcı hesabına veritabanı dosyalarını okuma veya bu dosyalara yazma erişimi vermeniz gerekir.

  NT Authority\Network Service hesabına Windows XP'de bir veritabanı dosyasını okuma ve dosyaya yazma erişimi vermek için:

  1. Windows Gezgini'nde, veritabanı dosyasını içeren klasöre gidin.
  2. Veritabanı dosyasını seçip sağ tıklatın ve sonra Özellikler'i tıklatın.
  3. ***Özellikler*** penceresinde bulunan ***Güvenlik*** sekmesinde, **Grup ve kullanıcı adları** alanının altındaki Ekle'yi tıklatın.
  4. *Kullanıcı, Bilgisayar veya Grup Seç* penceresinde, Ağ Hizmeti yazın ve Tamam'ı tıklatın.
  5. AĞ HİZMETİ hesabı, ***Özellikler*** penceresindeki **Grup ve kullanıcı adları** alanına eklenmiş olur.
  6. AĞ HİZMETİ'ni seçin ve **İzinler** alanında bu hesaba *Okuma* ve *Yazma* izinleri verin.
- Navision Uygulama Sunucusu hizmeti, varsayılan değer olarak NT Authority\Network Service hesabı olarak çalışır ve böylece Navision Database Server'a yerel olarak erişebilir. Bununla birlikte, veritabanı sunucusuna erişimi olmasını istiyorsanız, bir ağ üzerinde, Navision Uygulama Sunucusu hizmetinin Navision Database Server tarafından tanınan bir Windows etki alanı olarak çalışmasını sağlamanız gerekir. Bu hesap, etki alanında veya herhangi bir yerel bilgisayarda bir yönetici olmamalıdır.
- Navision'ın SQL Server Seçeneği'ni çalıştırıyorsanız, Microsoft SQL Server™ bir hizmet olarak çalışıyordur. Navision'ın SQL Server Seçeneği, SQL Server'ın kimlik doğrulama amacıyla Windows kullanıcı gruplarının listesini almak için Active Directory'de arama yapabilmesini gerektirir. Bu nedenle, SQL Server hizmetinin NT Authority\Network Service hesabı olarak çalışmasını sağlamanız gerekir.

  Hizmetin NT Authority\Network Service hesabı olarak çalışmasını sağlamak için:

  1. SQL Server bilgisayarında, MSSQLSERVER hizmetini bulun, sağ tıklatın ve Özellikler'i tıklatın.
  2. ***Özellikler*** penceresinde, ***Oturum Aç*** sekmesini tıklatın.
  3. ***Oturum Aç*** sekmesinde, Oturum açma türü altında Bu Hesap seçeneğini tıklatın ve *NT Authority\NetworkService* girip Tamam düğmesini tıklatın.

  SQL Server güvenliği hakkında daha fazla bilgi için şu sayfaları ziyaret edin:

  http://www.microsoft.com/security/guidance/prodtech/SQLServer.mspx

  ve

  http://www.microsoft.com/technet/security/prodtech/dbsql/default.mspx

- Commerce Gateway gibi bir Navision E-business ürünü çalıştırıyorsanız, Commerce Gateway Request Server'un hizmetler için varsayılan hesap ayarıyla doğru şekilde kurulmasını sağlamanız gerekir. Varsayılan hesap ayarı *CGRSUser* olarak adlandırılır ve Commerce Gateway Server'a, *MSSQLSERVER* hizmeti ve *BizTalk Service BizTalk Group* dahil, gerek duyduğu en az miktarda diğer hizmetler için erişim sağlar*: BizTalkServerApplication*, *Yerel Sistem* hesabının içerdiği gibi genel hesap ayarları içermez.
- Her zaman güçlü parolalar kullanın. Güçlü parolalar hakkında daha fazla bilgi için Güçlü Parolalar bölümüne bakın.
- Windows Oturumu Açma olanaklarını kullanın. Navision iki tür oturum açma oluşturmanıza olanak tanır – Veritabanı Oturumu Açma ve Windows Oturumu Açma. Windows Kimlik Doğrulaması kullandığından ve uygun bir parola ilkesi uygulamanıza olanak tanıdığından, Windows Oturumu Açma olanaklarını kullanmanızı öneririz.
- Parolaların yeniden kullanılmaması gerekir. Parolaları sistemlerde ve etki alanlarında yeniden kullanma çoğu kez yapılan bir uygulamadır. Örneğin, iki etki alanından sorumlu bir yönetici her bir etki alanında aynı parolayı kullanan Domain Administrator (Etki Alanı Yöneticisi) hesapları oluşturabilir ve hatta etki alanı bilgisayarlarında, tüm etki alanında aynı olan yerel yönetici parolaları ayarlayabilir. Bu durumda, tek bir hesap veya bilgisayar tehlikeli bir durumla karşılaşırsa, tüm etki alanı aynı tehlikeli durumla karşılaşabilir.
- Navision kurulduktan ve veritabanları oluşturulduktan veya güncelleştirildikten sonra, bir Windows Oturumu Açma hesabı oluşturmanız ve bu hesaba Navision'da SUPER rolünü atamanız gerekir. Bu SUPER kullanıcı, veritabanı yönetimini, güvenliğini vb. üstlenir. Bu oturum açma hesabı için bir sağlam parola ayarlayın. Bu parola gizli tutulmalıdır. SQL Server'da SA parolasına verdiğiniz korumanın aynısını sağlamalıdır. Tüm veritabanı erişimi SUPER rolü tarafından yönetilir ve en yüksek düzeyde koruma gerektirir. SUPER kullanıcının parolası yalnızca Sistem Yöneticileriniz tarafından bilinmelidir.
- Navision veritabanına erişimi olan tüm diğer kullanıcılar en az ayrıcalıkla çalışmalıdır. Bu, Navison'da kullanıcılara, yalnızca şirketteki görevlerini yapmak için gerek duydukları özelliklere ve işlevlere erişme olanağı sağlayan roller atamak anlamına gelir.
- Yalnızca şirket içindeki rolleri FOB dosyalarını almalarını, nesneleri yeniden tasarlamalarını ve veritabanı yedeklemeleri oluşturmalarını gerektiren kullanıcıların bunları yapabilmelerini sağlayın.
- Navision veritabanınızı düzenli olarak yedekleyin ve başarılı şekilde geri yüklenebilmeleri için yedeklemeleri sınamayı unutmayın.
- Yangın, duman, toz, yüksek ısı, şimşek ve çevre felaketleri (örneğin, deprem) gibi tehlikelerin etkilerini sınırlamak için yedeklerinizi güvenli bir yerde saklayın.
- Navision Windows'un çeşitli sürümlerinde çalışabilse de, en güncel güvenlik özelliklerini içeren en yeni işletim sistemini kullanmanız önerilir. Şu anda bu özellikleri taşıyan işletim sistemleri Windows XP, Service Pack 2 ve Windows Server 2003'tür.
- En yeni güvenlik güncelleştirmelerini uygulamak için, Windows 2000, Windows XP ve Windows Server 2003 ile birlikte sağlanan Windows Update hizmetini kullanın. Tüm istemci bilgisayarlarınızı en yeni güvenlik düzeltme ekleri, hizmet paketleri ve güncelleştirmelerle güncel tutmak için Windows'un Otomatik Güncelleştirme özelliğini kullanın.
- Navision istemcileri ve Navision Database Server arasında iletişim kurmak için, TCPS güvenli protokolünü kullanmanız önerilir. TCPS, TCP/IP'nin güvenli bir sürümüdür ve şifreleme yeteneği ve Kerberos kimlik doğrulaması içeren Güvenlik Desteği Sağlayıcısı Arabirimi'ni (SSPI; Security Support Provider Interface) kullanır. TCPS, Navision Database Server için varsayılan protokoldür.

- Müşterinin, olağanüstü bir durumun ardından hizmetlerin hızlı bir şekilde yeniden başlatılmasını sağlayan bir olağanüstü durum kurtarma planı olması gerekir.
  Bir kurtarma planının aşağıdakileri içermesi gerekir:
  - Yeni/geçici donanımı edinme.
  - Yedeklemeleri yeni sistemlere geri yükleme.
  - Kurtarma planının gerçekten çalıştığını sınama.

Fiziksel Güvenlik

Yazılım güvenliğiyle yeri hiçbir şekilde doldurulamayacağından, fiziksel güvenlik kesinlikle zorunludur. Örneğin, bir sabit disk çalınırsa, sonuç olarak o sürücüdeki veriler de çalınmış olur. Müşterinizle birlikte bir ilke geliştirirken aşağıdaki fiziksel güvenlik konularını gözden geçirin:

- Bu görev için belirlenen BT bölümleri tarafından yapılan büyük yüklemeler için, hizmet odalarının ve yazılımların depolandığı yerlerin kilitli olmasını sağlayın.
- Bu kategoride yer alan makineler aşağıdakileri içerir:
  - Microsoft SQL Server 2000 sunucusu
  - Navision yürütülebilir dosyalarının bulunduğu Dosya Sunucusu.
- Yetkisiz kullanıcıları bilgisayarlardan uzak tutun.
- Verilerin ne kadar duyarlı olduğuna bakmaksızın, hırsız alarmları kurulmasını sağlayın.
- Kritik önem taşıyan verileri içeren yedeklerin başka bir yerde depolanmasını ve yedeklerin yangına karşı dayanıklı konteynerlerde depolanmasını sağlayın.

