



Bilgi Güvenliği Temel Kavramlar

Eğitmen : Fatih Özavcı

Bilgi Nedir

- İşlenmiş veridir.
- Bilgi diğer önemli iş kaynakları gibi kurum için değeri olan ve dolayısıyla uygun bir şekilde korunması gereken bir kaynaktır.
- Bir konu ile ilgili belirsizliği azaltan kaynak bilgidir.
(Shannon – Information Theory)

Güvenlik Üzerine

- Güvenlik risk yönetimidir
 - Anonim
- Bir sistem, yazılımı ihtiyaçlarınız ve bekłentileriniz doğrultusunda çalışıyorsa güvenlidir
 - Practical UNIX and Internet Security
- Güvenlik, bulunurluk, kararlılık, erişim denetimi, veri bütünlüğü ve doğrulamadır
 - <http://www.sun.com/security/overview.html>

Güvenlik ve İnsan

- Güvenlik, teknoloji kadar insan ve o insanların teknolojiyi nasıl kullandığı ile ilgilidir.
- Güvenlik sadece doğru teknolojinin kullanılmasından daha ileride bir hedeftir.
- Doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılmasıdır.

Teknoloji Tek Başına Yeterli mi ?

“Eğer teknolojinin tek başına güvenlik probleminizi çözülebileceğini düşünüyorsanız, güvenlik probleminiz ve güvenlik teknolojileri tam anlaşılmamış demektir.”

Bruce Schneier – Şifreleme Uzmanı



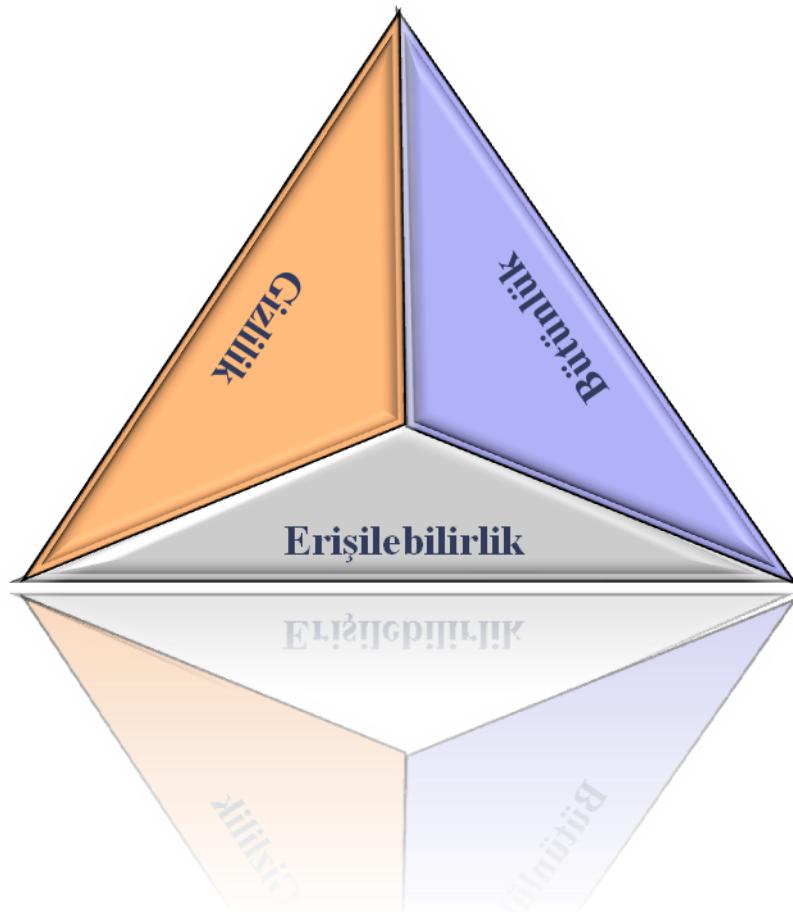
Güvenlik Yönetim Pratikleri

Güvenlik Yönetim Pratikleri

- Gizlilik, Bütünlük, Erişilebilirlik
- Risk Değerlendirmesi ve Yönetimi
- Politika, Prosedür ve Rehberler
- Politika Uygulamaları
- Eğitim
- Denetim

Gizlilik, Bütünlük, Erişilebilirlik

Hangisi Önemli ?



Gizlilik

Kuruma özel ve gizliliği olan bilgilere, sadece yetkisi olan kişilerin sahip olması

Bütünlük

Kurumsal bilgilerin yetkisiz değişim veya bozulmalara karşı korunması

Erişilebilirlik

Kurumsal bilgi ve kaynaklarının ihtiyaç duyan kişilerce sürekli erişilebilir durumda olması

Risk Değerlendirmesi

- Kurumsal işleyişi etkileyebilecek olan risklerin belirlenmesi ve değerlendirilmesi sürecidir.
- Bir risk değerlendirmesi yapılmadan, kurumsal işleyişin politika, prosedür ve uygulamalarıyla ne kadar korunduğu belirlenemez.
- Risk yönetimi konusunda yetkililere -tercihen üst yönetim- ihtiyaç duyulmaktadır.
- Üst yönetimin onayı ile sürecin önemi ve verimi artacak, çalışanlar politika ve prosedürlere daha fazla önem verecektir.

Risk Yönetimi

Risk Yönetimi

- Kurumun karşı karşıya olduğu risklerin belirlenmesi,
- Varlıkların zaafiyetlerinin ve karşı karşıya oldukları tehditlerin belirlenmesi,
- Ortaya çıkan riskin nasıl yönetileceği ve nasıl hareket edileceğinin planlanması

sürecidir.

Risk Yönetimi

Aşamalar

- Risk yönetim ekibi kurma
- Tehdit ve zaafiyetleri doğrulama
- Organizasyon varlıklarının değerlerini belirleme
- Riske karşı yapılacak hareketleri belirleme

Kavramlar

- Tehdit
- Zaafiyet
- Kontroller

Risk Yönetimi Kavramları

- Tehdit

Organizasyonu olumsuz etkileyebilecek olan insan yapımı veya doğal olaylar

- Zaafiyet

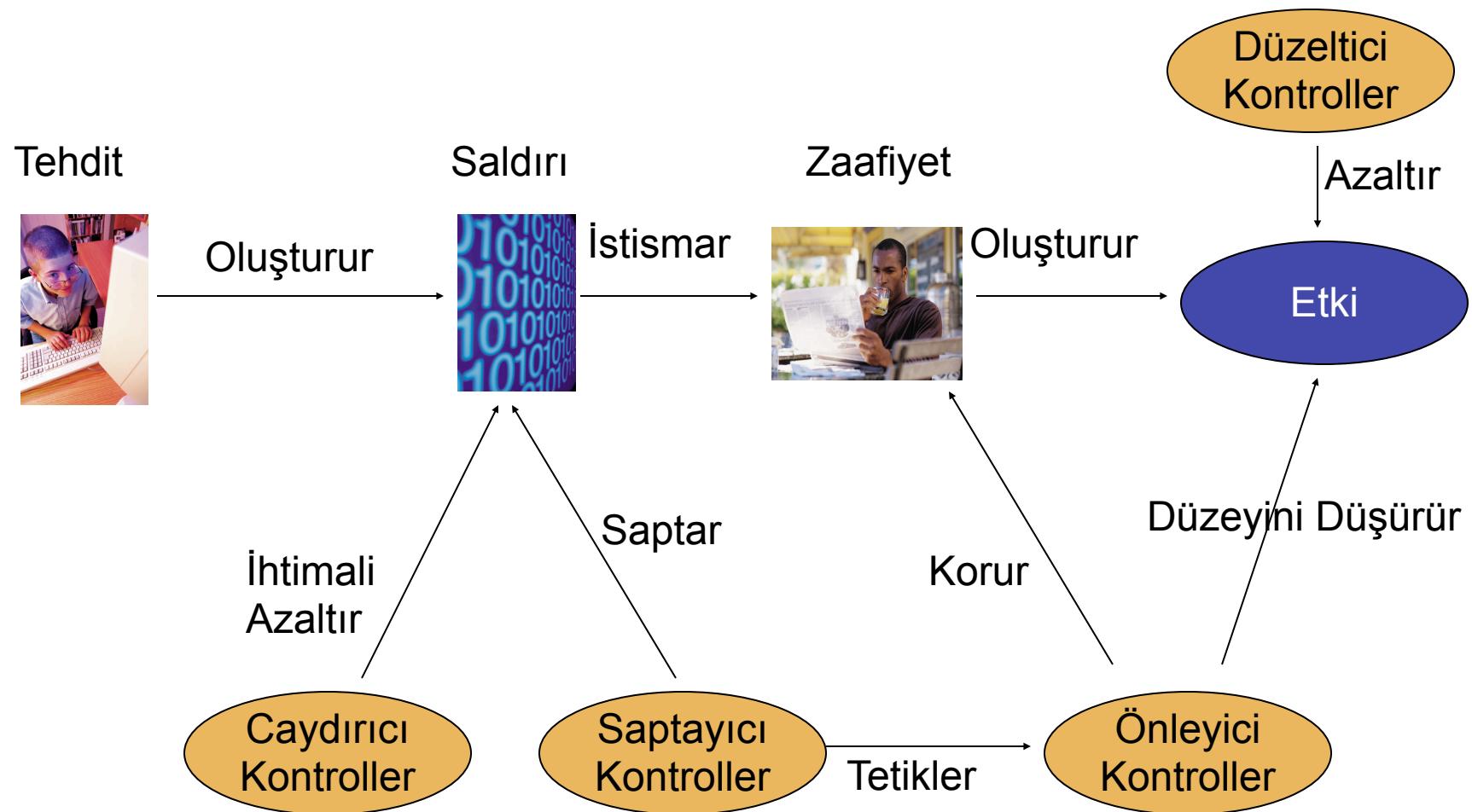
Varlıkların sahip olduğu ve istismar edilmesi durumunda güvenlik önlemlerinin aşılmasına neden olan eksiklikler

- Kontroller

Zaafiyetlerin boyutunu azaltıcı, koruyucu veya etkilerini azaltıcı önlemler

- Caydırıcı Kontroller
- Saptayıcı Kontroller
- Önleyici Kontroller
- Düzeltici Kontroller

Risk Yönetim Kontrolleri



Risk Yönetim Takımı

- Tek başına yapılabilecek bir iş değildir, yardımcılar ve diğer önemli departmanlardan çalışanlar ile yapılmalıdır. Böylece riski görmek ve kavramak daha kolay olacaktır.
- Potansiyel Gruplar ;
 - Bilişim Sistemleri Güvenliği
 - Bilişim Teknolojileri ve Operasyon Yönetimi
 - Sistem Yöneticileri
 - İnsan Kaynakları
 - İç Denetim
 - Fiziksel Güvenlik
 - İş Devamlılığı Yönetimi
 - Bilgi Varlıklarının Sahipleri

Tehditleri Belirleme

- Doğal Olaylar
 - Deprem, Sel, Kasırga
- İnsan Yapımı Olaylar
 - Dış Kaynaklı Olaylar
 - Virüs, Web Sayfası Değişimi, Dağıtık Servis Engellemesi
 - İç Kaynaklı Olaylar
 - Çalışanlar
 - E-Posta Okuma, Kaynaklara Yetkisiz Erişim, Bilgi Hırsızlığı
 - Eski Çalışanlar
 - Önceki Hakların Kullanımı, Bilgi Hırsızlığı, Gizli Bilgilerin İfşası

Zaafiyet, Tehdit ve Risk

Tehdit Tipi	Tehdit	Zaafiyet/İstismar	Oluşan Risk
İç Kaynaklı İnsan Yapımı	Çalışan	Kötü yetkilendirme ve izleme sistemi olmayışı	Veri değişimi veya yok edilmesi
Dış Kaynaklı İnsan Yapımı	Saldırgan	Hatalı güvenlik duvarı yapılandırması	Kredi kartı bilgilerinin çalınması
Doğal	Yangın	Kötü yanın söndürme sistemi	İnsan hayatı kaybı
Dış Kaynaklı İnsan Yapımı	Virüs	Güncellenmemiş anti-virus sistemi	İş devamlılığının aksaması
Teknik İç Tehdit	Sabit Disk Bozulması	Veri yedeği alınmaması	Veri kaybı, çok miktarda iş kaybı

Varlıkların Değerlerini Belirleme

- Gerçek risk yönetimi için hangi varlığın kurum için daha değerli olduğu doğru biçimde belirlenmelidir.
- Sayısal/Nicel Risk Değerlendirmesi yapılacak ise varlıklara para birimi cinsinden değer atanmalıdır.
- Eğer Sayılamayan/Nitel Risk Değerlendirmesi yapılacak ise varlıkların önceliklerinin belirlenmesi yeterlidir; ancak çıkacak sonuçların sayısal olmayacağı da ön görülmeli dir.

Nicel Risk Değerlendirmesi

- Sayısal risk değerlendirme yöntemidir, sayılar ve para birimleri ile risk belirlenir.
- Sürecin tüm elemanlarına sayısal değer verilmelidir.
 - Varlık, Etki Düzeyi, Korunma Verimliliği, Korunma Maliyeti vb.
- Temel kavamlar ve formüller ile risk değerlendirmesi yapılır.
 - Tekil Kayıp Beklentisi (SLE)
 - Tekil Kayıp Beklentisi = Varlık Değeri x Etki Düzeyi
 - Yıllık Gerçekleşme İhtimali (ARO)
 - Tehditin bir yıl içinde gerçekleşme ihtimali
 - Yıllık Kayıp Beklentisi (ALE)
 - Yıllık Kayıp Beklentisi = Tekil Kayıp Beklentisi x Yıllık Gerçekleşme İhtimali

Nitel Risk Değerlendirmesi

- Nicel tanımlama tüm varlıklara veya tehditlere kolayca uygulanamaz, Nitel tanımlama ise öncelik ve önem seviyelerine göre değerlendirmedir.
- Değerlendirme çıktısı sayısal olmayacağından, bu durum üst yönetim tarafından önceden bilinmelidir.
- Soru/Cevap veya Öneriler ile öncelikler belirlenebilir
- Örnek Önceliklendirme Değerleri : Düşük/Orta/Yüksek
 - Düşük : Kısa sürede telafi edilebilen durumlar için
 - Orta : Organizasyonda orta düzey maddi hasar oluşturan, giderilmesi için maddi harcamalar gereken durumlar için
 - Yüksek : Organizasyon sonlanması, müşteri kaybı veya yasal olarak önemli kayıp oluşturacak durumlar için
- * NIST 800-026

Riske Karşı Davranışı Belirleme

- Riskin Azaltılması
 - Bir önlem uygulanarak veya kullanılarak riskin azaltılması
- Riskin Aktarılması
 - Potansiyel hasar veya durumların sigorta ettirilmesi
- Riskin Kabul Edilmesi
 - Riskin gerçekleşmesi durumunda oluşacak potansiyel kaybın kabul edilmesi
- Riskin Reddedilmesi
 - Riskin inandırıcı bulunmaması ve gözardı edilmesi

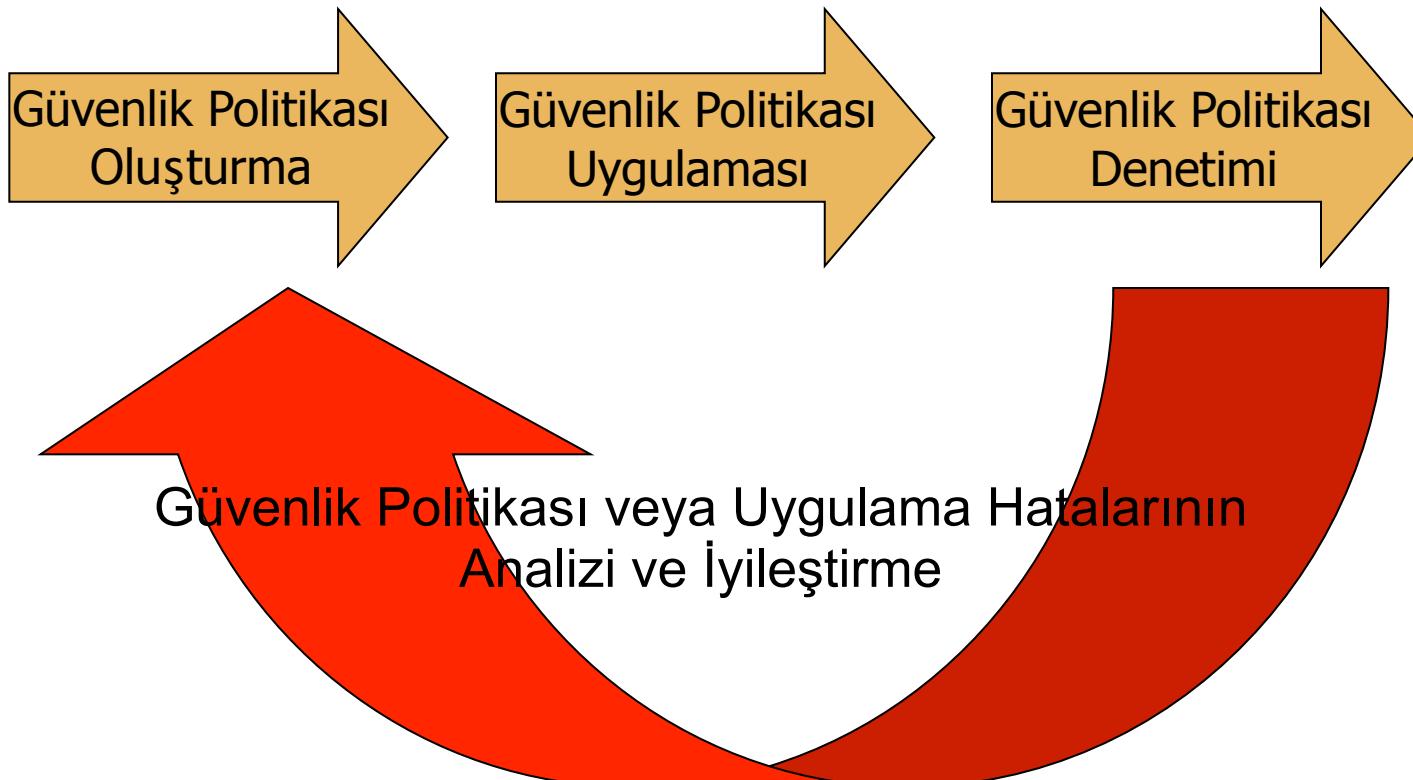
Risk Hesaplaması

Riske karşı davranış belirlenmesinde varlık değeri, hasar boyutu, önlem ve sigorta maliyeti, alınan önlemlerin maliyet etkinliği dikkatle değerlendirilmelidir.

Tehdit x Zaafiyet x Varlık Değeri = Toplam Risk

Toplam Risk - Önlemler = Arta Kalan Risk

Güvenlik Yönetim Süreci



Politika, Prosedür ve Rehberler

- Organizasyonun güvenlik öncelikleri, organizasyon yapısı ve beklentileri yazılı olarak hazırlanmalıdır.
- Üst yönetim, organizasyonun güvenlik önceliklerini belirlemede kilit role ve en üst düzey sorumluluğa sahiptir.
- Hazırlanan politika, prosedür ve rehberler, yasalarla ve sektörel sorumluluklarla uyumlu olmalıdır.
- Hazırlanan dökümanlar, çalışanlardan beklentileri ve karşılanması beklenen sonuçları açıkça ifade etmelidir.

Politikalar

- Güvenlik politikaları için mutlak suretle üst yönetimin onayı alınmalıdır.
- Politikalar, kurumsal güvenlik yaklaşımını ifade eden dökümanların en üstünde yer almaktadır. Bu doğrultuda genel yaklaşım ve olması gerekenler, basitçe ve uygulanabilir biçimde ifade edilmelidir.
- İyi hazırlanmış politikalar, politikanın sorumlularını, ihtiyaç duyulan güvenlik seviyesini ve kabul edilebilir risk seviyesini açıkça belirtmelidir.
- Özel bir durum veya sürece yönelik, kısıtlı tanımlama veya detaylar içermemelidir.

Politika Türleri

- Duyuru Politikaları
 - Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunması hedeflenmektedir.
- Bilgilendirici Politikalar
 - Çalışanların bilgilendirilmesini ve eğitilmesini sağlayarak, görevlerinin ve bekleyenlerin bilincinde olmaları hedeflenmektedir.
- Yasal Politikalar
 - Organizasyonun attığı adımların, yasal ve sektörel sorumluluklar ile uyumlu olmasının sağlanması hedeflenmektedir.

Standartlar, Temel Seviyeler, Rehberler ve Prosedürler

- Standartlar
 - Organizasyon süreçlerinin sahip olması gereken standartların belirlendiği dökümanlardır. Politikalardan daha özel tanımlamalar içermektedir.
- Temel Seviyeler
 - Sistem, ağ veya ekipmanların sahip olması gereken en temel güvenlik seviyelerinin tanımlandığı dökümanlardır.
- Rehberler
 - Bir işin nasıl yapılması gerekiği konusunda öneriler ve yöntemler içeren dökümanlardır. Çalışanların özel durumlarına uygulayabileceği biçimde esnek olmalıdır.
- Prosedürler
 - Bir işin nasıl yapılacağını adım adım belirleyen, işe veya sürece özel, ekipman değişimlerinde güncellenmesi gereken tanımlamaları içeren dökümanlardır.

Politika Uygulamaları

- Üst yönetimin onaylamadığı ve desteklemediği bir işlem uygulanamayacaktır.
- Çalışanlar, üst yönetimin onayının açıkça görülmediği bir işlemi yapmaya gönüllü olmayacaklardır.
- Önemli Adımlar ;
 - Veri Sınıflandırma
 - Roller ve Sorumluluklar
 - Güvenlik Kontrolleri

Veri Sınıflandırma

- Kurumsal gizlilik veya yasal hak içeren bilgiler korunmalıdır. Bu nedenle veri sınıflandırma yapılarak, verilerin sahip oldukları öncelik ve değerler belirlenebilir.
- Her bir veri, kurum için ifade ettiği değer, kullanılamaz hale gelmesi, değiştirilmesi veya ifşa edilmesi durumunda oluşacak zarar dikkate alınarak sınıflandırılmalıdır.
- Farklı sınıflandırma etiket grupları kullanılabilir
 - Sınıflandırılmamış, Kuruma Özel, Gizli, Çok Gizli
- Çalışanların, sahip oldukları güvenlik seviyesine göre verilere erişimine imkan sağlamaktadır.

