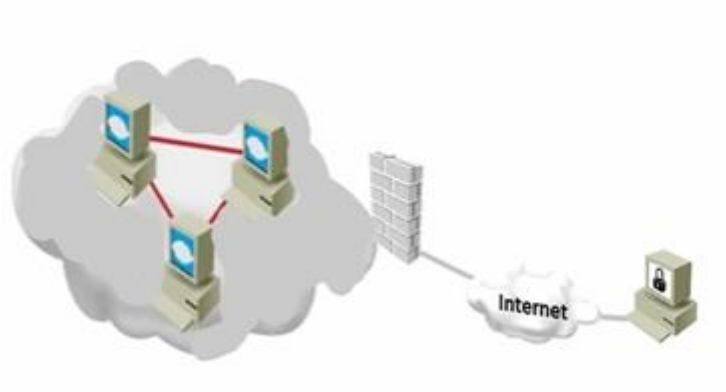
Windows Sıkılaştırma İşlemleri

Kurumsal firmalarda en çok kullanılan işletim sistemlerinin başında Windows işletim sistemi gelmektedir.
Windows sıkılaştırma İşlemleri nelerdir?
Windows sıkılaştırma işlemleri ,bir bilgisayar sisteminin veya sunucunun saldırı yüzeyinin en aza indirme işlemidir.

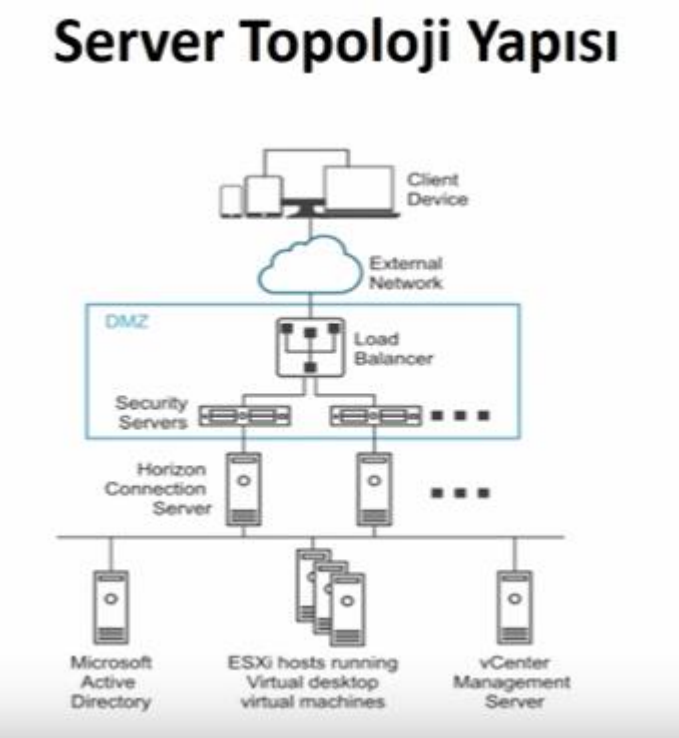


İşletim sistemleri sıkılaştırma işlemleri genellikle bir sunucunun veya işletim sisteminin yamalanmasını ve güvenliğinin sağlanmasını içerir. Genellikle kullanıcıların manuel veya otomatik yükleyebilecekleri güncellemeleri ,hizmet paketlerini ve yamalar yayınlanır. Bu sayede güvenlik işlemleri sağlanmış olur.