Çalışanlar

Tüm ürünler ve özellikler için yönetim haklarını sınırlamak iyi bir fikirdir. Varsayılan değer olarak, işlerini yapmak için daha fazla erişime gereksinim duymadıkça, müşteriler çalışanlarına sistem işlevleri için yalnızca okuma erişimi vermelidirler. Microsoft, en az ayrıcalık ilkesine uyulmasını önerir: Kullanıcılara, yalnızca verilere ve işlevselliğe erişmeleri için gereken en az ayrıcalığı verin.
Hoşnutsuz ve eski çalışanlar ağ güvenliği için bir tehlikedir. Müşterilerinizle güvenlik konusunda görüşürken, çalışanlarla ilgili olarak aşağıdaki ilkeyi önerin:

- Çalışanların işe alınmadan önceki durumlarıyla ilgili araştırmalar yapın.
- Hoşnutsuz ve eski çalışanlardan “intikam amaçlı davranışlar” bekleyin.
- Bir çalışan işten ayrıldığında, ilişkili tüm Windows hesaplarını ve parolalarını devre dışı bırakın. Raporlama amacıyla, kullanıcıları silmeyin. Hesapları yeniden kullanmayın.
- Kullanıcıları uyanık olmaları ve şüpheli etkinlikleri raporlamaları konusunda eğitin.
- Otomatik olarak ayrıcalık vermeyin. Kullanıcıların belirli bilgisayarlara, bilgisayar odalarına veya dosya kümelerine erişmeleri gerekmiyorsa, bu yerlere erişimlerinin olmamasını sağlayın.
- Gözetimcileri, olası çalışan sorunlarını belirlemeleri ve yanıtlamaları için eğitin.
- Çalışanların ağ güvenliğini sağlamadaki rollerini anlamalarını sağlayın.
- Şirket ilkelerinin bir kopyasını tüm çalışanlara verin.
- Kullanıcıların, işverenleri tarafından izin verilmeyen yazılımları yüklemelerine izin vermeyin.

Yönetici

Müşterinizin sistem yöneticilerinin, Microsoft tarafından sağlanan en yeni güvenlik düzeltmelerini izlemeleri önerilir. Saldırganlar, bir ağda büyük bir delik açmak için küçük hataları birleştirme konusunda çok beceriklidirler. Yöneticilerin, öncelikle her bilgisayarın mümkün olduğunca güvenli olmasını sağlamaları, sonra güvenlik güncelleştirmelerini eklemeleri ve virüslere karşı koruma yazılımları kullanmaları gerekir. Değerli bilgileri ve en iyi yöntemleri bulmanıza yardımcı olmak için, bu kılavuzda birçok bağlantı ve kaynak sağlanmıştır.

Karmaşıklık, ağınızın güvenliğini sağlarken seçimler yapmanızı gerektiren diğer bir alandır. Ağ ne kadar karmaşıksa, saldırgan bir kez erişim elde ettikten sonra güvenliği sağlamak veya sorunu düzeltmek o kadar güç olur. Yöneticinin, mümkün olduğunca basit tutmak amacıyla, ağ topografisini tam olarak belgelendirmesi gerekir.

Güvenlik, esas olarak risk yönetimiyle ilgilidir. Teknoloji her soruna çözüm sağlamadığından, güvenlik için teknoloji ve güvenlik ilkesinin birleştirilmesi gerekir. Diğer bir deyişle, paketinden çıkarıp ağınıza kurduğunuzda hemen mükemmel güvenlik sağlayabilecek bir ürün yoktur. Güvenlik, teknoloji ve güvenlik ilkesinden birlikte yararlanılarak elde edilen bir sonuçtur. Başka bir deyişle, bir ağın güvenlik düzeyini, teknolojiyi kullanma şekli belirler. Microsoft güvenlik konusunda bilinçli teknoloji ve özellikler sağlar; ancak, sizin yönlendirmeniz ile, her kuruluş için doğru ilkeleri yalnızca ağ yöneticisi belirleyebilir. Güvenlik planlamasını, uygulama ve yaygınlaştırma süreçlerinin başında yapmayı unutmayın. Müşterilerinizin neleri korumak istediklerini ve bunun için neleri yapmaya hazır olduklarını anlayın.

Son olarak, acil durumlar oluşmadan önce bu durumlarla ilgili olasılık planları geliştirin. Eksiksiz bir planı sağlam bir teknoloji ile birleştirirseniz, müşteriniz üst düzey güvenliğe kavuşmuş olur.

Genel olarak güvenlik hakkında daha fazla bilgi için, aşağıdaki adreste "The Ten Immutable Laws of Security Administration" (Güvenlik Yönetiminin On Değişmez Yasası) başlıklı makaleye bakın:
http://www.microsoft.com/technet/archive/community/columns/security/essays/10salaws.mspx

Ayrıca, aşağıdaki adresteki güvenlik yönetimiyle ilgili makaleleri okuyun: http://www.microsoft.com/technet/community/columns/secmgmt/smarch.mspx

Sunucu İşletim Sisteminin Güvenliğini Sağlama

Birçok küçük müşterinin bir sunucu işletim sistemi olmadığını görebilecek olsanız da, daha karmaşık ağ ortamlarına sahip büyük müşteriler için en iyi güvenlik yöntemlerini anlamanız ve kendilerine iletebilmeniz önemlidir. Ayrıca, bu belgede açıklanan ilkelerin ve yöntemlerin birçoğunun yalnızca istemci işletim sistemleri olan müşterilere kolayca uygulanabileceğini de bilmelisiniz.

Bu bilgiler esas olarak Windows Server 2003 Çevrimiçi Yardımı'ndan alınmış olsa da, bu bölümdeki kavramlar hem Microsoft Windows 2000 Server hem de Microsoft Windows Server 2003 ürünleri için geçerlidir. Windows Server 2003,

güçlü bir güvenlik özellikleri kümesi sunar. Windows Server 2003 Çevrimiçi Yardımı, tüm güvenlik özellikleri ve yordamlarıyla ilgili tam bilgi içerir.

Windows 2000 Server hakkında ek bilgi için, http://www.microsoft.com/technet/security/prodtech/win2000/default.mspx adresindeki Windows 2000 Server Güvenlik Merkezi'ni ziyaret edin ve aşağıdaki adresteki Windows 2000 Güvenliği Sağlamlaştırma Kılavuzu'nu okuyun: http://www.microsoft.com/technet/security/prodtech/win2000/win2khg/default.mspx

Windows Server 2003 ile ilgili ek bilgi için, http://www.microsoft.com/technet/security/prodtech/win2003/w2003hg/sgch00.mspx adresindeki *Windows Server 2003 Security Guide* (*Windows Server 2003 Güvenlik Kılavuzu) adlı kitaba bakın.*

Windows sunucu güvenliği modelinin temel özellikleri kimlik doğrulama, erişim denetimi ve çoklu oturum açmadır:

- Kimlik doğrulama, sistemin bir kullanıcının kimliğini oturum açma kimlik bilgilerini kullanarak doğrulamasıdır. Kullanıcının adı ve parolası bir yetki listesiyle karşılaştırılır. Sistem bir eşleşme saptarsa, yetkilendirme kullanıcıya o kullanıcıya ilişkin izin listesinde belirtilen ölçüde erişim sağlar.
- Erişim denetimi, kullanıcının kimliğine ve önceden tanımlanmış çeşitli gruplardaki üyeliklerine dayalı olarak, kullanıcının bilgilere ve bilgi işlem kaynaklarına erişimini denetler. Erişim denetimi genellikle sistem yöneticileri tarafından, kullanıcıların sunucular, dizinler ve dosyalar gibi ağ kaynaklarına erişimlerini denetlemek için kullanılır. Bu genellikle, kullanıcılara ve gruplara belirli nesneler için erişim sağlanarak gerçekleştirilir.
- Çoklu oturum açma, kullanıcıların tek bir parola kullanarak Windows etki alanında bir kez oturum açmalarına ve Windows etki alanındaki herhangi bir bilgisayar için kimlik doğrulamasından geçmelerine olanak tanır. Çoklu oturum açma, yöneticilerin tüm Windows ağında parola kimlik doğrulaması gerçekleştirmelerine ve son kullanıcılara erişim kolaylığı sağlamalarına olanak tanır.

Aşağıdaki bölümler, bu üç ana özelliğe ilişkin daha ayrıntılı açıklamaları içermektedir.

Kimlik Doğrulama

Kimlik doğrulama, sistem güvenliğinin temel bir özelliğidir ve etki alanında oturum açmaya veya ağ kaynaklarına erişmeye çalışan herhangi bir kullanıcının kimliğini doğrulamak için kullanılır. Çoğu kimlik doğrulama sistemindeki zayıf nokta kullanıcının parolasıdır.