Roller ve Sorumluluklar

- Roller ve sorumluluklar açıkça ayrılmış olmalıdır, böylece güvenlik ihlallerini yönetmek kolaylaşacaktır.
- Örnek Roller
 - Veri Sahibi
 - Veri İşletmeni
 - Kullanıcı
 - Güvenlik Denetmeni

Güvenlik Kontrolleri

- Güvenlik kontrollerinin amacı, kurumun geliştirdiği güvenlik mekanizmalarının uygulanmasını sağlamaktır.
- Güvenlik Kontrol Türleri
 - Yönetimsel
 - İşe Alım Süreci
 - Çalışan Kontrolleri
 - İşten Çıkarma Süreci
 - Teknik
 - Fiziksel

Eğitim

- Çalışanlar, kurum politikaları, görevleri, sorumlulukları, kullanmakta oldukları ekipmanlar ve gerekli teknolojiler konusunda eğitilmelidir.
 - Kısa Süreli Eğitimler
 - Uzun Süreli Eğitimler
 - Farkındalık Eğitimleri
- Eğitim Süreci Bileşenleri
 - Organizasyonun Hedefleri ve Gereksinim Değerlendirmesi
 - İhtiyaçlar Doğrultusunda Uygun Eğitimin Belirlenmesi
 - Eğitim Yöntemleri ve Araçlarının Belirlenmesi
 - Eğitim Verimlilik Değerlendirmeleri

Denetim

- Organizasyonun sahip olduğu güvenlik altyapısı ve güvenlik yönetim süreci periyodik olarak denetlenmelidir.
- Denetim süreci kullanılarak, politikalar ile uygulamaların uyumluluğu, doğru kontrollerin doğru yerlerde uygulandığı ve çalışanlara sunulan eğitimlerin gerçekten işe yaradığı doğrulanabilir.
- Politika denetimlerinde standart yöntem ve şekiller uygulanması zordur. Ancak uygulanan politikaların uyumlu olduğu standartların denetim süreçleri bu konuda rehberlik sağlayabilir.
- Kurum içi veya bağımsız denetçiler tarafından sağlanabilir.



Sistem Mimarisi ve Modelleri

Sistem Mimarisi ve Modelleri

- Bilgisayar Sistem Mimarisi
- Güvenlik Mekanizmaları
- Denetim Güvenlik Modelleri
- Dökümanlar ve Rehberler
- Sistem Doğrulama

Sistem Mimarilerine Yönelik Sıkıntılar

- Programlama Hataları
 - Bellek Taşmaları (Buffer/Heap/Stack Overflow)
 - Karakter Biçim Tanımlamaları (Format String Attacks)
- Arka Kapılar
- Asenkron Saldırılar
- Gizli Kanallar
- Artımlı Saldırılar
- Servis Engelleme

Güvenlik Mekanizmaları

Tehditlere çözüm olarak, süreçler ve uygulamalar için güvenlik mekanizmaları oluşturulmuştur. Temelde sağlanan güvenlik ile çok sayıda saldırı daha başlamadan engellenecek veya etki alanı azaltılmış olacaktır.

- Süreç Ayrımı
- Operasyon Durumları
- Koruma Halkaları
- Güvenilir Bilgisayar Temelleri

Süreç Ayrımı

- Süreç ayırmı, her bir sürecin bellek bölgelerinin belirlenmesi ve bellek sınırlarının yönetilmesi işlemidir.
- Sistem güven seviyesini yönetmek için süreç ayırmı gereklidir. Çok seviyeli güvenlik sistemi olarak sertifikalanmak içinde süreç ayırmı desteklenmelidir.
- Süreç ayırmı yapılmaz ise kötü niyetli bir süreç sistemde bulunan daha önemli süreçlere ait verileri okuyabilir, değiştirebilir veya sistemin kararlılığını etkileyerek çökmesine neden olabilir.
- Sanal makineler, süreç mantıksal/fiziksel olarak süreç ayırmı uygulanan sistemlerde, kullanıcıları/süreçleri tüm sisteme erişebildiklerine inandırabilir.

Operasyon Durumları

- Bilgiler farklı önem seviyelerindedir; bu nedenle sistemler hassas bilgileri işlerken veya kaydederken, hassasiyetine uygun hareket etmelidir. Bu görevlerin uygulama biçimlerini yönetici veya sistemin kendisi belirler.
- Tek durumlu sistemlerde bilgilerin hassasiyet seviyesi eşit kabul edilir. Bilgilerin işlenmesi konusunda yönetim sorumluluğu, sistemlerin yönetim politikalarını ve prosedürlerini hazırlayan yöneticidir. Genellikle adanmış ve tek amaçlı sistemler olurlar.
- Çok durumlu sistemlerde, bilgilerin işleyışı için yöneticiye ihtiyaç yoktur. Farklı hassasiyet ve güvenlik seviyeleri belirlenmiş ve uygulanmaktadır. Süreçler kompartmanlanmıştır, bilgiler gerektiği kadar bil prensibi ile dağıtılır.
- Beklenmeyen Operasyon Sonlanması :
 - Fail Safe (Bir süreç hata üretirse, tüm servisler ve sistem durdurulur)
 - Fail Soft (Bir süreç hata üretirse, sadece kritik olmayan servisler durdurulur)
 - Fail Open (Bir süreç hata üretirse, sistem çalışmaya devam eder)

Koruma Halkaları

- İşletim sisteminin , sistem bileşenlerine duyacağı güveni belirlemek amaçlı oluşturulmuştur. Güven seviyeleri şeklinde planlanmıştır. Sadece konsept için kullanılmaktadır, bazı özel işletim sistemi veya sistemler tarafından kullanılmaktadır.
- Güven seviyesi oranında komutlar işlenecektir, halka modelinin dışına doğru yetkiler azalmaktadır.
 - Halka 0 (İşletim Sistemi Çekirdeği, En Yetkili Bölüm)
 - Halka 1 (İşletim Sisteminin Yetkisiz Çalışacak Bileşenleri)
 - Halka 2 (Gird/Cıktı İşlemleri, Sürücüler, Düşük Seviye İşlemler)
 - Halka 3 (Ağ servisleri, Uygulamalar, Kullanıcı İşlemleri)

Güvenilir Bilgisayar Temelleri

- Güvenilir Bilgisayar Temeli (Trusted Computing Base - TCB), sistemin koruma mekanizmalarının olması ve sistem güvenlik politikalarının uygulanması için sorumlu olmaları anlamına gelir.
- Güvenilir Bilgisayar Temeli, Gizlilik ve Bütünlüğü Hedeflemektedir.
- 4 Temel Fonksiyon Vardır :
 - Girdi/Çıktı Operasyonları
 - Çalışma Alanları Değişimi
 - Bellek Koruması
 - Süreç Etkinleştirmesi
- Referans monitörü önemli bir bileşendir, sadece yetkili süreçlerin nesne erişimlerini ve kullanımlarını sağlar. Referans monitörü, sistemin kalbi olan ve tüm erişim isteklerini yöneten güvenlik çekirdeği ile uygulanır.
- Güvenlik Çekirdeğinin Sağlaması Gereken Özellikler :
 - Tüm erişimlerin denetimi yapmalı
 - Değişim ve düzenlemeye karşı kendisini korumalı
 - Doğru yapılandırıldığı test edilmeli, doğrulanmalı

Denetim Güvenlik Modelleri

- Denetim güvenlik modelleri, kimin/nezin nesnelere erişileceği, nasıl erişebileceği ve erişince neler yapabileceğini, bir politika dahilinde gizlilik ve bütünlük zorlamalarıyla sağlamaktadır.
- Bütünlük
 - Biba
 - Clark-Wilson
- Gizlilik
 - Bell-LaPadula
 - Take-Grant Model
 - Brewer and Nash

Dökümanlar ve Rehberler

- Rainbow Series
 - NSA (NCSC) tarafından hazırlanmışlardır
 - Orange Book (TCSEC) - Gizlilik - Tekil sistem
 - Red Book (TNI) - Gizlilik + Bütünlük - Ağ
- ITSEC
 - Avrupa standartı, gizlilik+bütünlük+erişilebilirlik sağlamayı hedefler
 - 10 F (işlevsellik), 7 E (garanti) sınıfı bulunur
 - F1-5 ve E0-6 birlikteliklerinin TCSEC'te karşılığı vardır
 - F6-10 arası ise bütünlük ve erişilebilirliği tanımlar
- Common Criteria
 - ISO tarafından hazırlanan çok sayıda standarta çözümdür
 - ISO 15408, EAL 0-7
- ISO27001-27002

ISO 27001

1. Risk Değerlendirme ve Tehditlendirme
2. Güvenlik Politikası
3. Güvenlik Organizasyonu
4. Varlık Yönetimi ve Sınıflandırma
5. İnsan Kaynakları Yönetimi
6. Fiziksel ve Çevresel Güvenlik
7. İletişim ve Operasyon Güvenliği
8. Erişim Denetimi
9. Bilgi Sistemleri Temini, Geliştirilmesi ve Yönetimi
10. Güvenlik İhlal Yönetimi
11. İş Devamlılık Yönetimi
12. Yasalar ve Standartlarla Uyumluluk

Sistem Doğrulama

- %100 güvenlikten bahsedilemez, her zaman bir risk vardır
- Bilgi güvenliği yöneticileri ve uzmanları, riskleri anlamalı, değerlendirmeli ve nasıl karşılamaları gerektiğini bilmelidir
- Sistemlerin sahip olmaları gereken güvenlik seviyeleri belirlenmeli, düzenli aralıklarla denetimler ve risk değerlendirmeleri yapılmalı
- Kurumlar, çalışıkları sektörlerine bağlı olarak, sistemlerinin güvenlik seviyelerini taahhüt veya belgelemek durumunda olabilirler
 - Sarbanes & Oxley
 - Basel I-II
 - Gramm-Leach-Bliley Act
 - ISO27001
 - Cobit



Erişim Denetimi

Erişim Denetimi

- Erişim Denetimine Yönelik Tehditler
- Erişim Denetim Tipleri
- Kimliklendirme, Doğrulama, Yetkilendirme
- Merkezi Doğrulama
- Veri Erişim Denetimi
- Saldırı Tespit/Önleme Sistemleri
- Sistem ve Ağ Sızma Testleri

Erişim Denetimi

- Erişim denetimi kullanılarak, çalışanların ve diğer kişilerin yetkileri oranında kaynaklara erişebilmesinin sağlanması ve yetkisiz erişimlerin engellenmesi hedeflenmektedir.
- Teknik veya Fiziksel Erişim Denetim Yöntemleri
 - Biyometrik Sistemler, Kullanıcı/Şifre Kullanımı, Merkezi Doğrulama vb.
- Erişim Denetim Yöntemlerine Saldırılar
 - Servis Engelleme, Kimlik Sahteciliği, Şifre Kırma
- Saldırı Tespit/Önleme Sistemleri

Erişim Denetimine Yönelik Tehditler

- Saldırılarda en çok hedef alınan sistemler erişim denetimi sistemleridir.
- Şifre Saldırıları
 - Sözlük Saldırıları
 - Deneme/Yanılma Saldırıları
 - Pasif Şifre Kırma Saldırıları
- Elektrik Sinyalleri Sızması
 - TEMPEST
- Servis Engelleme Saldırıları
 - Tekil Servis Engelleme Saldırıları
 - Dağıtık Servis Engelleme Saldırıları

Erişim Denetim Tipleri

- Yönetimsel
 - Şifre politikaları, işe alım / işe son verme süreçleri, kullanıcı farkındalık eğitimleri vb.
- Teknik
 - Çok faktörlü doğrulamalar, kriptolama, ağ izolasyonu, DMZ, anti-virus sistemi vb.
- Fiziksel
 - Kamera sistemleri, kilitler, güvenlik görevlileri vb.

Kimliklendirme, Doğrulama, Yetkilendirme

- Kim Giriş İstiyor, Kimliği Doğrumu, Yetkileri Neler ?
- Kimliklendirme; kullanıcının sistemlerde bir kimliğe sahip olması süreci
- Doğrulama; kullanıcı kimliğinin sistemlerdeki geçerliliğinin doğrulanması süreci
- Yetkilendirme; kullanıcının geçerliliği doğrulanın kimliğinde sahip olduğu yetkilerin kullanıcıya atanması süreci

Doğrulama

- Yöntemler
 - Kullanıcı Adı / Şifre
 - Tek Kullanımlık Şifre Cihazları
 - Akıllı Kartlar
 - Manyetik Kartlar
 - Sertifikalar
 - Biyometrik Sistemler
- Çok Faktörlü Doğrulama
 - Bildiğiniz Şey (Şifre, Pin)
 - Sahip Olduğunuz Şey (Sertifika, Akıllı Kart, OTP Cihazları)
 - Olduğunuz Şey (Biyometrik Sistemler)

Doğrulama Yöntemleri

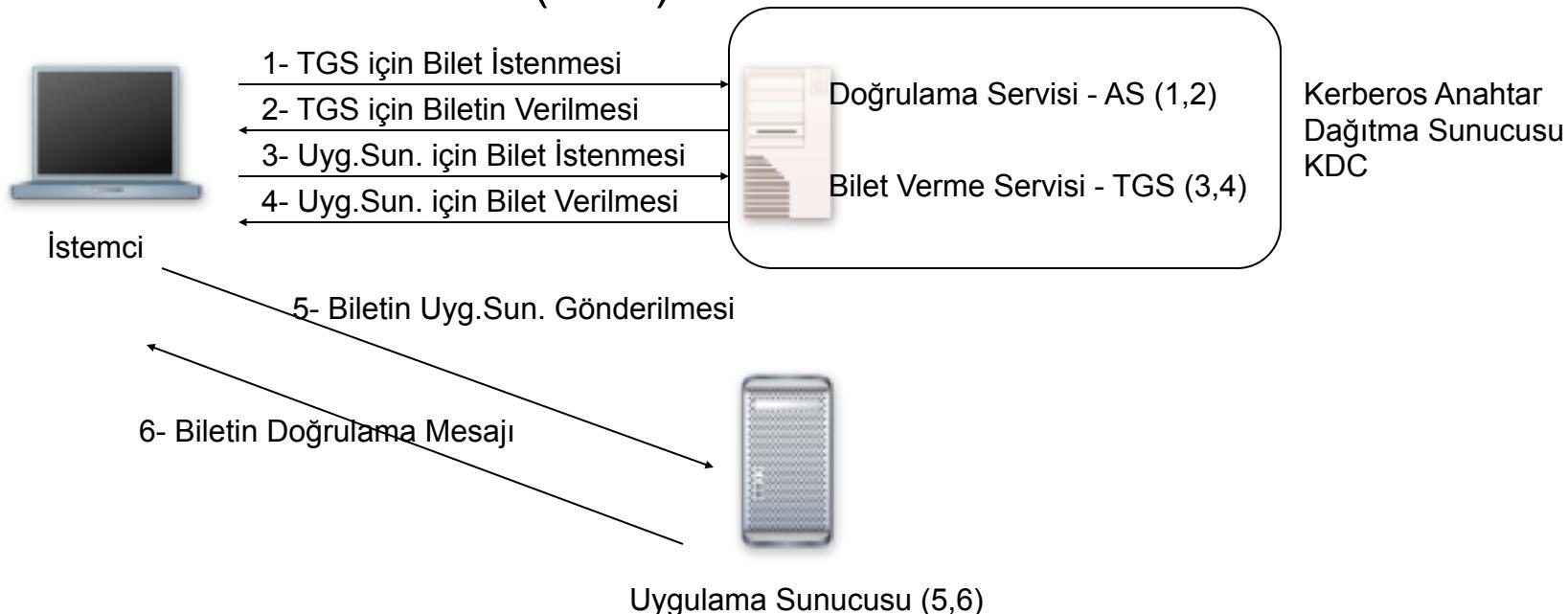
- Şifreler
 - Düz Şifre, Şifre Karmaşıklığı, Şifre Politikaları
- Ardışık Sorularla Doğrulama
- Tek Seferlik Şifre Cihazları
 - Senkron
 - Asenkron
- Biyometrik Sistemler
 - Parmak izi, El geometrisi, Avuç içi, İris, Retina, Ses, Klavye Hareketi
 - Kullanıcıların Kabulü, Yaş, Cinsiyet, Fiziksel Engeller
 - Hata Türleri, Tip 1, Tip 2, CER

Merkezi Doğrulama

- Sorun : Çok sayıda kullanıcı, çok sayıda kullanıcı hesabı, birçok şifre, çok sayıda sistem ve ağ servisi
- Merkezi doğrulama, tek bir sistemde kullanıcı kimliklerinin bulunması, ağ ve sistem servislerinin doğrulamayı bu sistem üzerinden yapması sürecidir.
- Kullanıcı sadece merkezi doğrulama sunucusuna giriş yapar, istekte bulunduğu sistem ve ağ servisleri kullanıcının geçerliliğini merkezi doğrulama sisteme sormaktadır.
- Kerberos, SESAME, Krypto Knight (IBM) ve NetSP, Thin Client

Kerberos

- MIT tarafından 1985'te geliştirildi. Üç temel bileşen var; istemci, sunucu ve KDC (Anahtar Dağıtma Sunucusu)
- Anahtar Dağıtma Sunucusu (KDC)
 - Doğrulama Servisi (AS)
 - Bilet Verme Servisi (TGS)



Kerberos'un Zaafiyetleri

- Dağıtık bir yapı olmasından dolayı Devamlılık ve Erişilebilirlik sorunları oluşabilmektedir.
- Zaman temelli bir servis olması, tüm doğrulamala ve bilet geçerliliklerinde zaman kısıtı olmasından dolayı ağ üzerinde zaman senkronizasyonu oldukça iyi yapılmalıdır.
- Bir saldırgan doğrudan Kerberos sunucusuna saldırarak, tüm servislere erişim hakkı kazanabilir.
- Kerberos sunucusu “tek noktada hata” sebebidir, yedekleme veya kümeleme gerekebilir.
- Ortadaki adam saldırılardan etkilenebilmektedir.
- Kullanılan DES algoritması kırılabilmektedir; ancak bu sorun 5. sürüm ile ortadan kalkmıştır
- İstemcinin bağlanacağı sunucu/servis, istemcinin hakları hakkında bilgi sahibi olmalıdır. Kerberos yetkilendirmeyi kapsamamaktadır.

Erişim Denetim Modelleri

- Merkezi Erişim Denetimi

Kullanıcı kimlikleri, hakları ve izinleri tek bir merkezden yönetilir.

Erişim kararlarını tek bir sistem verir

Servis sahibi hangi kullanıcıların erişebileceğine karar verir, merkezi yönetim içerik sağlar.

RADIUS, TACACS, LDAP

- Dağıtık Erişim Denetimi

- Kullanıcı kimlikleri, hakları ve izinleri ağ üzerinde farklı yerleşimlerde bulunur.

- Kaynağa en yakın olan merciye yönetim devredilir. (Bölüm Yöneticisi gibi.)

- Çok sayıda alan ve güven ilişkisi yönetilebilir.

- Erişim istekleri merkezi olarak yönetilmez.

- Ağlar arası ilişkilerde, veritabanı yönetim sistemlerinde kullanılır.

- Hatalı standartlaşma veya güven ilişkisi beraberinde güvenlik açıkları getirir.

RADIUS

- Remote Authentication and Dial-In User Service (1997)
RFC2058-2059
- Merkezi olarak Doğrulama (Authentication), Yetkilendirme (Authorization) ve Hesap Yönetimi (Accounting) servislerini sunar.
- Tüm kullanıcı profilleri merkezi olarak tutulur ve UDP temelli doğrulama servisi ile diğer sistemlere sunulur.
- Uzak Erişim (RAS) ve kablosuz ağlarda sıkılıkla kullanılmaktadır.

RADIUS'un Çalışma Prensipleri

- İstemci, RADIUS istemcisine bağlanarak kullanıcı bilgilerini verir.
- RADIUS istemcisi kullanıcı bilgilerini kriptolayarak RADIUS sunucusuna aktarır.
- RADIUS sunucusu bilgileri doğrular, reddeder veya ek bir işlem yapılmasını talep eder.
- Bilgiler doğrulanırsa istemci istenen kaynağa erişebilir.



LDAP

- Lightweight Directory Access Protocol (1993)
- Kullanıcı ve sistem profilleri merkezi olarak tutulur, LDAP protokolü aracılığıyla diğer sunucu ve servislere sunulur.
- Merkezi doğrulama yapılabilmektedir.
- Dizin sistemleri tarafından desteklenmekte ve yaygın olarak kullanılmaktadır.
 - Distinguished Name (DN), Her girdinin tekil doğrulayıcısıdır.
cn=Fatih Ozavci, ou=Guvenlik, dc=gamasec, dc=net
- Kullanıcı bilgilerinin sorgulanması amaçlı sıkça kullanılmaktadır.

Veri Erişim Denetimi

Veri erişim denetimi

- verilere nasıl erişilebileceğini,
- kimlerin erişebileceğini,
- erişince neler yapabileceklerini tanımlamaktadır.

