MUH442 Bilişimde Güvenlik – 2

Prof. Dr. Hasan Hüseyin BALIK

(5. Hafta)

İçerik

- 2.Yönetim Sorunları
  - 2.1. BT Güvenlik Yönetimi ve Risk Değerlendirmesi
  - 2.2.BT Güvenlik Kontrolleri, Planları ve Prosedürleri
  - 2.3.Fiziksel ve Altyapı Güvenliği
  - 2.4. İnsan Kaynakları Güvenliği
  - 2.5. Güvenlik Denetimi
  - 2.6. Bilişim Güvenliğinde Yasal ve Etik Hususlar

2.4.İnsan Kaynakları Güvenliği

2.4.İçerik

- Güvenlik Bilinci, Eğitim ve Öğretim
- İstihdam Uygulamaları ve Politikaları
- E-Posta ve İnternet Kullanım Politikaları
- Bilgisayar Güvenliği Olay Müdahale Ekipleri

Güvenlik Bilinci, Eğitim, ve Öğretim

Güvenlik bilinci, eğitimi ve öğretimi konusu, ISO 27002 (*Bilgi Güvenliği Yönetimi Uygulama Esasları- Code of Practice for Information Security Management) ve* NIST SP 800-100 (*Bilgi Güvenliği El Kitabı: Yöneticiler İçin Bir Kılavuz- Information Security Handbook: A Guide for Managers).*

Kuruluşlara Faydaları

Güvenlik bilinci, eğitim ve öğretim programları kuruluşlara dört ana fayda sağlar:

- Çalışan davranışını iyileştirir
- Çalışan sorumluluğunu artırır
- Çalışan davranışı için yükümlülüğü azaltır
- Düzenlemelere ve sözleşme yükümlülüklerine uymayı sağlar

