Ağ Güvenliği Sistemlerin büyümesi ve sistem içerisindeki birimlerin farklı özelliklere sahip olması durumunda her bir düğümün güvenliğin sağlanması oldukça zor olacaktır. Bu da ağın güvenliğinin sağlanması çalışmalarına yönelmeye zorlamaktadır. Bu yaklasımdan yola çıkarak bütün cihazlara tek tek ulaşılıp kontrol edilmesi gerekir. Her ağ güvenlik açıkları sayesinde içeriden yada dışarıdan izinsiz erişimler olabilmektedir. Önemli verilerin sadece iç ağdaki kullanıcılara değil, aynı zamanda dışarıdan girebilecek kişilere karşı da korunmuş olması gerekir. Dıştaki güvenilmez ağ ile, içteki güvenilir ağ ile arasındaki korunma sağlayan yapıya "Güvenlik Duvarı" denir.

Güvenlik Duvarının kullanılması komple güvenlik çözümünü oluşturan esaslar olan;

- Güvenlik politikası belirlenir.
- fiziksel güvenlik
- Erişim Kontrolü
- Kimlik onaylama
- Şifreleme
- Takip

fonksiyonlarını sadece bir parçasını oluşturmaktadır.

- fiziksel Güvenlik

Ağ güvenliği fiziksel güvenlikle bağlantılıdır. Ağdaki makinelerin boyutu ve şeklinin yanı sıra boyutu ve şeklinin yanı sıra ağın ihtiyaçtan dolayı ve karşılıklı güven ilişkilerine dayalı olarak bir binayı, kampüsü, ülkeyi yada dünyayı sarabilme ihtimali vardır. fiziksel güvenlik politikasının ağ güvenliği politikası oluşturulurken yenilenmesi ve dikkate alınması gereklidir.

2-) Erisim Kontrol: Erisim kontrol gelen her ağ paketinin içeriye alınıp alınmayacağına ve pakete karşı yapılacak davranısa karar verir. Bir güvenlik duvarı paketin veya oturumun tanımlanmıs olan güvenlik politikasına uygunluğunu belirler. İyi tasarlanmış güvenlik duvarı detaylı güvenlik politikalarını gerçekleştirebilir.

Güvenlik duvarı özel bir ağı koruyan en ucuz ve basit yöntemidir.
Güvenlik duvarı özel bir ağı uzaktan erişim zayıflıklarına karsı koruyan en iyi çözüm yöntemidir.

3-) Kimlik Onaylama: Kimlik onaylama yetkili personel ve bölümlerin serbestçe haberlesmesini sağlarken izinsiz erişimi engellemektedir. Kullanılan onaylama yöntemi kullanıcının nereden ve nasıl onaylandığına bağlıdır. İnternet ve diğer uygulamalar için en popüler onaylama yöntemleri "Neredeler?", "Neleri var?", "Neleri biliyorlar?" sorularının cevabıdır.

Ancak ip adres onaylaması veya Neredeler? yöntemi ip adres sahtekarlığı saldırı yöntemi kullanılarak geçilebilir.

4-) Sifreleme

Sifreleme islemi veri bütünlüğünü garantileyebilir, ve güvenli hatlardan yollanan bilgiyi koruyabilir. Önemli sirket bilgilerine uzaktan erisimde veya organizasyon intraneti'ne (iç ağı) erisimde korumanın sağlanabilmesi için şifreleme kullanılabilir. Ancak şifrelemede önemli olan anahtarların hangi yoldan gönderileceği ve nasıl yaratılacağı konularıdır. Anahtarlar verinin şifrelenmesi ve açılmasında kullanılır. otomatik anahtar yönetimi bir açık düğümü bulunan bir sarttır.

5-) Takip: Güvenlik politikası uygulanmaya baslandıktan sonra bütün sistem parçaları ve personelin güvenlik politikasına uygunluğunu periyodik olarak kontrol edilmesi gerekmektedir. Yeterli denetimin olmaması durumunda bir güvenlik ihlalli sonrası takip için yeterli delil olmaması durumunda takip için yeterli bilgi bulunmayabilir. denetimin yapılması problemleri önceden tespit ederek güvenlik boşluklarına dönüsmelerini engelleyebilir. Günlük kayıt ve anında uyarı mesajının yollanması kısa sürede önlem alınmasını ve saldırı kaynağının tespitini kolaylastırır.