- Mandatory Access Control (MAC)
- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)
- Ruleset-Based Access Control (RSBAC)



İletişim ve Ağ Güvenliği

İletişim ve Ağ Güvenliği

- İletişim ve Ağ Güvenliği
- Ağ Güvenliğine Yönelik Tehditler
- Yerel Ağ ve Bileşenleri
- Uzak Alan Ağı ve Bileşenleri
- Ağ Modelleri ve Standartlar
- TCP/IP Protokol Ailesi
- Ağ Cihazları
- Uzak Erişim
- IPSEC
- Mesajlaşma Güvenliği
- Ağ Erişim Denetimi

İletişim ve Ağ Güvenliği

- İletişim ve ağ altyapıları, birden fazla sistem veya ağın haberleşmesi için hayatı öneme sahiptir.
- İletişim Altyapısı Bileşenleri
 - Temel Ağ Cihazları
 - Ağ Protokolleri
 - Ses İletişim Sistemleri
 - Uzak Erişim Sistemleri
 - Kriptolama
 - Ağ Güvenlik Cihazları

Ağ Güvenliğine Yönelik Tehditler

- Servis Engelleme Saldırıları
 - SYN Flood, Land, Teardrop, Smurf, PoD, DDOS
- Bilgi Elde Etme
 - Sniffing, ARP/DNS Spoofing, Phishing, War Dialing/Driving, Virus/Worm/Spyware
- Zarar Verme, Veri Değişimi, Hırsızlık
 - Veritabanı Saldırıları, Cep Telefonu Saldırıları, Kimlik Hırsızlığı, Şifre Kırma, Yetki Yükseltimi, Para Değişim Saldırıları, Yazılım Korsanlığı, Oturum Yakalama, Spam

Yerel Ağ ve Bileşenleri

- İletişim Protokolleri
 - IEEE 802 Ailesi
- Ağ Topolojileri
 - Bus
 - Yıldız
 - Ring
- Kablolama
 - Coaxial
 - Twisted Pair
 - Fiber-optic
- Kablosuz Ağlar (802.11)
- Bluetooth

Uzak Alan Ağı ve Bileşenler

- Bölgeler ve uzak mesafelerde yer alan yerel ağları birbire bağlar
- Paket Anahtarlama
 - X.25 (Paket anahtarlama, Analog, Telefon Hatları, 56Kbps)
 - Frame Relay (Sanal devre anahtarlama, PVC/SVC)
 - ATM (Hücre anahtarlama, 53-Byte)
 - VOIP (Paket anahtarlama, IP üzerinden ses)
- Devre Anahtarlama
 - POTS (Analog, 9.6-56Kbps)
 - ISDN (B(64K)/D(16K) Kanalları, BRI(128Kbps), PRI (1.544 M)
 - T Taşıyıcıları (Kiralık Hatlar, T1 (24xDS0[64K]), T3 (672xDS0[K])
 - xDSL (simetrik =IDSL, HDSL, SDSL, asimetrik = ADSL, VDSL)
 - Kablo Modemler

Ağ Modelleri ve Standartlar

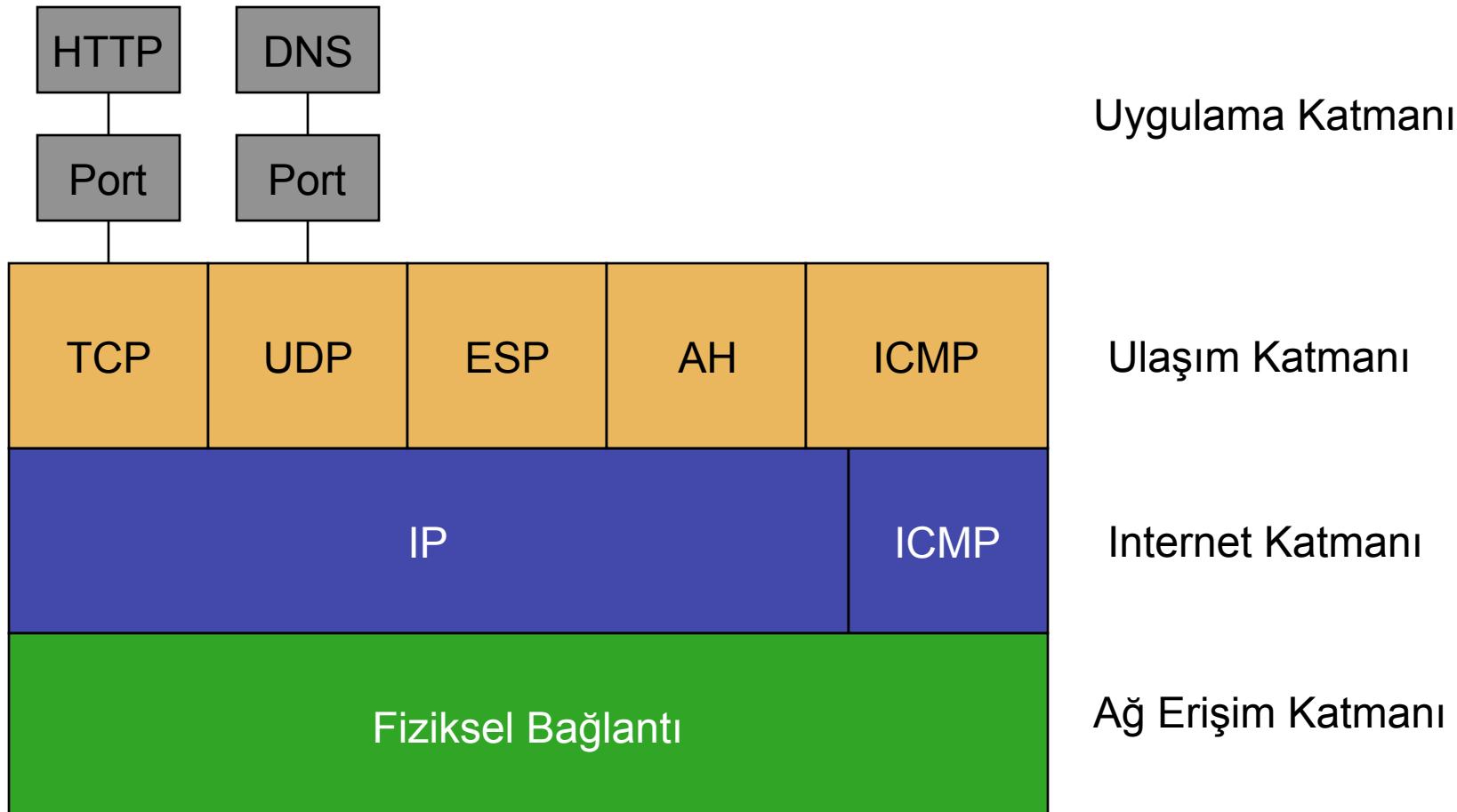
OSI Katmanları

Uygulama Katmanı	Http, Ftp, Smtp, Mail, Web
Sunum Katmanı	Veri Kriptolama, Çözme, Çevrim
Oturum Katmanı	RPC, SQL
Taşıma Katmanı	TCP, UDP, ESP, AH
Ağ Katmanı	IP, Yönlendirici, Güvenlik Duvarı
Veri Bağı Katmanı	Switch, Ağ Kartı, ARP
Fiziksel Katman	Kablolama, Hub

TCP/IP Protokol Ailesi

- 1982'de DOD tarafından standartlaştırıldı.
- Katmanlar
 - Ağ Erişim Katmanı (OSI 1 ve 2'ye karşılık gelmektedir)
 - Internet Katmanı
 - IP (X.X.X.X/Y - 10.0.0.0, 172.16-32.0.0, 192.168.0.0, 127.0.0.0)
 - ICMP (Echo, Time Stamp, Redirect, Destination Unreachable vs.)
 - ARP (MAC/IP Çevrimi, Doğrulama Yapmaz)
 - Ulaşım Katmanı
 - TCP (Oturum Temelli, Sıra Numarası, Bayraklar)
 - UDP (Sorgulama Temelli, Sorgu Numarası)
 - Uygulama Katmanı
 - HTTP, SMTP, FTP vb.

TCP/IP Şeması ve Protokol Bağlantıları



Ağ Cihazları

- Hub
 - Fiziksel Katman, Standart Bağlantı Bileşeni, Güvenlik Bulunmuyor
- Bridge
 - Veri Bağı Katmanı, Uzak Mesafelerde Kullanılıyor
- Switch
 - Veri Bağı Katmanı, Port Anahtarlama Yapıyor, Yönetilebilir, VLAN Oluşturulabilir
- Yönlendirici (Router)
 - Ağ Katmanı, IP veya IPX Yönlendirmesi, RIP/OSPF/BGP
- Modem
 - Fiziksel Katman, Farklı Bağlantı Türlerinde Kullanılabilir



Uzak Erişim

- PPP (Point to Point Protocol)
 - 1994 IETF, her bağlantı türünde ve hızında çalışabilir.
- Doğrulama Protokolleri
 - PAP (Düz Metin, Kullanıcı Adı / Şifre)
 - CHAP (3 Yollu Doğrulama, MD5, MS-CHAP)
 - EAP (Sertifika, OTP, MD5 vb.)
 - Merkezi Doğrulama (RADIUS, TACACS)
- Sanal Özel Ağlar
 - Güvensiz ağlardan güvenli iletişim
 - Ağlar arası veya istemciler arası yapılabilir
 - PPTP, L2TP, IPSEC, SSL-VPN, MPLS

IPSEC Protokolü

- En sık kullanılan sanal özel ağ sistemidir
- Protokoller
 - IKE/ISAKMP (TCP/500, Anahtar Değişimleri ve Doğrulama)
 - ESP (İletişim İçeriğinin Filtrelenmesi)
 - AH (Başlık Bilgilerinin Filtrelenmesi)
- Bağlantı Türleri
 - Transport (İstemciler arası kullanım)
 - Tunnel (Ağlar arası bağlantı, IPSEC sunucusu ağ geçidi olur)
- L2TP, IPSEC üzerinden tunnellenebilir
- Standart olmasa da X509 v3 sertifikalarını çoğu IPSEC sunucusu destekler

Mesajlaşma Güvenliği

- Gereklilik
 - İnkar Edilemezlik
 - Gizlilik
 - Bütünlük
- PGP (Pretty Good Privacy)
 - Phil Zimmerman 1991
 - Otorate Gereksinimi Yoktur, Güven Anahtar Kullanıcısına Bağlı
 - MD5/SHA1, DES/3DES/AES, Diffie-Hellman, RSA, DSS
- S/MIME (Secure Multipurpose Internet Mail Extensions)
 - x.509 Sertifikaları Kullanılır
 - Sertifika Otoritesi Gereklidir
- PEM (Privacy Enhanced Mail)
 - Kullanılmıyor, x.509 Temelli Anahtar Yönetimi

Ağ Erişim Denetimi

- Güvenlik duvari (Firewall), ağ iletişiminde erişim denetimi işlemi için kullanılan sistemlere verilen genel isimdir
 - Yönlendirici
 - Switch
 - Güvenlik Duvarı
- Güvenlik Duvarı Mimarileri
 - Statik Paket Filtreleme
 - Dinamik Paket Filtreleme
 - Proxy
 - Uygulama Seviyesi Proxy
 - Devre Seviyesi Proxy
 - SOCKS Proxy
- Ağ Adres Çevrimleri
 - NAT (Network Address Translation)
 - PAT (Port Address Translation)
- DMZ (De-Militarized Zone)



Uygulama ve Sistem Geliştirme Güvenliği

Uygulama ve Sistem Geliştirme Güvenliği

- Uygulama Güvenliğine Yönelik Tehditler
- Dosya Sistemi Değişim Kontrolleri
- Operasyon Durumları
- Sistem Geliştirme Yaşam Çevrimi
- Yazılım Geliştirmeye Modelleri
- Değişim Yönetimi
- Programlama Dilleri
- Veritabanı Yönetimi
- Veritabanı Kavramları

Uygulama Güvenliğine Yönelik Tehditler

- Virüs/Worm/Truva Atı/Casus Yazılım
- Bellek Taşmaları (Buffer/Heap/Stack Overflow)
- Karakter Biçim Tanımlamaları (Format String Attacks)
- Değiştirilmiş Girdi Saldırıları (SQL/Command/Xpath Injection, XSS)
- Servis Engelleme Saldırıları
- Asenkron Saldırılar
- Arka Kapılar
- Gizli Kanallar
- Servis Engelleme

Dosya Sistemi Değişim Kontrolleri

- Düzenli Yedekleme
- Değişimlerde Geri Dönüş Gereksimi
- Dosya Sisteminde Aralıklı Değişim Kontrolü
 - Dosyaların HASH bilgileri oluşturulur ve kaydedilir
 - Aralıklı olarak yeni HASH'ler oluşturulur ve kontrol edilir
 - Değişimler gözlenir, kritik dosyalardaki değişim incelenir
 - HASH Algoritmaları
 - Checksum
 - MD5
 - SHA-1

Operasyon Durumları

- Uygulamalara yönelik saldırıların büyük bölümü, uygulama veya alt sürecin sonlanmasını takiben komut çalıştırılmasına dayanmaktadır
- Beklenmeyen Operasyon Sonlanması :
 - Fail Safe (Bir süreç hata üretirse, tüm servisler ve sistem durdurulur)
 - Fail Soft (Bir süreç hata üretirse, sadece kritik olmayan servisler durdurulur)
 - Fail Open (Bir süreç hata üretirse, sistem çalışmaya devam eder)
- Yazılımların geliştirilmesinde, işletim sisteminin sağlamış olduğu oturum davranışları ile paralel hareket edilmelidir

Sistem Geliştirme Yaşam Çevrimi

- Sistem Geliştirme, her aşamasında ihtiyaç duyulan güvenlik gereksinimlerinin belirlenmesi ve uygulanması gereken bir süreçtir
- Standartlar
 - NIST 800-64, "Security Considerations in the Information System Development Life Cycle,"
 - NIST 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems."
- NIST 800-14'e Göre Sistem Geliştirme Aşamaları
 - Proje İlklenidleme
 - Geliştirme/Temin
 - Uygulama
 - Operasyon/Bakım
 - Sonlandırma

Proje İkklendirme

- Proje Ekibi Oluşturulması
- Projenin Hedefinin Tüm Ekip Üyelerince Anlaşılması
- Proje Başlangıç, Bitiş ve Diğer Aşamalarının Planlanması
- İşlenecek Bilgilerin Hassasiyet Seviyesinin Belirlenmesi
- Süreç İçinde Karşılaşılabilecek Riskler ve Sonuçlarının Analizi

Geliştirme / Temin

- Bu Aşamada Sistem Tasarlanır, Geliştirilir, Programlanır ve/veya Temin Edilir.
- Programlama Güvenliğine Hassasiyet Gösterilir;
 - Girdi/Çıktı İşlemleri
 - Girdi Türleri Belirlenmesi
 - Aktarım/Oturum Kullanımı
 - Hata Saptama ve Düzeltme
 - Geçerlilik Kontrolleri
 - Yetkilendirme Kontrolleri
 - İzleme Mekanizmaları
 - Dosya Koruma Şemaları
- Çalışılacak Platformun Kısıtlamalarına Güvenilmelidir

Kabul Edilebilirlik Testi ve Uygulama

- Yazılım geliştirme sonrası kabul edilebilirlik testleri uygulanmalıdır
 - Geliştiriciler
 - Güvenlik Ekibi
 - Diğer Ekip Üyeleri
- Kabul edilebilirlik testlerinde “görev ayımı” uygulanmalıdır. Aynı ekip tarafından geliştirme, düzenleme ve doğrulama yapılmamalıdır
- Kalite kontrol mühendisleri, programcılar ve proje ekibinin onayının ardından sistem yerleştirme için hazır hale getirilir

Operasyon / Bakım

- Sistem/Uygulama planlanan platforma aktarılır
- Hazırlanan platform için Sertifikalandırma ve Onaylama gereksinimi
 - Teknik sertifikalandırma, sistem güvenliğinin, güvenlik bileşenlerinin, koruma mekanizmalarının ve üretici/müşteri memnuniyeti için gerekli standartların kontrol edilerek belgelenmesi adımıdır
 - Onaylama aşaması, Sistem/Uygulamanın istenen biçimde ve şartlarda çalıştığını yönetim resmi onayından geçmesidir

Sonlandırma

- Sistem veya uygulama için gerekmeyen verilerin yok edilmesi aşamasıdır
- Sonlandırma Aşamaları
 - Uygulamaların Sonlandırılması
 - Yedek/Arşiv Bilgilerinin Temizlenmesi
 - Disk Temizlenmesi
 - Ekipmanların Sonlandırılması
- Disk üzerinden veri silmek yeterli değildir, kazımak olarak bilinen “WIPE” işlemi yapılmalı ve verinin tekrar erişilemeyecek durumda olduğu doğrulanmalıdır

Yazılım Geliştirme Modelleri

- Waterfall
 - Aşamalardan oluşur, belgeleme kolaydır, büyük projelerde uygulanması zordur
- Spiral
 - 1988, Barry Boehm, Aşamalardan oluşur, her aşama kendi risk değerlendirmesine sahiptir, müşteri tarafından inceleme yapılır, proje ilerlemesi yavaştır
- JAD (Joint Application Development)
 - 1977, IBM, Kullanıcılar ve geliştiricilerin beraber bulunduğu ortamda geliştirme yapılır,
- RAD (Rapid Application Development)
 - Hızlı yazılım geliştirme, zaman limiti olan projelere uygundur, hızlı karar verme gerektirir, kritik projelerde kullanılmamalı
- CASE (Computer-Aided Software Engineering)
 - Yazılım geliştirme araçlarıyla sistematik analiz, tasarım, geliştirme ve uygulama yapılır, büyük ve karmaşık projelere uygundur, geliştiricilerin eğitimi gereklidir

Değişim Yönetimi

- Yazılım geliştirmenin önemli bir bileşenidir
- Geliştirme ekibi ve dış katılımcılara ait değişimlerin senkronize olması ve tüm değişim endişelerinin tartışılmamasını sağlamaktadır
- Aşamalar ;
 - Değişim yönetimi süreci ve yöntemlerinin belirlenmesi
 - Değişim isteklerinin alımı
 - Değişimlerin uygulanmasının planlanması ve belgelenmesi
 - Değişimlerin uygulanması ve izlenmesi, Gerekliyorsa ek değişim önerilerinin belirlenmesi
 - Uygulanan değişimlerin incelenmesi ve raporlanması
 - Gerekliyorsa değişim yönetim sisteminde düzeltmeler yapılması



Kriptolama

Kriptolama

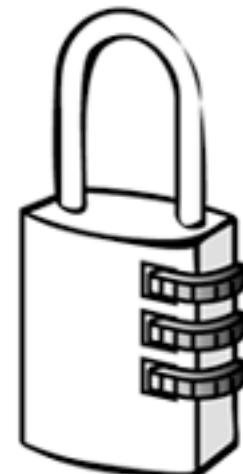
- Kriptolama
- Kriptolama Tarihi
- Simetrik Kriptolama
- Asimetrik Kriptolama
- Bütünlük ve Doğrulama
- Açık Anahtar Altyapısı (PKI)
- Kriptografi Kullanılan Servisler
- Kriptografi Saldırıları

Kriptografi Saldırıları

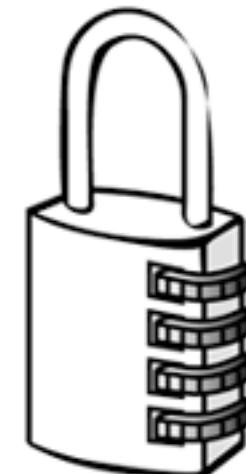
- Bilinen Düz Metin Saldırısı
- Sadece Çevrilmiş Metin Saldırısı
- Doğum Günü Saldırısı
- Ortadaki Adam Saldırısı
- Seçilmiş Çevrilmiş Metin Saldırısı
- Tekrarlama Saldırısı

Kriptolama

- İlk olarak gizlilik için ihtiyaç duyulmuştur. Daha sonra bütünlük ve inkar edilemezlik gereklilikleri ortaya çıkmıştır
- Kriptolama Kavramları
 - Algoritma
 - Kriptografik Anahtar
 - Kriptolama
 - Kriptoanaliz
 - Sayısal İmza
 - Düz Metin
 - Çevrilmiş Metin
- Düz Metni Çevirme Yöntemleri
 - Blok
 - Akış



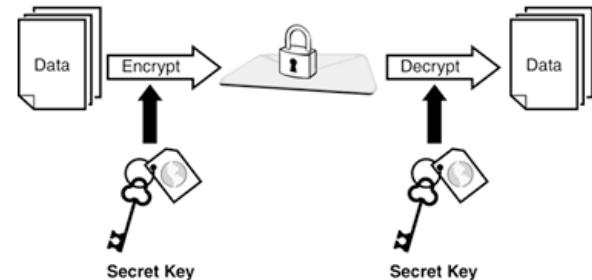
Three-digit lock



Four-digit lock

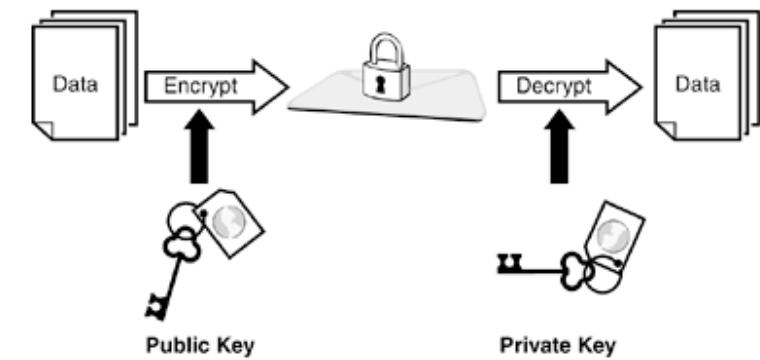
Simetrik Kriptolama

- Paylaşılan tekil bir anahtar ile kriptolama yapılması işlemidir
- En eski kullanım yöntemidir, Sezar ve Scytale simetrik kriptolamadır
- Algoritmalar
 - DES 56 Bit (ECB, CBC, CFB, OFB)
 - 3DES 168 Bit (EEE2, EDE2, EEE3, EDE3)
 - AES 128/192/256 Bit
 - IDEA 128 Bit
 - Blowfish 448 Bit
 - Twofish
 - RC4 128 Bit (Blok) RC5 2040 Bit (Akış,



Asimetrik Kriptolama

- Kriptolama ve çözme anahtarları farklıdır, her taraf için bir açık/genel bir gizli/özel anahtar bulunmaktadır
- Asimetrik kriptolamada en önemli sorun açık anahtar dağıtımıdır
- Kriptolamada göndericinin gizli anahtarı ve her alıcının açık anahtarları kullanılır. Çözmede her alıcı kendi gizli anahtarını kullanır.
- Algoritmalar
 - Diffie-Helman
 - El Gamal
 - ECC (Elliptic Curve Cryptosystem)
 - RSA



Bütünlük ve Doğrulama

- Veri Özетleri
 - MD Ailesi (MD2, MD4, MD5)
 - SHA Ailesi (SHA-1, SHA-256, SHA-512)
 - HAVAL
 - HMAC (Hashed Message Authentication Code)
- Sayısal İmza
 - MAC (Message Authentication Code)
 - DSA (Digital Signature Algorithm)

Stenografi

- Stenografi, gönderilecek bilginin bir başka dosyanın içeriğinde gizlenmesi işlemidir
- Genellikle resim dosyaları kullanılır
- Önemsiz birkaç bit değiştirilerek veri kaydedilir, dosyayı işleyen yazılım değişiklik farketmez ve resim ise görüntüde bozulma olmaz
- “*USA Today*” gazetesi 11 Eylül saldırılarını düzenleyen El Kaide terör örgütünün stenografi kullanarak haberleştiğini iddia etmiştir

Açık Anahtar Altyapısı (PKI)

- Bileşenler
 - Sertifika Otoritesi (CA)
 - Kayıt otoritesi aracılığıyla gelen sertifika isteklerini doğrular
 - Sertifika talep edenin kimliğinin geçerliliğini doğrular
 - Kişi ile açık anahtarın uyuştuğunu gösteren bir sertifika oluşturur
 - Kayıt Otoritesi (RA)
 - Sertifika talebini kabul eder, talep edenin kimliğini doğrular, sertifika otoritesine isteği ve kimliği iletir
 - Sertifika Geçersizlik Listeci (CRL)
 - Sayısal Sertifika
 - x.509 v3, açık anahtarın bütünlüğünü, sertifikada bulunan bilgiler ile açık anahtarın örtüşüğünü kanıtlar.
 - Sertifika Dağıtım Sistemi
- Kurum içi kullanım (Sertifika üretimi, dağıtımı, kurulumu, depolanması, değişimi, kontrolü, sonlandırılması)

Kriptografi Kullanılan Servisler

- Güvenli E-Posta
 - PGP, S/MIME, PEM
- Uygulama Katmanı Çözümleri
 - SSH, S-HTTP, SET
- Taşıma Katmanı Çözümleri
 - SSL, TLS
- IPSEC
 - ESP, AH, IKE (ISAKMP, OAKLEY)
- Düşük Seviye Kriptografi Kullanımı
 - PAP, CHAP, PPTP



Operasyonel Güvenlik



Operasyonel Güvenlik

- Saldırganlar
- Saldırı Metodolojisi
- İnsan Kaynakları Güvenliği
- Denetim ve İzleme
- Kontrol Türleri
- Fax Yönetimi

