Bilgi Güvenliği ve Risk Analizi

BSP 572 Ağ ve Bilgi Güvenliği Dersi – Necmettin ÇARKACI

Sunumda özgün katkım çok azdır. Sunum büyük çoğunluğu kaynaklardan derlenmiştir.

Haftalık Ders Takip Listesi

- Siber Güvenliğe Genel Bakış ve Güncel Trendler
- **Bilgi Güvenliğinde Risk Analizi**
- **Kriptoloji**
- **Sızma Testi ve Bilgi Toplama Teknikleri**
- **Ağ Güvenliği ve Keşif ve Zafiyet Tarama**
- **Dijital Adli Analiz**
- **Nüfuz Tespit, Güvenlik Duvarı ve Biyometrik Güvenlik**
- **Zararlı Yazılım Analiz Yöntemleri**
- **Bilgi Toplama ve Sosyal Mühendislik Saldırıları**
- **Exploit Geliştirmenin Temelleri**

Geçen Haftadan...

Maslov İhtiyaç piramidi

Geçen Haftadan...

- Siber savunma ile ilgili yanlış düşünceler
- Bilgi Güvenliği ve Siber Güvenlik
- Siber Tehditlerin Özellikleri
- Dünyada ne değişti
- Siber Tehditlerin Hedefleri
- Siber Savaş mı?
- APT (Hedef Odaklı Saldırılar)

Bilgi Güvenliğinde Risk Analizi

Bilgi Güvenliği Yönetimi

- Güvenlik yönetimi ilgilendiren bir konudur.
- Varlıkları korumak için oluşturulur.
- Başlayıp bitirilen değil devam eden bir süreçtir.

Bilgi Güvenliği Programı

İyi bir bilgi güvenliği programı

- Bilgiyi sınıflandırmayı
- Politika, prosedür ve standartlarını
- Güvenlik eğitimini
- Güvenlik örgütlenmesini
- Risk yönetimini içerir.

Güvenlik Programının Hedefleri

- Kısa vadeli **Operasyonel** hedefleri olmalıdır. Örn : İşletim sistemi güncellemesi
- Orta vadeli **Taktik** hedefleri olmalıdır. Örn : Bütün makineler domain yapısına dahil edilecek.
- Uzun vadeli **Stratejik** hedefler olmalıdır. Örn : Merkezi bir bilgi güvenliği yapısının olması

Hedefler

- Kurumdan kuruma ve aynı kurumda zamanla değişir
  - Askeri Kurumlar : Gizlilik
  - Bankalar : Bütünlük
  - Bireysel Yapılar : Prestij
  - Ticari Kurumlar : Erişebilirlik
  - Devlet kurumları : Gizlilik, bütünlük, prestij, erişebilirlik

Bilgi Güvenliği Risk Yönetiminin Amacı

Bilgi güvenliğini en uygun maliyetle sağlamak

Bilgi Güvenliği Risk Yönetiminin Amacı

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?

Korunacak Varlıklar

- İnsanlar *(personel, müşteriler, tedarikçiler..)*
- Bilgi *(kağıt ve elektronik ortamdaki)*
- Yazılım varlıkları
- Fiziksel varlıklar *(bilgisayar ve iletişim donanımı, altyapı varlıkları)*
- Hizmetler *(bilişim, ısıtma, havalandırma..)*
- Kurum imajı ve itibarı

O Halde Ne kadar Güvenlik Gerekli?

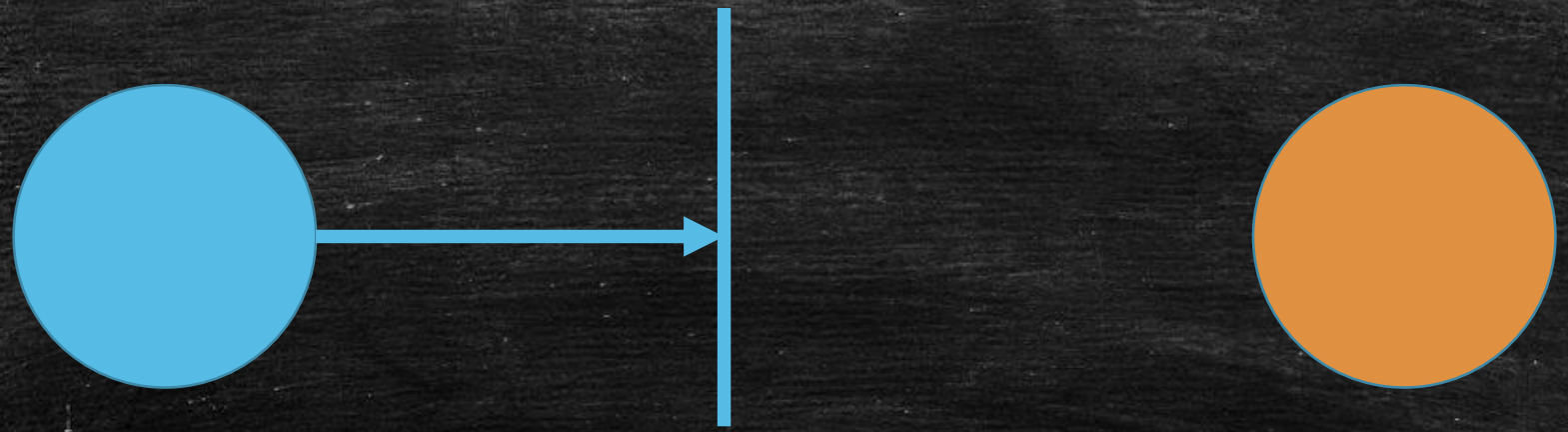
- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?