Parolalar, etki alanına ve yerel bilgisayarlara yetkisiz erişime karşı ilk savunma hattını sağlar. Aşağıdaki en iyi parola yöntemlerini önerin:

- Her zaman sağlam parolalar kullanın.
- Parolaların kağıda yazılması gerekiyorsa, kağıdı güvenli bir yerde saklayın ve gerekmediğinde yok edin.
- Parolanızı kesinlikle birisine söylemeyin.
- Tüm kullanıcı hesapları için farklı parolalar kullanın.
- Parolaları düzenli aralıklarla değiştirin.
- Parolaların bilgisayarda depolandıkları yer konusunda dikkatli olun.

Sağlam Parolalar

Parolaların kuruluş ağının güvenliğini sağlamada oynadığı rol genellikle fazla önemsenmez ve gözardı edilir. Daha önce belirtildiği gibi, parolalar ağınıza yetkisiz erişime karşı ilk savunma hattıdır. Bu nedenle, müşterilerinizin çalışanlarından sağlam parolalar kullanmalarını istemlerini sağlamanız gerekir.

Bununla birlikte, parola kırma araçları gelişmeye devam etmekte ve parolaları kırmak için kullanılan bilgisayarlar giderek güçlenmektedir. Yeterli zaman tanınması durumunda, otomatik parola kırma aracı herhangi bir parolayı kırabilir. Yine de, sağlam parolaların kırılması, zayıf parolaların kırılmasına göre çok daha zordur.

Kullanıcının anımsayabileceği sağlam parolalar oluşturulmasına ilişkin kurallar için bkz:

http://www.microsoft.com/athome/security/privacy/password.mspx

ve

http://www.microsoft.com/ntworkstation/technicalresources/PWDguidelines.asp

Parola İlkesini Tanımlama

Müşterinize parola ilkelerini tanımlamada yardımcı olurken, tüm kullanıcı hesaplarının sağlam parolalara sahip olmasını gerektiren bir ilke oluşturmaya dikkat edin. Çoğu sistem için, Windows Server 2003 Güvenlik Kılavuzu'ndaki önerilere uymak yeterlidir:

- Önceki birçok parolanın anımsanması için, **Parola geçmişini uygulama** ilke ayarını tanımlayın. Bu ilke ayarıyla, kullanıcılar parolalarının süresi dolduğunda aynı parolayı kullanamazlar.

  Önerilen ayar: 24

- Müşterinin ortamına göre, parolaların geçerlilik süresinin gerektiği kadar sık sona ermesi için **En fazla parola geçerlilik süresi** ilke ayarını tanımlayın.

  Önerilen ayar: 42 (varsayılan) ve 90 arasında.

- Birkaç gün kullanılmadan değiştirilememeleri için, **En az parola geçerlilik süresi** ilke ayarını tanımlayın. Bu ilke ayarı, **Parola geçmişi uygula** ilke ayarıyla birlikte çalışır. En az parola geçerlilik süresi tanımlanırsa, kullanıcılar özgün parolalarını kullanmak amacıyla **Parola geçmişi uygula** ilke ayarını atlatmak için parolalarını sürekli olarak değiştiremezler. Kullanıcıların parolalarını değiştirmek için belirli sayıda günün geçmesini beklemeleri gerekir.

  Önerilen ayar: 2.

- Parolaların en azından belirtilen bir sayıda karakter içermesi için **En az parola uzunluğu** ilke ayarını tanımlayın. Yedi veya daha fazla karakter içeren uzun parolalar, genellikle kısa olanlardan daha sağlamdır. Bu ilke ayarıyla, kullanıcılar boş parola kullanamazlar ve en azından belirli bir sayıda karakter içeren parolalar oluşturmaları gerekir.

  Önerilen ayar: 8.

- **Parolalar karmaşıklık gereklerine uymalıdır** ilke ayarını etkinleştirin. Bu ilke ayarı tüm parolaları denetleyerek temel sağlam parola gereklerine uymalarını sağlar. Bu ayar,

parolaların dört kategoriden (büyük harf, küçük harf, sayılar, alfasayısal olmayan simgeler) en az üç simge içermelerini ve kullanıcı adının herhangi bir bölümünü veya kullanıcının adını veya soyadını içermemelerini sağlar.

Not
Bu gereksinimleri karşılayan parolalar çok sağlam demek değildir. Örneğin, “Parola1” bu gereksinimleri karşılar.

Önerilen ayar: Evet

- Bu gereksinimlerin listesi için, Windows Server Çevrimiçi Yardımı’nda “Parolalar karmaşıklık gereklerine uymalıdır” konusuna bakın.
- Tersine çevrilebilir şifreleme kullanan sağlam parolalar – Tersine çevrilebilir şifreleme, bir uygulamanın temiz metinli parolalara erişmesi gereken sistemlerde kullanılır. Çoğu dağıtımda gerekli değildir.

  Önerilen ayar: Hayır.

Daha fazla bilgi için Windows Server 2003 Güvenlik Kılavuzu’na bakın:

http://www.microsoft.com/technet/security/prodtech/Win2003/W2003HG/SGCH00.mspx

Hesap Kilitleme İlkesi Tanımlama

Hesap kilitleme ilkesi tanımlarken dikkatli olun. Yetkili kullanıcıların hesaplarının kilitlenmesi olasılığı çok yüksek olduğundan ve bu durum müşteriniz için çok maliyetli olabileceğinden, hesap kilitleme ilkesi küçük bir kuruluşta hiçbir zaman ayarlanmamalıdır.

Müşteri hesap kilitleme ilkesi uygulamaya karar verirse, parolalarını birçok kez yanlış yazmaları nedeniyle kullanıcılarının hesaplarının kilitlenmemesi için, **Hesap kilitleme eşik değeri** için yeterince yüksek bir sayı ayarlayın.

Hesap kilitleme ilkesi hakkında daha fazla bilgi için, Windows Server Çevrimiçi Yardımı’nda “Hesap Kilitleme İlkesine Genel Bakış” konusuna bakın.

Hesap kilitleme ilkesinin nasıl uygulanacağı veya değiştirileceği hakkında bilgi için, Windows Server Çevrimiçi Yardımı’nda “Hesap kilitleme ilkesini uygulamak veya değiştirmek için” konusuna bakın.

Erişim Denetimi

Bir Windows ağının ve kaynaklarının (Navision dahil) güvenliği, kullanıcıların, kullanıcı gruplarının ve diğer bilgisayarların ağda hangi haklara sahip oldukları göz önünde bulundurularak sağlanabilir. Kullanıcı veya gruplara belirli kullanıcı hakları vererek bir veya birden çok bilgisayarın güvenliğini sağlayabilirsiniz. Kullanıcıların veya grupların bir nesne üzerinde belirli eylemleri yapmalarına olanak tanıyan izinler atayarak, bir dosya veya klasör gibi nesnenin güvenliğini sağlayabilirsiniz. Erişim denetimini oluşturan temel kavramlar aşağıdakileri içerir:

- İzinler
- Nesnelerin sahipliği
- İzinleri devralma

- Kullanıcı hakları
- Nesne denetimi

İzinler

İzinler, dosyalar, klasörler ve kayıt nesneleri gibi bir nesne veya nesne özelliği için bir kullanıcıya veya gruba sağlanan erişim türünü tanımlar. İzinler, dosyalar veya kayıt nesneleri gibi güvenli nesnelere uygulanır. İzinler herhangi bir kullanıcıya, gruba veya bilgisayara verilebilir. Gruplara izin atamak iyi bir yöntemdir.

Nesnelerin Sahipliği

Bir nesne oluşturulduğunda, o nesneye bir sahip atanır. Windows 2000 Server'da varsayılan değer olarak, sahip nesnenin oluşturucusudur. Bu durum, Administrators grubunun üyeleri tarafından oluşturulan nesneler için Windows Server 2003'te değişmiştir.

Administrators grubunun bir üyesi Windows Server 2003'te bir nesne oluşturduğunda, nesneyi oluşturan bireysel hesap değil, Administrators grubu nesnenin sahibi olur. Bu davranış, Yerel Güvenlik Ayarları Microsoft Yönetim Konsolu (MMC) eklentisinde, **Sistem nesneleri:** Administrators grubunun üyeleri tarafından oluşturulan nesnelerin varsayılan sahibi ayarı kullanılarak değiştirilebilir. Nesne için hangi izinlerin düzenlendiğine bakılmaksızın, nesnenin sahibi nesne izinlerini istediği zaman değiştirebilir.

Daha fazla bilgi için Windows Server Çevrimiçi Yardımı'nda "Sahiplik" konusuna bakın.

İzinleri Devralma

Devralma, izinlerin yöneticiler tarafından kolaylıkla atanıp yönetilmesine izin verir. Bu özellik, kapsayıcı içindeki nesnelerin, bu kapsayıcının devralınabilir tüm izinleri otomatik olarak devralmasına neden olur. Örneğin, bir klasör içinde dosyalar oluşturduğunuzda, dosyalar o klasörün izinlerini devralırlar. Yalnızca devralınmak üzere işaretlenen izinler devralınır.