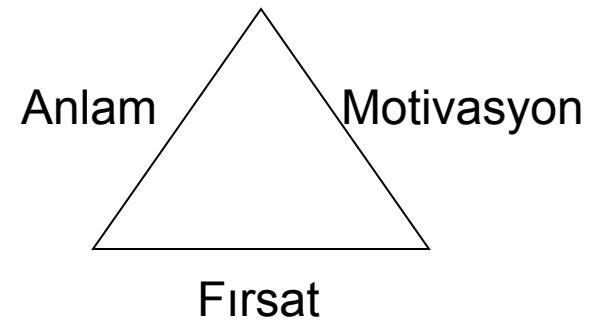
Saldırganlar

Saldırgan Türleri

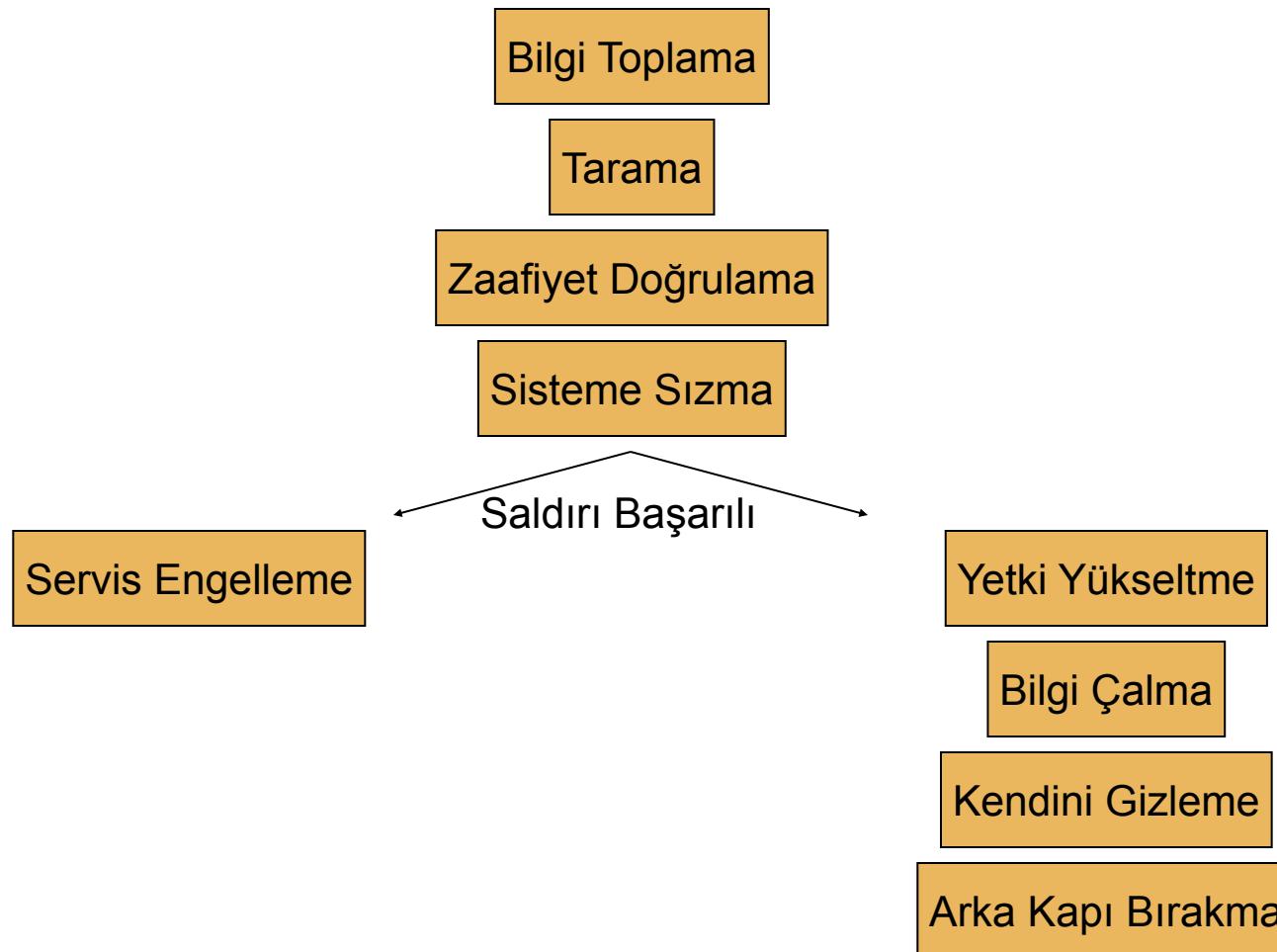
- Dahili Saldırganlar
- Harici Saldırganlar
 - Genç Saldırganlar
 - Teknoloji Casusları
 - Ülke Casusları
 - Suçlular ve Suç Örgütleri



Suç Üçgeni



Saldırı Metodolojisi



İnsan Kaynakları Güvenliği

- İşe Alım
 - Sicil İnceleme, Gizlilik Sözleşmesi, Politika Bildirimi, Eğitim
- Görev Ayrımı
 - Düşük Yetki Yaklaşımı, Tek Görevin Çok Kişiye Dağıtılması
- Görev Yeri Değişimi
 - Çalışanların Tecrübe Artışı, Gizli İşlemlerin Ortaya Çıkması, Yedekleme
- Düşük Yetki Yaklaşımı
 - Sadece Gereken Yetkiler, Hedefin Cazibesini Azaltır
- Zorunlu Tatiller
 - Gizli İşlem ve İstismarların Önlenmesi, Yedekleme Testi
- İş Sonlandırma
 - Sistem Yetkilerinin Kapatılması, Görevli Eşliğinde Toplanma ve Binadan Ayrılma, Şirket Kart ve Kimliklerinin Alımı

Denetim ve İzleme

- Takip edilebilirlik esastır, kullanıcı/süreç takip edilecek veriye sahip değilse denetim ve izleme yapılamaz
- Ağ iletişimini, kullanıcı hareketleri, ihmaller ve değişimler izlenmelidir
- Denetim
 - İşlemlerin olması gereki̇ği şekilde yapıldığının kontrolüdür
 - Yardımcı araçlar kullanılabilir : Sistem Kayıtları, Paket Yakalayıcı
- Eşik Seviyeleri
 - Normal hata sayısından fazlasına izin verilmemesi
- Saldırı Tespiti
 - Normal ile Anormal işlemlerin ayrıştırılması, Ağ veya Sunucu
- Klavye İzleme
- Ortam Erişim Kontrolleri
 - Kamera sistemleri, biometrik/kartlı sistemler,alarmlar, geçitler

Kontrol Türleri

- Önleyici Kontroller
 - Risk veya Politika ihlallerinin artmasını önleyen işlemler
- Saptayıcı Kontroller
 - Güvenlik ihllalerini saptamayı ve doğrulamayı sağlayan işlemler
- Düzeltici Kontroller
 - Yapılan işlemin tersini yaparak riski veya etkiyi azaltmayı sağlayan işlemler
- Kurtarma Kontrolleri
 - Olay/İhlal sonrası sistemi tekrar normale döndüren işlemler
- Caydırıcı Kontroller
 - Olay/İhlalin gerçekleşme olasılığını düşüren işlemler
- Yönlendirici Kontroller
 - Olay/İhlalin gerçekleşmesini engelleyici işlemler

Fax Yönetimi

- Fax İletişiminin Sorunları
 - İletişim kriptosuz olduğundan trafik durdurulabilir ve dinlenebilir
 - Gönderi hedefine vardığında cihazın haznesinde bekleyecektir, herhangi bir kişi evrağa erişebilir
 - Çoğu fax cihazı şerit kullanır, atılan şeritler aracılığıyla gönderilerin kopyası edinilebilir
- Güvenli Fax İletişimi
 - Fax sunucusu aracılığıyla iletişim kriptolanması mümkündür
 - Fax sunucusu aldığı ve gönderdiği belgeleri elektronik ortamda alacak, politikalar doğrultusunda arşivleyebilecektir
 - Fax sunucusu Alınan bir belgenin ilgili kişiye otomatik veya manuel olarak gönderimini sağlayacaktır
 - İşlem ve hata kayıtları tutarak sistemin izlenmesini de sağlayacaktır
- * Fax sunucuları aynı zamanda bir ağ bileşeni olduklarıdan farklı güvenlik sıkıntları da bulunmaktadır.

Ağ ve Sistem Sızma Testleri

- Güvenlik açıkları bulma, doğrulama ve kullanma amaçlı yapılan testlerdir.
- Ağ veya sistemler ile ilgili tam bilgi veya yarı bilgi ile yapılabileceği gibi hiçbir bilgi olmadan da test gerçekleştirilebilmektedir.
- Bağımsız kurumlar aracılığıyla sunulur, ilgili kurumun bilgisi ve onayı gereklidir.
 - Önemli aşamalar : Bilgi toplama, ağ haritalama, uygulama haritalama, güvenlik açıklarını saptama, güvenlik açıkları kullanımı
 - Ek aşamalar : Uygulama testleri, sesli iletişim sistemleri testi, kablosuz ağ testleri, servis engelleme, sosyal mühendislik



İş Sürekliliği

İş Süreklliliği

- İş Süreklliliğine Yönelik Tehditler
- İş Süreklliliği Yönetimi
- İş Süreklliliği Planı
- Proje Yönetimi ve İlklenme
- İş Etki Analizi
- Kurtarma Stratejisi
- İş Süreklliliği Plan Tasarımı ve Geliştirilmesi
- Test, Bakım Farkındalık Eğitim
- Yıkımdan Kurtarma Planı
- Alternatif Yerleşim ve Donanım Yedeği
- Yazılım ve Veri Yedeği

İş Süreklliliğine Yönelik Tehditler

- Felaket Türleri
 - Doğal Afetler (Deprem, Fırtına, Sel, Kasırga)
 - Teknik Afetler (Kesintiler, Virüs/Worm Saldırganlar)
 - Destek Sistemleri (Elektrik Sorunları, Ekipman Ömrü)
 - İnsan Yapımı/Politik (Art Niyetli Çalışanlar, Politik Ambargo, Protesto, Terör)
- İş Kesinti Etki Düzeyleri
 - Düşük (1 Günden Kısa İş Kesintisi)
 - Orta (1 Gün veya Fazla Süre İş Kesintisi, Geçici Yer Değişimi)
 - Yüksek (Tam Yıkım, Günler veya Aylar Sürebilir, Uzun Süreli Yerleşim Değişimi)

İş Sürekliği Yönetimi

- İş Sürekliği yönetimi, bir sorun nedeniyle işin kesilmesi durumunda kurtarmak değildir; sorunlara rağmen işin devamlılığının korunmasıdır
- Amaç, sorun durumunda oluşan süreyi kısaltmak değil, işin devamı için gerekli önlemleri ve değişimleri bulmaktadır
- Kuruma özel olarak planlanmalıdır ;
 - Yerleşim yeri özellikleri
 - Kapasite kullanımı
 - Güvenlik ekipmanı kullanımı

İş Sürekliği Planı

- İşin oluşabilecek kesintilere rağmen devam edebilmesi için geliştirilir
- Potansiyel kayıpların oluşma ihtimalini azaltacak önlemleri de içermektedir
- İş Sürekliği Planı Adımları
 - Proje Yönetimi ve İlklenme
 - İş Etki Analizi
 - Kurtarma Stratejisi
 - Plan Tasarımı ve Geliştirmesi
 - Test, Bakım, Farkındalık ve Eğitim

Proje Yönetimi ve İlklenendirme

- Öncelikle üst yönetimin desteği alınmalıdır
- Risk analizi yapılmalı, kritik iş süreçlerinin potansiyel kesintileri belirlenmelidir
- Proje Planı Oluşturulması
 - Proje Kapsamının Belirlenmesi
 - Proje Planlayıcısının Atanması
 - Ekip Üyelerinin Belirlenmesi
 - Proje Planının Oluşturulması
 - Veri Toplama Yöntemlerinin Belirlenmesi

İş Etki Analizi

- İş etki analizi, olası bir kesintinin oluşturacağı potansiyel kaybın belirlenmesini hedefler
- İş Etki Analizi Adımları
 - İlgili Kişilerle Görüşülmesi
 - Veri Toplama Yöntemlerinin Belirlenmesi
 - Özel Sorular Hazırlanmalı, Her Bileşen veya Özelliğin Kesintisi Durumunda Oluşacak Nicel/Nitel Etki Düzeyini İçermelidir
 - Toplanan Verilerin Analizi
 - Zaman-Kritik İş Süreçlerinin ve Bileşenlerin Belirlenmesi
 - Her Süreç için Tahammül Edilebilir Sürenin Hesaplanması
 - İş Süreçlerinin Tahammül Edilebilir Süreye Göre Önceliklendirilmesi
 - Bulguların Belirlenmesi ve Tavsiyeler ile Yönetime Raporlanması
- Kayıp/Etki Ölçüm Kriterleri
 - Kabul Edilebilir İş Kesintisi
 - Finansal ve Operasyonel Karşılık
 - Yasal/Uyumluluk Gereklilıklar
 - Organizasyonel Reddetme

Kurtarma Stratejisi

- Kesinti Sebepleri
 - Veri Kesintileri (Veri Kurtarma, Yedekleme, İkizleme)
 - Operasyonel Kesintiler (RAID, Yedek Güç Kaynakları)
 - Ortam ve Destek Kesintileri (Yangın, Havalandırma, İletişim)
 - İş Kesintileri (Personel Kaybı, Ekipman Arızası)
- Doğru Kurtarma Yönteminin Bulunması
 - Olası Alternatiflerden Herbiri için Maliyet Hesaplaması
 - Gerekli Dış Hizmetlerin Maliyetlerinin Belirlenmesi
 - Dış Hizmetler için Sözleşmelerin Hazırlanması
 - Tamamen Yerleşim/Ortam Kaybı için Alternatif Stratejilerin Araştırılması
 - Bulgular ve Yorumların Raporlanarak Yönetimin Onayına Sunulması

İş Devamlılığı Plan Tasarımı ve Geliştirilmesi

- Kritik Süreçlerin Kurtarılması için Kısa ve Uzun Vadeli Plan Oluşturulmalı
 - Yeniden yerleşim için kritik süreç ve önceliklerin doğrulanması
 - Kritik süreçlerin ihtiyaç duyduğu destek sistemlerinin doğrulanması
 - Potansiyel yıkımların ve tam yıkımdan kurtarma için gerekli olan en az kaynakların hesaplanması
 - Kurtarma stratejisi seçilmesi ve gerekli olan personel, sistem ve teçhizatların belirlenmesi
 - Yeniden yerleşim ve test süreçlerini yönetecek kişinin belirlenmesi
 - Projenin tamamlanması için gerekli mali kaynakların hesaplanması
- Plan aynı zamanda müşteriler, iş ortakları ve acil servisler ile nasıl bir iletişim kurulacağını da içermeli
- Hazırlanan plan “İş Devamlılığı Planı” ile karşılaştırılmalı ve birleştirilmeli

Test, Bakım, Farkındalık ve Eğitim

- Test Yöntemleri
 - Liste Denetimi (Kağıt üzerinde her adımıın testi)
 - Masada Test (Ekip üyelerinin bir arada olduğu toplantı)
 - Tatbikat (Kesinti varmış gibi davranışılacak, yeni yerleşim dahil değil)
 - İşlevsel Test (Tatbikatın yeni yerleşimde kapsaması, iki yerleşimin eş zamanlı çalışması)
 - Tam Kesinti (Doğru hesaplama ve önlemlerle tam bir kesinti)
- Planda gerekli düzenleme ve güncellemeler yapılmalı, sürüm güncellenerek ilgili birimler bilgilendirilmeli
- İş Devamlılığı Planı İşleyiş Sorumluları
 - Yönetim (Proje İkkwendirme, Tam Sorumluluk, Onay ve Destek)
 - Orta Düzey Yönetim (Kritik Sistemlerin Doğrulanması ve Önceliklendirilmesi)
 - İş Devamlılık Ekibi (Planlama, Günlük Yönetim, Uygulama ve Test)
 - İlgili İş Birimleri (Planın Uygulanması, İletişim ve Test)
- İş devamlığındaki rollere göre uygun eğitimlerin sunulması

Yıkımdan Kurtarma Planı

- Kurumun bir yıkım durumundan kurtarılarak kritik iş süreçlerinin devam ettirilmesini hedefler
- Kısmi Kurtarma (Zarar gören teçhizat ve yerleşimin işlevselliğinin geri kazandırılması)
 - Hasar boyutunun ve kapsamının değerlendirilmesi
 - Kurtarılabilir teçhizatların kurtarılması
 - Yerleşimdeki onarım ve temizliğin yapılması
 - Yerleşimin tamamen işlevsel haline geri döndürülmesi
- Tam Kurtarma (Yedek yerleşimin etkinleştirilmesi)

Alternatif Yerleşim ve Donanım Yedeği

- Yerleşim Yeri Paylaşma Anlaşması
- Alternatif Yerleşim Yerleri
 - Soğuk (Elektrik bulunan, bilgisayar kullanılabilen boş yerleşim)
 - İllik (Soğuk yerleşime ek olarak veri cihazları, kablolama vb.)
 - Sıcak (Tamamen işlevsel, ikiz kaynaklar ve cihazlar)
- Çoklu Veri Merkezleri (Farklı bir kurumda ikiz sistem odası)
- Servis Büroları (Sorumlulukların devri, işin bürodan yönetilmesi)
- Diğer Alternatifler
 - RAID Kullanımı (Çoklu disk, kapasite ve devamlılık avantajı)
 - Veritabanı İkizleme (Veritabanının iki ayrı disk veya sistemde olması)
 - Elektronik İkizleme (Alternatif yerleşime otomatik yedek alma)
 - Senkronizasyon (Alternatif yerleşim ile gerçek zamanlı senkronizasyon)

Yazılım ve Veri Yedeği

- Geliştirici veya destek veren kurumların sonlanması ihtimaline karşı kritik yazılımlara özel kaynak kod teslim anlaşması hazırlanabilir
- Yedekleme
 - RAID (Gerçek Zamanlı Yedekleme)
 - Ağ Temelli Depolama Sistemleri
 - Yedekleme Türleri
 - Tam Yedekleme
 - Artımlı Yedekleme
 - Farklılık Temelli Yedekleme
 - Yedekleme Ortamı Değiştirme Yöntemleri
 - Basit (Günlük 5, Aylık 12 Ortam)
 - Büyükbaba-Baba-Oğul (Günlük 4, Haftalık 4, Aylık 12 Ortam)
 - Honai Kulesi



Acil Müdahale ve İhlal Yönetimi

Güvenlik İhlalleri

- Kurumun var olan güvenlik politika ve prosedürlerine uygunsuz olarak, bilginin gizliliğine, bütünlüğüne veya erişilebilirliğine yönelik yapılan işlem ve hareketler
- Güvenlik İhlali Türleri
 - Fiziksel Güvenlik İhlalleri
 - Kurum Çalışanlarının Güvenlik İhlalleri
 - Kurum Dışı Kişilerin Güvenlik İhlalleri
 - Bilgiye İzinsiz Erişim
 - Bilginin Değiştirilmesi, Büyüklüğünün Bozulması
 - Servisin Engellenmesi

Güvenlik İhlali Yönetimi

- Acil Müdahale Ekibi
 - Ekip üyeleri, görevleri ve yönetiminin belirlenmesi
- İhlal Bildirim Süreci
- Acil Müdahale Planı
 - Potansiyel ihlal türlerinin ve atılması gereken adımların belirlenmesi
 - Elde edilen bulguların raporlanması sürecinin tanımlanması
- Plan Testi
 - Düzenli olarak acil müdahale planı tatbikat veya masa üstü analizler ile test edilmelidir
- Eğitim ve Farkındalık
 - Ekip üyeleri, müşteriler, iş ortakları, diğer çalışanlar

Acil Müdahale Ekibi

- Ekip Üyeleri
 - Bilişim Bölümü, Fiziksel Güvenlik Bölümü, Bölüm Yöneticileri
 - İç Denetim
 - Güvenlik Sorumluları
 - Halkla İlişkiler
 - Hukuk Bölümü
 - Ağ ve Sistem Yönetimi
 - İnsan Kaynakları
 - Yönetim, Görev ve Yetki Dağılımı
- Ekip Üyeleri Yetkinliği
 - Uzmanlık Alanında Görevlendirme
 - Müdahale Alanına Özel Eğitimler
 - Genel Hareket Planı ve Müdahale Eğitimleri

İhlali Bildirim Süreci

- Bildirim Sürecinin Tanımlanması
 - Bildirimin doğrudan ve tek bir kanala yönlendirilmesi
 - Erişimi kolay, dikkat çekici bir iletişim yöntemi kullanılması
 - Bildirim güvenliğinin sağlanması, güvenli iletişim
 - Bildirim Formları
 - Potansiyel Zaafiyet / Oluşmuş İhlal Ayrımı
 - Görevliye Yardımcı Olabilecek Bilgilerin Girilebilmesi
 - Bildirimi Gerçekleştirenin Yapması Gerekenlerin Talimatlandırılması
 - Gizlilik Bildirimi
- Bildirim Yönetimi
 - Bildirim Durumu Takibi
 - Görevlilere Dağıtım
 - Ekip Yönetiminin Haberdar Edilmesi

Acil Müdahale Planı

- Farklı türlerdeki ihlaller için prosedürler hazırlanması
 - Bilgi hırsızlığı, servis engelleme, bilgi değişimi, virüs/worm
- Müdahale Adımlarının Belirlenmesi
 - İhlalin doğrulanması, analizi, etki alanın belirlenmesi
 - Doğru müdahale şekli ve yönteminin belirlenmesi, uygulanması
 - Kurtarma veya etkilenen kurumlar için gerekli iletişimın sağlanması
 - Üst yönetime olay bulgu ve sonuçlarının raporlanması
- Kanıt Toplama Yöntemlerinin Belirlenmesi
 - Geçerli ve gerekli kanıtların tanımlanması
 - Kanıtların alınma ve saklanma yöntemlerinin belirlenmesi
- Kurtarmada Dikkat Edilmesi Gerekenler
 - Sadece yetkili ve ilgili kişilerin sistemlerde bulunduğu
 - Canlı veya devre dışı analizlerde sistem bütünlüğüne zarar verilmemesi
 - Kurtarılan sistemlerin devamlılığı ve bütünlüğünün en kısa sürede doğrulanması
 - Atılan tüm adımların detaylı olarak belgelenmesi
 - Üst yönetime düzenli ve istenen tarzda raporun sunulması

Acil Müdahale Planı Testleri

- Bildirim Süreci Testleri
 - Farklı bildirim türleri ve görevlilere erişimin sorgulanması
 - Bildirim formlarının yeterliliğinin kontrolü
- Müdahale Planı Testleri
 - Masa üstünde ekip üyeleriyle senaryo analizleri
 - Tatbikatlar ile görevlilerin ve işlemlerin kontrolü
 - Analiz yapılan sistemlerin bütünlüğünün korunma kontrolü
 - Kanıt toplama sürecinin kontrolü
 - Örnek raporlama ve ihtiyaç analizi
- Müdahale Planı veya Bildirim Sürecinde İyleştirmeler
- Düzenli Aralıklarla Plan Test Edilmelidir

Eğitim ve Farkındalık

- Bildirim süreci işlemezse ihlal olayından öğrenme gerçekleşir !
- Ekip Üyeleri ve Alt Görevliler
 - Müdahale Aşamaları ve Yöntemleri
 - Gizlilik Gereksinimi ve Sorumluluklar
- Çalışanların Eğitimi
 - Potansiyel Zaafiyet ve İhlal Tanımları
 - Bildirim Yöntemleri
 - Gizlilik Gereksinimi ve Sorumluluklar
- İş Ortakları ve Müşteriler
 - Zaafiyet Bildirim Formları
 - Gizlilik Gereksinimi



Bilgi Güvenliği Teknolojileri

Yeni Nesil Güvenlik Teknolojileri

- Güvenlik tehditlerinin logaritmik büyümesi, tehditlerle başa çıkması gereken teknolojilerin sayıca artmasının sonucu olarak çok sayıda yeni nesil güvenlik teknolojisi oluşmuştur
- Yeni güvenlik teknolojilerinin büyük bölümü uzun zamandır kullanılan teknolojilerin yetersizliklerinin kapatılması, yönetimin kolaylaştırılması ve yeni nesil bilişim altyapısına uygun sistemlerin sorunlarına çözüm için geliştirilmiştir
- Bazıları halen kullanılabilmeyen uzak olmasına rağmen, çok sayıda yeni teknoloji günümüz ağlarında yerini almıştır
 - Birleşik Tehdit Yönetim Sistemleri (UTM)
 - Son Nokta Güvenlik Teknolojileri (Endpoint Security)
 - Kablosuz Ağ Saldırı Tespit Sistemleri
 - IP Üzerinden Ses ve Görüntü Güvenliği Teknolojileri
 - Mobil Cihazlar için Güvenlik Teknolojileri