Saldırıların Sınıflandırılması

Süreçsel

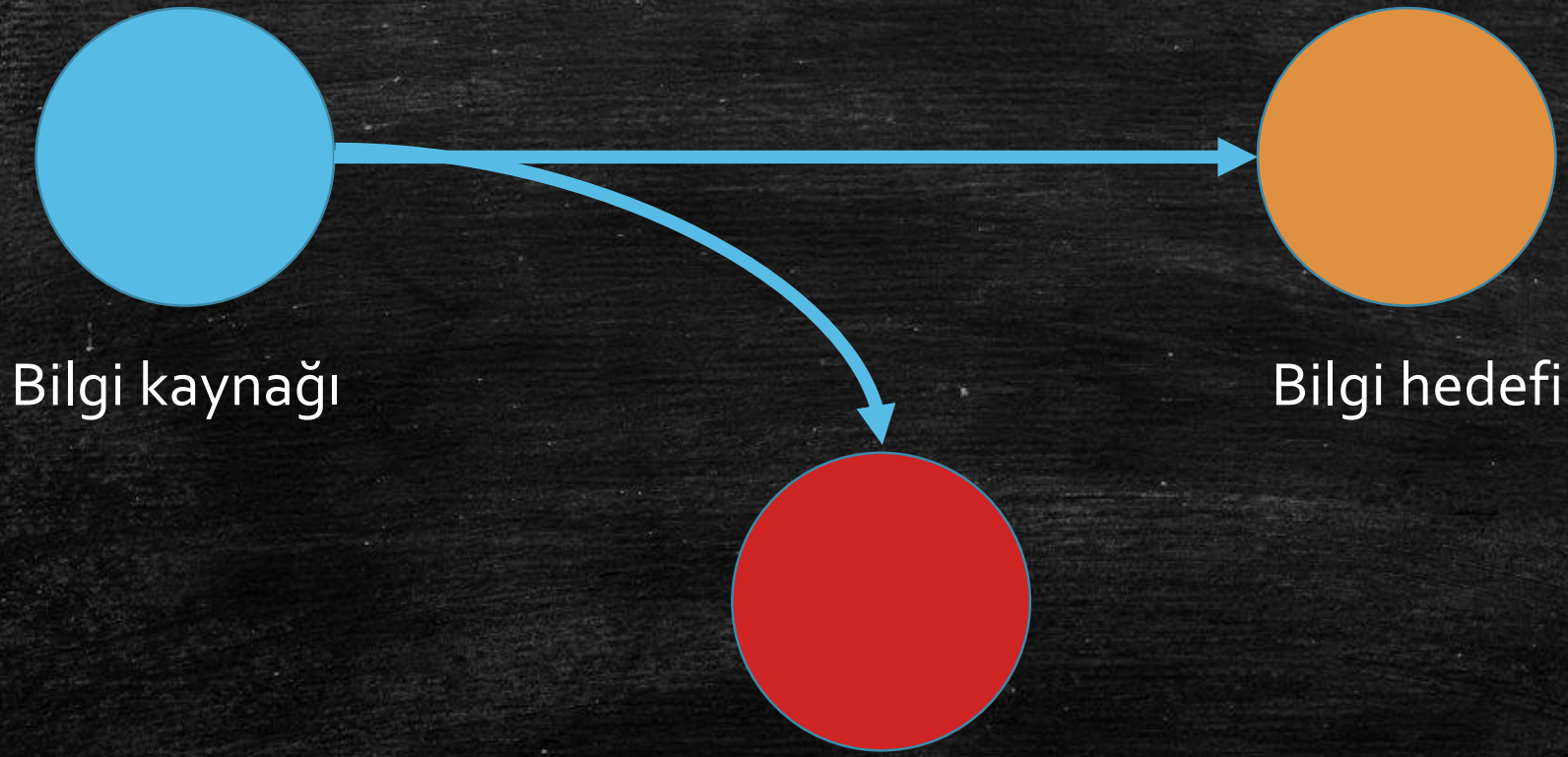
İşlemsel

Süreçsel Sınıflandırma

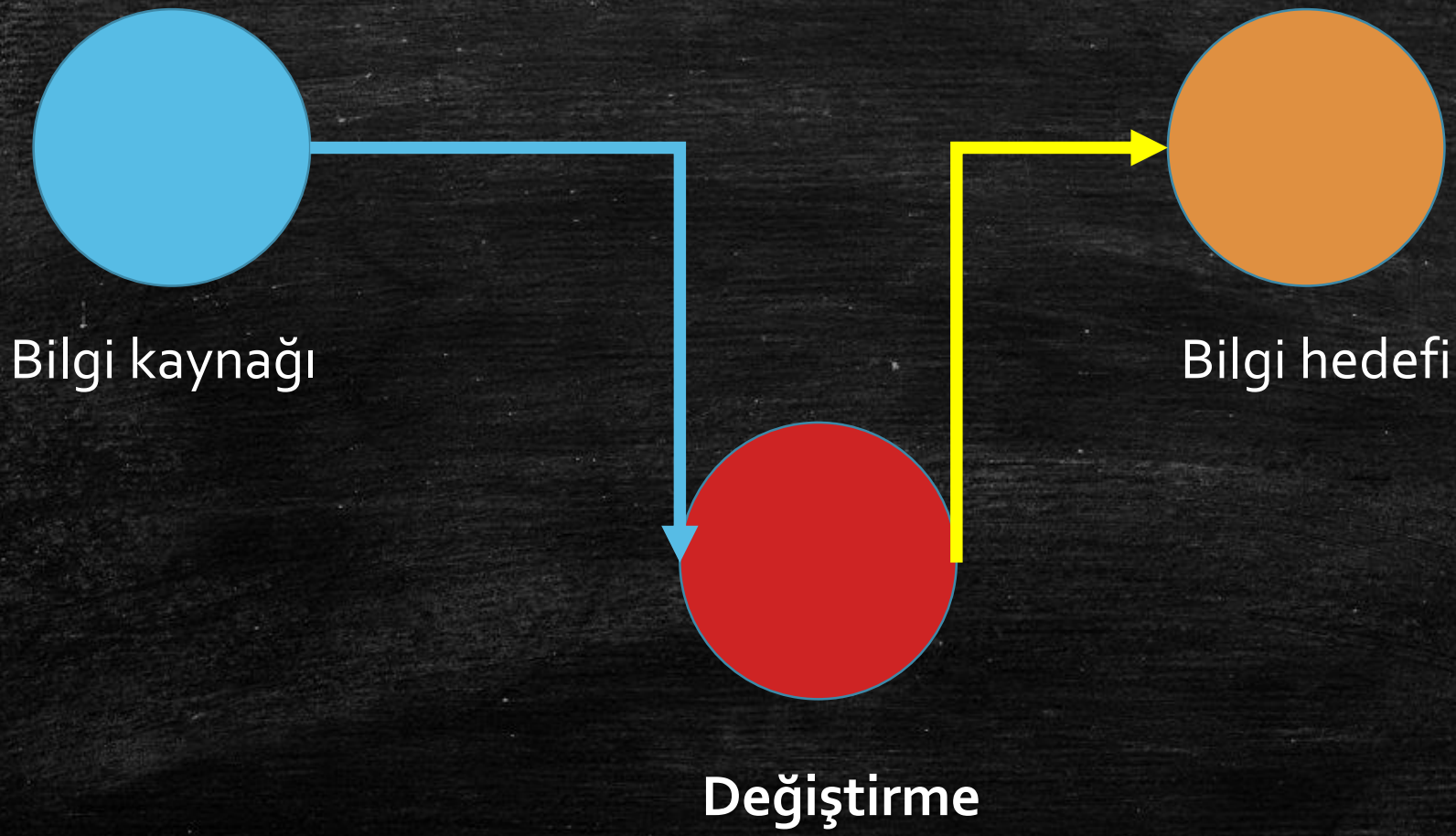


Engelleme

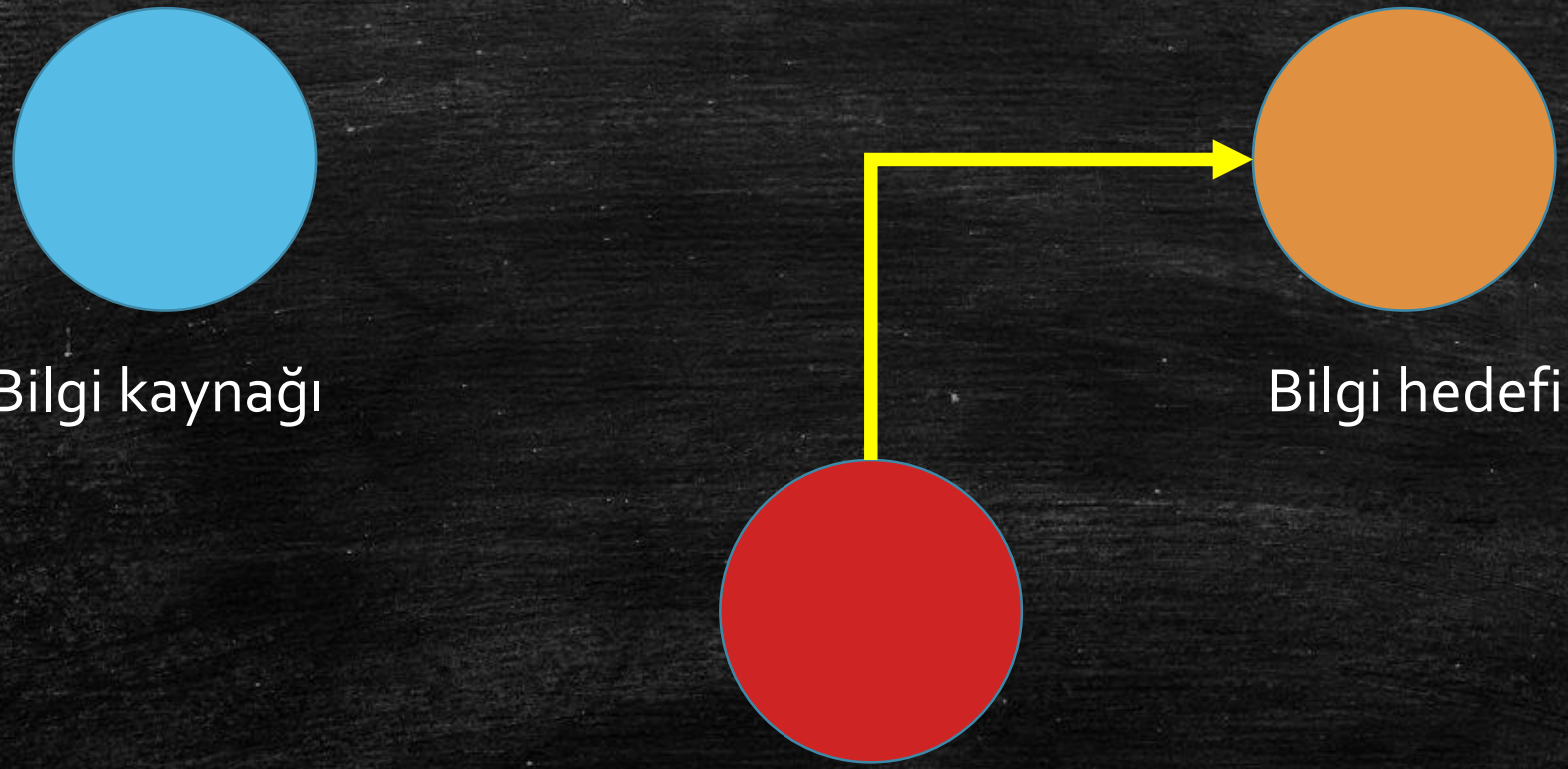
Süreçsel Sınıflandırma



Süreçsel Sınıflandırma



Süreçsel Sınıflandırma



İşlemsel Sınıflandırma

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?
- Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?

Saldırganlar ve Amaçları

Saldırganlar	Araçlar	Erişim	Sonuç	Amaç
Bilgisayar Korsanları	Kullanıcı komutları	Uygulama zayıflıkları	Bilgi bozma	Finansal kazanç
Casuslar	Komut dosyası veya program	Tasarım zayıflıkları	Bilgi çalma yada açığa bilgi çıkarma	Politik kazanç
Teröristler	Araç takımı	Yapılandırma zayıflıkları	Hizmet çalma	Sosyal statüye meydan okuma
Meraklılar	Dağıtık araçlar	İzinsiz erişim	Hizmet önleme	Zevk için
Profesyonel Suçlular	Veri dinleyici sistemler			