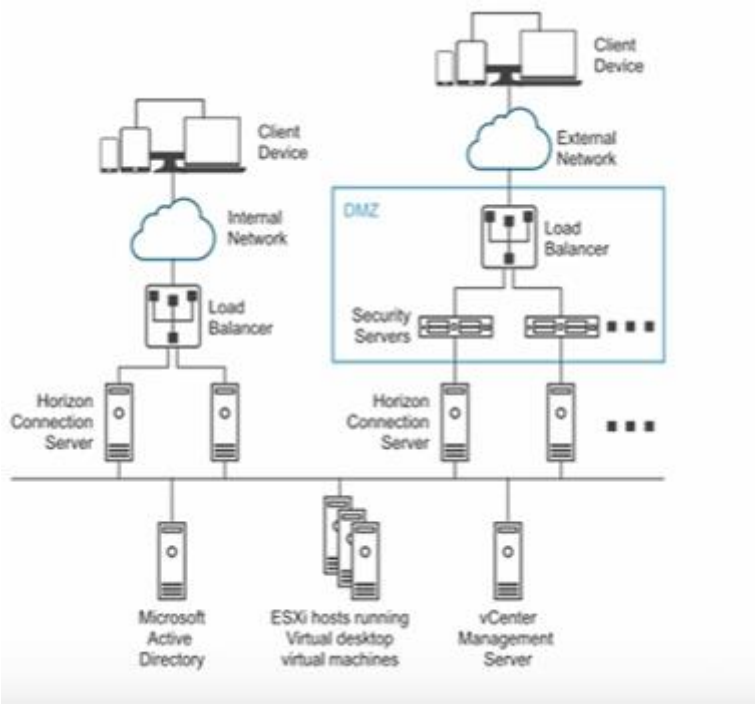
Windows Sıkılaştırma Temelleri

*Windows ve Windows server güvenlik temeline dayanarak tasarlanmıştır.
*Microsoft belirli tönleri güvence altına alınır.Bu işlemlerin yanı sıra kurum ve kuruluşlara daha ayrıntılı gvenlik yapılandırılması sağlayan denetimler sunar.
*Windows ürün grupları ,müşteriler ve ortaklarından alınan geri bildirimlere dayalı bir grup yapılandırma işlemi mevcuttur.

Server Topoloji Yapısı



Doğru bir sıkılaştırma işlemi kadar doğru topoliyi kurmak bi o kadar da önemlidir.Bir kaç güvenlik yapısı mevcuttur.Resimdeki topoloji yapısı bir DMZ teki yük dengeli güvenlik sunucularını gösteren bir topoloji yapısı örneğidir.Burda DMZ nedir? İşler workunu çok fazla tehlikeye atmadan internetten gelebilecek saldırılara karşı korumak aynı zamanda da dünyayla bağlantıyı devam ettirmek istediğimiz(FTP Server,Main server) gibi dış dünyaya açtığımız alandır.Bu örnekte güvenlik sunucuları dahili ağ içinddeki iki horizon connection server örneği ile iletişim kurar .Horizon connection server da istemci bağlantıları için bir aracı görevi gören bir yapıdırActive Directory aracı ile kullanıcıların kimliklerini doğrular bize .Yani bu örnekteki topolojide kurumsal ağ dışındaki kullanıcılar bir güvenlik sunucusuna bağlandığında uzak masaüstlerine ve uygulamalara erişmeden önce kimlik bilgilerini başarıyla doğrulamaları gerekmektedir.



İkinci örneğimize geçersek bu topoloji örneği birden fazla güvenlik sunucuları içermektedir. Bu topolojide dahili ağdaki örnekten dahili ağdaki kullanıcılara ,harici ağdaki örnekler ise harici ağdaki kullanıcılara atanır. Bu topolojinin mantığında farklı olarak güvenlik sunucuları ile eşleştirilmiş bağlantı sunucuları kimlik doğrulamaları eşleştirilirse burada tüm kullanıcıların kimlik doğrulaması yapması gerekir.

Windows Sitemlerde Ağ Hizmetleri Sıkılaştırılması

*Ağ cihazlarını sıkılaştırmak bir ağın yetkisiz erişim riskini azaltır.

*Yapılandırmaya başlamadan önce dikkat etmemiz gereken en önemli noktalardan birisi yapılandırma adımlarını belirlemek olacaktır.

İnternet Yönüne Trafiğin Denetlenmesi

Sunucu ağların İnternet yönüne trafiği engellenmelidir.

Son kullanıcı bilgisayarların web trafiği denetlenebilir olması gerekir.

VLAN'lar Arası Port Bazlı Erişimlerin Kısıtlanması

Vlan yapılandırılmaları güvenlik duvarı izleniminde devam ederek ,Vlanlar arasında port ve servis bazlı erişim kısıtlamaları uygulanmalı

DMZ ve sunucu ağları, belirlenen güvenlik kriterlerine göre farklı ağlara ayrılmalıdır.

Kablosuz ağlar ve misafir kurum ağlarını iç ağdan bağımsız hale getirmek gerekir.

Uzak Erişim Denetimleri

*Kritik verilerin ve sistemlerin etkilenebileceği cihazlara internet erişiminin kapatılması gerekmektedir. Eğer böyle bir durumun yapılamaması durumunda çoklu kimlik doğrulaması uygulanmalıdır.

*Uzak erişim sağlayan yönetimsel servisler olan SSH,RDP,MSSQL gibi servislerin erişimleri engellenmelidir.

Güvenlik Cihaz ve Yazılımların Yapılandırılması

Antivürüs yazılımlarının tüm kullanıcılar ve sunucularda yüklü olmalı

Antivürüs yazılımlarının kapatılıp açılması gibi özelliklerinin kısıtlanması gerekmektedir.