Kimlik Doğrulama ve Yetkilendirme Teknolojileri

Kimlik Doğrulama ve Yetkilendirme

- Kim Giriş İstiyor, Kimliği Doğrumu, Yetkileri Neler ?
 - Kimliklendirme; kullanıcının sistemlerde bir kimliğe sahip olması süreci
 - Doğrulama; kullanıcı kimliğinin sistemlerdeki geçerliliğinin doğrulanması süreci
 - Yetkilendirme; kullanıcının geçerliliği doğrulanın kimliğinde sahip olduğu yetkilerin kullanıcıya atanması süreci
- Kimlik Doğrulama Yöntemleri
 - Kullanıcı Adı / Şifre
 - Tek Kullanımlık Şifre Cihazları
 - Akıllı Kartlar
 - Manyetik Kartlar
 - Sertifikalar
 - Biyometrik Sistemler
 - Güçlü Doğrulama
 - Bildiğiniz Şey
 - Sahip Oldığınız Şey
 - Oldığınız Şey

Merkezi Doğrulama ve Yetkilendirme

- Merkezi Doğrulama ve Yetkilendirme Altyapıları
 - Merkezi Kullanıcı ve Yetki Veritabanı
 - LDAP
 - RADIUS
 - TACACS
 - Merkezi Tekil Giriş/Çıkış (Single Sign On - Single Signout)
 - IDM
 - Kerberos
- Günümüz Ağlarındaki Yaklaşım
 - Kimlik Yönetimi (IDM)
 - Tüm Uygulamalar için Harici Doğrulama ile beraber Ortak Kullanıcı Veritabanı, Yetkilendirme ve Doğrulama
 - Active Directory / Open Directory / OpenLDAP+Kerberos
 - LDAP Temelli Kullanıcı, Yetki ve Özellikler Veritabanı
 - Kerberos ile Doğrulama Yönetimi

LDAP

- Lightweight Directory Access Protocol (1993)
- Kullanıcı ve sistem profilleri merkezi olarak tutulur, LDAP protokolü aracılığıyla diğer sunucu ve servislere sunulur.
- Merkezi doğrulama yapılabilmektedir (LDAP v3)
- Dizin sistemleri tarafından desteklenmekte ve yaygın olarak kullanılmaktadır.
- Distinguished Name (DN), Her girdinin tekil doğrulayıcısıdır
- cn=Fatih Ozavci, ou=Guvenlik, dc=gamasec, dc=net
- Kullanıcı bilgilerinin sorgulanması amaçlı sıkça kullanılmaktadır
- Merkezi doğrulama uygulamalarının önemli bileşenlerindendir
 - Active Directory
 - Open Directory
 - eDirectory

RADIUS

- Remote Authentication and Dial-In User Service (1997)
- Merkezi olarak Doğrulama (Authentication), Yetkilendirme (Authorization) ve Hesap Yönetimi (Accounting) servislerini sunar.
- Tüm kullanıcı profilleri merkezi olarak tutulur ve UDP temelli doğrulama servisi ile diğer sistemlere sunulur.
- Uzak Erişim (RAS) ve kablosuz ağlarda sıkılıkla kullanılmaktadır.
- İşleyiş :
 - İstemci, RADIUS istemcisine bağlanarak kullanıcı bilgilerini verir.
 - RADIUS istemcisi kullanıcı bilgilerini kriptolayarak RADIUS sunucusuna aktarır.
 - RADIUS sunucusu bilgileri doğrular, reddeder veya ek bir işlem yapılmasını talep eder.
 - Bilgiler doğrulanırsa istemci istenen kaynağa erişebilir.

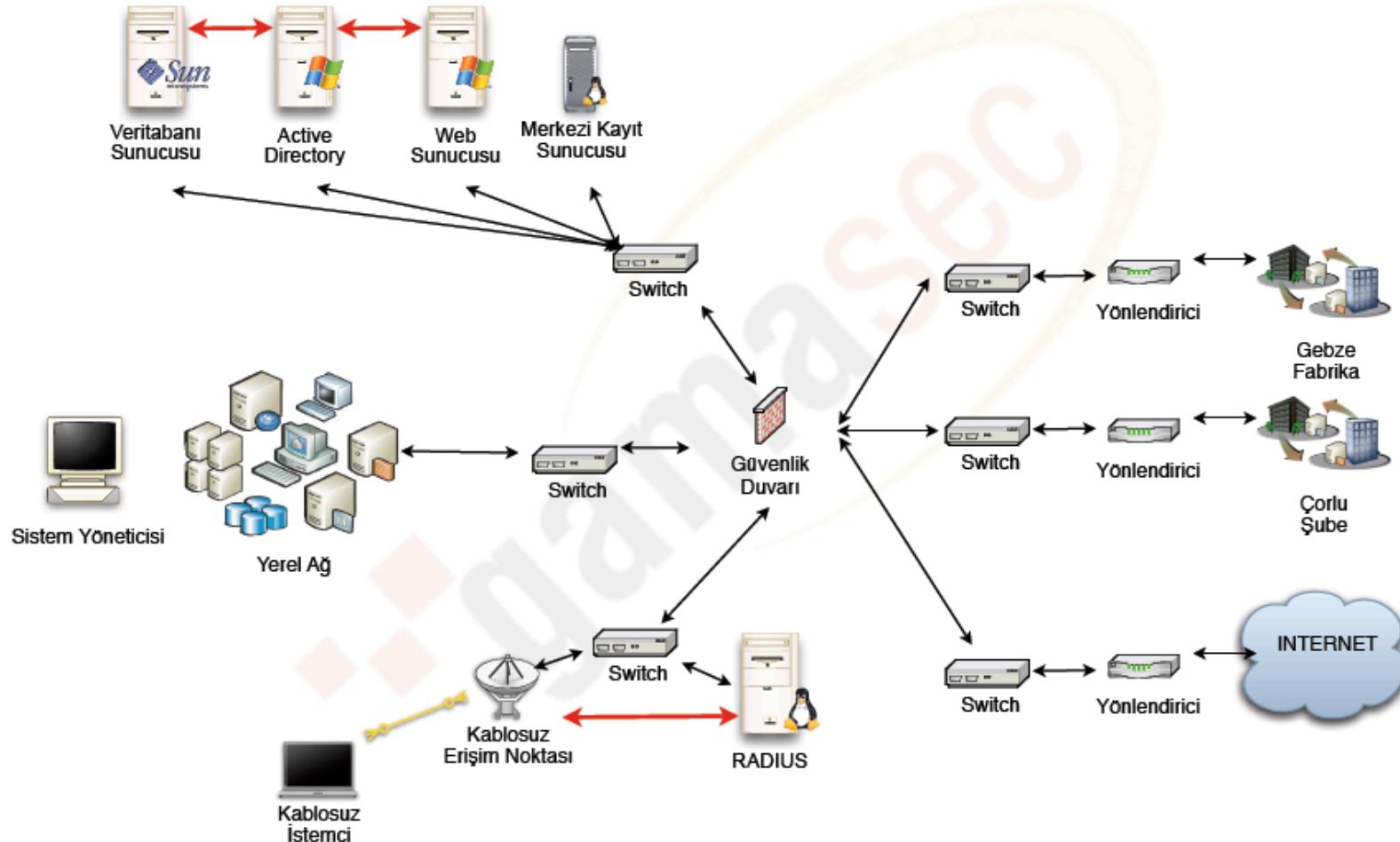
Kimlik Yönetimi (IDM)

- Merkezi Kimlik Yönetimi
 - Hesap Eşleştirme/Karşılaştırma
 - İş Akışı Otomasyonu
 - Yönetim Görevi Aktarımı
 - Şifre Senkronizasyonu
 - Servis Üzerinden Şifre Sıfırlama
- Tekil Giriş/Çıkış ve Web Üzerinden Giriş
- Diğer Uygulamalar için Dizin Servisleri
- Farklı Türkdeki Uygulamalar için Merkezi Doğrulama/Yetkilendirme
 - Web Uygulaması
 - Kablosuz Ağ Uygulamaları
 - Sunucu/Ağ Servisi
 - Kullanıcılar
 -

Kerberos

- MIT tarafından 1985'te geliştirildi. Üç temel bileşen var; istemci, sunucu ve KDC (Anahtar Dağıtma Sunucusu)
- Anahtar Dağıtma Sunucusu (KDC)
- Doğrulama Servisi (AS)
- Bilet Verme Servisi (TGS)

Merkezi Doğrulama Yaklaşımı





Erişim Denetim Teknolojileri



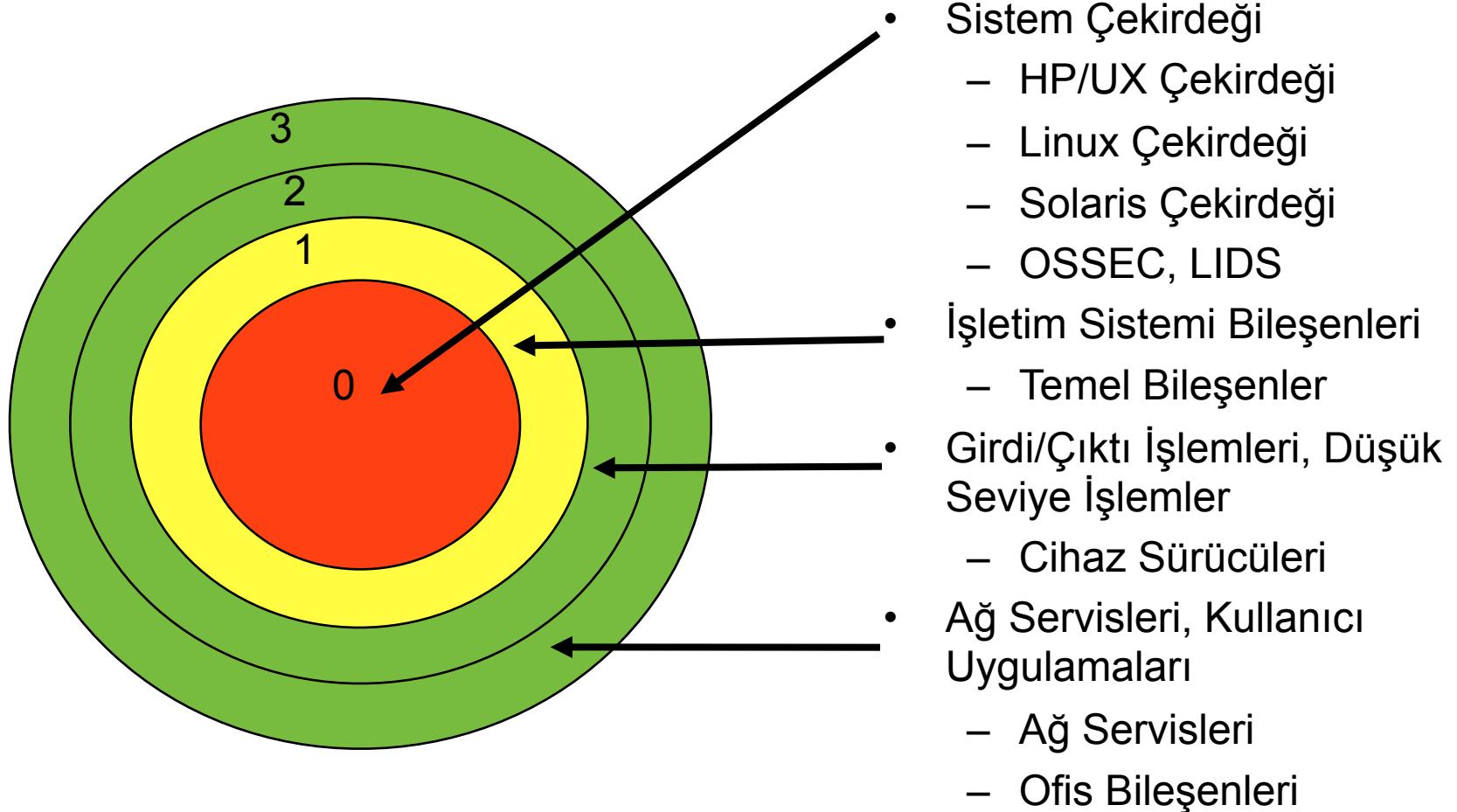
Erişim Denetim Teknolojileri

- Erişim Denetimi
 - Kim/Ne, Hangi Şartlarla ve Hangi Amaçla Erişebilir
- Erişim Denetimi, yetkilerin yaşama geçirilmesidir
 - Kimliklendirme, Doğrulama ve Yetkilendirme; Erişim Denetiminden bağımsız iken anlamsızdır
 - Erişim Denetimi uygulayan bileşen aynı zamanda Yetkilendirme sağlamak zorunda değildir
 - Farklı uygulama alanları mevcuttur
 - İşletim Sistemi, Harici Uygulamalar, Web Uygulamaları
 - Güvenlik Duvarı, Saldırı Önleme Sistemi, Web Güvenlik Duvarı
- Erişim Denetim Modelleri
 - MAC, DAC, RBAC, RSBAC
- Erişim Denetimi standartlarca zorunluluk olarak talep edilebilir
 - TCSEC (Orange Book), ITSEC, Common Criteria (ISO 15048)

Erişim Denetim Sistemleri

- Erişim Denetimi Yapılabilmesi için gerekenler
 - Yetkilendirme yapan bir sistem
 - Kaynak ile Hedef arasında bulunmak
- Veri veya Kaynağa Erişimi Denetlemeyi Hedeflemektedirler
 - Sistem Seviyesinde (Veri, Süreç, Sistem Kullanımı)
 - İşletim Sistemi Çekirdeği
 - İşletim Sistemi Uygulamaları veya Harici Uygulamalar
 - Web Uygulamaları ...
 - Ağ Seviyesinde (Ağ İletişimi, Servisler, Sistemler)
 - Güvenlik Duvarı
 - Yönlendirici
 - Saldırı Önleme Sistemi ...

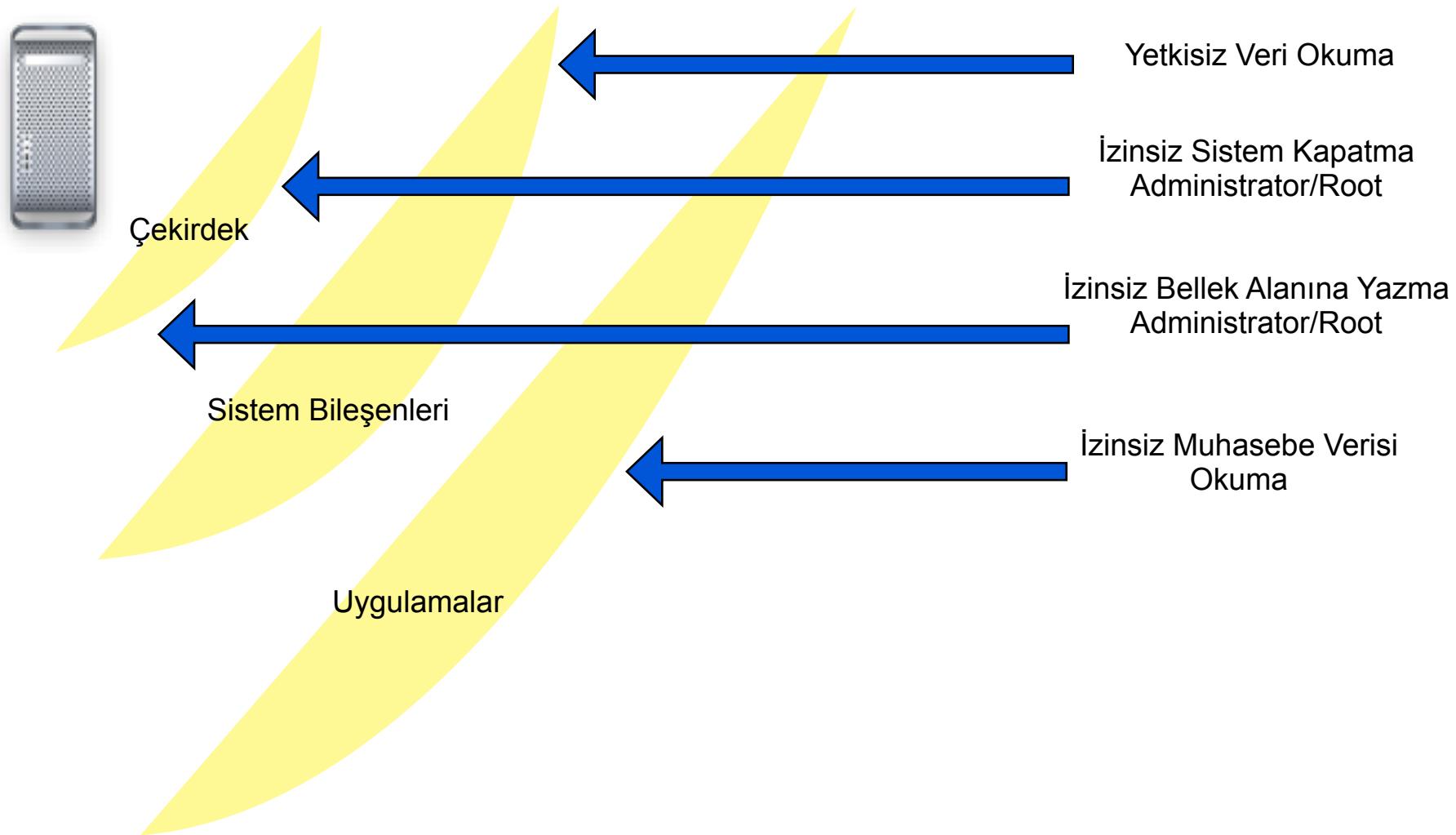
İşletim Sistemi - Koruma Halkaları



Çekirdek Seviyesinde Güvenlik

- Çekirdek : Sistem Güvenliğinin En Önemli Bileşeni
- Çerkideklerin Güvenlik Özellikleri
 - İşlemci ve Bellek Kullanımı
 - Giriş/Çıkış Yönetimi
 - Süreç Yönetimi
 - Kullanıcı Yönetimi
 - İzleme
- Çekirdek Seviyesinde Güvenlik
 - Trusted Solaris (EAL 4+) (Solaris Trusted Extensions)
 - Linux
 - LSM, OSSEC, LIDS, GRSecurity, SELinux, RSBAC
 - IBM Redhat Linux (EAL 4+)
 - Windows 2000 (EAL 4+ ?)
 - Windows Vista/Server 2008
- Çekirdek Yamaları

Sistem Seviyesinde Güvenlik



Sistem Seviyesi Erişim Denetimi Yapılandırması

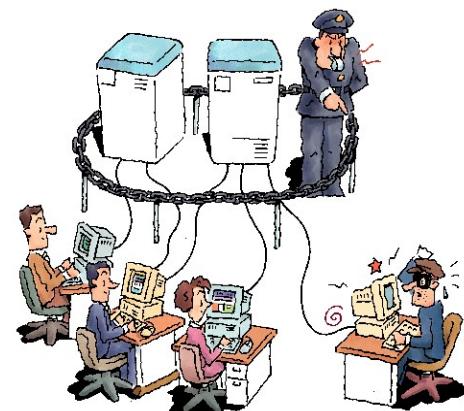
- Sistem ile “Çekirdek” seviyesinde bütünlüğecek bir yapı oluşturulmalı
 - Çekirdek yamaları, Ticari yazılımlar, Özel işletim sistemleri
- Kalıcı olması gereken şeyler “Çekirdek” seviyesinde tanımlanmalı
 - Süreç Yönetimi, Disk/Dosya Sistemi Yönetimi, İşlemci Yönetimi, Bellek Yönetimi, Girdi/Cıktı Yönetimi, Kritik Sistem Servisleri Yönetimi
- Kimlik/Yetki tanımlamalarının alındığı sistemlerin yapılandırmasına özen gösterilmelidir
 - Kerberos, LDAP, RADIUS
- Uygun denetim modeli seçilerek, doğru biçimde uygulanmalıdır
- Kullanılan uygulamaların erişim denetim sistemi olduğu, işletim sistemi bünyesindeki erişim denetim yapısı ile örtüştüğü doğrulanmalıdır

Ağ Seviyesinde Erişim Denetimi

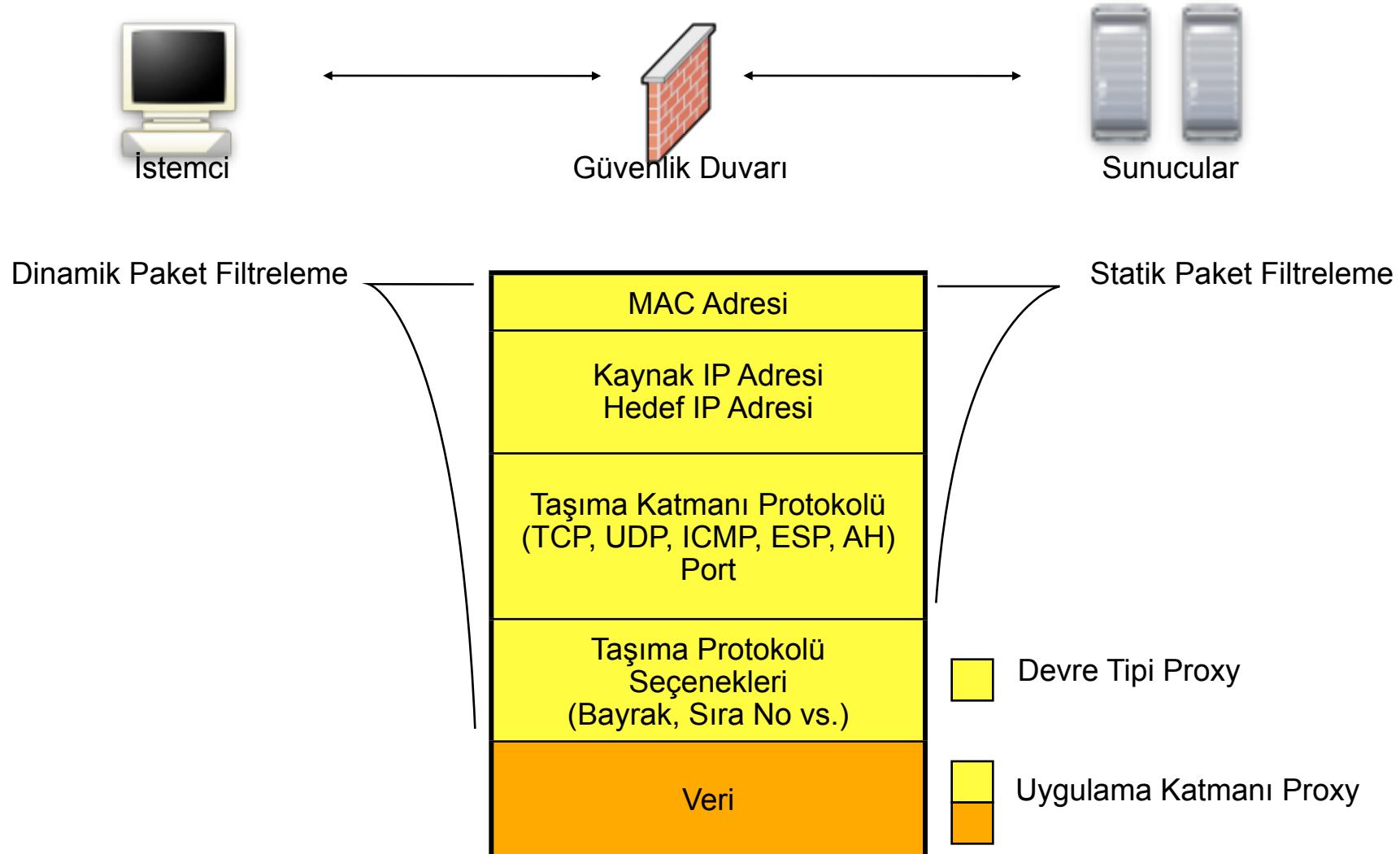
- Ağlar arası veya sistemler arası yapılacak olan erişimlerin denetlenmesi hedefelenmektedir
- Her OSI katmanı ayrı bir erişim denetim kriteri gerektirir
 - Veri Bağı Katmanı -> MAC Adresi, ARP Soru Türü
 - Ağ Katmanı -> IP Başlık Bilgileri
 - Taşıma/Oturum/Sunum Katmanları -> Diğer Protokol Başlık Bilgileri (TCP/UDP/ESP/AH/ICMP Protokol Türleri, Port Bilgisi, ISN/Sıra Numaraları)
 - Uygulama Katmanı -> Pakette Bulunan Veri İçeriği
- Ağ üzerinde erişim denetimi yapan teknolojiler “Güvenlik Duvarı” olarak çağrılmaktadır, yeni nesil teknolojilerde ek özellikler ile bilinen tanımda farklılıklar oluşmakta ve tekil tehdit yönetimi kullanılmaktadır
 - Yazılım veya Donanım olarak bulunabilir
 - Cihaza/Yazılıma gömülü bir özellik olabilir (Yönlendirici, Switch, Güvenlik Duvarı, Saldırı Önleme Sistemi, Tehdit Yönetim Sistemi, Web Güvenlik Duvarı vb.)