Kullanıcı Hakları

Kullanıcı hakları, bilgisayar ortamınızdaki kullanıcı ve gruplara belirli ayrıcalıklar ve oturum açma hakları verir.

Kullanıcı hakları hakkında bilgi için Windows Server Çevrimiçi Yardımı'nda "Kullanıcı Hakları" konusuna bakın.

Nesne Denetimi

Kullanıcıların nesnelere erişimini denetleyebilirsiniz. Olay Görüntüleyicisi'ni kullanarak, güvenlikle ilgili olayları güvenlik kütüğünde görüntüleyebilirsiniz.

Daha fazla bilgi için Windows Server Çevrimiçi Yardımı'nda "Denetim" konusuna bakın.

Erişim Denetimi En iyi Yöntemleri

- İzinleri kullanıcılar yerine gruplara atayın. Kullanıcı hesaplarını doğrudan saklamak verimli olmadığından, kullanıcı temelinde izin atamak özel durum olarak ele alınmalıdır.
- Belirli özel durumlar için İzin Verme ayarını kullanın. Örneğin, İzin Ver uygulanmış bir grubun bir alt kümesini dışlamak için İzin Verme seçeneğini kullanabilirsiniz.
- Nesne için Herkes grubuna her zaman erişim izni verin Bir nesneye Herkes erişimini reddederseniz, bu yöneticileri de içerir. Diğer kullanıcı, grup veya bilgisayarlara bu nesne üzerinde izinler verdiğiniz sürece, en iyi çözüm Herkes grubunu kaldırmak olabilir. Hiç izin tanımlanmaması durumunda hiçbir erişime izin verilmeyeceğini unutmayın.
- Ağaçta olabildiğince yüksekte yer alan nesneye izinler atayın ve güvenlik ayarlarını ağaçta yaymak için devralmayı uygulayın. Erişim denetimi ayarlarını, bir üst nesnenin tüm alt nesnelerine veya alt ağacına hızla ve etkili şekilde uygulayabilirsiniz. Böyle yaparak, en az çabayla en büyük etki derecesini elde edersiniz. Oluşturduğunuz izin ayarları, kullanıcı, grup ve bilgisayarların çoğunluğu için yeterli olmalıdır.
- Özel izinler bazen devralınan izinlerin geçersizleştirebilir. Devralınmış İzin Verme ayarları, nesnenin açık bir İzin Ver ayarı varsa, bu nesneye erişimi engellemez. Özel izinler, devralınan izinlere, hatta devralınan İzin Verme ayarına göre önceliklidir.
- Active Directory® nesneleriyle ilgili izinler için, Active Directory nesnelerine özgü en iyi yöntemleri kavradığınızdan emin olun.

Daha fazla bilgi için Windows Server 2003 Çevrimiçi Yardımı'nda "Active Directory nesnelerine izin atamak için en iyi yöntemler" konusuna bakın.

Dış Güvenlik Duvarı

Güvenlik duvarı, belirli bir ağa veri paketlerinin girmesini veya veri paketlerinin ağdan çıkmasını engelleyen bir yazılım veya donanım parçasıdır. Trafik akışını denetlemek için, güvenlik duvarındaki bağlantı noktaları bilgi paketlerine açılır veya kapatılır. Güvenlik duvarı, her bir veri paketindeki çeşitli bilgi parçalarına bakar: paketin teslim edilmesinde kullanılan protokol, paketin hedefi veya göndericisi, pakette yer alan içerik türü ve gönderilmekte olduğu bağlantı noktası. Güvenlik duvarı belirtilen protokolü hedeflenen bağlantı noktası üzerinden kabul edecek şekilde yapılandırılırsa, paketin geçmesine izin verilir. Microsoft Windows Small Business Server 2003 Premium Edition, güvenlik duvarı çözümü olarak Microsoft Internet Security and Acceleration (ISA) Server 2000 ile birlikte teslim edilir. Small Business Server Standard Edition da bir güvenlik duvarı içerir.

ISA Server 2004

Internet Security and Acceleration (ISA) Server 2000, Internet ve iç ağ üzerindeki istemci bilgisayarlar arasındaki talepleri ve yanıtları güvenli şekilde yönlendirir.

ISA Server, yerel ağ üzerindeki istemciler için Internet'e güvenli ağ geçidi olarak hareket eder. ISA Server bilgisayarı, iletişim yolundaki diğer taraflar için

saydamdır. Kullanıcı ISA Server bilgisayarının erişimi reddettiği bir hizmete erişmeyi veya bir siteye gitmeyi denemedikçe, Internet kullanıcısının bir güvenlik duvarı sunucusunun var olduğunu söyleyememesi gerekir. Erişilmekte olan Internet sunucusu, ISA Server bilgisayarından gelen talepleri talepler istemci uygulamadan kaynaklanmış gibi yorumlar.

Internet Protokolü (IP) parça filtrelemeyi seçtiğinizde, Web Proxy ve Güvenlik Duvarı hizmetlerinin paket parçalarını filtrelemelerini etkinleştirmiş olursunuz. Paket parçaları filtrelenerek, parçalanan tüm IP paketleri düşürülür. İyi bilinen bir "saldırı", parçalanmış paketler göndermeyi ve sonra bu parçaları sisteme zarar verecek şekilde yeniden birleştirmeyi içerir.

ISA Server'da, ağa bir saldırıda bulunulan zamanı saptayan ve saldırı yapılması durumunda yapılandırılmış bir eylem (veya uyarı) kümesini uygulayan bir yetkisiz erişim algılama düzeneği bulunur.

ISA Server bilgisayarında Internet Information Services (IIS) yüklüyse, ISA Server'ın giden Web talepleri ve gelen Web talepleri için kullandığı bağlantı noktalarını (varsayılan değer olarak 8080 ve 80) kullanmayacak şekilde yapılandırmanız gerekir. Örneğin, IIS'yi bağlantı noktası 81'i izleyecek şekilde değiştirebilirsiniz ve sonra ISA Server bilgisayarını gelen Web taleplerini IIS'nin çalıştığı yerel bilgisayardaki bağlantı noktası 81'e yönlendirecek şekilde yapılandırabilirsiniz.

ISA Server ve IIS'nin kullandığı bağlantı noktaları arasında bir çakışma varsa, kurulum programı IIS yayımlama hizmetini durdurur. Böylece, IIS'yi farklı bir bağlantı noktasını izleyecek şekilde değiştirebilir ve IIS yayımlama hizmetini yeniden başlatabilirsiniz.

ISA Server İlkeleri

Gelen ve giden erişimi belirleyen bir ISA Server ilkesi tanımlayabilirsiniz. Site ve içerik kuralları, hangi sitelere ve içeriğe erişilebileceğini belirtir. Protokol kuralları, gelen ve giden iletişim için belirli bir protokolün erişilebilir olup olmadığını gösterir.

Site ve içerik kuralları, protokol kuralları, Web yayımlama kuralları ve IP paket filtreleri oluşturabilirsiniz. Bu ilkeler, ISA Server istemcilerinin Internet ile nasıl iletişim kuracaklarını ve hangi iletişime izin verileceğini belirler.

Virüslere Karşı Koruma

Bilgisayar virüsü, kendisini kopyalamak, veri dosyalarını veya programları silmek veya bozmak ve algılanmaktan kaçınmak üzere tasarlanmış çalıştırılabilir bir dosyadır. Gerçekte, virüsler algılanmamaları için çoğu kez yeniden yazılır ve ayarlanır. Virüsler çoğu kez e-posta ekleri olarak gönderilir. Yeni ve değiştirilmiş virüsleri aramaları için virüslere karşı koruma programlarının sürekli olarak güncelleştirilmeleri gerekir. Virüsler, bilgisayarlara zarar vermek için en çok kullanılan yöntemdir.

Virüslere karşı koruma yazılımları, virüs programlarının algılanması ve engellenmesi için özel olarak tasarlanır. Her zaman yeni virüs programları

oluşturulduğundan, virüslere karşı koruma ürünleri üretenlerin çoğu yazılımlarını müşterileri için güncelleştirirler. Microsoft, müşterinizin ortamında virüslere karşı koruma yazılımı kullanmanızı kesinlikle önerir.

Virüs yazılımları genellikle şu üç konuma yüklenir: kullanıcı iş istasyonları, sunucular ve e-postaların kuruluşa geldiği (ve bazı durumlarda kuruluştan gittiği) ağ.

Virüs Türleri

Bilgisayar sistemlerini etkileyen üç temel virüs türü vardır: önyükleme kesimi virüsleri, dosyalara bulaşan virüsler ve Truva atı programları.