* Kötü niyetli saldırganlar

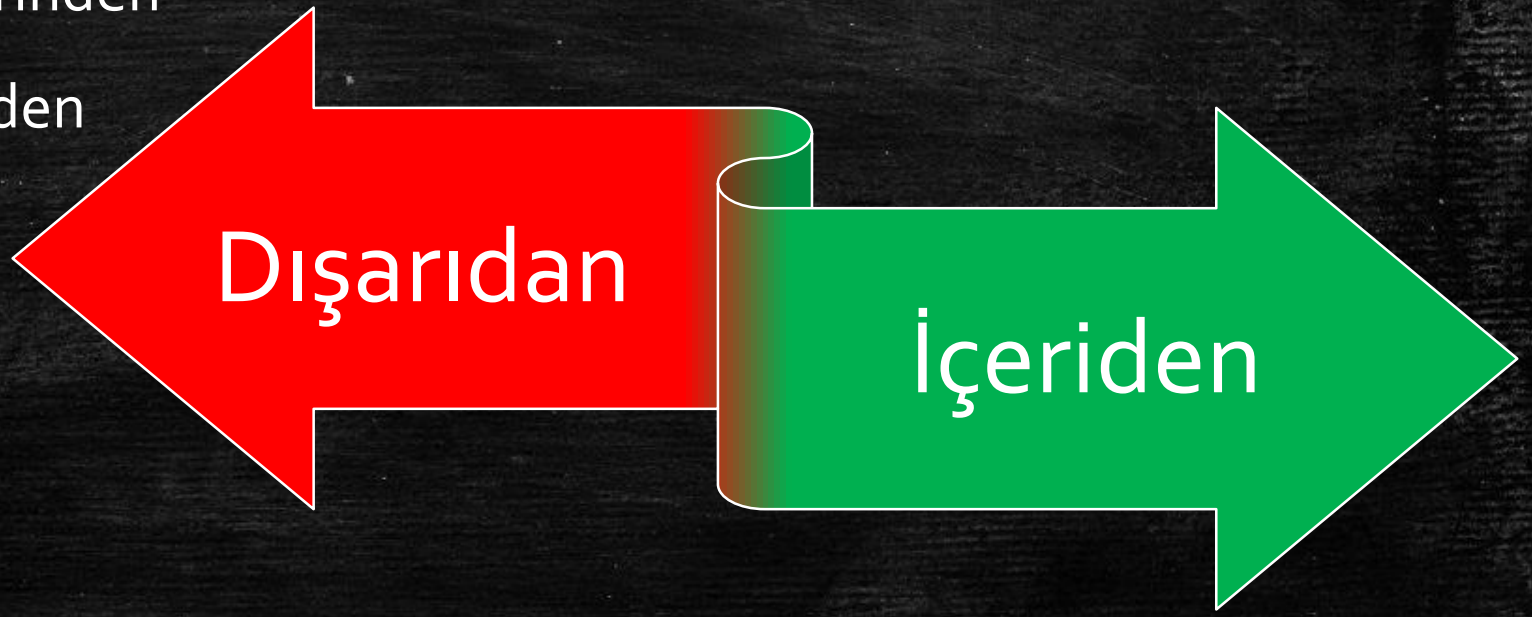
** Kötü niyetli olmayan saldırganlar

Bize kim tehlikeli saldırı yapabilir

- Çalışan İşçiler
- Geçici veya Danışman Personel
- Rakipler
- Organizasyonun görüş ve maçlarından çok farklı düşünceye sahip olan şahıslar.
- Organizasyona düşmanlığı olan şahıslar veya onları personeli
- Sizin Organizasyonunuzun halka açık görüntüsünden dolayı şöhret kazanmak isteyen kişiler.

Potansiyel Saldırı Kaynakları

- Dahili Sistemler
- Çevre ofis erişim noktaları
- Bir iş ortağına olan geniş alan ağ bağlantısı üzerinden
- Internet bağlantısı üzerinden
- Modem havuzu üzerinden



Örnek Saldırı Senaryoları

- Sistem Yöneticisi : Diploma sahte, referanslar sahte
- Bakanlık : Kurumda yetkili kullanıcı «RedHack» üyesi

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?
- Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?

Bir Saldırı İhtimali Nedir?

- Kaynakları ve olabilecek saldırı türlerini belirlemek gereklidir, kuruluşun saldırılara karşı potansiyel risklerinin değerlendirilmesi gereklidir.
- **Risk analizi ve Risk Yönetimi**

Risk Yönetimi

- Riski
  - Belirlemek
  - Değerlendirilmesi : Risk Analizi ve Risk Derecelendirme
  - Kabul edilebilir seviyeye çekmektir.

- **%100 güvenlik yoktur.**
- Riskler bertaraf edilmeli veya devredilmelidir
- Riski %100 ölçmekte mümkün değildir. Sadece ölçeklendirilebilir.

Risk Analizi Amaçları

- Varlıkları ve değerlerini belirlemek
- Zafiyet ve tehditleri belirlemek
- Zararın maddi boyutunu belirlemek
- Kabul edilebilir maliyetli çözümler ortaya koymak

Risk Nedir?

- **Varlık** üzerinde **tehdit** oluşturan bir **zafiyetin** bir **tehdit ajanı** tarafından kullanılmasına bağlı **zarar beklentisidir**.

Risk = f (varlık, açıklık, tehdit) -> zarar beklentisi

Risk Çeşitleri

- Fiziksel tehditler
- İnsan etkeni
- Cihaz hatası
- İç ve dış saldırılar
- Verinin yanlış kullanılması
- Veri kaybı
- Uygulama hatası

Risk Terimleri

- Varlık (Assets)
- Zafiyet (Vulneralibity)
- Tehdit (Threat)
- Tehdit ajanı (Threat agent)
- Risk (Risk)
- Karşı önlem ve Koruma (Countermeasure)

Risklerin Belirlenmesi

- **Varlıkların** ve varlık **sahiplerinin** belirlenmesi
- Varlığa yönelik **tehditlerin** belirlenmesi
- Bu tehditlerin kullanabileceği **zafiyetlerin** belirlenmesi
- Tehdit ve açıklıkların varlığın gizlilik, bütünlük veya erişilebilirliğine **etkisinin belirlenmesi**

Varlıklar

- İnsanlar *(personel, müşteriler, tedarikçiler..)*
- Bilgi *(kağıt ve elektronik ortamdaki)*
- Yazılım varlıkları
- Fiziksel varlıklar *(bilgisayar ve iletişim donanımı, altyapı varlıkları)*
- Hizmetler *(bilişim, ısıtma, havalandırma..)*
- Kurum imajı ve itibarı

Varlık Sahipleri

- **Varlık sahibi** = Birey veya birim
- Varlığın üretilmesinden, geliştirilmesinden, bakımından, kullanımından ve güvenliğinden sorumludur.
- İş sürecine, bir uygulamaya veya veri setine sahip atanabilir.

Varlık Listesi Oluşturma

- Neyi korumak istediğimizi listeleriz
- Risk analizi için başlangıç noktasıdır
- Varlık listesine, varlıkların fiziksel yeri, formatı, yedeği olup olmadığı gibi olası bir felaketten kurtarma durumunda gerekli olacak bilgiler girilir.
- Varlıkların sahipleri ve değeri belirlenerek varlık envanteri oluşturulur

Varlık Listesinin Oluşturulması

Varlıkların İsimlerinin Belirlenmesi

Güvenlik Kriterlerinin Belirlenmesi

Varlık, organizasyon için değeri olan, bu nedenle korunması gereken şey olarak tanımlanmaktadır

Varlık Listesi Oluşturma

- Önce varlıkların isimleri tespit edilmeli
- Donanım varlıkları en somut varlıklar olduğu için buradan başlanması kolaylık sağlayacaktır.
- Donanım varlıkları listelenirken bilgi işleyen her türlü varlık listelenir. Klavye, fare gibi bilgi işlemeyenler yazılmayacak.
- Tabloda varlıkların bulunduğu yerin olması da tüm varlıkların sıralandığı tespitini doğrulacaktır.
- Donanım varlıkları listesi üzerinden yazılım varlıkları listelenecektir
- Bu yazılımların işlediği bilgiler üzerinden bilgi varlıkları listelenecektir

Varlık Envanteri

	Sahibi	Değeri	Konumu
Personel			
Bilgi (Elektronik / Basılı)			
Yazılım Varlıkları			
Donanım			
Hizmetler			

Varlık Envanteri Oluşturma

- Varlık listesindeki her bir varlık için daha somut tanımlayıcı olacak (seri no, sahibi, lisans bilgisi vs.) kullanılarak varlık envanteri oluşturulur.

Uygulama 1 – Risk Belirleme Tablosu

- Bir kurumsal iş sürecinin;
  - Bilgi
  - Yazılım
  - Donanım, altyapı
  - İnsan
  - Alınan hizmet

varlıklarını ve varlık sahiplerini Risk Belirleme Tablosu.xls dosyasına listeleyiniz.

Tehditler


Tehditler
İnsani
Kasıtlı
- Dinleme
- Bilgi değiştirme
- Hırsızlık
- Kötücül yazılım
Hata, Kaza
- Unutma, bozma
- Dosya silme
- Hatalı yönlendirme
Çevresel
- Deprem
- Şimşek
- Sel
- Yangın

Uygulama 2 – Tehdit Listesi

- Tehdit Listesi dosyasını inceleyiniz.
- Uygulama-1'de listelenen bilgi varlıklarına yönelik *tehditleri* aynı dosyada ilgili varlığın karşısına kaydediniz.