Güvenlik Duvarı

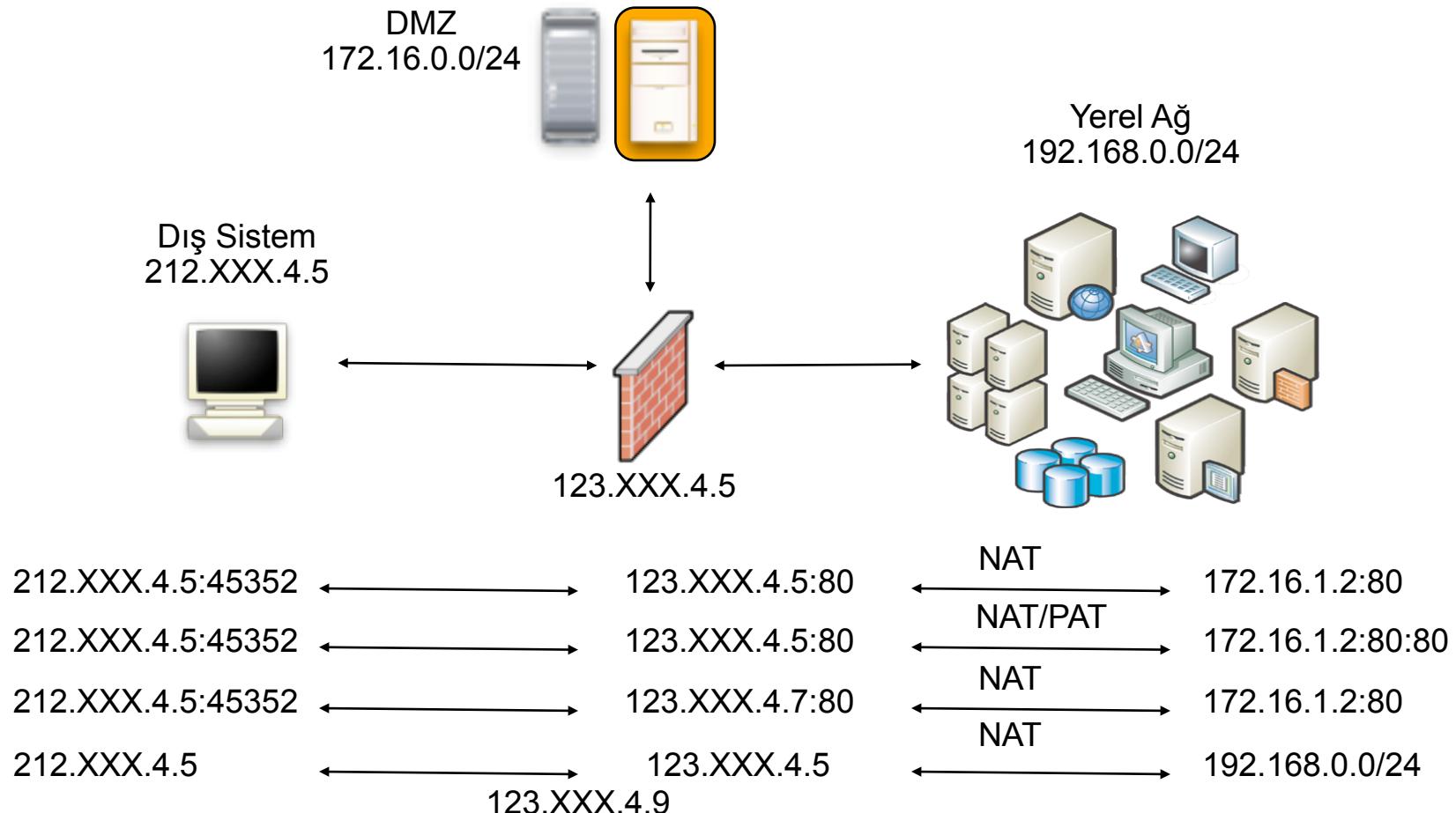
- Güvenlik duvarı (Firewall), ağ iletişiminde erişim denetimi işlemi için kullanılan sistemlere verilen genel isimdir
- Ağ temelli sistemlerde güvensiz ağlar ile güvenli ağlar/sistemler arasındaki iletişimizi izole etmek ve belirli şartlar altında erişime izin vermek için kullanılırlar
- En temel güvenlik uygulamasıdır, irili ufaklı birçok kurumda farklı amaçlar için farklı güvenlik duvari uygulamaları kullanılmaktadır
- Güvenlik Duvarı Türleri
 - Statik Paket Filtreleme
 - Dinamik Paket Filtreleme
 - Proxy Tipinde Filtreleme
 - Devre Tipi Filtreleme
 - Uygulama Katmanında Filtreleme
- Ağ Adres Çevrimi (NAT, PAT?, Port Yönlendirme?),
- DeMilitarized Zone (DMZ)



Güvenlik Duvarı İşleyışı



Güvenlik Duvarı İşleyışı



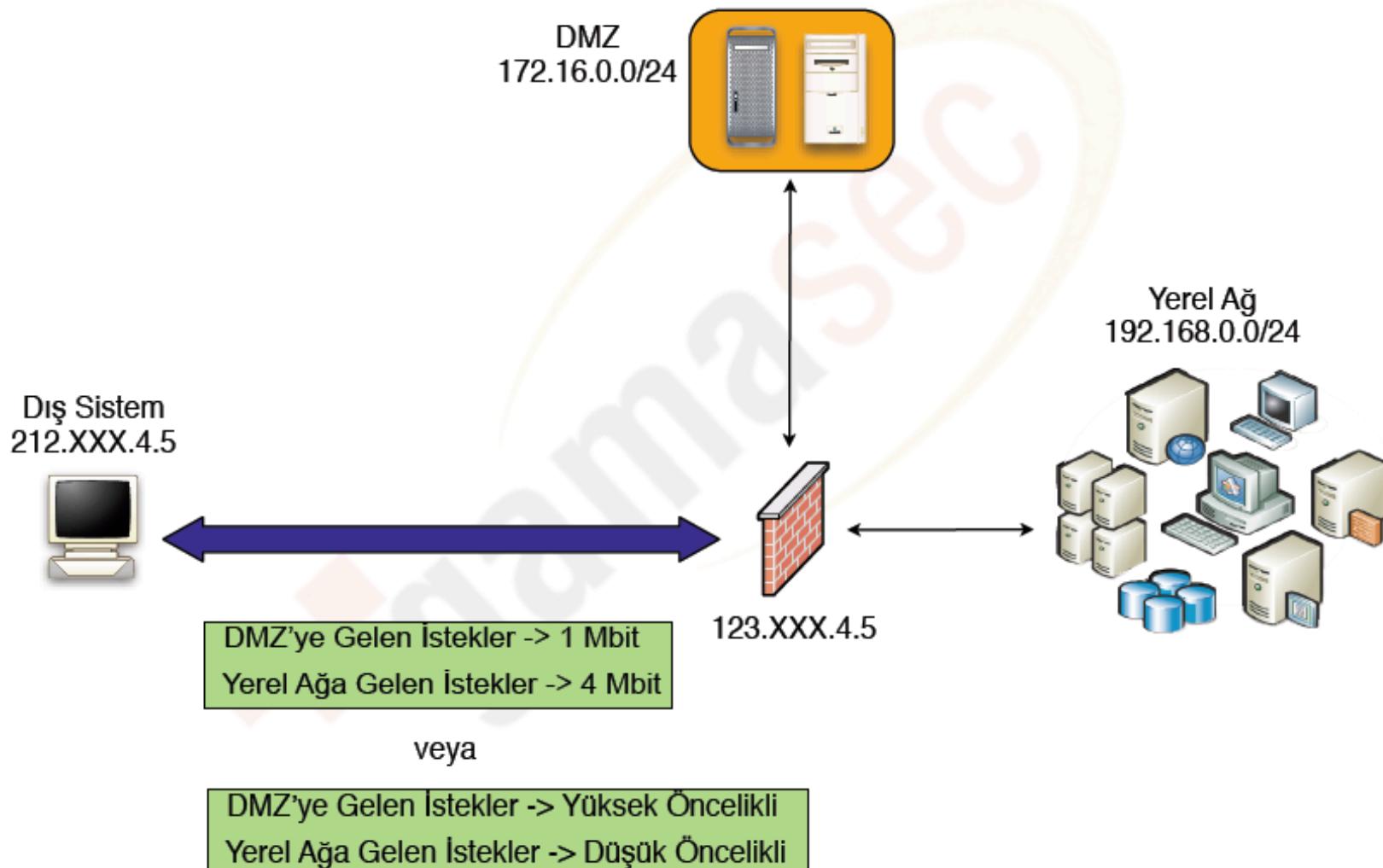
Güvenlik Duvarı Yapılandırması

- Kullanım amacı doğrultusunda doğru mimari seçilmelidir
- Güvenlik duvarının sahip olduğu dahili servislerden gerekmeyenler kapatılmalı, erişim engellenmelidir
- Bölgeler arası veya ağ bölümleri güvenlik duvarı ile ayırtılmalıdır
- Ağ yapısına uygun NAT ve DMZ yapılandırması kullanılmalıdır
- En az düzeyde kural benimsenmeli, erişim politikaları belirlenerek işlemler politikalara/gruplara atanmalı, gerekmeyen erişimlere izin verilmemelidir
- Güvenilmeyen ağlardan gelen bozuk paketler engellenmelidir
 - Kaynağı özel IP adresleri olan paketler (192.168., 127., 10. ...)
 - Bozuk TCP bayrakları olan paketler
 - Bir oturumun devamı olmayan paketler
 - Bozuk/Anlamsız/Geçersiz TCP/IP seçenekleri taşıyan paketler
- Diğer güvenlik teknolojileri ile bütünlüğünün “kararlı çalışma özelliği”ni kaybettirmemesi sağlanmalıdır
- Normal-Dışı ve Özel erişimler izlenmelidir
- Kural ve yapılandırma yedekleri düzenli olarak alınmalıdır

Servis Kalitesi Yönetimi

- Ağ seviyesinde Erişim Denetimi, kaynaklara erişim izinlerinin yönetimi demek değildir; erişime sunulan kaynakların hangi oranda kullanılabileceğini de yönetmektir
- Ağ geçitlerinde uygulanmalıdır; uçtan uca uygulanmadıkça gerçek verim alınamaz
- Servis Kalitesi Yönetim Kavramları
 - Type Of Service - Servis Tipi
 - Quality Of Service - Servis Tipine Bağlı Önceliklendirme
 - Class Of Service - Servis Tiplerinin Sınıflandırılması ile Önceliklendirme
- Bant Genişliği Yönetimi
 - Kuyruk Bölümleme ve Trafik Ayristırma
 - Servislerin veya İşaretlenmiş İsteklerin Önceliklendirilmesi

Servis Kalitesi Yönetimi





İzleme ve Analiz Teknolojileri

İzleme ve Analiz Sistemleri

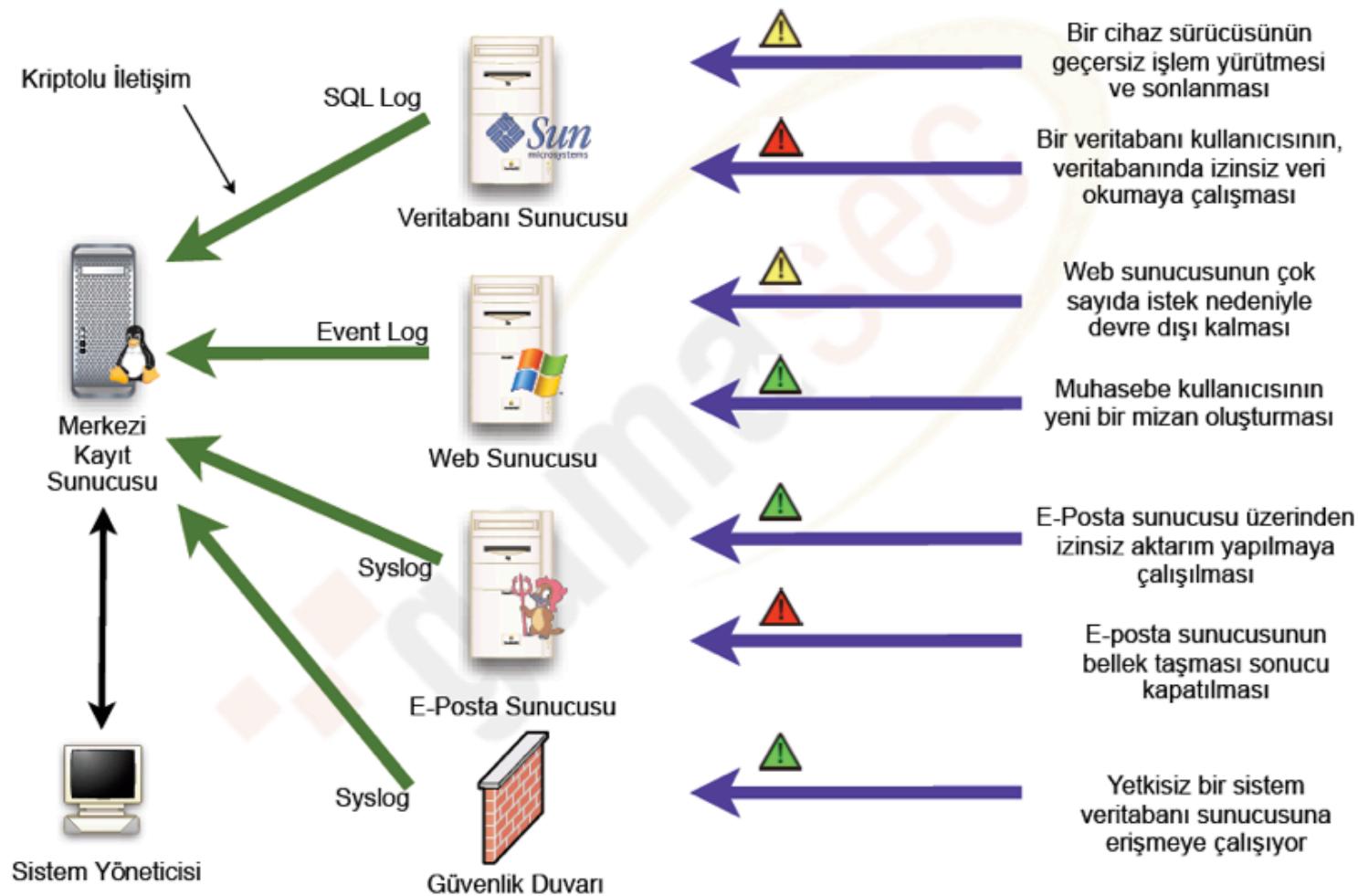
- İzleme ve Analiz sistemleri, planlanan güvenlik kriterlerinin beklenen biçimde uygulamaya geçirildiğinin doğrulanmasını sağlamaktadır
 - Tasarım Sorunları
 - Uygulama Sorunları
 - Yapısal Sorunlar
- Olay izleme, denetim, sorun giderme ve ihlal/sorun geri dönüşlerinde kritik önem taşımaktadırlar
- İzleme ve Analiz Sistemleri Türleri
 - Sunucu, Sistem ve Yazılım
 - Süreçler
 - Kullanıcı İşlemleri
 - Ağ
 - Ağ Servisleri
 - Ağ Erişimleri



Sunucu İzleme Sistemleri

- Bir sunucu veya sistem üzerinde yer alan, bütünsel izleme ve kayıt oluşturma teknolojileridir
 - İşletim Sistemi Çalışma Takip Arabirimı
 - Uygulama ve Süreçlerin Normal Dışı İşlemlerinin İzlenmesi
 - Debug Desteği ile Sorun Giderme Özelliklerinin Kullanımı
 - Dahili Kayıt Tutma Sistemi (Event Viewer, Syslog vb.)
 - Harici Kayıt Sistemi (Merkezi Sistem, Ticari Kayıt Sistemleri vb.)
 - Harici Yazılımların Kayıt Tutma Sistemi
 - Klavye, Ekran, Çalışma Ortamı ve Diğer Kayıt Mekanizmaları
- Sunucu İzleme ile Hedeflenenler
 - Çekirdek ve Temel İşletim Sistemi Bileşenlerinin İşleyiş Takibi
 - Harici Yazılımların Takibi
 - Kullanıcı İşlemlerinin Takibi
 - Sorun Giderme ve İhlal İncelemesi için Girdi Hazırlama

Merkezi Sistem Kaydı Planlaması



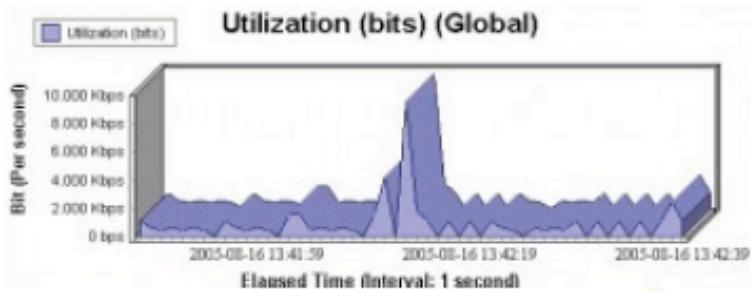
Ağ İzleme Sistemleri

- Ağ üzerinde etkin işlemleri, servis yükünü ve veri akışını izlemeyi sağlayan yazılımlardır
 - Ağ ve Servis Yükü İzleme
 - Belirli İşlem ve Protokollerin Kayıt Edilmesi
 - İşlem Hakkında Bilgi Mesajı
 - İletişimin Tamamen Kaydedilmesi
 - Etkin veya Sorunlu Servislerin/Ağ Bağlantılarının Takibi
- Ağ İzleme ile Hedeflenenler
 - Gerçek Zamanlı ve Belirli Süreleri İçeren Ağ Trafik Yükü Takibi
 - Sorun Giderme ve İhlal İnceleme için Girdi Hazırlama
 - Ağ Servislerinin Yükü ve Kullanım Tipi Takibi
 - Kullanıcı İşlemlerinin Takibi
 - Ağ Bağlantısı veya Servislerindeki Anlık Kesintilerin Takibi

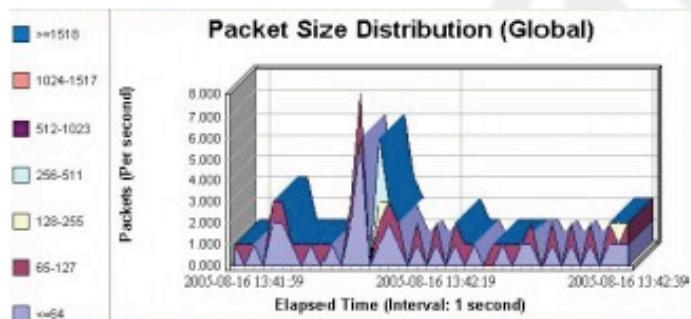


Ağ İzleme Yazılımları

Gebze Fabrika Ağ Kullanımı



Internet Çıkışı Ağ Kullanımı



Aktif Sunucu ve Ağlar



Web Sunucusu Bağlantıları

```

192.168.0.1 : 46550 ----> webserver : 80
192.168.5.8 : 36450 ----> webserver : 443
192.168.0.1 : 18550 ----> webserver : 80
172.16.1.9 : 54443 ----> webserver : 80
192.168.0.1 : 43223 ----> webserver : 443
  
```

Saldırı Tespit Sistemleri

- Saldırı, Normal-Dışı İşlem ve Yetki İhlali izleme/önleme amaçlı olarak kullanılmaktadır
- Kullanım amaçlarına bağlı olarak bir “Erişim Denetim” sistemi gibi de çalışabilmektedirler
- Ağ, sunucu veya belirli bir uygulamaya yönelik olan saldıruları tespit etmek veya önlemek amaçlı kullanılabilmektektir
 - Ağ Temelli (Ağ Geçidi veya Dinleme Temelli)
 - Sunucu Temelli
 - Web Uygulaması Güvenlik Duvarı
 - Veritabanı Uygulaması Güvenlik Duvarı
- Saldırı Tespit Yöntemleri
 - Tanımlı Saldırı İmzaları ile Saptama
 - Tanımlı Zaafiyet İmzaları ile Saptama
 - Normal / Anormal Tanımı Ayırıştırması ile Saptama

Sunucu Temelli Saldırı Tespit Sistemleri

- Sistem çekirdeği ile bütünlüğe; süreçlerin yapmış oldukları normal dışı işlemleri saptamak ve durdurmak hedeflenmektedir
- Saldırı tanımı farklı şekillerde yapılabilir
 - İşletim sistemi bileşenlerinin normal dışı davranışları
 - Süreçlerin normal dışı sonlanması veya sistem görevi ihlali
 - Kullanıcı işlemlerinin tanımlanmış yetkileri ihlal etmesi
 - Diğer saldırısı/ihlali imzalarının tanımlanması
- İşletim sistemi ile bütünlüğe ve diğer saldırısı tespit sistemleri ile beraber çalışma önemlidir
 - İşletim Sistemleri Arası Farklılıklar
 - Platformlar Arası Farklılıklar
 - Farklı Saldırı Tespit Sistemlerinin Haberleşmesi
- Etkin tepki yönetimi çekirdek seviyesinde sağlanmalıdır