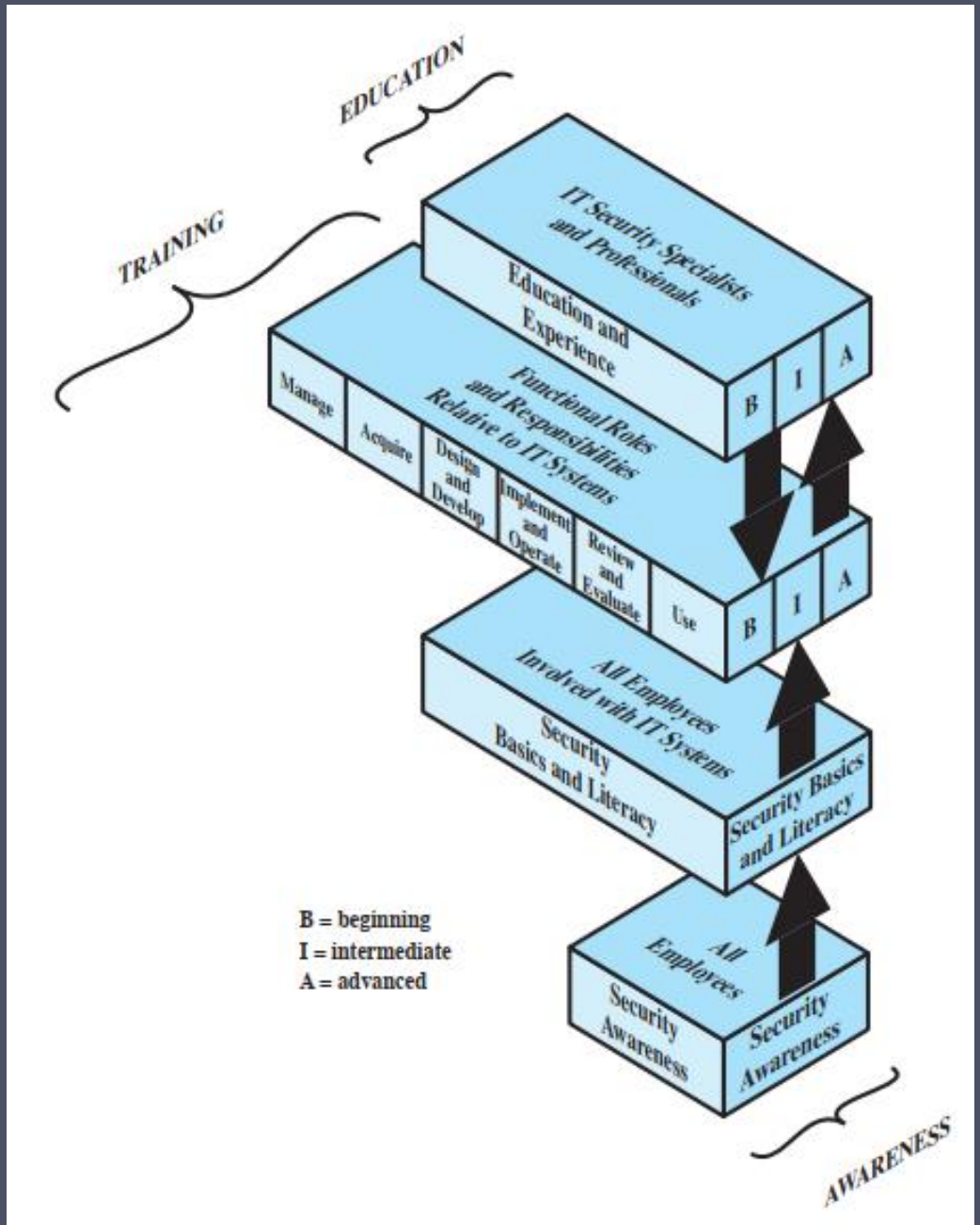
İnsani Faktörler

Çalışan davranışı, bilgisayar sistemlerinin ve bilgi varlıklarının güvenliğini sağlamada kritik bir husustur

Çalışan davranışıyla ilgili başlıca sorunlar şunlardır:

Hatalar ve eksiklikler	**Sahtekarlık/hile**	**Hoşnutsuz çalışanların eylemleri**

Bilgi Teknolojisi (IT) Öğrenme Sürekliliği



Karşılaştırmalı Çerçeve

	Farkındalık	Eğitim	Öğretim
Nitelik	"Ne"	"Nasıl"	"Neden"
Düzey	Bilgi	Tecrübe	Kavrama
Amaç	Tanıma	Beceri	Anlama
Öğretme Yöntemi	Medya • Videolar • Bültenler • Posterler, vb.	Pratik talimatlar • Ders • Vaka çalışması • Saha Uygulamalı	Teknik talimatlar • Tartışma semineri • Arka plan okuma
Ölçme Değerlendirme	Doğru yanlış Çoktan seçmeli (öğrenmeyi tanımlama)	Problem çözme (öğrenmeyi uygulama)	Deneme (öğrenmeyi yorumlama)
Etki Süresi	Kısa Vade	Orta Vade	Uzun Vade

Farkındalık

- Çalışanın dikkatini organizasyon içindeki güvenlik sorunlarına odaklamaya ve bilgilendirmeye çalışır
  - Güvenliği sağlama konusundaki sorumluluklarının ve eylemleri üzerindeki kısıtlamaların farkına varır
  - Kullanıcılar, kuruluşun refahı için güvenliğin önemini anlar
  - Coşkuyu ve yönetimin katılımını teşvik eder
- Program, organizasyonun ve hedef kitlenin ihtiyaçlarına göre uyarlanmalıdır.
- Güvenlik mesajını çeşitli şekillerde çalışanlara sürekli olarak tanıtmalıdır
- Tüm çalışanlara bir güvenlik bilinci politikası belgesi sunmalıdır

NIST SP 800-100 (*Bilgi Güvenliği El Kitabı: Yöneticiler İçin Bir Kılavuz*)farkındalık programlarının içeriğini genel hatlarıyla şu şekilde açıklar:

"Farkındalık araçları, bilgi güvenliğini teşvik etmek ve kullanıcıları, güvenliğin ne olduğunu, ancak nasıl olmadığını açıklayarak ve neye izin verildiğini ve neye izin verilmediğini bildirerek, kısımlarını veya bölümlerini ve kişisel çalışma ortamlarını etkileyen tehditler ve güvenlik açıkları hakkında bilgilendirmek için kullanılır. Farkındalık, yalnızca izlenmesi gereken bilgi güvenliği politikalarını ve prosedürlerini iletmekle kalmaz, aynı zamanda uyumsuzluk nedeniyle uygulanan her türlü yaptırım ve disiplin cezası için temel oluşturur. Farkındalık, bir kurumun bilgi sistemlerini ve bilgilerini kullanmak için davranış kurallarını açıklamakta kullanılır ve bilgi ve bilgi sistemlerinin kabul edilebilir kullanımına ilişkin bir beklenti düzeyi oluşturur.."