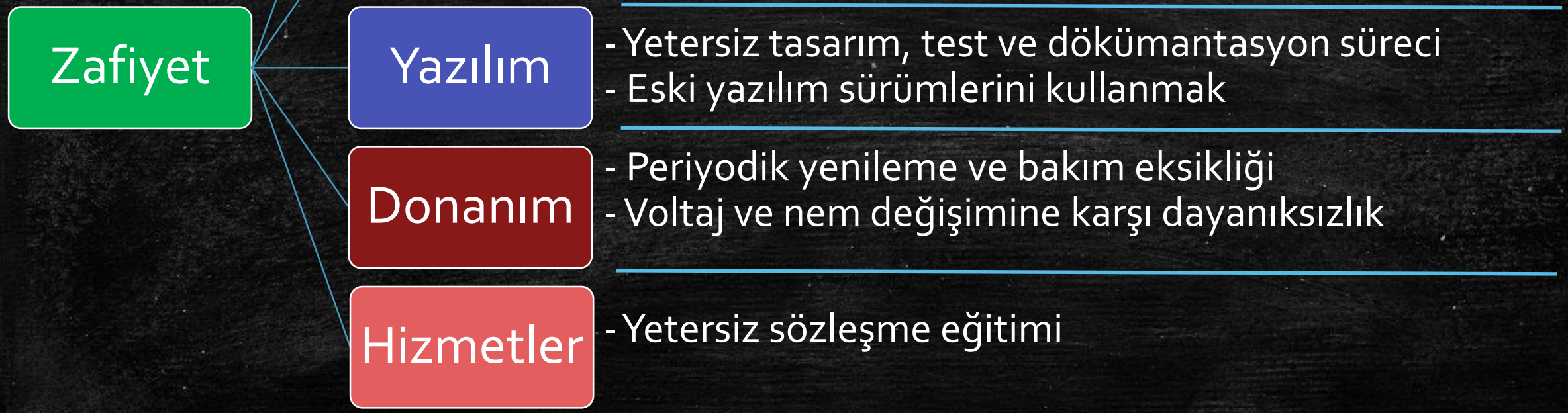
Zafiyet

- Saldırgana fırsat verebilecek yazılım, donanım, prosedüre zafiyeti

Örnek :

- Güncellenmemiş yazılımlar
- Açık modemler
- Lisansız yazılımlar
- Server odasının açık olması

Zafiyet Nedenleri



Uygulama 3 – Zafiyet Listesi

- Zafiyet Listesi dosyasını inceleyiniz.

- Uygulama-2'de belirlediğiniz tehditlerin kullanabileceği *zafiyetleri* aynı dosyaya kaydediniz.

Tehdit Ajanı

- Zafiyetten faydalanacak kişi veya örgüt

Varlıklara Değer Atanması

- Varlığın güvenliğinin sağlanamaması sonucu karşılaşılacak zararın tahmini değerini atamaktır.
- Varlıkla ilgili sağlanması gereken bilgi güvenliği seviyesi ile eşdeğerdir

Varlıklara Değer Atanması

- **Gizlik (Confidentaility) :** Verilerin , başkaları tarafından öğrenilmesi istenmeyebilir.
  - â Amaç : Herşeyi gizlemek değil, veriye sadece yetkisi olanların ulaşabilmesini sağlamak; trafik akışının analiz edilmekten korunması.
- **Bütünlük (Integrity) :** Sahip olunan verilerin başkaları tarafından değiştirilmesi istenmeyebilir.
  - â Amaç :Veri üzerinde yetkisiz ve izinsiz değişiklikler engellenir.
- **Erişebilirlik (Availability) :** Verilerin istendiği zaman ulaşılabilir olup kullanıma hazır olması istenir.
  - â Amaç : Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması

Varlıklara Değer Atanması

İnsan varlığının değeri nasıl atanacaktır?

İnsan Varlığı

- Tüm çalışanlar varsa üçüncü taraflar olarak listelenir.
- Listelemeyi gruplar halinde yapmak faydalı olmaktadır.
- Riskler gruplara karşı farklılık göstermektedir.
- Gruplar Karar Vericiler, Kullanıcılar, Sistemi İşletenler ve Uygulama Geliştiriciler şeklinde düzenlenebilir.
- Kurum insan kaynağını kişi bazında mı, iş unvanı/tanımı bazında mı tanımlamalıdır?
- Kişiler değişebilir ancak iş tanımlarının (rollerin) kalıcı olduğu düşünülerek iş unvanı/tanımı bazında bir listeleme kullanışlı olacaktır

İnsan Varlığı İçin Gizlilik Değeri

Gizlilik Değeri	*Açıklaması*
Düşük	İlgili rol veya üçüncü taraf erişimi "Tasnif Dışı" olarak sınıflandırılmış bilgi varlıklarıyla sınırlıdır. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rol veya üçüncü tarafın erişimi "Tasnif Dışı" ve "Hizmete Özel" olarak sınıflandırılmış bilgi varlıklarıyla sınırlıdır. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rol veya üçüncü taraf "Gizli" olarak sınıflandırılmış bilgileri veya kritik BT varlıklarını içerecek şekilde her türlü erişime sahiptir. Bu rollerdeki kişilerden kaynaklanacak gizlilik ihlali iş operasyonlarını ciddi derecede etkiler.

İnsan Varlığı İçin Bütünlük Değeri

Bütünlük Değeri	***Açıklaması***
Düşük	İlgili rol ve üçüncü taraf sadece "Tasnif Dışı" veya "Hizmete Özel" olarak sınıflandırılmış bilgi varlıklarını değiştirme hakkına sahiptir ve izlemeye tabidir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rol ve üçüncü taraf sadece "Tasnif Dışı" veya "Hizmete Özel" olarak sınıflandırılmış bilgi varlıklarını değiştirme hakkına sahiptir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rol ve üçüncü taraf sadece "Gizli" olarak sınıflandırılmış bilgi varlıklarını veya kritik BT varlıklarını değiştirme hakkına sahiptir. Bu rollerdeki kişilerden kaynaklanacak bütünlük ihlali iş operasyonlarını ciddi derecede etkiler.

İnsan Varlığı İçin Erişebilirlik Değeri

Erişilebilirlik Değeri	*Açıklaması*
Düşük	İlgili rolün atandığı kişinin mevcut olmayışı/ erişilememesi iş operasyonlarını etkilemez/az etkiler.
Orta	İlgili rolün atandığı kişinin mevcut olmayışı/erişilememesi iş operasyonlarını orta derecede etkiler.
Yüksek	İlgili rolün atandığı kişinin mevcut olmayışı/erişilememesi iş operasyonlarını ciddi derecede etkiler.

Uygulama 4 -

- Uygulama-2 ve Uygulama-3'te belirlenen tehdit ve zafiyetlerin bilgi varlıklarının
  - Gizlilik,
  - Bütünlük ve
  - Erişilebilirliğine

etkisini belirleyiniz.