Önyükleme Kesimi Virüsleri

Bir bilgisayar başladığında, işletim sistemini veya diğer başlatma dosyalarını yüklemeden önce sabit diskin önyükleme kesimini tarar. Bir önyükleme kesimi virüsü, sabit diskin önyükleme kesimlerindeki bilgilerin yerine kendi kodunu yerleştirecek şekilde tasarlanmıştır. Bir bilgisayara bir önyükleme kesimi virüsü bulaştığında, her şeyden önce virüsün kodu belleğe okunur. Virüs belleğe yerleştikten sonra, bulaştığı bilgisayarda kullanılmakta olan tüm diğer disklere kendisini kopyalayabilir.

Dosyalara Bulaşan Virüsler

En yaygın virüs türü olan, dosyalara bulaşan virüs, kendi kodunu çalıştırılabilir dosyaya ekleyerek kendisini çalıştırılabilir bir programa iliştirir. Virüs kodu genellikle algılanmayacak şekilde eklenir. Virüs bulaşan dosya çalıştırıldığında, virüs kendisini diğer çalıştırılabilir dosyalara iliştirebilir. Bu tür bir virüsün bulaştığı dosyalar genellikle .com, .exe veya .sys dosya adı uzantılıdır.

Dosyalara bulaşan bazı virüsler özel programlar için tasarlanmıştır. Çoğu kez hedef alınan program türleri, yer paylaşımı (.ovl) dosyaları ve dinamik bağlantı kitaplığı (.dll) dosyalarıdır. Bu dosyalar çalıştırılmasa da, çalıştırılabilir dosyalar onları çağırır. Çağrı yapıldığında, virüs iletilir.

Virüs tetiklendiğinde, veriler zarar görür. Bir virüs, virüsün bulaştığı bir dosya çalıştırıldığında veya belirli bir ortam ayarı (örneğin, belirli bir sistem tarihi) gerçekleştiğinde tetiklenebilir.

Truva Atı Programları

Bir Truva atı programı gerçekte bir virüs değildir. Virüsle ve Truva atı programı arasındaki temel fark, Truva atı programının kendisini çoğaltmamasıdır; Truva atı programı yalnızca sabit diskteki bilgilere zarar verir. Bir Truva atı programı, normal bir oyun veya yardımcı program görünümüne bürünür. Çalıştırıldığında, verileri yok edebilir veya karıştırabilir.

Virüslere Karşı Korunma için En iyi Yöntemler

Bir makro virüsün yayılması engellenebilir. Müşterilerinizle paylaşmanız gereken, virüs bulaşmasını önleyecek bazı öneriler:

- Internet'ten gelen iletilerde, ileti yönlendiriciden geçmeden önce virüs taraması yapan bir virüse karşı koruma çözümü yükleyin. Bu, e-postalarda bilinen virüsler için tarama yapılmasını sağlar.
- Alınan belgelerin kaynaklarını bilin. Müşteri, güvenilirliğinden emin olmadığı kişilerden gelen belgeleri açmamamalıdır.
- Belgeyi oluşturan kişiyle konuşun. Kullanıcılar belgenin güvenli olduğundan emin olamıyorlarsa, belgeyi oluşturan kişiyle görüşmelidirler.
- Microsoft Office makro virüs korumasını kullanın. Office'teki uygulamalar, bir belge makro içerdiğinde kullanıcıyı uyarırlar. Bu özellik, belge açılırken kullanıcının makroları etkinleştirmesine veya devreden çıkarmasına olanak verir.
- Makro virüsleri algılamak ve silmek için virüs tarama yazılımı kullanın. Virüs tarama yazılımı makro virüslerini algılayabilir ve çoğu kez belgelerden silebilir. Microsoft, Uluslararası Bilgisayar Güvenliği Birliği (ICSA) onaylı virüslerden korunma yazılımı kullanılmasını önerir.

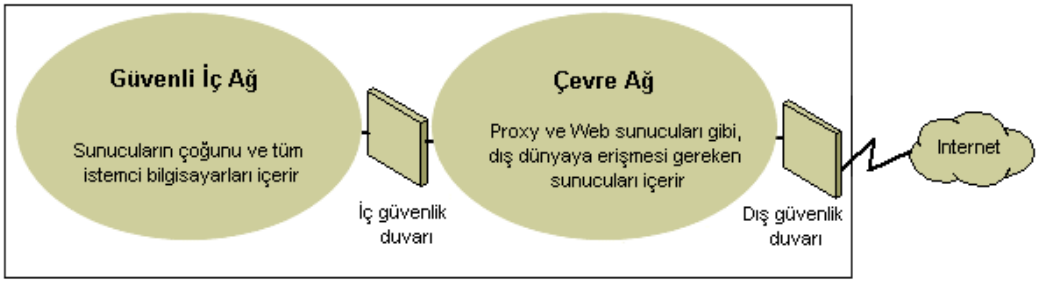
Virüsler ve bilgisayar güvenliği hakkında ayrıntılı bilgi için şu Microsoft Güvenlik web sitelerini ziyaret edin:

- http://www.microsoft.com/security/default.asp adresindeki Microsoft Güvenlik
- Microsoft TechNet http://www.microsoft.com/technet/security/Default.mspx adresindeki güvenlik belgeleri.

Ağ Güvenliği Stratejileri

Bir IP ağlar arası ortamın tasarımı ve dağıtılması özel ve genel ağlarla ilgili kaygıların dengelenmesini gerektirdiğinden, güvenlik duvarı ağ bütünlüğünü korumada temel bir unsur haline gelmiştir. Bir güvenlik duvarı tek bir bileşen değildir. Ulusal Bilgisayar Güvenliği Birliği (NCSA) güvenlik duvarını "iki veya daha fazla sayıda ağ arasında bir sınır oluşturan bir sistem veya sistemler bileşimi" olarak tanımlar. Farklı terimler kullanılsa da, bu sınır çoğu kez çevre ağ olarak bilinir. Çevre ağ, Internet veya diğer büyük ağlardan erişimi denetleyerek, intranet'inizi veya kurumsal yerel ağınızı (LAN) yetkisiz erişimlere karşı korur.

Aşağıdaki diyagramda, özel ağın güvenliğini sağlamak için güvenlik duvarlarıyla çevrilmiş ve bir özel ağ ile Internet arasında yerleştirilmiş bir çevre ağ gösterilmiştir:



Temel Çevre Ağ

Kuruluşlar, güvenliği sağlamak üzere güvenlik duvarı kullanımına farklı yaklaşımlar gösterirler. IP paket filtreleme zayıf güvenlik sunar, yönetilmeye elverişli değildir ve kolayca devre dışı bırakılabilir. Uygulama ağ geçitleri, yalnızca belirli bir e-posta sistemi gibi birkaç belirli uygulamayla ilgili olduklarından, paket filtrelerinden daha güvenlidir ve yönetilmeleri daha kolaydır. Bir ağ uygulaması kullanıcısı o uygulama tarafından geçirilen verilerden daha önemli olduğunda, devre ağ geçitleri özellikle daha etkilidir. Proxy sunucusu, bir uygulama ağ geçidi, adsız kullanıcılar için güvenli erişim ve diğer hizmetleri içeren kapsamlı bir güvenlik aracıdır. Aşağıda, bu farklı seçeneklerle ilgili bazı bilgiler verilmiştir:

- **IP Paket Filtrelemesi**
  IP paket filtrelemesi, ilk gerçekleştirilen güvenlik duvarı teknolojisi uygulamasıdır. Paket üstbilgisi kaynak ve hedef adresleri, İletim Denetim Protokolü (TCP) ve Kullanıcı Datagram Protokolü (UDP) bağlantı noktası numaraları ve diğer bilgiler için incelenir. Paket filtreleme, örneğin çevre ağın dışındaki hiçbir şeye güvenilmeyen ve çevre ağın içindeki her şeye güvenilen temiz güvenlik ortamlarında en iyi şekilde çalışan, sınırlı bir teknolojidir. Son yıllarda, çeşitli satıcılar paket filtreleme çekirdeğine akıllı karar verme özellikleri ekleyerek paket filtreleme yöntemini geliştirdiler ve böylece *durum bilgili protokol incelemesi* olarak adlandırılan yeni bir paket filtreleme formu oluşturdular. Paket filtrelemeyi, özel türdeki paketleri kabul edip tüm diğer paketleri reddedecek şekilde veya özel türdeki paketleri reddedip tüm diğer paketleri kabul edecek şekilde yapılandırabilirsiniz.
- **Uygulama Ağ Geçitleri**
  Bir uygulamanın asıl içeriği en önemli olduğunda, uygulama ağ geçitleri kullanılır. Teknolojideki değişikliklere kolayca uyum sağlayamadıklarından, uygulamaya özgü olmaları hem güçlü yanları, hem de sınırlılıklarıdır.
- **Devre Ağ Geçitleri**
  Devre ağ geçitleri, bir güvenlik duvarı içinden geçecek şekilde oluşturulan ve bir taraftaki belirli süreçleri veya sistemleri diğer taraftaki belirli süreçlere veya sistemlere bağlayan tünellerdir. Devre ağ geçitleri, bir uygulamayı kullanan kişinin o uygulama tarafından taşınan bilgilerden potansiyel olarak daha büyük bir risk oluşturduğu durumlarda en iyi şekilde kullanılır. Devre ağ geçidinin paket filtresinden farkı, başka bilgiler ekleyebilecek bant dışı bir uygulama şemasına bağlanma yeteneğidir.
- **Proxy Sunucuları**
  Proxy sunucuları, LAN'a giden ve LAN'dan gelen Internet trafiğini yöneten güvenlik duvarı ve uygulama ağ geçidi işlevselliğini içeren kapsamlı güvenlik araçlarıdır. Proxy sunucuları ayrıca belgeleri ön belleğe yazma ve erişim denetimi olanağı sağlar. Bir proxy sunucusu, popüler bir Web sayfası gibi sık talep edilen verileri önbelleğe yazarak ve doğrudan sağlayarak performansı yükseltebilir. Bir proxy sunucusu ayrıca, özel dosyalara yetkisiz erişim talepleri gibi sahibin uygun görmediği talepleri filtreleyebilir ve atabilir.