Eğitim

İnsanlara BT ile ilgili görevlerini daha güvenli bir şekilde gerçekleştirme becerilerini öğretmek için tasarlanmıştır	• İnsanlar *ne* yapmalı ve *nasıl* yapmalılar
Genel kullanıcılar	• Odağı İyi bilgisayar güvenliği uygulamalarınadır
Programcılar, geliştiriciler, sistem koruyucular	• Geliştiricide bir güvenlik zihniyeti geliştirir
Yönetim Düzeyi	• Güvenlik riskleri, maliyet ve fayda arasında nasıl denge kurulur
Yönetici Seviyesi	• Risk yönetimi hedefleri, ölçüm, liderlik

Öğretim

- En kapsamlı programdır
- İşleri güvenlik konusunda uzmanlık gerektiren güvenlik uzmanlarına yöneliktir
- Çalışan kariyer gelişimi kategorisine uyar
- Genellikle dış kaynaklar tarafından sağlanır
  - Üniversite kursları
  - Uzmanlaşmış eğitim programları

İstihdam Uygulamaları ve Politikaları

- Potansiyel erişime sahip personeli yönetmek, bilgi güvenliğinin önemli bir parçasıdır
- Çalışan katılımı:
  - Uygun prosedürleri takip etmeyerek bir ihlalin işlenmesine farkında olmadan yardım etmek
  - Güvenlik hususlarını unutmak
  - Bir güvenlik açığı yarattıklarının farkında olmamak
  - Kontrolleri veya prosedürleri bilerek ihlal etmek

İşe Alma Sürecinde Güvenlik

- Amaç:
  - "Çalışanların, yüklenicilerin ve üçüncü taraf kullanıcıların sorumluluklarını anlamalarını ve üstlendikleri rollere uygun olmalarını sağlamak ve hırsızlık, dolandırıcılık veya tesislerin kötüye kullanılması riskini azaltmak"
- Uygun arka plan kontrollerine ve taramaya ihtiyaç var
  - Ayrıntıların doğruluğunu araştırın
- Son derece hassas pozisyonlar için:
  - Bir soruşturma kurumunun geçmişini kontrol etmesini sağlayın
  - Adli sicil kaydı ve kredi kontrolü yapın

İş Sözleşmeleri

Çalışanlar, aşağıdakileri içermesi gereken iş sözleşmelerinin hüküm ve koşullarını kabul etmeli ve imzalamalıdır:

I. Bilgi güvenliği için çalışan ve kurumsal sorumluluklar

II. Gizlilik ve ifşa etmeme sözleşmesi

III. Kuruluşun güvenlik politikasına referans

IV. Çalışanın politikayı okuyup anladığına ve bu politikaya uymayı kabul ettiğine dair onay

İstihdam sırasında

Mevcut çalışanlarla ilgili hedefler:

- Çalışanların, yüklenicilerin ve üçüncü taraf kullanıcıların bilgi güvenliği tehditleri ve endişeleri ile bilgi güvenliğine ilişkin sorumluluk ve yükümlülüklerinin farkında olmalarını
- İşlerinde kurumsal güvenlik politikasını destekleyecek donanıma sahip olmalarını sağlamak
- İnsan hatası riskini azaltmak

İstihdam sırasında personel güvenliğinin iki temel unsuru şunlardır:

- Kapsamlı bir güvenlik politikası belgesi
- Devam eden bir farkındalık ve eğitim programı

Güvenlik ilkeleri:

- En az ayrıcalık
- Görevlerin ayrılması
- Kilit çalışanlara sınırlı güven

İşe son verilmesi

- Sonlandırmada güvenlik hedefleri:
  - Çalışanların, yüklenicilerin ve üçüncü taraf kullanıcıların düzenli bir şekilde kuruluştan ayrılmasını veya istihdamı değiştirmesini sağlar
  - Tüm ekipmanların iadesinin ve tüm erişim haklarının kaldırıldığından emin olunur

Kritik yapılması gerekenler

- İsmini tüm yetkili erişim listelerinden kaldır
- Güvenlik personelini, eski çalışanın genel erişimine izin verilmediği konusunda bilgilendir
- Kişisel erişim kodlarını kaldır, fiziksel kilitleri ve kilit kombinasyonlarını değiştir, erişim kartı sistemlerini yeniden programla
- Çalışan kimliği, taşınabilir USB depolama aygıtları, belgeler ve ekipman dahil tüm varlıkları emniyete al
- Not veya e-posta ile ilgili departmanlara bildir