Risk Değerlendirme

- Risk analizi ve risk derecelendirme süreçlerinin bütünü
- Risk değerlendirmesi sonucunda:
  - Kabul edilebilir risk seviyesi belirlenir
  - Hangi risk için ne yapılacağı belirlenir:
    - Risk işleme
    - Diğer seçenekler
  - Riskler kritiklik sırasına göre sıralanır.
  - Azaltılacak risk kalemlerinin öncelikleri belirlenir.

Risk Analizi ve Derecelendirme

- Güvenlik ihlalinin oluşması sonucunda kurumun karşılaşacağı **zararın belirlenmesi**
- Güvenlik ihlalinin oluşma **olasılığının belirlenmesi**
- Riskin hesaplanması
- Riskin, önceden tanımlanmış olan risk ölçeğine göre değerlendirilmesi

Zarar Belirleme Ölçeği

Zararın Etki Derecesi		Zararın Açıklaması
4	Çok yüksek	- Kurumun itibarının kaybolması - Hayati tehlike / can kaybı - Çok yüksek düzeyde maddi kayıp
3	Yüksek	- Kurumun itibarının ciddi düzeyde zarara uğraması - Belirgin hayati tehlike / can kaybı olasılığı - Yüksek düzeyde maddi kayıp
2	Orta	- Kurumun itibarının orta düzeyde zarara uğraması - Orta düzeyde hayati tehlike - Orta düzeyde maddi kayıp
1	Düşük	- Kurumun itibarının hafif düzeyde zarara uğraması (durum kurtarılabilir) - Düşük düzeyde hayati tehlike - Düşük düzeyde maddi kayıp

Uygulama 5 -

- Güvenlik ihlallerinin oluşması halinde kurumun karşılaşacağı zararı belirleyiniz.

Tehdit Olasılığı Belirleme Ölçeği

Tehdit ajanın zafiyetten yararlanma olasılığı

Olasılık Değeri	Gerçekleşme sıklığı	Değer Adı
5	Günde en az bir defa	ÇY (Çok yüksek)
4	Haftada en az bir defa	Y (Yüksek)
3	Üç ayda bir defadan çok	O (Orta)
2	Yılda bir defadan çok	D (Düşük)
1	Yılda bir defadan az	ÇD (Çok düşük)

Uygulama 6

- Güvenlik ihlallerinin oluşma olasılıklarını belirleyiniz

Riskin Hesaplanması

Risk = F(Varlık, Açıklık, Tehdit)

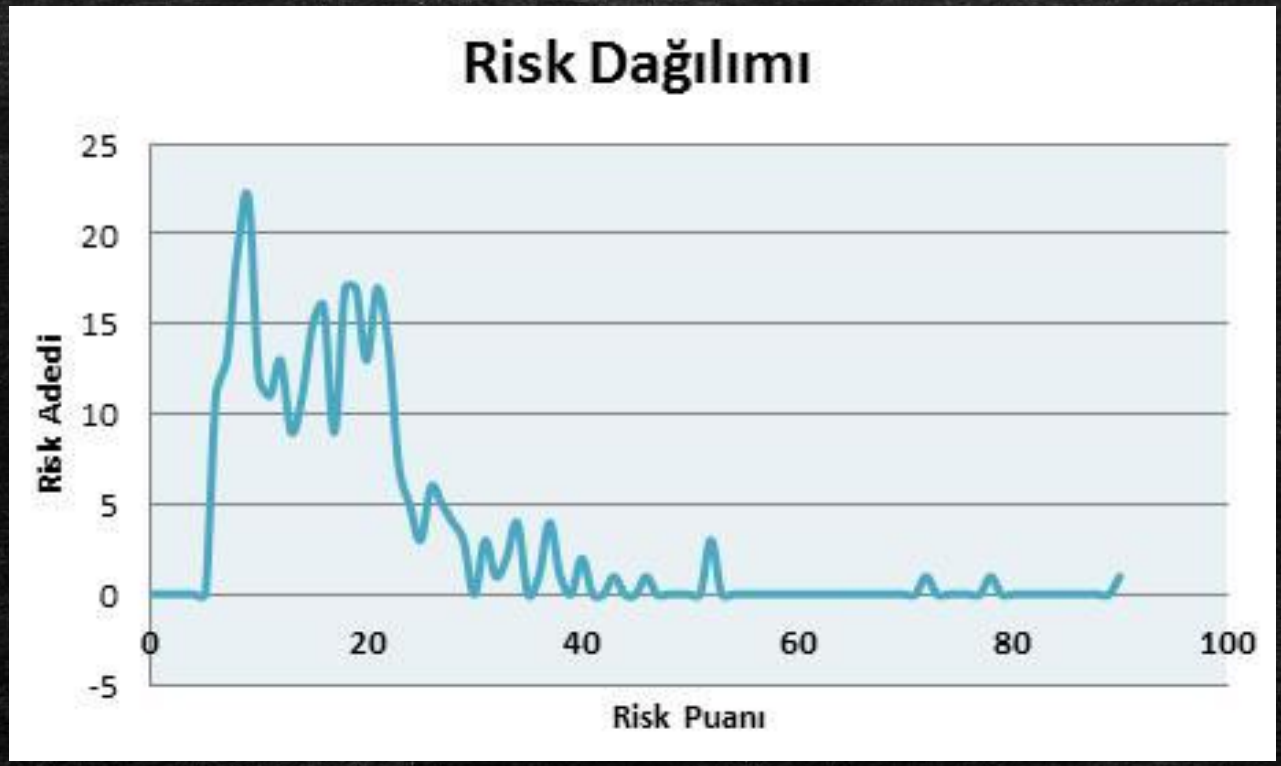
Uygulama 8

- Risk değerlerini belirleyiniz.

Riske Karşı Üç Temel Seçim

- **Kabul** : Eğer korunmasızlık çok küçük boyutlarda ve onu koruma altına almak büyük maliyet getiriyorsa, politikanız riski kabul edebilir.
- **Devretme :** Bazı durumlarda riske karşı direk olarak koruma almaktansa onun için birini görevlendirmek daha az maliyet getirebilir.
- **Kaçınma :** Güvenlik olaylarının neredeyse hiç olmayacağı yerleri korumaya almak maliyet getireceğinden bundan kaçınılmalıdır.

Kabul Edilebilir Risk Seviyesi



Uygulama 9

- Risk değerleri gözden geçirilerek kabul edilebilir risk seviyesini belirleyiniz.