ELEKTRONİK POSTA GÜVENLİĞİ

MD5 } şifreleme algoritmalarıdır
RSA

SNMP → Simple Network Management Protocol

(Basit ağ yönetim protokolü)

SNMPV1
SNMPV2
SNMPV3

Ağ üzerindeki e-postaların güvenli bir şekilde gönderici ve alıcı arasında yol alması amacıyla değişik uygulamalar değişik protokolleri, bu protokollerde farklı şifreleme ve imzalama algoritmalarını kullanmaktadırlar. Bunlardan biri olan **PGP** protokolünde **x-509**'a benzer bir sertifikasyon yapısı bulunur. PGP protokolünde her kullanıcı aynı zamanda bir sertifikasyon otoritesidir (CA) bunun anlamı ise her kullanıcı kendine ait gizli bir anahtar seçip bu anahtara uygun bir açık anahtar oluşturacak ve bu anahtarı kimlik bilgisi ile birlikte ağ üzerinde ortak kullanılan bir sunucuya aktaracaktır kendisine ait gizli bir anahtarı uygun biryerde saklayan kullanıcı haberleşeceği adresin açık anahtarını ise **"Public Key ring"** adı verilen bir sayada toplayacaktır PGP, açık anahtarlı algoritma olarak RSA, gizli anahtarlı algoritma olarak IDEA ve özetleme fonksiyonu olarak MD5 algoritmasını kullanmaktadır. Kendi simetrik algoritmasına ait üretilen gizli anahtarla mesajı şifreleyen kullanıcı gizli anahtarıda alıcı kişinin açık anahtarlı algoritmasına ait açık anahtarla şifreleyecek ve bütün bu şifreli kısımlarıda kendine ait gizli anahtarla imzalayacak ve alıcıya gönderecektir alıcı ise açık anahtarlı algoritmasının gizli anahtarıyla, şifrelenmiş olan anahtarı açacak ve buradan elde edilen anahtarlada şifrelenmiş mesajı açacaktır mesajın imzasını ise gönderenin açık anahtarıyla kontrol edecektir

AĞ YÖNETİM GÜVENLİĞİ

Birbirlerine bağlı ağların kullanımının artması ile birlikte ağların yönetim sistemlerindeki güvenlik problemlerinin çözülmesi gerektiğinde önem kazanmıstır. ağ yönetim protokollerinden SNMPv1 protokolünde sadece ulasım kontrolü bulunmaktaydı. Güvenlik ile ilgili eklemeler yapılarak 2. sürümü çıkartıldı. SNMPv2 protokolünde ulasım kontrolünün yanında kimlik doğrulama ve gizlilik fonksiyonlarıda bulunmaktaydı. SNMPv3 de ise sadece sistem güvenliği ön plana çıkmıstır.

İsletim Sisteminin Güvenliği:

isletim sistemi secilirken; kurulum kolaylığı, donanım gereksinimleri ve sürücü edinebilme, kullanım ve yönetim, güvenilirlik, güvenlik, uyumluluk, fiyat destek gibi özelliklere bakılarak secilebilir. Bu özelliklerin icinde bulunan güvenlik özelliği, eğer sistem ağa acılacaksa cok büyük önem kazanacaktır.

Windows'un Güvenlik Bilesenleri:

1.) Logon Process (Giris Süreçleri): Kullanıcıların giriş isteklerini kabul eder. Kullanıcının ismi ve parolası kontrol edildikten sonra tanımlanan haklara (yetkilere) göre hareket etmesini sağlayan sistemdir.

2-) Yerel Güvenlik Makamı (Local security authority): Kullanıcının sisteme erisim iznini denetler. Bu bilesen güvenlik alt sisteminin cekirdeğidir. erisim jetonlarını üretir yerel güvenlik prensiplerini yönetir ve etkilesimli kullanıcı onaylama hizmetlerini sağlar. yerel güvenlik makamı aynı zamanda kayıt denetimi prensiplerinide denetler ve güvenlik kayıt mesajını kaydeder.

3-) Güvenlik Hesap Yöneticisi (SAM): Kullanıcı hesapları veritabanına bakarak kullanıcı yönetimini sağlar veritabanında tüm kullanıcı ve grupların hesapları bulunur SAM yerel güvenlik makamı tarafından kullanılan kullanıcı geçerli kılma hizmetlerini sağlar.

4-) Güvenlik ~~talan~~ Başvuru İzleyicisi (security reference monitor)(hts kayıtları): Kullanıcının bir nesneye erişim izninin olup olmadığının kontrolünü ve yaptığı işlemleri denetler SAM tarafından tanımlanmış olan erişim iznini geçerli kılma kayıt hesabı üretim prensiplerini gerçekleştirir hem çekirdek hemde kullanıcı kitlelerine, bir nesneye erişmek isteyen kullanıcı ve süreçlerin gerekli izinlerini bulunduğunu denetleyen hizmetler sunar Bu bileşen gerektiğinde kayıt hesabı mesajlarıda üretir

..UNIX... GÜVENLİK BİLEŞENLERİ...