Müşterinin, kendisine yardımcı olabilecek bu güvenlik duvarı özelliklerinden yararlandığından emin olun. Bir çevre ağını ağ topolojisinde kurumsal ağın dışından gelen tüm trafiğin dış güvenlik duvarı tarafından korunan çevre ağından geçeceği bir noktada konumlandırın. Müşterinin gereksinimlerini karşılamak için güvenlik duvarına ilişkin erişim denetimine ince ayar yapabilir ve güvenlik duvarlarını tüm yetkisiz erişim girişimlerini raporlayacak şekilde yapılandırabilirsiniz.

İç güvenlik duvarı üzerinde açmanız gereken bağlantı noktası sayısını en aza indirmek için, ISA Server 2000 gibi bir uygulama katmanı güvenlik duvarı kullanabilirsiniz.

TCP/IP hakkında daha fazla bilgi için http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deployguide/en-us/dnsbb_tcp_overview.asp adresinde “Designing a TCP/IP Network” (TCP/IP Ağı Tasarlama) konusuna bakın.

Kablosuz Ağlar

Varsayılan olarak, kablosuz ağlar genellikle kablosuz sinyallerin gizlice dinlenmesine izin verilecek şekilde yapılandırılır. Bazı kablosuz donanım üzerindeki varsayılan ayarlar, kablosuz ağın sunduğu erişilebilirlik ve var olan şifreleme yöntemleri nedeniyle erişim elde eden kötü niyetli bir yabancıya açık olabilirler. Gizlice dinlemeye karşı koruma sağlayan yapılandırma seçenekleri ve aralar vardır ancak bunların Internet bağlantısı üzerinden giren saldırganlara ve virüslere karşı bilgisayarları korumak için hiçbir şey yapmadıklarını unutmayın. Bu nedenle, bilgisayarları Internet üzerinden gelecek istenmeyen saldırganlara karşı korumak için bir güvenlik kullanmak çok önemlidir.

Kablosuz bir ağı koruma hakkında daha fazla bilgi için http://support.microsoft.com/default.aspx?scid=kb;en-us;309369 adresinde “How to Make Your 802.11b Wireless Home Network More Secure” (802.11b Kablosuz Ev Ağını Nasıl Daha Güvenli Hale Getirebilirsiniz) konusuna bakın.

Ağ Güvenliği Senaryoları

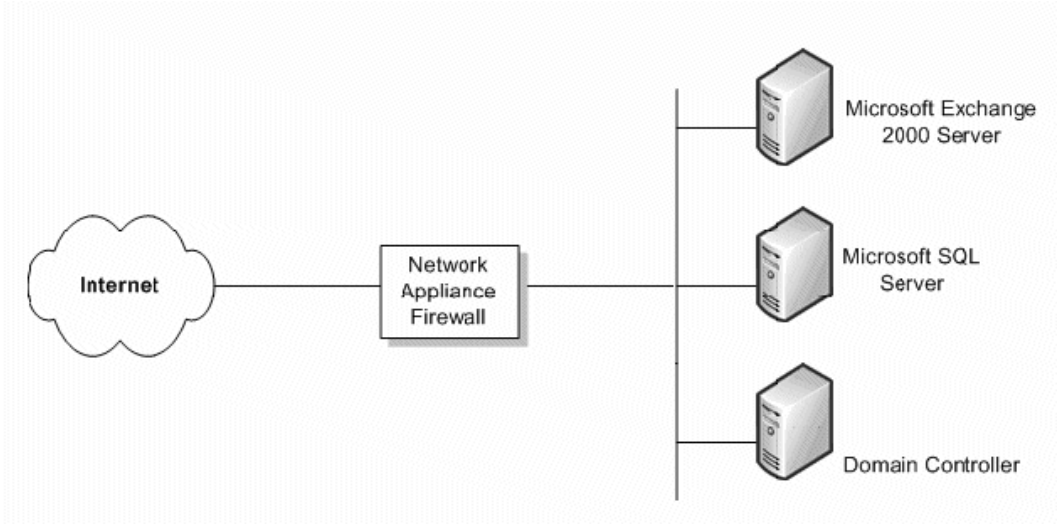
Müşterinin kuruluşunun gerektireceği ağ güvenliği düzeyi çeşitli etmenlere bağlıdır. Genellikle, bütçe ile kurumsal verilerin güvenceye alınması arasında bir denge sağlamayı gerektirir. Küçük bir kuruluşun olası en yüksek düzeyde ağ güvenliği sağlayan çok karmaşık bir güvenlik yapısı olabilir, ancak küçük bir kuruluş böyle bir güvenlik düzeyinin maliyetini karşılayamayabilir. Bu bölümde, dört senaryo inceleyeceğiz ve farklı güvenlik düzeyleri sağlayan bu senaryolarla ilgili önerilerde bulunacağız.

Güvenlik Duvarı Olmadığında

Müşterinizin Internet bağlantısı olduğu halde güvenlik duvarı yoksa, ağ güvenliği için bazı önlemlerin alınması gerekir. Olası saldırganların çoğunu vazgeçirmek için yeterli güvenlik sağlayan basit ağ güvenlik duvarı uygulamaları vardır.

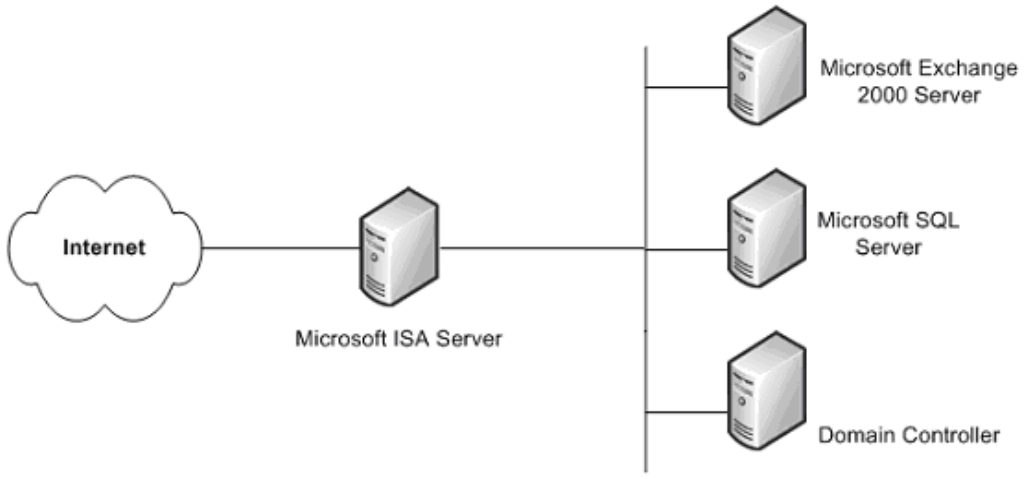
Tek Bir Basit Güvenlik Duvarı

Önerilen en düşük güvenlik düzeyi, Internet ile müşterinizin verileri arasında tek bir güvenlik duvarı bulunmasıdır. Bu güvenlik duvarı gelişmiş bir güvenlik düzeyi sağlamaz ve çok güvenli olduğu düşünülmemelidir. Ancak, hiç yoktan iyidir.



Basit Güvenlik Duvarı

Müşterinin bütçesinin, kurumsal verilerini koruyacak daha güvenli bir çözüme olanak tanıması ümit edilir. ISA Server bu tür bir çözüm olabilir. Bu ek sunucunun artırılmış maliyeti, genellikle yalnızca ağ adresi çevirisi (NAT: Network Address Translation) ve paket filtreleme sağlayan ortalama tüketici güvenlik duvarlarından çok daha fazla güvenlik sağlar.