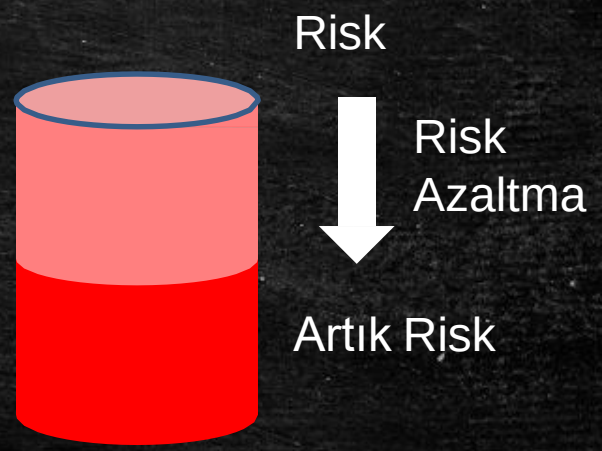
Artık Risk

Risk işleme sonrasında kalan risk (“residual risk”)…

Artık riski değerlendirin (Kabul edilebilir / edilemez…)

- Daha fazla kontrol uygulayın
- Kabul etmek zorunda kalınabilir

🕐 **Yönetim onayı gerekir.**



Karşı Önlem ve Koruma

- Potansiyel riskleri azaltmak için alınacak önlemler
- Bir tehdit ajanın zafiyeti istismar etmesini önleyecek bir önlem

- % 100 önlem olmaz

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?
- Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?

Acil Maliyet Nedir?

- Saldırı sonucunda fonksiyonunu yapamayacak olan her bir varlık için acil maliyetin hesaplanması gereklidir.
- Örneğin bir sabit disk bozulmasından dolayı sunucunun kapalı kalmasının kabaca dakikada 14.50 dolarlık bir ivedi maliyeti olacağı söylenebilir.
- Bazen ivedi maliyetin hesabı oldukça güç olabilir.
- Örneğin, bazı rakiplerin çalacağı şema, çizim, ve yeni üretilecek parçaların projelerinden dolayı maliyet daha fazla olacaktır. Bu ise rakiplerin daha gelişmiş ürün tasarlamalarına neden olacaktır. Böyle bir kayıp çok daha yıkıcı olabilecektir.

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?
- Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?
- Bir atak veya bozulmanın **geri kazanma maliyeti** ne olacaktır?

Geri Kazanma Maaliyeti Nedir?

- Bozulma veya zararlı saldırının başlangıç maliyetini hesapladıktan sonra bu bozulmanın getireceği toplam maliyetin hesaplanması gereklidir.

Geri Kazanma Maliyeti Nedir?

- Örneğin şirket bilgisini saklayan bir sunumcu bozulmasındaki maliyetler için;
- Bütün kullanıcıların bağlantılarının kesilmesinin ani maliyeti ne olur.
- Yapılan saldırının hangi kaynakları ne kadar süre erişilemez yaptığının maliyeti nedir.
- Silinen veya bozulan kritik dosyaların onarım maliyeti nedir.
- Her bir donanım elemanının onarın maliyeti nedir.
- Bütünüyle bir sunumcunun onarım maliyeti nedir.
- Bilgi çalınmış ve hırsız bulunamamış ise bunun maliyeti ne olacaktır..

O Halde Ne kadar Güvenlik Gerekli?

- **Ne tür varlık**ları korumak gereklidir?
- Bu varlıkları **nelere karşı** korumalıyız?
- Bize **kim** tehlikeli **saldırı** yapabilir ve ne kazanabilir?
- Bir **tehdit**'in varlıklarımızı **bozma olasılığı** ne kadardır?
- Eğer bir tehlikeli saldırı olursa bunun **ivedi maliyeti** ne olacaktır?
- Bir atak veya bozulmanın **geri kazanma maliyeti** ne olacaktır?
- Bu varlıklar, **etkin maliyet** ile nasıl korunabilir?

Bu Varlıklar Etkin Maliyet İle Nasıl Korunabilir?

- Maliyetin en az olmasına dikkat edilmelidir.
- Bu nedenle koruncak olan varlıkların risk analizlerinden korumanın seviyesi belirlenmiş olacaktır
- Bazı güvenlik seçimlerinde güçlüklerle karşılaşabiliriz.
  - Örneğin Internet bağlantısında paket filtreleme yeterli midir.? Yoksa bir güvenlik duvarı yatırımı yapılmalı mıdır.?
- Bunlar güvenlik uzmanlarının düşünüp çözüm bulacakları önemli sorulardır.

Güvenlik Önlemleri Bütçesinin Çıkarılması

- Uygulanacak Güvenlik önlemlerinin maliyetinin çıkartılarak tahmini bütçenin ne olduğunun belirlenmesi gereklidir.
- Bunlar Sunumcu donanımı güvenlik duvarı ve güvenli bölgelerin kurulumunu ve güvenlik personeli, testler, ve sistem bakımını içerebilir.
- Burada hiçbir zaman “bütün yumurtaları aynı sepete koyma” sözünü unutmamak gerekir.

Bulunanların Yazılı Olarak Dökümante Edilmesi

- Bu çalışmalar sonucunda elde edilen bulguların yazılı olarak raporlanması gereklidir.
- Çünkü bu doküman daha sonraki güvenlik önlemlerinin geliştirilmesinde temel kaynak olacaktır.
- Ayrıca daha sonra yapılan işlemlerin günlük olarak kayıtlarının tutulması gereklidir.

Güvenlik Politikası

- Kolay anlaşılabilir olmalıdır
- Öneri tavsiye değil emir kipi kullanır
- Teknik değildir
- Güvenlik işlerini tüm kurum faaliyetlerine entegre etmeyi amaçlar
- Zamanla güncellenmelidir

Güvenlik Politikası Oluşturulması

- Güvenlik politikası aynı zamanda kuruluşun tamamının güvenlik hedeflerini açıklamalıdır.
- Politika, güvenliğin temelini oluşturur.
- Kurumun önemli gördüğü ve korunması gereken bilgiler ile bu bilgileri tehdit eden hareketleri belirler.
- İdeal güvenlik, ağ tasarımı, bilginin gizlilik derecesini ve kullanıcı hakları ile uygulama sınırlamalarını hesaba katan sağlam bir güvenlik politikası ile başlar.

Güvenlik Politikası Oluşturulması

- Güvenlik politikasının oluşturulmasında sorulacak anahtar sorular şunlardır.

1. Kime, nereye, ne zaman, nereden ve hangi yetkiyle izin verilebilir ?
2. Hangi aktiviteler tehdit olarak görülür ve güvenlik riski yaratırlar ?
3. Ne tip gözden kaçmalar ve dikkatsizlikler olabilir?
4. Güvenlik politikasının gerçekleştirilmesinde kim, ne yetki ve sorumluluğa sahiptir?

Güvenlik Politikası Temelleri

- Farklı tiplerdeki bilgilere erişim için kişilere yetki sağlar.
- Ne tür ve ne kadar güvenlik zorunluluğu ve ölçülerine uyulması gerektiğine bakarak kuralları ve standartları belirler.
- Neredeyse bütün kurumların bir bilgi güvenliği politikası vardır. Fakat bazı kurumlarda politika açıkça yazılmamıştır.
- Politika yazılmazsa, organizasyon çalışanların yanlış anlamalarından dolayı risk altındadır demektir.
- Ayrıca bir güvenlik problemi olması durumunda cezanın boyutu da belirsiz olacaktır.
- Bir politika yazmak, organizasyonun kararlılığının başlangıcıdır.