Unix işletim sisteminde windowsda olduğu gibi sistem yöneticisine dayalı olarak kullanıcı hesap prensipleri belirlenirken birtakım özellikler sağlanır sistemlerin içerdikleri donanım ve yazılımlara göre güvenlik seviyeleri belirlenmeli ve gerekirse yükseltme işlemi gerçekleştirilmelidir 1985 yılında DOD tarafından TCSEC yayınında 4 güvenlik seviyesi ve bunların alt sınıfları belirtilmiştir

UNIX GÜVENLİK SEVİYELERİ

Güvenlik Seviyeleri	Alt Seviye	Özet Bilgi
D	D1	En düşük seviye kolay geçilir Donanım koruması sağlamaz erişim kontrolü yoktur
C	C1	isteğe bağlı güvenlik kullanıcı hatalarından sistemi korur dışarıdan gelecek saldırılara karşı koruma sağlamaz. Donanım elemanları için koruma sağlar erişim kontrolü yapılır
	C2	Kontrollü erişim kaynaklara kontrollü erişim ve yapılan işlemler kayıt altına alınır bu işlem işlemci zamanı ve diskten yer kaplama alanı arttırır.
B	B1	Etiketli güvenlik, güvenliği sağlanılacak nesneler birbirinden ayrılır. (güvenli, en iyi güvenli.)
	B2	Yapısal güvenlik sistemindeki bütün nesnelerin etkilenmesi gerekir. farklı güvenlik seviyesindeki cihazların haberleşmesi sorun yaratabilir
	B3	Güvenlik alanı koruma, daha sağlam ve daha ciddi bir sistem güvenlik yönetimi güvenli kurtarma ve saldırıların yada oluşan zararın sistem yöneticisine hemen bildirir.
A	A1	En iyi düzeyde güvenlik B3'e ek olarak güvenli dağıtım özelliği eklenmiştir. Sisteme ilişkin yazılım ve donanım bileşenleri üzerinde güvenlik sistemini etkileyecek değişikliklerin sistemlerin aktarılması aşamasında tekrar güvenliğin sağlanması gerekir.

Ne Kadar Güvenlik Gerekli ??

Ağ güvenliğinin seviyesine karar vermeden önce yapılacak ilk iş korumanın seviyesine karar vermektir. Bunun icin ağın güvenlik analizinin yapılması gereklidir

1-) Risk Analizi

Korunması istenen varlıkların ve onlara karşı olan potansiyel saldırıların belirlenme sürecidir. Biçimsel bir risk analizi aşağıdaki sorulara cevap vermelidir

- Ne tür varlıkları korumak gereklidir?
- Bu varlıkları nelerden korumalıyız?
- Ağa kim saldırı yapabilir ve ne kazanabilir?
- Herhangi bir tehditin varlıklarımızı kosma olasılığı ne kadardır?
- Eger tehlikeli bir saldırı olursa bunun ivedi (en hızlı) maliyeti ne olacaktır?
- Bir atak ağa bozulmanın geri kazanma maliyeti ne olacaktır?
- Bu varlıklar etkin maliyet ile nasıl korunabilir?

2-) Korunacak Varlıklar:

Bir ağ üzerinde güvenlik ile ilgili calısma yapılmaya baslandığında ilk karar verilmesi gereken nelerin korunması gerektiğidir. Korunması gereken varlıklar veriler, kaynaklar, zaman, saygınlık olarak gruplandırılır.

3-) Kaynaklar kimden Korunmalı?

Ağın yapısına bağlı olarak saldırganlar değişebilir. Saldırıların büyük çoğunluğu iç ağdan gelmektedir. Ağa açılan bilgisayarların verdiği hizmetlere göre ne tür saldırılara uğrayacağı ve saldırgan türlerinde ortaya çıkabilir. Potansiyel saldırı kaynakları şunlardır:

- Dahili Sistemler
- Cevre, ofis erisim noktaları
- Bir iş ortağı olan geniş alan ağı (WAN)
- İnternet bağlantısı
- Modem Havuzu.

4-) Ağa Kim Tehlikeli Saldırı yapabilir?

Potansiyel Saldırı yapabilecek kişiler şunlardır:

- Calısan Personel
- Gecici veya danısman personel
- Rakipler

5-) Bir Saldırı ihtimali Nedir?