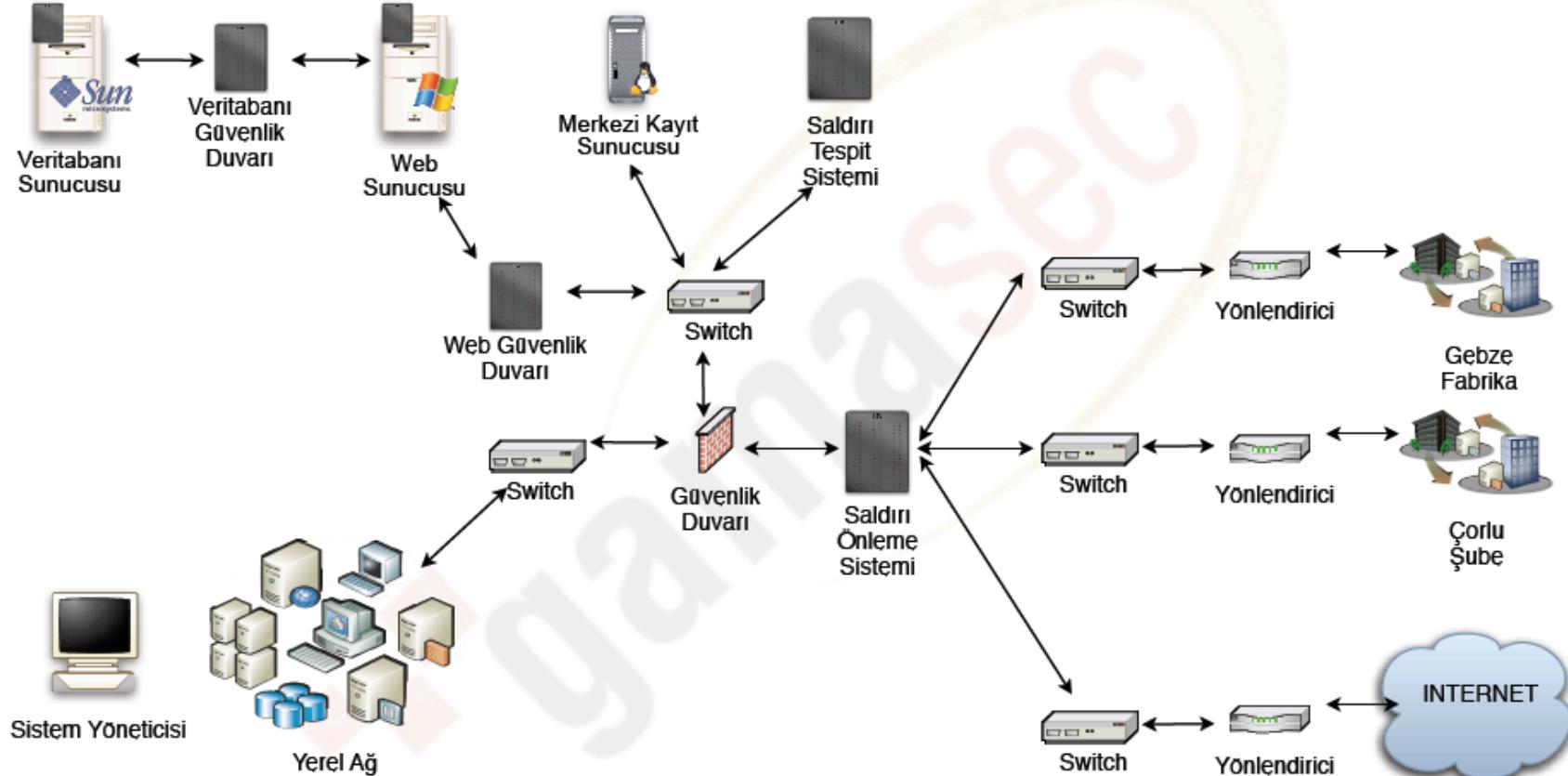
Ağ Temelli Saldırı Tespit Sistemleri

- Ağ üzerinde akmakta olan veri trafiği içinde genel veya özel normal dışı işlemleri saptamak ve önlemek için kullanılır
 - Hat İçi Saldırı Tespit Sistemleri (Intrusion Prevention System)
 - Switch üzerinde port yönlendirme yapılan sensörler
- Ağ Yerleşimi ve Kriptolama
 - İzlenecek Sistemlerin Tüm Trafiği Tekil Olarak Alınmalıdır
 - Kriptolu İletişim Sonlandırıldıktan Sonra İzlenmelidir
- Saldırı Saptama Yöntemleri
 - Anormal ağ trafiği ve yükü oluşumu
 - Ağ protokollerinin içinde olası saldırı imzalarının aranması
 - Ağ protokollerindeki normal dışı davranışlar
- Saldırı Önleme Yöntemleri
 - TCP/Reset ve ICMP Hata Mesajları
 - Hat İçi Kullanımda Paketin Düşürülmesi
 - Güvenlik Duvarı veya Yönlendirici ile Uzun Süreli Engellemeye

Uygulama ve Veritabanı Güvenlik Duvarları

- Ağ ve Sunucu temelli saldırı tespit sistemlerinin uygulamalara özel davranışlarda karşılaşıkları zorlukları aşmak için kullanılmaktadır
- Web Temelli Uygulama Güvenlik Duvari
 - Saldırı Yöntemi Tanımlanabilir, Zaafiyet Tanımlaması Zordur
 - Web Uygulaması İçeriği Doğru Biçimde Çözümlenebilmeli
 - SSL/TLS Sonlandırması Sonrası Yerleşim Sağlanmalı
 - Önleme Dahili Olarak Yapılmalı
- Veritabanı Güvenlik Duvari
 - Veritabanı Sunucusu Yazılımı Konusunda Bilgili Olmalı
 - SQL Cümlecikleri ve Veritabanı Yetkilendirmesi Tanımlanabilmeli
 - Yerleşim, Web Uygulaması ile Veritabanı Arasında Omalıdır
 - Önleme Dahili Olarak Yapılmalı
- Diğer saldırı tespit sistemleri ile entegrasyon önleme ve tespit adına oldukça önemlidir

Saldırı Tespit Sistemleri Yerleşimi



Saldırı Tespit Sistemi Yapılandırması

- Saldırı tespitine bütün olarak bakılmalı, tüm saldırı tespit bileşenleri ve teknolojileri merkezi olarak yönetilebilmeli ve iletişim içinde olmalıdır
- Criptolu iletişimler izleme öncesinde sonlandırılmalıdır
- Saptanan saldırılar veya normal dışı işlemler merkezi olarak kayıt edilmelidir
- Saldırı önleme için genel bir davranış modeli benimsenmeli ve uygulanmalıdır
- Düzenli olarak kural ve saldırı imzası veritabanı güncellenmelidir
- Ağ temelli sistemlerde yoğun veri trafiğinin işlemci kullanımını artıracası ve bazı iletişimlerin yakalanamayacağı dikkate alınmalıdır
- Ağ temelli sistemlerde amaca uygun olarak her bir iletişim noktasında farklı sensörler veya saldırı tespit bileşenleri kullanılmalıdır
- Üretilen kayıtlar ve raporlar düzenli olarak izlenmeli ve incelenmelidir
- Kural ve yapılandırma yedekleri düzenli olarak alınmalıdır

Güvenlik Açığı Analiz Sistemleri

- Yazılımların, ağ cihazlarının, ağ servislerinin ve işletim sistemlerinin, yayınlanmış güvenlik açıklarının denetimi amaçlı kullanılırlar
- Güvenlik açığı tespit yöntemleri
 - Bilinen saldırı yöntemlerinin kullanımı
 - Bilinen güvenlik açıklarının kontrolü
 - Sıkça yapılan yapılandırma hatalarının kontrolü
- Farklı mimarileri ve kullanım alanları bulunmaktadır
 - Ağ temelli zaafiyet analizi
 - Sunucu temelli zafiyet analizi
 - Web uygulaması temelli zaafiyet analizi
 - Veritabanı sunucusu temelli zaafiyet analizi
- Yapılandırma
 - İlgili sisteme özel tarama profilleri oluşturulmalı
 - Düzenli olarak güvenlik açığı veritabanı güncellenmeli
 - Güvenlik açığı denetimleri düzenli olarak yapılmalı ve çıktılar sonucunda çözümler üretilmeli



Kriptolama Teknolojileri

Kriptolama Teknolojileri

- Kriptolama, gizlilik, bütünlük ve inkar edilemezlik için kullanılmaktadır
- Kullanım amaçları doğrultusunda farklı kriptolama algoritmaları ve kriptolama türleri bulunmaktadır
 - Veri Özeti Algoritmaları (MD5, SHA-1, SHA-256)
 - Simetrik Algoritmalar (DES, 3DES, AES)
 - Asimetrik Algoritmalar (RSA)
 - El Değiştirme Protokolü (Diffie-Helman)
 - Sayısal İmza (DSA)
 - Veri İçine Veri Saklama (Stenografi)
- Genel Kullanım Yöntemleri
 - Dosya ve Verilerin Bütünlüğünün Kontrolü
 - Verilerin ve İletişimin Gizlenmesi
 - Alınan Verinin Gönderici Kimliğinin Doğrulanması

Kriptolama Teknolojilerinin Uygulama Alanları

- Açık Anahtar Altyapısı
 - Sayısal Sertifika veya Açık Anahtar Kriptolama ile oluşturulan, toplu iletişim altyapısı
 - Merkezi açık anahtar yönetimi, açık anahtar algoritmaları ve sayısal imza kullanımı
- Kriptolu Ağ İletişimi
 - Web, E-Posta ve diğer ağ protokollerinin içeriğinin kriptolanması
 - Kriptolu tünel ve taşıma ortamları oluşturulması
- Kriptolu Saklama ve Depolama
 - Kriptolu dosya sistemi, gizli içeriğin taşınması, güvenli yedekleme
- Kimlik Doğrulama
 - Kullanıcı kimliklendirilmesi, sayısal imza ile inkar edilemezlik
- Kriptolu Yazışma
- Verilerin Bütünlüğünün Kontrolü
- Verilerin Geri Döndürülemez Hale Dönüşürülmesi

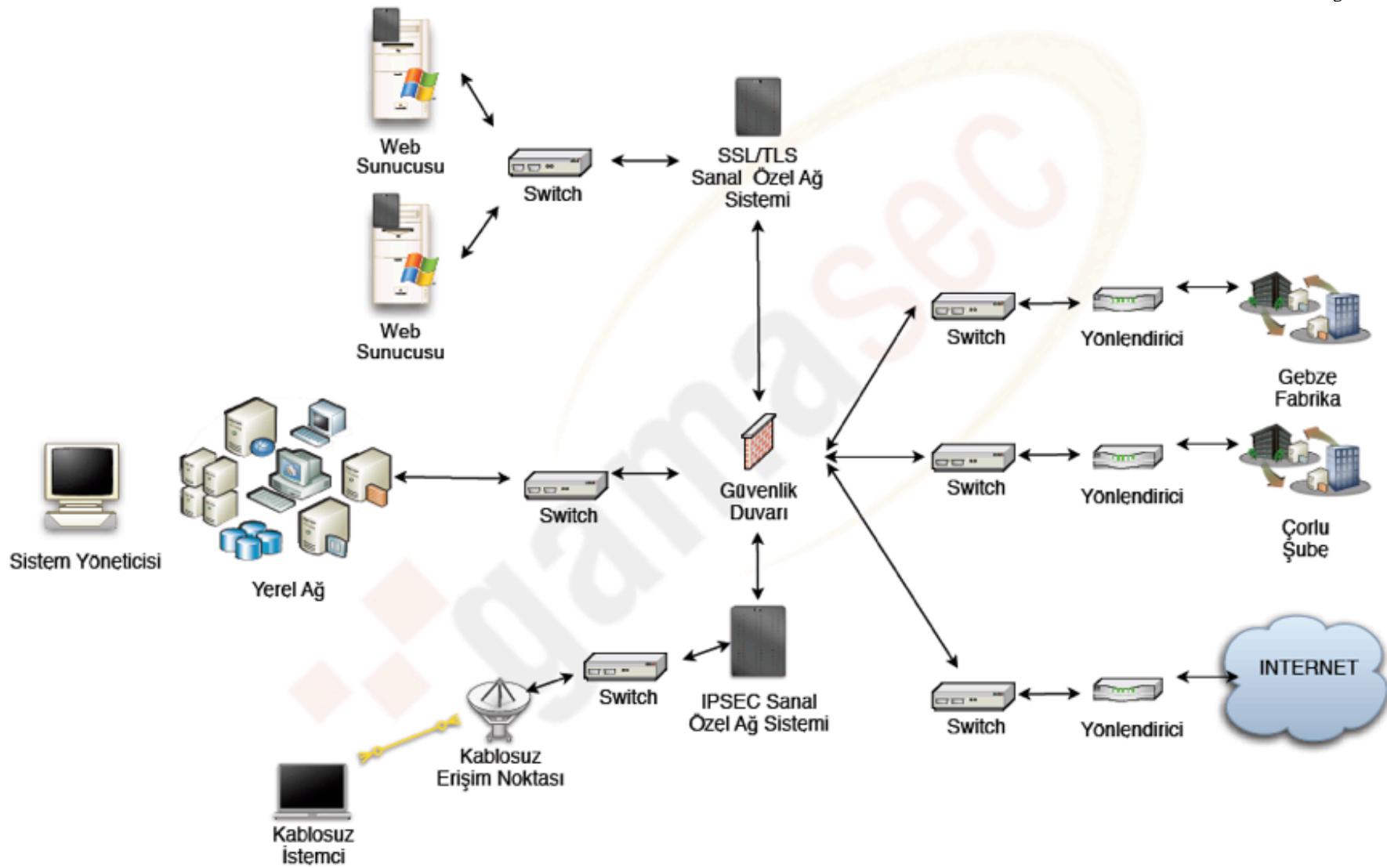
Sanal Özel Ağ Teknolojileri

- Güvensiz ağlar üstünden güvenli iletişim kurabilmek için geliştirilmiştir
 - Mobil çalışma
 - Sunucular arası veya ağlar arası güvenli iletişim
- Birçok farklı protokol ile uygulanabilir, esas amaç IP protokolü üzerinde güvenli olarak farklı protokollerini taşıyabilmektir
 - IPSEC (ESP, AH, IKE/ISAKMP)
 - PPTP, L2TP, MPLS
 - TLS/SSL
- Ağlararası yapılabileceği gibi, Ağ-İstemci ve İstemci-İstemci modelleriyle de uygulanabilir
- İletişim güvenliğine bağlı olarak farklı kriptolama algoritmaları kullanımı gerektirebilmektedir
- Harici doğrulama sistemleri ile kimlik tanımlama ve doğrulama yapılmalıdır

Sanal Özel Ağ İletişim Protokollerı

- IPSEC (Internet Protocol SECurity)
 - ESP (Encapsulating Security Payload) Protokol : 50
 - AH (Authentication Header) Protokol : 51
 - IKE (Internet Key Exchange Protocol) Protokol : TCP/UDP 500
 - ISAKMP
- PPTP (Point to Point Tunneling Protocol) Protokol : TCP 1723
- L2TP (Layer 2 Tunneling Protocol) Protokol : 115
- SSH (Secure Shell) Protokol : TCP 22
- GRE (Generic Routing Encapsulation) Protokol : 47
- MPLS (Multi Protocol Label Switching)

Sanal Özel Ağ Yerleşimi



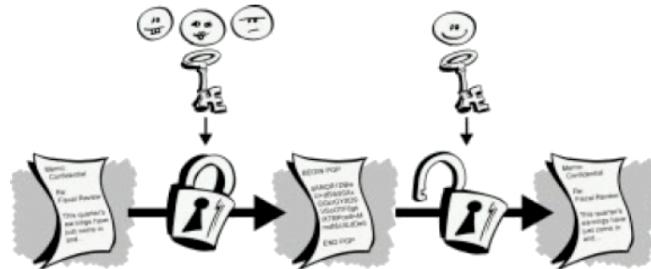
Sanal Özel Ağ Yapılandırması

- Sanal Özel Ağ sunucusu güvenlik duvarının DMZ alanında yer almalı
- Sanal Özel Ağ, güvenlik duvarından kriptosuz olarak geçecek biçimde yapılandırılmalı ve yerleştirilmeli
- Kullanıcı ve istemci kimliklerinin yönetimi için harici doğrulama sistemleri tercih edilmelidir
 - Sayısal Sertifika, Tek Kullanımlık Şifre, Biyometrik Doğrulama
- İşlem ve iletişim kayıtları tutulmalı, düzenli olarak incelenmeli ve sunulan hizmetler ile iletişim türleri karşılaştırılmalıdır
- Amaca uygun kriptolama algoritmaları tercih edilmelidir, zaafiyet barındıran algoritmalar kullanılmamalıdır
- Tercih edilen istemci yazılımlarının ek güvenlik özellikleri taşımmasına özen gösterilmelidir
 - İstemci Güvenlik Duvarı
 - Anti-Virüs Yazılımı

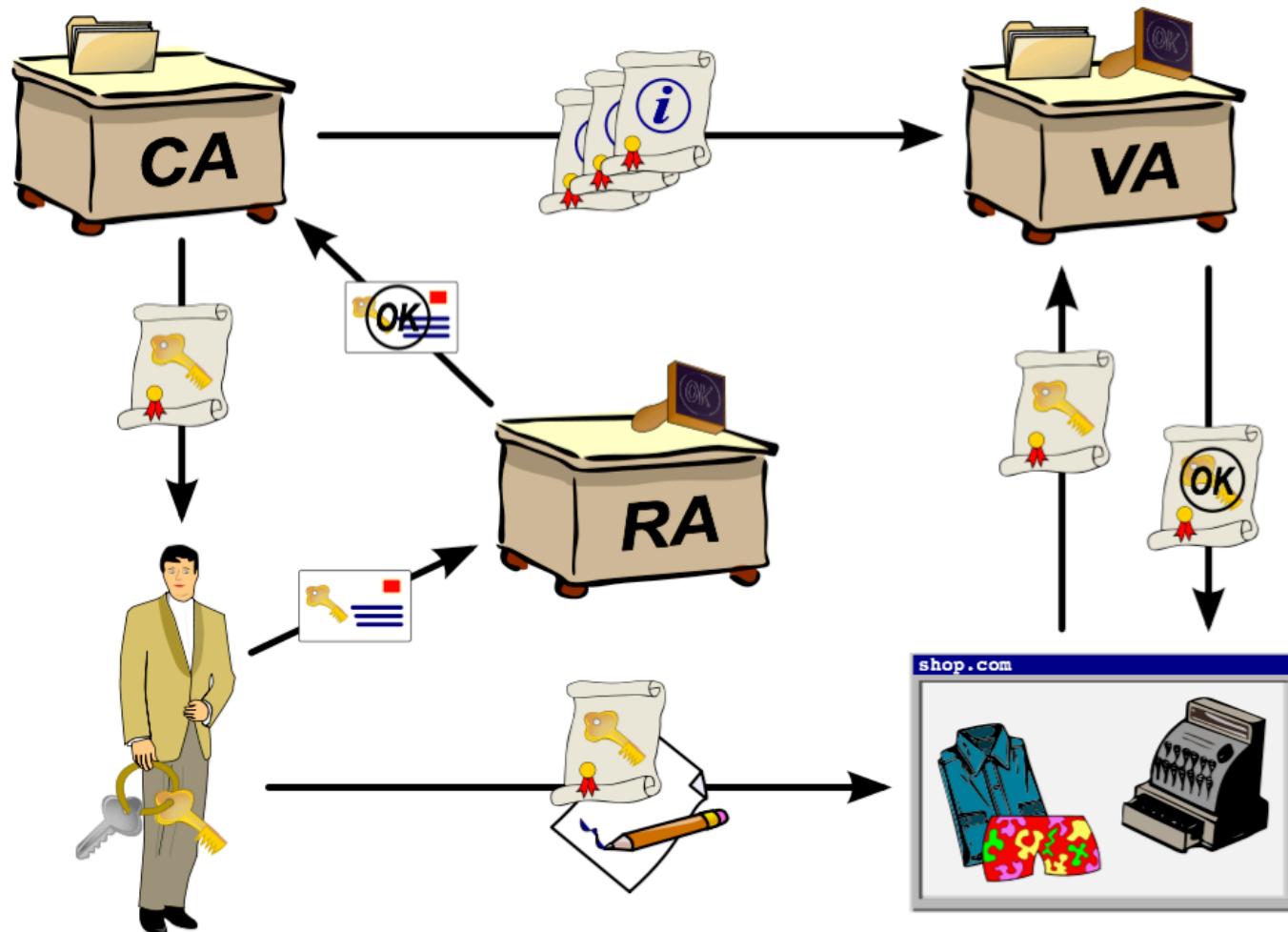
Açık Anahtar Altyapısı (PKI)

- Açık anahtar kriptolamanın temel problemi olan açık anahtarın dağıtılması ve yönetilmesi sorununa çözüm olarak geliştirilmiştir
- Açık Anahtar Altyapısı
 - Sertifika Otoritesi
 - Kayıt Otoritesi
 - Doğrulama Otoritesi
 - Sayısal Sertifika (x.509)
 - Sertifika Geçersizlik Listesi (CRL)
 - Sertifika Dağıtım Sistemi
- Sık Kullanım Alanları
 - S/MIME
 - SSL/TLS
 - Sayısal Sertifika ile Doğrulama

Açık Anahtar Gizli Anahtar



Açık Anahtar Altyapısı (PKI)



PGP

- PGP
 - Açık anahtar kriptolama uygulamasıdır ; gizlilik, bütünlük ve inkar edilemezlik sağlar
 - Açık Anahtar Altyapısından farklı olarak Sertifika Otoritesi gerektirmez, Güven Web'i ile çalışır
 - Herkes kendi anahtarlarını oluşturma, yayınlama ve kendi güven ilişkilerini belirleme özgürlüğüne sahiptir
 - Merkezi anahtar sunucusu ve açık anahtar yönetim sistemi oluşturma imkanı mevcuttur
 - OpenPGP standartı doğrultusunda kriptolama yapılır
- Kullanım Alanları
 - Yazılımı iletişim
 - Disk kriptolama

Bütünlük Takip Sistemleri

- Dosya sistemi üzerinde yapılan değişiklikleri takip etmek için kullanılmaktadır
 - Kritik sistem dosyalarındaki değişimler
 - Verilerin tutulduğu hassas dosyalardaki değişimler
 - Arka kapı, virüs veya truva atı nedeniyle oluşan değişimler
- Dosya ve dizinlerin “veri özeti” tek yönlü kriptolama algoritmaları ile alınır ve düzenli olarak karşılaştırılır
 - MD5, SHA-1, SHA-256
- Yapılandırma
 - Veri özetleri aynı dosya sisteminde tutulmamalıdır
 - Veri özeti için birden fazla algoritma kullanılmalıdır
 - Düzenli olarak sistem bütünlüğünü kontrol edilmeli, bütünlük doğrulandıktan sonra veri özetleri güncellenmelidir

SSL ve TLS

- HTTP protokolünün düz metin olarak veri akışını sağlama, güvenliğin önemli olduğu durumlarda tatmin edici değildir. Bu amaçla SSL teknolojisi oluşturulmuş ve daha sonra yerini TLS'e bırakmıştır
 - SSL (Secure Socket Layer)
 - TLS (Transport Socket Layer)
- Açık anahtar altyapısını kullanmaktadır
- Sayısal sertifikalar, veri özetleri, sertifika otoriteleri ve sayısal imzalar en önemli yapı taşılardır
- Amaç başlangıçta HTTP trafiğinin kriptolu olarak akmasını sağlamak iken zaman içinde farklı protokoller (FTP, IMAP, POP3, SMTP) için de kullanılabilecek hale gelmiştir
- SSL VPN olarak anılan ve Web üzerinden ağ erişim sağlayan sanal özel ağ çözümü de mevcuttur