Güvenlik Politikası Yazılması

- Bir bilgi güvenliği politikası bir vakum içinde yazılmaz.
- O kurumun ihtiyaçlarıyla direk olarak ilişkilidir. Bütün kurumlara tam olarak uyan genel bir güvenlik politikası yoktur.
- Güvenlik politikası oldukça kısa olmalıdır. Yaklaşık olarak beş sayfa olabilir.
- Platform bağımlı terimler olmamalı, genel olmalıdır.
- Yapı ve teknolojideki değişimlere göre esnek olarak hazırlanmalıdır.
- Birkaç yıllık bir ömrü olmalıdır.
- Politika yayınlanmalı ve bütün kullanıcılara açık olmalıdır

Güvenlik Politikası Yazılması

Güvenlik Politikası Kavramlar

- Yönerge : Önerilerdir; kural değil işin daha iyi yapılamasını sağlayacak yol göstericilerdir.
  - Politikanın uygulanmasına yönelik detayları belirler. Örnek : Şifre en az 8 karakterden oluşmalıdır.
- Temel (Baseline) : Bir sistem veya ağ için asgari güvenlik önlemleri
  - Örnek : İşletim sistemleri güncel olmaldır
- Standart : Yapılaması zorunlu kurallar
- Prosedür : Belirli bir durumda yapılması gerekenleri adım adım anlatır. Politikanın en alt basamağıdır. Poltikanın kişiye yansıyan halidir. Örnek . Windows kurulumu için izlenecek adımlar.

Güvenlik Politikası Kavramlar

- İşe Alım Süreçleri :
  - Çalışanların geçmişi araştırılmalı
  - Çalışanlar gizlilik sözleşmesi imzalamalı
  - Eğitim / Öğrenim durumu kontrolü yapılmalı
  - Referans kontrolü yapılmalı
- Rotasyon :
  - Görevler arasında rotasyon olmalı
  - Süreçler birden fazla kişinin hakim olması sağlanmalı. Tek bir kişinin belirli süreçler üzerinde fazla yetkiye sahip olması engellenmeli. Görevler Ayrılığı : tek bir kişinin kritik bir süreci tamamlayamaması sağlamak
- Görevler Ayrılığı : tek bir kişinin kritik bir süreci tamamlayamaması sağlamak
- Zorunlu İzin :
  - Başkalarının süregelen usulsüzlükleri bulabilmesini sağlar.
  - Sürecin personelden bağımsız işleyebildiğini gösterir.

Güvenlik Politikası Kavramlar

- Bilginin Bölünmesi :
  - Tek bir kişinin kritik bir süreci tamamlayacak bilgiye sahip olmasını engeller
    - Örnek : Kasa parolasının sadece yarısını bilen banka müdürleri
- İşten Çıkarmalar :
  - Personelin nasıl işten ayrılacağı net bir şekilde belirlenmeli
  - Çıkış mülakatı
  - Giriş kartlarının teslim edilmesi
  - Hesaplara erişimin kesilmesi
  - E-posta hesaplarının kapatılması

Güvenlik Sorumluluğu

- Politika, güvenlik için kimlerin sorumlu olduğunu belirtmek zorundadır.
- Politika bütün kullanıcılardan sahip oldukları sistem ve veriler için, güvenlik bilgi ve sorumluluklarının anlaşılmasını ve sözleşme yapılarak imzalanmasını ister.

İyi Bir Güvenlik Politikası Nasıl Olmalı

- Kuruluşun bütün üyeleri tarafından kolaylıkla erişilebilmelidir.
- Güvenlik hedeflerini açıkça tanımlamalıdır.
- Politikada açıklanan her bir konu doğru bir şekilde tanımlanmalıdır.
- Her bir konuda kuruluşun konumunu açıkça göstermelidir.
- Her konu hakkındaki politikanın savunulmasını açıklamalıdır.
- Ne koşullarda konseptin uygulanabileceğini açıklamalıdır.

İyi Bir Güvenlik Politikası Nasıl Olmalı

- Kuruluş üyelerinin görev ve sorumlulukları, açıklanan sonuçlarda belirtilmelidir.
- Açıklanan politikaya uymayanların durumu hecelenerek açıklanmalıdır.
- Açıklanan konseptin sonraki detaylarının veya açıklamalar için başvuru bilgisi içermelidir.
- Kullanıcıdan beklenen gizliliğin seviyesini tanımlamalıdır.
- Tanımlanmayan konulardaki kuruluşun tutumunu içermelidir.

Bir Güvenlik Politikası Örneği

- Bu politika özel olarak, “Internet tabanlı Web sunucu kaynaklarına erişim” i amaçlar
- Kuruluşun konumu, “iş ilişkili olan görevlerin yapılmasında kullanılacaktır” şeklinde açıklanır. Web browsing sadece iş ilişkili aktivitelerde kullanılacaktır.
- Bu politika sadece ağ kaynaklarının etkin ve verimli bir şeklide kullanımını amaçlar.
- Politika bütün çalışanlara eşit olarak uygulanacaktır. Bu politika üretimde ve üretim dışındaki zaman periyodunda kullanılacaktır.

Bir Güvenlik Politikası Örneği

- Politikada ağ personeli web sunucuyu gözleyecek, Ayrıca her bir çalışan web erişimi için yöneticisinden izin alacaktır. Bunun anlamı her yöneticinin web erişimi için izin verme yetkisi olacağıdır.
- Bu politikaya uymayanların yazılı olarak ikaz edileceğinin belirtilmesi gereklidir.
- Daha fazla bilgi için lütfen doğrudan ağ yöneticiniz ile irtibata geçiniz. şeklinde olacaktır.
- Bütün web erişimleri ağ personeli tarafından izlenecektir. Böylece personeli gizlilik seviyesi sıfırdır.

Sözleşmenin İçereceği Konular

- Kurumun sistem ve verileri vardır
- Kullanıcılar yetkilerinin olmadığı veri ve yazılım kopyalarına erişmemeyi kabul etmelidirler
- Kullanıcılar parolalarını uzun olarak seçmeli ve gizli yerlerde saklamayı kabul etmelidirler
- Kullanıcılar güvenlik için kurum haklarını koruduklarını bilmelidirler

ISO 27001

- ISO 1946'dan beri standart hazırlıyor.
- 27000 türevleri bilgi güvenliği konularını içeriyor.
- Bilgi Güvenliği Yönetim Sistemi Standardı
- Bilgi güvenliği risklerini değerlendirmek
- Bu değerlendirmeye göre riskleri yönetmek

Kaynakça

- İbrahim Soğukpınar, Veri ve Ağ Güvenliği Ders Notları
- Alper Başaran, Siber Güvenlik ve Hacking
- Tahsin Türköz, Bilgi Güvenliğinde Risk Yönetimi
- Tolga Mataracıoğlu, Ünal Tatar, Örnek Varlık Envanteri Oluşturma Metodolojisi
- Günce Öztürk, Varlık Değerlemesinde İnsan