Kaynakları ve olabilecek saldırı türlerini belirledikten sonra kuruluşun saldırılara karşı potansiyel risklerini değerlendirilmesi gerekmektedir.

- Kurulus, yalıtılmış bir ağa mı sahip veya ağ birçok noktadan genis alan ağına (WAN) mı bağlı, Modem havuzu var mı veya VPN ile mi bağlı.
- Bütün bu bağlantı noktaları güçlü yetkilendirme sistemlerine sahip mi? Yoksa güvenlik duvarı ile mi? korunuyor ve bazı alarmlar var mı?

6-) Acil Maliyet Nedir?

Saldırı sonucunda fonksiyonunu yapamayarak olan herbir varlık icin acil maliyetin hesaplanması gerekmektedir. Nakliye gibi uzun süreli etkiler bu hesaplama icerisinde olmamalıdır. Bazen acil maliyetin hesabı güclesebilir. Örnegin rakiplerin calacagı sema, cizim yeni üretilecek parcaların projelendirilmesinden dolayı maliyet artacaktır. Bu ise rakiplerin daha gelismis ürün tasarrufuna neden olacaktır

7-) Bir atak veya Bozulmanın geri kazanma maliyeti nedir?

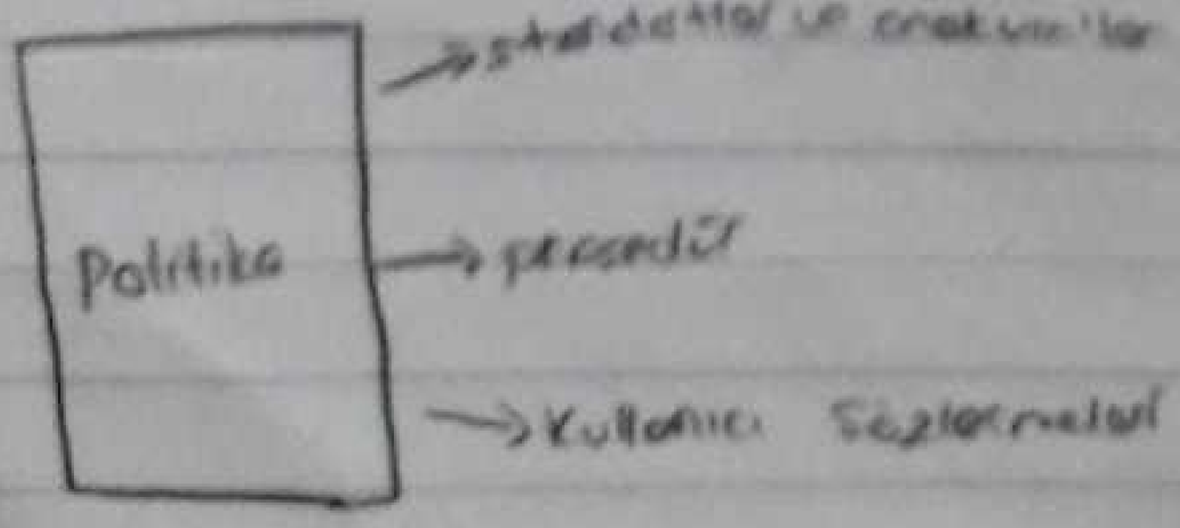
Bozulma veya zararlı saldırının baslangıc maliyetini hesapladıktan sonra bu bozulmanın getireceği toplam maliyetin hesaplanması gerekir

8-) Bu varlıklar etkin maliyet ile Nasıl Korunabilir?