ISA Server Güvenlik Duvarı

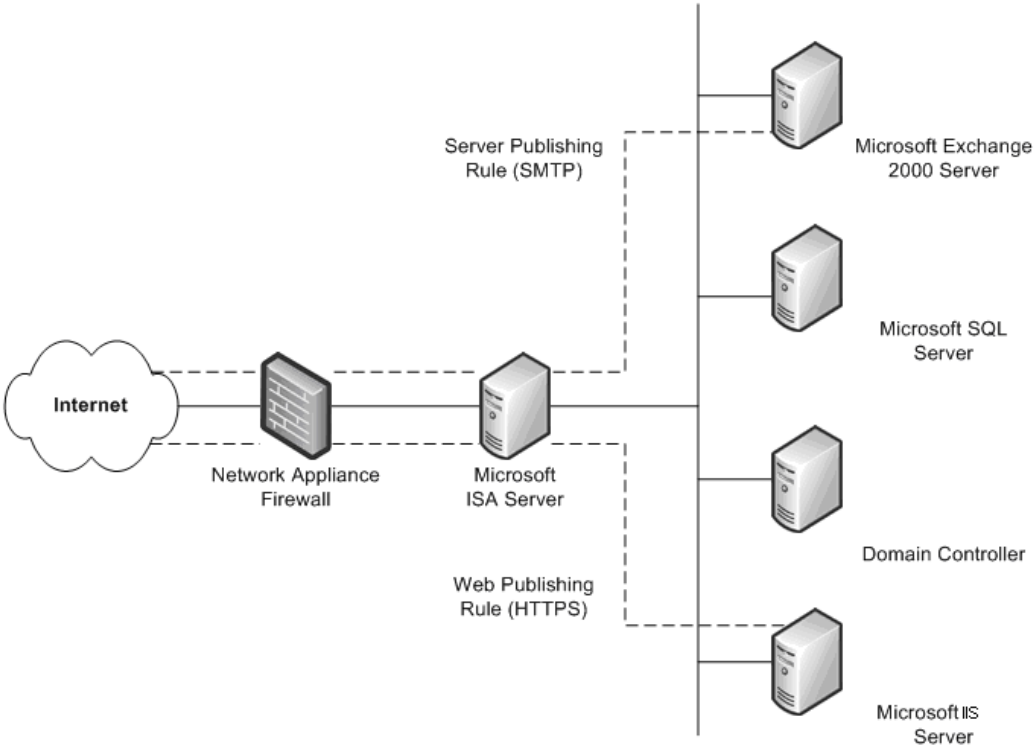
Tek güvenlik duvarı içeren bu çözüm, herhangi bir giriş düzeyi güvenlik duvarı uygulamasından daha güvenlidir ve Windows'a özgü güvenlik hizmetleri sağlar.

Var Olan Tek Bir Güvenlik Duvarı

Müşterinin intranet'lerini Internet'ten ayıran bir güvenlik duvarı varsa, iç kaynakları Internet için yapılandırmak üzere çeşitli yollar sağlayan ek bir güvenlik duvarı kullanmak isteyebilirsiniz.

Web yayımcılığı, bu tür bir yöntem olarak düşünülebilir. Bu, bir ISA Server'ın bir kuruluşun Internet kullanıcılarına erişim sağlayan Web sunucusu önüne yerleştirilmesi durumudur. Web talepleri geldiğinde, ISA Server Web içeriğine ilişkin istemci taleplerini kendi önbelleğinden karşılayarak, dış dünyaya bir Web sunucusu rolü oynayabilir. ISA Server, yalnızca talepler kendi önbelleğinden karşılanabilir olmadığında talepleri Web sunucusuna iletir.

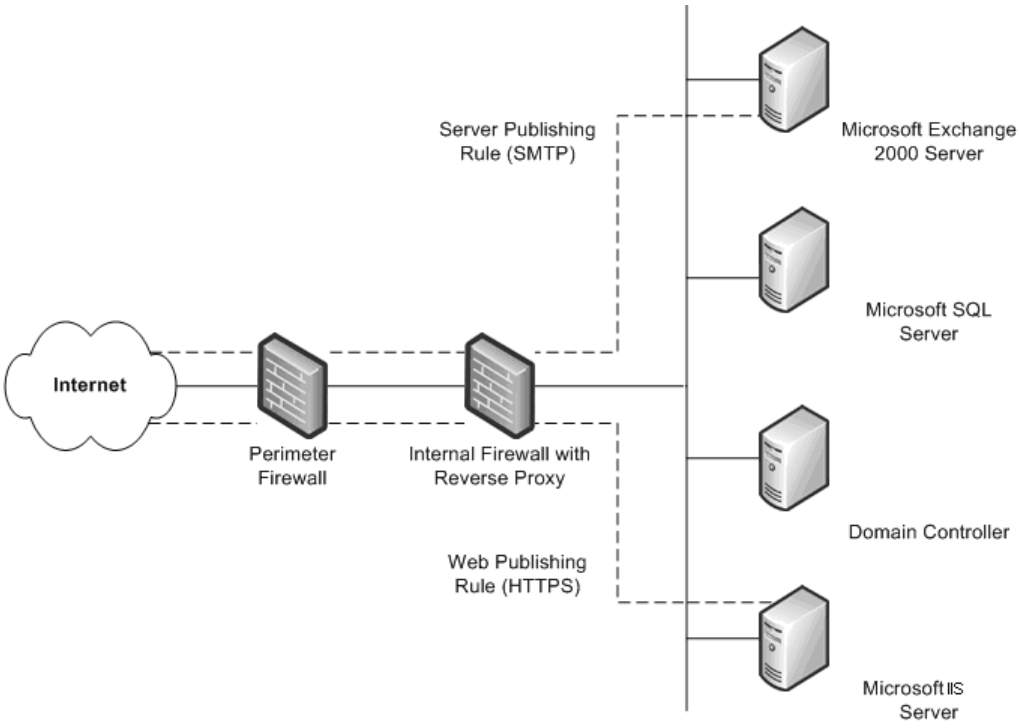
Diğer bir yöntem, sunucu yayımlamasıdır. ISA Server, iç ağın güvenliğini tehlikeye atmadan iç sunucuların Internet'e yayımlamalarına izin verir. Hangi taleplerin yerel ağdaki bir sunucuya gönderileceğini belirlemek için Web yayımlama ve sunucu yayımlama kurallarını yapılandırabilir ve böylece iç sunucular için daha yüksek düzeyde güvenlik sağlayabilirsiniz.



ISA Server Eklenmiş Olarak Var Olan Güvenlik Duvarı

Var Olan İki Güvenlik Duvarı

Dördüncü senaryoda, kuruluşun kurulu bir çevre ağ (DMZ) ile birlikte iki güvenlik duvarı vardır. Internet istemcilerinin intranet'teki sunuculara doğrudan erişmelerini önlemek için, bu sunuculardan biri veya birkaçı tersine proxy hizmetleri sağlamaktadırlar. Internet istemcilerinin intranet'teki sunuculara doğrudan erişmeleri yerine, güvenlik duvarlarından biri, ideal olarak iç güvenlik duvarı, iç sunucular için ağ taleplerini durdurmakta, o paketleri incelemekte ve sonra onları Internet ana sistemi adına iletmektedir.



Var Olan İki Güvenlik Duvarı

Bu senaryo, ikinci güvenlik duvarı eklendikten sonra önceki senaryoya benzer. Tek fark, tersine proxy'yi destekleyen iç güvenlik duvarının bir ISA Server olmamasıdır. Bu senaryoda, güvenlik ilkesine uygun sunucu yayımlama kuralları tanımlamak için her bir güvenlik duvarının yöneticileriyle yakın bir şekilde birlikte çalışmanız gerekir.

Güvenlik Düzeltme Eki Yönetimi

İşletim sistemleri ve uygulamalar çoğu kez son derece karmaşıktır. Farklı programcılar tarafından yazılan milyonlarca kod satırından oluşabilirler. Yazılımın güvenilir şekilde çalışması ve BT ortamının güvenliğini veya tutarlılığını tehlikeye atmaması şarttır. Olası sorunları en aza indirmek için, programlar yayınlanmadan önce ayrıntılı olarak sınanır. Bununla birlikte, saldırganlar sürekli olarak yazılımların zayıf yanlarını bulmaya çalıştıklarından, gelecekteki tüm saldırıları önceden kestirmek mümkün değildir.

Birçok kuruluş için, düzeltme eki yönetimi, genel değişiklik ve yapılandırma yönetimi stratejilerinin bir parçasını oluşturur. Bununla birlikte, kuruluşun yapısı ve boyutu ne olursa olsun, henüz kuruluşta etkili bir değişiklik ve yapılandırma yönetimi uygulamaya konulmamış olsa da, iyi bir düzeltme eki yönetimi stratejisine sahip olmak büyük önem taşır. Bilgisayar sistemlerine karşı düzenlenen başarılı saldırıların büyük çoğunluğu, güvenlik düzeltme eklerinin yüklenmediği sistemlere yapılır.

Güvenlik düzeltme ekleri, çoğu kuruluş için özel bir durum oluşturur. Yazılımda zayıf bir nokta ortaya çıktığında, saldırganlar genellikle bu durumla ilgili bilgiyi saldırgan topluluğuna hızlı bir şekilde yayarlar. Yazılımlarında zayıf bir nokta ortaya çıktığında, Microsoft en kısa zamanda bir güvenlik düzeltme eki

yayınlamaya çalışır. Düzeltme eki dağıtılıncaya kadar, müşterinin gereksindiği ve beklediği güvenlik ciddi ölçüde azalabilir.