Güvenlik duvarındaki kurallarda ANY kural tanımlamalarından kaçınılmalıdır.

Güvenlik cihazlarının güncel olmasına dikkat edilmelidir.

Ağ Güvenliği Ayarları

Yerel sitemin NTLM için bilgisayar kimliğini kullanmasına izin verilmeli

Kerberos için izin verilen şifreleme türlerini yapılandırmalıyız.
Tüm profillerde Windows güvenlik duvarının etkinleştirilmesi gereklidir.
Varsayılan olarak gelen trafiği engellemek için tüm profiller de Windows güvenlik duvarını yapılandırılması gereklidir.
Ağ ayarlarından dosya ve baskı paylaşımını kaldırın.

Windows Sistem ve Domain Sıkılaştırmaları

Domain sunucu rolü, herhangi bir ortamda güvence altına alınması gereken en önemli rollerden biridir.
Kurumsal sistemlerin neredeyse tamamı domain yapısına sahiptir.Güvenilir yapılandırlmamış bir domain yapısına sahip şirketler büyük sorunlara sebebiyet verebilir.

Kullanıcı ve Parola Güvenliğinin İyileştirilmesi

*Sunucular üzerinde yerleşik olarak gelen "Administrator" kapatılmalıdır.
*Sistemler üzerinde kullanılan lokal admin kullanıcıları her sistem üzerinde farklı parolaya sahip olmalıdır.
*Domain kullanıcılarına lokal admin yetkisi verilmemelidir, iş gereksinimleri dolayısıyla kendi sistemleri üzerinde lokal admin hakkı verilen kullanıcılar için ekstra güvenlik ve izleme yöntemleri uygulanmalıdır.
*Domain parola politikası sıkılaştırılmalı; parola değiştirme zorunluluğu istisnası tamamlanan hesap olmamalı ,iş gereksinimi nedeniyle zorunlu olan kullanıcılar için ekstra güvenlik ve izleme yapılandırılmaları uygulanmalıdır.

Yönetimsel Süreçlerin İyileştirilmesi

*Yüksek yetkili yönetici ve servis hesapları güvenliğini sağlamak için "Kısıtlı Admin Profili"gibi domain politikalarının incelenmesi ve uygulanması gerekmektedir
*"Domain,Admin" vb yüksek yetkili gruplardaki kullanıcılar düzenli aralıklarla kontrol edilmeli ve gereksiz kullanıcılar kaldırılmalıdır.
* "Domain,Admin" vb yüksek yetkili gruplardaki kullanıcıların bireysel hesapları ile yetkili kullanıcıları ayırmalıdır.
*SMB,RDP vb. uzak yönetim için kullanılabilecek servisler gerekli değil ise kapatılmalı ,gerekli olan kullanımlar için kısıtlama ve sıkılaştırılmalar (Örneğin uzak masaüstü için kaynak IP aralığı kısıtlaması) uygulanmalıdır.

Domain Yapısının İyileştirilmesi

*DMZ de bulunan sunucular ile kullanımı gereği fazla atak vektörü bulunan cihazlar (ortak kullanım ihtiyacı ,İnternetten erişim vb.)domainden çıkartılmalıdır.
*Güvenlik gereksinimleri karşılamayan uygulama barındıran cihaz ya da düşük sürüm işletim sistemi olan cihazlar domaine alınmamalıdır.

*Domain politikasında varsayılan olarak gelen herhangi bir son kullanıcının domaine cihaz ekleyebilme özelliği kurum ihtiyaçları gözetilerek kaldırılmalıdır.

LDAP güvenliği

*Domain sunucuya anonim olarak bağlanılmamalı ve aktif dizin bölümlerine anonim olarak erişim ve sorgulama yapılmamalıdır.
*Domain yapısında sunucunun LDAP imzalamayı zorunlu olarak tutmaması trafiğin güvenliğini tehlikeye atar.
*LDAP,SSL/TLS içerisinden şifreli olarak gitmemesi iletişim güvenliğini tehlikeye atar.

Windows Politika Prosedür ve Süreç İyileştirmeleri

Sıkılaştırmalar oldukça kritiktir,bu sebeple güvenliğin korunması için bazı önlemlerin alınması gereklidir.Politika prosedür ve süreç iyileştirmeleri konusuna baktığımızda da kurum içerisinde sıkılaştırılma işlemlerini destekleyici adımların neler olduğunu göreceğiz.

Envanter Yönetimi

Donanım ve üzerindeki yazılım/servis bilgileri envanteri tutulmalıdır.