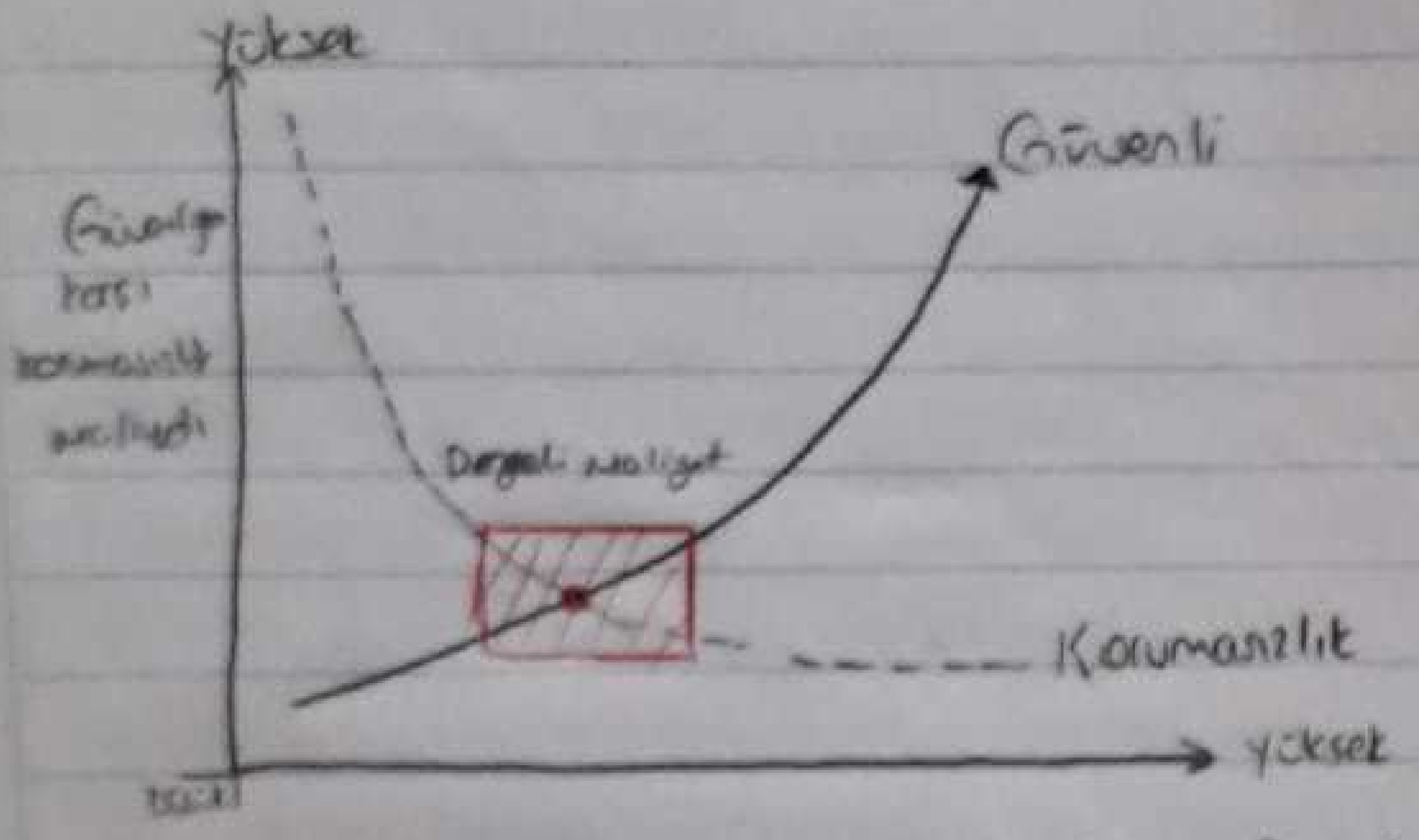
Ağ ortamının korumanın bir maliyeti olacaktır. Ancak bu maliyetin en az seviyede olmasına dikkat edilmelidir. Bu nedenle korunacak olan varlıkların risk analizlerinden korumanın seviyesi belirlenmis olacaktır.

9-) Güvenlik önlemlerinin bütcesi cıkarılması.
10) Bulunan sonucların yazılı olarak dökümante edilmesi
11-) Güvenlik politikasının gelistirilmesi
12-)

Bir organizasyonun güvenlik politikası o kurumun ihtiyacları ile direkt olarak ilişkilidir. Bütün kurumlara tam olarak uyan genel güvenlik politikası yoktur. Güvenlik politikası dökümanı; standartlar ve ana kurallar, kullanıcı sözlesmeleri ve prosedürlerle ilişkili olmalıdır



Güvenlik politikasında risk değerlendirmesi en kötü durum senaryosuna göre oluşturabilir. Burada bir maliyet hesabı yapılır. Risk yönetimi risk ve korunmasızlık maliyetine karşı koruma maliyetini dengeleyen bir süreçtir. Koruma ve korunmasızlık maliyetinin aynı olduğu nokta dengelenmiş ve mantıklı güvenlik ölçülerini göstermektedir. Yoksa güvenlik için gereğinden fazla harcama yapılabilir, yada daha az bir harcama ile sistem korumasız bırakılarak risk miktarı arttırabilir.



Güvenlik-Korumasızlık maliyetinin Dengelenmesi

Analiz sonucu ekle edilir
sorgu → " " edilmez } farklı

L2, L3 switchlerin farklı
katlı katman
Aralarında veri iletişimi
yapılamazsa halfduplex

Router ıp üzerinden farklı lanları bağlar.

[illegible]