İçerik Denetim Teknolojileri

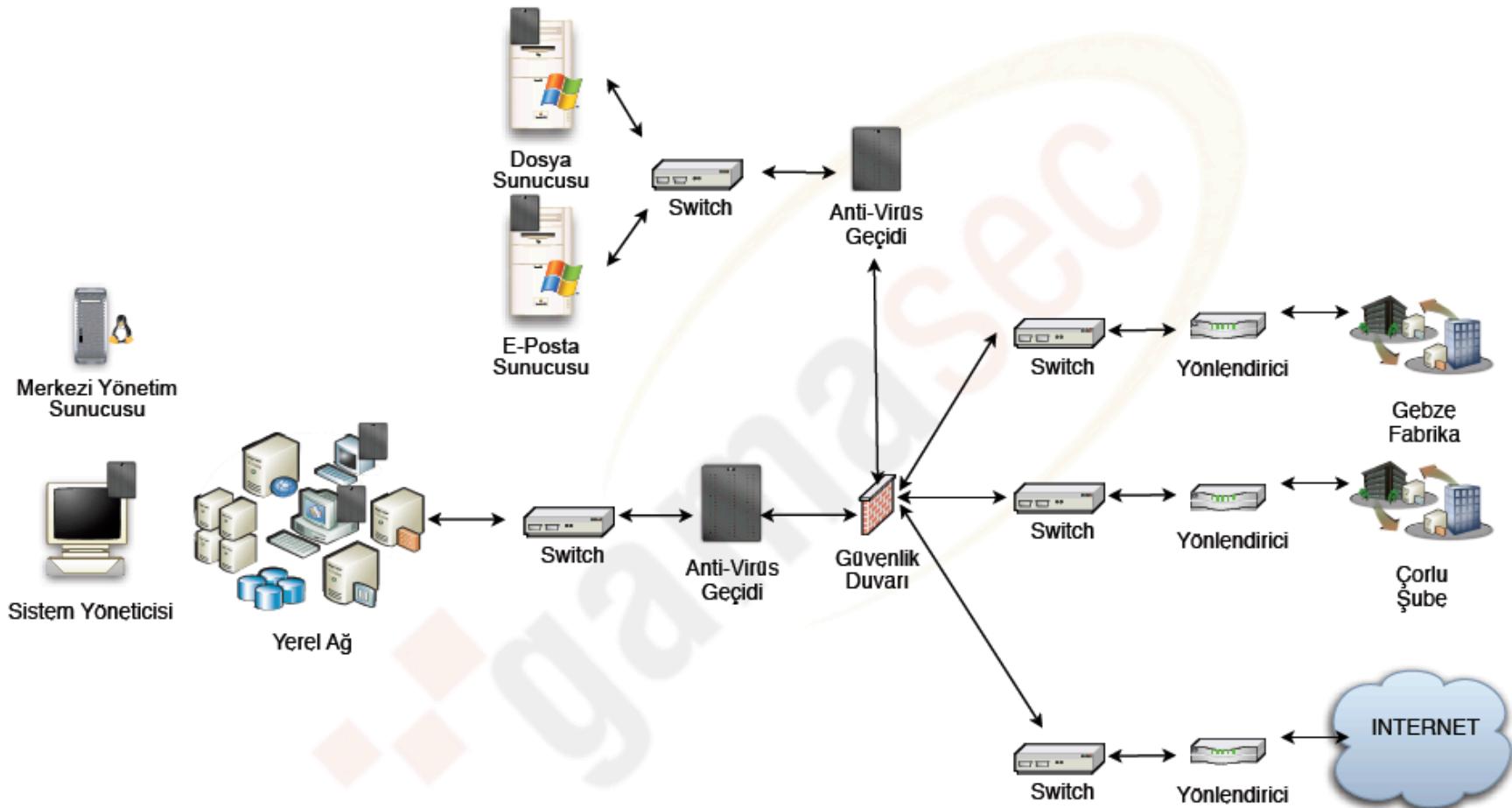
İçerik Denetim Sistemleri

- E-Posta, web sayfaları ve diğer ağ iletişimleri üzerinde istenmeyen içeriğin kurum ağına girmesini önlenmesi amacıyla kullanılmaktadır
 - İstenmeyen E-Postalar (Spam, Dosya Ekleri)
 - Zararlı Kodlar (Virüs, Worm, Truva Atı, Casus Yazılım)
 - İstenmeyen Web Sayfalarının İçeriği
- Amaçları doğrultusunda gruplanırlar
 - Anti-Virüs Sistemi
 - Casus Yazılım Önleme Sistemi
 - Web Sayfası İçerik Filtrelemesi
 - Spam Önleme Sistemi
- Amaçlara göre kullanım şekilleri de değişmektedir
 - Ağ Geçidi
 - Proxy Geçidi
 - Sunucuya Kurulum (E-Posta, Web vb.)
 - İstemciye Kurulum

Anti-Virüs Sistemleri

- Kötü niyetli yazılımların tespiti, temizlenmesi veya karantinaya alınması için kullanılırlar
- Kötü niyetli yazılımların bazı özelliklerine göre imzalar oluşturur ve bu imzaları tarama yöntemiyle çalışırlar
- Tahmini olarak bir kötü niyetli yazılımı saptayabilmektedirler
 - Normal olmayan süreç davranışısı
 - Normal olmayan dosya içeriği
- Sıkıştırılmış veya özel formattaki dosyaların içeriklerini de tarayabilmektedirler
 - Sıkıştırma Algoritmaları
 - Dönüştürme Algoritmaları
 - Criptolama Algoritmaları
- Sunucularda, istemcilerde kullanılabilıldığı gibi ağ geçidi olarak yada güvenlik duvarı ile beraber çalışarakta kullanılabilirler
- Merkezi bir yönetim arabiriminden yönetilmeleri tercih edilmelidir

Anti-Virüs Sistemi Yerleşimi



Anti-Virüs Sistemi Yapılandırması

- Amaca uygun mimari ve yerleşim seçilmelidir
- Virüs İmzaları Güncellemesi
 - Otomatize olarak yapılmalıdır
 - Virüs veritabanları merkezi olarak yönetilebilmeli, izlenebilmelidir
 - Elle virüs imzası ekleme imkanı bulunuyorsa kullanılmalıdır
- Her kritik noktada bir Anti-Virüs bileşeni olmalıdır
 - Dosya, E-Posta, Web, Proxy sunucuları
 - İstemcilerin tamamı
 - Ağ geçidi, güvenlik duvarı
- Sunucu veya İstemciye yüklenen sürümlerinin yapılandırılması değiştirilememelidir
- Merkezi yönetim üzerinden izlemeler yapılmalı, Anti-Virüs sistemlerinin güncelleme, virüs kayıtları ve aldıkları önlemler takip edilmelidir

Casus Yazılım Önleme Sistemleri

- Anti-VİRÜS sistemlerinin casus yazılımlara karşı yetersizliklerinden dolayı gelişmiş bir teknolojidir
- Ağırlıklı kullanımı istemci sistemleridir
- Ortak casus yazılım veritabanları ile tanımlanmamış veya normal-dışı davranış gösteren süreçleri incelemektedirler
- Sürekli etkin durumda olmaları gerekmektedir, casus yazılımlar birçok ücretsiz/deneme sürümü uygulamalarda bulunmaktadır
- İşletim sistemleri ile bütünleşik çalışmalıdır
 - Normal süreçlerin tanınması
 - Normal işleyişte düzeltilemeyen özelliklerin, özel modda düzeltilebilmesi
 - Mimarisel eksiklerin kapatılması
- Merkezi yönetim arabirimini takip edilmeli, casus yazılım veritabanları güncellenmeli ve ağıdaki istemciler düzenli olarak denetlenmelidir

Spam Önleme Sistemleri

- Günümüzde yaygınlaşan ve e-posta trafiğinin %80'ine ulaşabilen istenmeyen e-postaların ayıklanabilmesi amacıyla kullanılmaktadır
- Yerleşim
 - E-Posta Sunucusu
 - Ağ Geçidi
 - İstemci Sistemleri ve E-Posta İstemcileri
- Mimariler
 - Tanımlanan kurallar ile değerlendirme
 - Bayesian ile öğrenme
 - Normal durumların matematiksel olasılığı
 - Normal olmama ihtimalinin hesaplanması
- Her iki mimariyi destekleyen sistemler tercih edilmeli, zaman içinde eğitilmeli ve özelleştirilmelidir

Web Sayfası İçerik Denetim Sistemleri

- Kullanıcıların gezmiş oldukları web sayfalarının içeriklerinin denetimini ve izlenmesini sağlamaktadırlar
- Kelime bazında veya listelenmiş sitelerin engellenmesi bazında çalışmaktadır
- Sezgisel tanımlama ve önleme, özellikle büyük veritabanına sahip yazılımlar tarafından daha verimli yapılmaktadır
- Cinsel, siyasi veya illegal içerik barındıran sitelerin engellenmesi amacıyla kullanılabilmektedir
 - Kurum çalışmalarını aksatacak içerikler (oyun, eğlence vb.)
 - Kurumu sorumluluk altına sokabilecek içerikler (siyasi, cinsel vb.)
- İçerik denetim sistemleri ortak tanımlamalar ile çalışmaktadır
- Listelenen web sitelerinin ve kötü niyetli site içeriği tanımlarının düzenli olarak güncellenmesi gerekmektedir
- Web sayfalarının art niyetli olma ihtimalleri de içerik üzerinde yapılan anlam çıkarma ile saptanabilmektedir



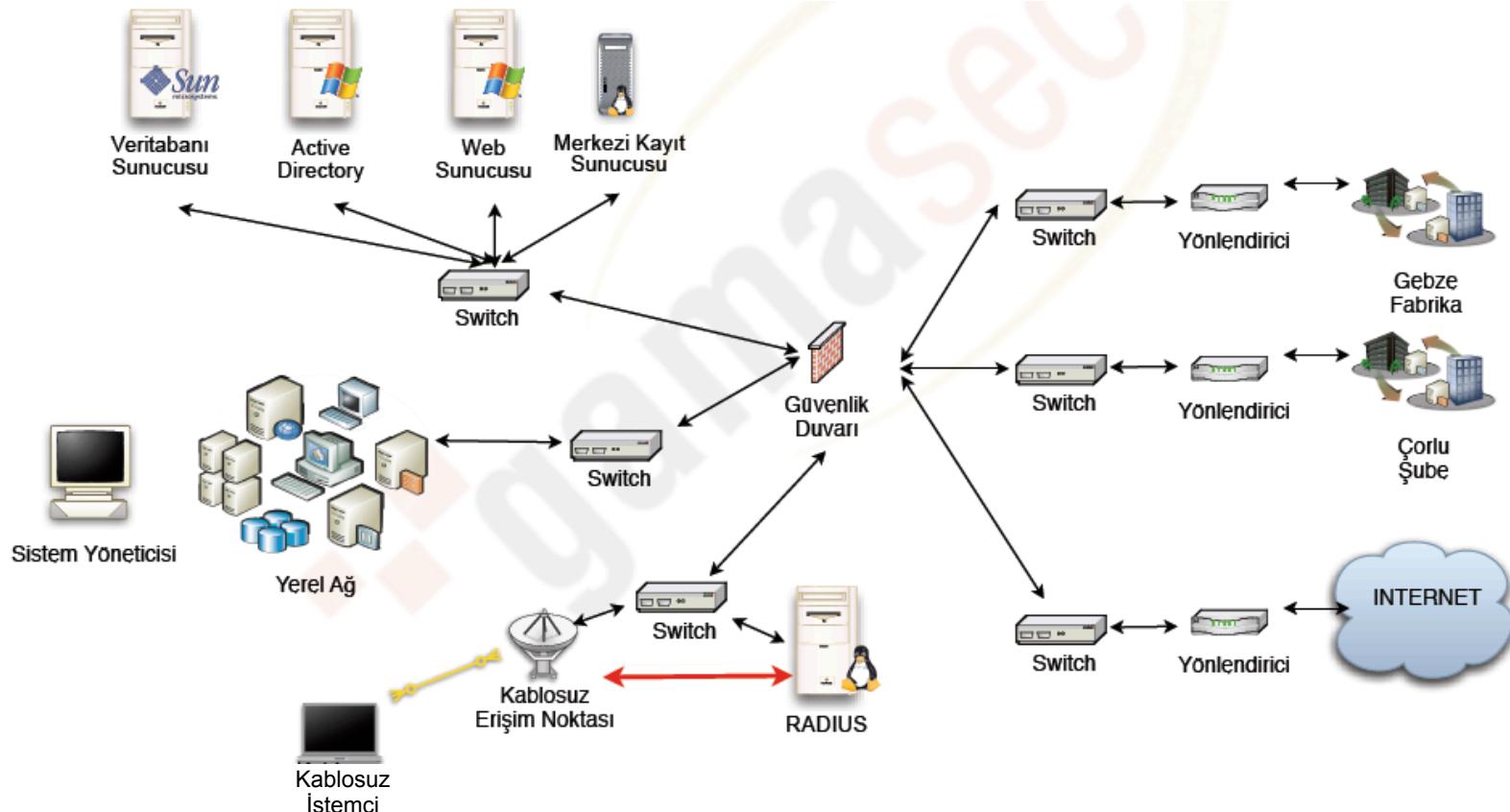
İş Sürekliliği ve Yük Dağılımı Teknolojileri

İş Süreklliliği

- Erişilebilirlik kavramının en önemli yansımasıdır
- Sunucu, Ağ Servisi, İletişim gibi kritik olabilecek her bilişim sistemi iş sürecindeki rolünü aksatmadan sürdürmelidir
- Tek Noktada Hata Analizi
- İş Süreklliliği Çözümleri
 - Kümeleme
 - Hata Toleransı
 - Yük Paylaşımı
 - Yük Dağılımı
 - Ortak Kaynak Kullanımı
 - Sistem İkizleme
 - İstek Yönlendirme
 - Veri Depolamada Sürekllilik
 - RAID
 - Ortak Depolama
 - Kesintisiz Güç Kaynağı

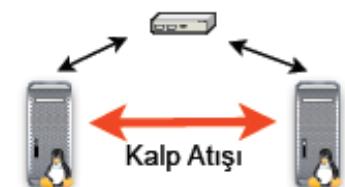
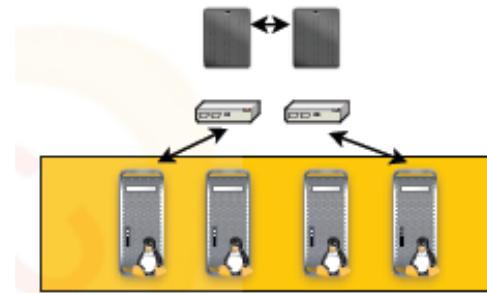
Tek Noktada Hata Analizi

- Her bir ağ/sistem bileşeni için yapılan, devre dışı kalması durumunda oluşabilecek aksamanın hesap edilmesi, sistem önceliklendirme



Kümeleme

- Birlikte Çalışabilirlik
 - Ortak Süreçler
 - Donanım Kaynakları Paylaşımı
- Yük Dağılımı
 - Yük Dağıtıcı
 - Bağımsız/Bağımlı Sistemler
- Hata Toleransı Yapısı (Failover)
 - Kalp Atışı
 - Verilerin Senkronizasyonu
 - Asıl Sistem Yerine Geçme



Diğer İş Sürekliliği Çözümleri

- Ağ Protokollerleri ile İş Sürekliliği
 - BGP
 - DNS
 - ARP
- Donanım İkizleme
 - RAID
 - Çift Ağ Kartı
 - Çift Güç Kaynağı
- Sanal Sistemlerin Kullanımı
 - Sanal Sunucu
 - Sanal Makine

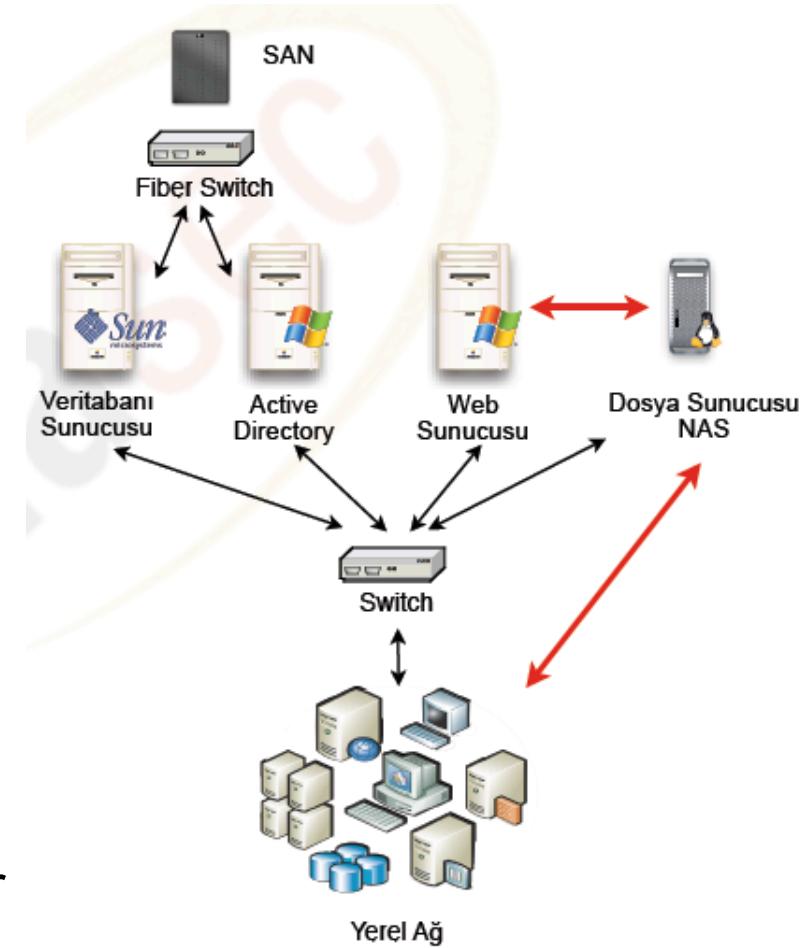
Veri Depolama ve Yedekleme Teknolojileri

Veri Depolama

- İş sürekliliği, gizlilik ve bütünlük kriterleri doğrultusunda verilerin doğru biçimde depolanması gerekmektedir
 - Veriler Sürekli Erişilebilir Olmalı
 - Verilerin Gizliliği Önceliklendirilebilmeli
 - Aktarım veya Depolama Ortamında Veri Bozulması
 - Erişim Denetimi ve Yetki Yönetimi
- Dosya Sistemleri
 - Fat32, Ntfs, Ext3, Ext4, XFS, ReiserFS
- Kriptolu Dosya Sistemleri
 - EFS, Crypto Loopback, File Vault, PGP Disk
- Ağ Temelli Veri Depolama
 - Dosya Paylaşımı ile Merkezi Depolama (Samba, NFS+, AFS)
 - NAS/SAN Çözümleri
- RAID Çözümleri

Dosya Sunucusu, NAS ve SAN

- Dosya Sunucusu
 - Ağ Servisleri ile Dosya Paylaşımı
 - Standart İşletim Sistemi
- NAS (Network Attached Storage)
 - Ağ Servisleri ile Dosya Paylaşımı
 - Kısıtlı Özellikli İşletim Sistemi
- SAN (Storage Area Network)
 - Fiber Kanal ile Kullanılır
 - Dosya Sistemini Sunucular Yönetir



RAID

- Çok sayıda diskin tek disk olarak çalıştırılabilmesi
 - Kapasite Arttırımı
 - Yedekleme
 - Donanımsal Sorunların Önüne Geçme
 - Performans Artışı
- Yazılımsal veya Donanımsal olarak sağlanabilir
- SCSI ve IDE disklerde yapılabilir, harici RAID kartı gerekli değildir; iş sürekliliği söz konusu ise RAID kartı, SCSI disk ve anlık tak/çıkar desteği tercih edilmelidir
- RAID Türleri
 - 0 -> İki diskin parite kontrolü olmadan tek disk gibi çalışması
 - 1 -> İki diskten birinin sürekli diğerine ikizlenmesi
 - 3 -> En az 3 diskin (parite diski sabit olmak üzere) pariteli olarak tek disk gibi çalışması
 - 5 -> En az 3 diskin pariteli olarak tek disk gibi çalışması

Yedekleme

- Veri yedekleme, felaket veya ihlalden geri dönüşlerde kritik önem arz etmektedir
- Kritik veriler kriptolu olarak yedeklenmelidir ve veri özeti alınmalıdır
- Veriler, geri dönüşü kolay ortamlarda ve biçimde yedeklenmelidir
- Merkezi Yedekleme Yapısı
 - Yedekleme Sunucusu
 - Dosya Sunucusu / NAS / SAN ile Yedekleme
- Yedekleme Türleri
 - Tam Yedekleme
 - Artımlı Yedekleme
 - Farklılık Temelli Yedekleme
- Yedekleme Ortamı Değiştirme Yöntemleri
 - Basit (Günlük 5, Aylık 12 Ortam)
 - Büyükbaba-Baba-Oğul (Günlük 4, Haftalık 4, Aylık 12 Ortam)
 - Honai Kulesi



İstemci Güvenliği Teknolojileri

İstemci Güvenliği

- Çalışanların kullanmakta olduğu sistemler, en riskli ve müdahalesi en zor sistemlerdir
 - Mobil Kullanıcılar (PDA, Taşınabilir Bilgisayar, Cep Telefonu)
 - Kişisel Bilgisayarlar (Güncel Yazılımlar, Oyunlar)
 - Kullanılan Harici Donanımlar (Taşınabilir Disk, Kamera, Kablosuz Ağ)
- İstemci Sistemlerindeki Sorunlar
 - Taşınabilir Depolama Ortamları
 - Müdahaleye Kapalı İşletim Sistemi
 - İstemci Yazılımlarının Yetersizliği ve Sistem Yükü
 - Bağlantı Türleri ve Yöntemleri
 - Kullanıcıların Kısıtlı Bilgisi
- İstemci Güvenliğine Çözümler
 - Güvenlik Teknolojilerinin İstemci Sürümleri
 - Bütünleşik İstemci Güvenliği Yazılımları
 - Çalışanların Cihazlarına ve Kurumal Ağa Erişim Haklarının Kısıtlanması

Bütünleşik İstemci Güvenliği Yazılımları

- Çok sayıda amaç için birçok teknolojiyi barındıran tek bir uygulama
 - Güvenlik Duvarı
 - Saldırı Tespit/Önleme Sistemi
 - Spam Koruma
 - Anti-Virüs, Casus Yazılım Sistemi
 - Taşınabilir Disk Takibi
 - Veri ve İletişim Kriptolama
- Merkezi Yönetim
 - Kurum ağında iken düzenli izleme ve inceleme
 - Kurum dışı çalışmalarında, bağlantı anında inceleme
- Mobil Cihazlara Özel Güvenlik Teknolojileri
 - Cep Telefonu ve El Bilgisayarı Güvenliği
 - Kablosuz Ağ ve Bluetooth Koruması
- Önceden tanımlanmış çalışma şeklinin kullanıcı tarafından değiştirilememesi

Kaynaklar

- The CISSP Prep Guide: Gold Edition
- IT Governance: A Manager's Guide to Data Security and BS 7799 / ISO 17799
- Information Security Management Handbook
- Writing Information Security Policies
- Security Engineering: A Guide to Building Dependable Distributed Systems
- Applied Cryptography: Protocols, Algorithms, and Source Code in C
- Business Continuity Planning: A Step-by-Step Guide