Envanterin tutulup güncellenmesi için bir personel/ekip sorumlu tutulmalı ve envanterde belirtilen kaynakların da sorumlu personelin/ekibin belirlenmesi gerekmektedir.

İç ve Dış Sızma Testlerinin Gerçekleştirlmesi

Kurum bünyesinde düzenli zafiyet taramaları ve güvenlik testleri gerçekleştirilmelidir.

Tespit edilen veya bildirilen zafiyetlere yönelik zafiyet yönetimi gerçekleştirilmelidir.

Olay müdahale ve Süreçlerin Belirlenmesi

Siber olay müdahale sürecinde sorumluluk alacak personelin ve ilişki kurum dışı birim iletişimleri belirlenmelidir.

Veri çıkarma ,erişim engellenmesi, kurum içi personel saldırıları vb. senaryolar üzerinde planlama yapılmalıdır.

Sistem ve Altyapı Sıkılaştırmaları

Bilgi sistemleri altyapısında kullanılan ağ cihazları ,sunucular ,işletim sistemi ve yazılımlar kurulun aşamasından sonra üretici firma ve diğer güvenilir kaynaklarda belirtilen yönergelere göre sıkılaştırılarak kullanıma alınmalıdır.

Kurum genelindeki hiçbir cihaz ve uygulama için jenerik kullanıcı adları kullanılmamalıdır.

İLERİ SEVİYE GÜVENLİK GEREKTİREN ALANLAR

Risk Analizi

Kurumun yaptığı iş ile ilgili en değerli varlıklar belirlenerek bu amaçla kullanılan cihaz sunucu, yazılım ve kullanıcılar kritik varlık olarak belirlenmelidir.

Ağ cihazları yedekleme ve sanallaştırma sistemleri başta olmak üzere diğer sistemleri etkileyebilecek tüm cihaz ve sunucular kritik varlık olarak belirlenmelidir.

Kurum domain yapısı ana bileşenleri (Domain Controller, Exchange Server, LDAP vb.)kritik varlık olarak belirlenmelidir.

Erişim ve Denetim Sıkılaştırmaları

Kritik cihazlara erişim görevler ayrılığı ilkesine göre planlanmalıdır.

Kritik Cihazlara Özel Log Yönetimi

Kritik cihazlara tüm erişim denemeleri detaylarının (başarılı ve başarısız ,erişim başlangıcı ve bitişi vb.)izlenebilir olması gerekmektedir.

Kritik cihazların erişilebilirliği düzenli olarak kontrol edilmeli ve disk doluluk ile performans durumları takip edilmelidir.

Windows Kullanıcı Yönetimi

5 başlık altında inceleyebiliriz;

Gereksiz hesapları kaldırma

Yerel kullanıcı hesapları otomatik olarak oluşturulur. Administrator ,Guest ve Help-Assistant hesaplar oluşturulur .Administrator hesabı yönetici hesabıdır ve en yetkili hesaptır. Bu Administrator hesabı silinmez .Bu hesabı korumak için devre dışı bırakabilir ya da ismini değiştirebiliriz, böylelikle kötü niyetli kişilerin varsayılan olarak erişmesini engellemiş oluruz.

Normal Hesap Kullanımı

Kullanıcı Hesapları yönetiminde en iyi uygulama elbette ,yöneticilerin de bir normal hesap (Administrator olmayan) kullanımları olacaktır. Eğer zararlı yazılım çalıştırılırsa onu çalıştıran kullanıcının yetkilerine sahip olacaktır.

Administrator Hesap

Ağınızda ya da bilgisayarınızda birden çok yönetici kullanıcı varsa hepsi için farklı ,kişiselleştirilmiş yönetici hesapları oluşturmanız gerekmektedir. Bu şekilde administrator yetkisinde bir sorun ortaya çıktığında kimin sorumlu olduğunu veya kasten yaptığını anlayabiliriz.

Yerel Kullanıcı ve Yerel Grup Yapılandırılması

Grup ilkeleri ile yapılan bir takım sıkılaştırılmalar veya güvenlik ürünlerindeki bazı kontroller sadece domainde ki kullanıcılar ile yapılmaktadır.Yerel Kullanıcılar tarafından yapılan bazı işlemler gözden kaçabilmektedir.Bu sebeple gerekli kontroller tüm kullanıcılar için yapılmalıdır.

Kullanıcı Hakları

Ağ üzerinden bilgisayara bağlanabilme
Terminal Services
Debug Programlar
Log on Locally(Yerel olarak oturum Açma)
Grup üyeliklerini sınırlamak
Microsoft hesabı oluşturmak