Navision ortamında, müşterilerinizin en yeni güvenlik düzeltme eklerini sistemlerine yüklemiş olmalarını sağlamanız gerekir. Müşterinin, Microsoft tarafından kullanıma sunulan teknolojilerden birini kullanmasını sağlayın. Bu teknolojiler şunları içerir:

- **Microsoft Güvenlik Bildirimi Hizmeti**
  Güvenlik Bildirimi Hizmeti, bir güncelleştirme kullanıma sunulduğunda uyarılar dağıtan bir e-posta listesidir. Bu uyarılar, öngörülmüş güvenlik stratejisinin değerli bir parçası olarak işlev görür. Ayrıca, TechNet Ürün Güvenliği Bildirimi web sitesinden de erişilebilirler: http://www.microsoft.com/technet/security/bulletin/notify.mspx
- **Microsoft Otomatik Güncelleştirmeler**
  Windows, güvenlik güncelleştirmelerini otomatik olarak makinelerinize uygulayabilir.
- **Microsoft Güvenlik Bülteni Arama Aracı**
  Güvenlik Bülteni arama aracı, Güvenlik Bülteni Hizmeti web sitesinde kullanılabilir: http://www.microsoft.com/technet/security/current.aspx Müşteri, çalıştırmakta oldukları işletim sistemine, uygulamalara ve servis paketlerine dayalı olarak hangi güncelleştirmelere gerek duyduklarını belirleyebilir.
- **Microsoft Baseline Security Analyzer (MBSA)**
  Bu grafik aracı Microsoft Baseline Security Analyzer web sitesinde kullanılabilir: http://www.microsoft.com/technet/security/tools/mbsahome.mspx Bu araç, bir bilgisayarın geçerli durumunu Microsoft tarafından tutulan bir güncelleştirme listesiyle karşılaştırarak çalışır. MBSA ayrıca, parola gücü ve kullanım süresi ayarları, misafir hesabı ilkeleri ve birkaç başka alanla ilgili bazı temel güvenlik denetimleri de gerçekleştirir. MBSA ayrıca Microsoft Internet Information Services (IIS), SQL Server™ 2000, Exchange 5.5, Exchange 2000 ve Exchange Server 2003'teki bazı güvenlik açıklarını da arar.
- **Microsoft Yazılım Güncelleştirme Hizmetleri (SUS)**
  Daha önce Windows Update Corporate Edition olarak bilinen bu araç, kuruluşların herkese açık Windows Update sitesinde kullanıma sunulan tüm kritik güncelleştirmeleri ve güvenlik toplama paketlerini (SRP) yerel bilgisayarlarda barındırmalarına olanak tanır. Bu araç, güçlü bir otomatik karşıdan yükleme ve kurma stratejisinin temelini oluşturmak için yeni bir otomatik güncelleştirme (AU) istemcileri sürümüyle çalışır. Yeni AU istemci kümesi, Windows 2000 ve Windows Server 2003 işletim sistemleri için bir istemci içerir ve karşıdan yüklenen güncelleştirmeleri otomatik olarak yükleme yeteneği vardır. Microsoft SUS hakkında daha fazla bilgi için bkz: http://www.microsoft.com/windows2000/windowsupdate/sus/default.asp
- **Microsoft Systems Management Server (SMS) Software Update Services Feature Pack**
  SMS Software Update Services Feature Pack (SMS Yazılım Güncelleştirme Hizmetleri Özellik Paketi) tüm işletmede yazılım güncelleştirmelerini yayınlama sürecini kolaylaştırmayı hedefleyen bazı araçları içerir. Araçlar, bir Güvenlik Güncelleştirme Envanteri Aracı'nı, bir Güncelleştirmeler için Microsoft Office Envanter Aracı'nı, Yazılım Güncelleştirmeleri Dağıtım Sihirbazı'nı ve Yazılım Güncelleştirmeleri için Web Raporları Eklentisiyle SMS Web Raporlama Aracı'nı içerir. Her bir araçla ilgili daha fazla bilgi için bkz: http://www.microsoft.com/smserver/downloads/20/featurepacks/suspack/

Bu araçların her biriyle ilgili olarak müşterilerinizle konuşun ve kullanmaları için onları teşvik edin. Güvenlik sorunlarının mümkün olan en hızlı şekilde ele alınması ve bu sırada ortamın güvenilirliğinin korunması çok önemlidir.

SQL Server 2000 Güvenlik Ayarları

Navision SQL Server 2000 üzerinde de çalıştığından, müşterinin SQL Server 2000 kurulumunun güvenliğini artırmak için önlemler almanız önemlidir. Aşağıdaki adımlar SQL Server güvenliğini artırmaya yardımcı olur:

- En yeni işletim sisteminin ve SQL Server 2000 servis paketlerinin ve güncelleştirmelerinin yüklendiğinden emin olun. En son ayrıntılar için, http://www.microsoft.com/security/default.asp adresindeki Microsoft Güvenlik web sitesini ziyaret edin.
- Dosya sistemi düzeyinde güvenlik için, tüm SQL Server 2000 veri ve sistem dosyalarının NTFS bölümlerine yüklendiğinden emin olun. NTFS izinlerini kullanarak, dosyalara yalnızca yönetimsel veya sistem düzeyi kullanıcıların erişmelerini sağlamanız gerekir. Bu, MSSQLSERVER hizmeti çalışmadığı sırada o dosyalara erişen kullanıcılara karşı koruma sağlar.
- SQL Server 2000 hizmeti (MSSQLSERVER) için, NT Authority\Network Service veya LocalSystem (önerilen) hesabı gibi düşük ayrıcalıklı bir etki alanı hesabı kullanın. Etki alanında bu hesabın en alt düzeyde hakları olmalıdır ve tehlike durumunda sunucuya yapılacak bir saldırının kontrol altına alınmasına (ancak durdurulmasına değil) yardımcı olmalıdır. Diğer bir deyişle, etki alanında bu hesabın yalnızca yerel kullanıcı düzeyinde izinleri olmalıdır. SQL Server 2000 hizmetleri çalıştırmak için bir Domain Administrator (Etki Alanı Yöneticisi) hesabı kullanıyorsa, sunucunun tehlikeye maruz kalması, tüm etki alanının tehlikeye maruz kalmasına neden olur. Bu ayarı, SQL Server Enterprise Manager'ı kullanarak değiştirin. Dosyalar, kayıt defteri ve kullanıcı haklarıyla ilgili erişim denetimi listeleri (ACL) otomatik olarak değiştirilir.
- SQL Server 2000'in çoğu sürümü, iki varsayılan veritabanıyla birlikte yüklenir: **Northwind** ve **pubs**. Her iki veritabanı da, sınama, eğitim ve genel örnekler için kullanılan örnek veritabanlarıdır. Bir üretim sistemi içinde dağıtılmamaları gerekir. Bu veritabanlarının var olduğunu bilmek, bir saldırganı varsayılan ayarları ve varsayılan yapılandırmayı kullanarak saldırıda bulunmaya teşvik edebilir. Üretim SQL Server 2000 bilgisayarında **Northwind** ve **pubs** varsa, kaldırılmaları gerekir.
- SQL Server 2000 sisteminin denetlenmesi, varsayılan olarak devre dışı bırakılmıştır, bu nedenle hiçbir koşul denetlenmez. Bu durum, yetkisiz erişimin algılanmasını güçleştirir ve saldırganların saldırılarını gizlemelerine yardımcı olur. En azından, başarısız oturum açma girişimlerinin denetlenmesini etkinleştirmeniz gerekir.

En güncel SQL Server 2000 güvenlik bilgileri için bkz:
http://www.microsoft.com/sql/techinfo/administration/2000/security/default.asp

Microsoft Business Solutions Hakkında

Microsoft'un bir bölümü olan Microsoft Business Solutions, küçük, orta boy ve kurumsal ölçekli işletmelerin müşterileriyle, çalışanlarıyla, ortaklarıyla ve tedarikçileriyle daha yakından bağlantı kurmalarına yardımcı olmak için tasarlanmış çok çeşitli tümleşik ve uçtan uca iş uygulamaları ve hizmetleri sunar. Microsoft Business Solutions'ın uygulamaları, finansal yönetim, analiz, insan kaynakları yönetimi, proje yönetimi, müşteri ilişkileri yönetimi, saha servisi yönetimi, tedarik zinciri yönetimi, e-ticaret, üretim ve perakende yönetimi alanlarında stratejik iş süreçlerini en iyi duruma getirir. Uygulamalar, müşterilerin işlerinde başarıya ulaşmalarına yardımcı olmak için bilgi sağlamak üzere tasarlanmışlardır. Microsoft Business Solutions hakkında daha fazla bilgi http://www.microsoft.com/BusinessSolutions/ adresinde bulunabilir.