E-posta ve İnternet Kullanım Politikaları

- Kuruluşlar, belirli e-posta ve İnternet kullanım politikalarını güvenlik politikası belgelerine dahil etmelidir
- İşverenler için endişeler:
  - İşle ilgili olmayan faaliyetlerde harcanan çalışma süresi
  - Bilgisayar ve iletişim kaynakları, BT kaynaklarının desteklemek üzere tasarlandığı misyondan ödün vererek tüketim.
  - Kötü amaçlı yazılımları içe aktarma riski
  - Zarar verme, taciz etme, uygunsuz çevrimiçi davranış olasılığı

Önerilen Politikalar

(E-posta ve İnternet Kullanım Politikaları)

Yalnızca iş kullanımı	**Politika kapsamı**	**İçerik sahipliği**	**Mahramiyet**
Davranış standardı	**Makul kişisel kullanım**	**Yasa dışı faaliyet**	**Güvenlik Politikası**
Şirket politikası	**Şirket hakları**	**Disiplin eylemi**	

Güvenlik Olayı Müdahalesi

- Olaylara müdahale prosedürleri çoğu kuruluş için önemli bir kontroldür.
  - Prosedürler, bir olayın kuruluş üzerindeki olası sonuçlarını yansıtmalı ve uygun bir müdahaleye izin vermelidir.
  - Prosedürleri önceden geliştirmek paniği önlemeye yardımcı olabilir
- Olay müdahale yeteneğine sahip olmanın faydaları:
  - Sistematik olay yanıtı
  - Kayıp, hırsızlık ve hizmet kesintisini en aza indirmek için daha hızlı kurtarma
  - Gelecekteki olaylara daha iyi hazırlanmak için olay işleme sırasında elde edilen bilgilerin kullanımı
  - Olaylar sırasında ortaya çıkabilecek yasal sorunlarla gerektiği gibi ilgilenme

Bilişim Güvenliği Olay Müdahale Ekibi (CSIRT)

Müdahale ekibi şunlardan sorumludur:

- **Olayları hızlı bir şekilde tespit etmek**
- **Kayıp ve tahribatı en aza indirmek**
- **Kötüye kullanılan zayıflıkları azaltmak**
- **Bilgi işlem hizmetlerini geri yükleme**

Güvenlik Olayları

"Bir sistemdeki gizlilik, bütünlük, kullanılabilirlik, hesap verebilirlik, özgünlük ve güvenilirlik gibi klasik güvenlik hizmetlerinden birini veya birkaçını tehdit eden herhangi bir eylemdir"

Sisteme yetkisiz erişim

- Görme yetkisi olmayan bilgilere erişim
- Bilgileri görme yetkisi olmayan bir kişiye iletmek
- Erişim mekanizmalarını atlatmaya çalışmak
- Başka birinin şifresini ve kullanıcı kimliğini kullanmak

Sistemdeki bilgilerin yetkisiz değiştirilmesi

- Değerli olabilecek bilgileri bozmaya çalışmak
- Bilgileri yetkisiz bir şekilde değiştirmeye çalışmak
- Bilgilerin yetkisiz bir şekilde işlemek

Güvenlik Olayı Terminolojisi

Eser/kalıntı (Artifact)	Bir sistemde bulunan, sistemleri ve ağları araştırmak veya bunlara saldırmakla ilgili olabilecek veya güvenlik önlemlerini yenmek için kullanılabilecek herhangi bir dosya veya nesne. Eser, bilgisayar virüslerini, Truva atı programlarını, solucanları, açıklardan yararlanma skriptlerini ve araçlarını içerir, ancak bunlarla sınırlı değildir.
Bilgisayar Güvenliği Olay Müdahale Ekibi (CSIRT)	Tanımlanmış bir sorumluluk bölgesindeki siteleri içeren bilgisayar güvenliğiyle ilgili olaylara yanıt verilmesine yardımcı olmak amacıyla kurulmuş bir yetenek; ayrıca bilgisayar olay müdahale ekibi (CIRT) veya CIRC (Bilgisayar Olayı Müdahale Merkezi, Bilgisayar Olayı Müdahale Yeteneği) olarak da adlandırılır.
Sorumluluk bölgesi	CSIRT tarafından hizmet verilen kullanıcılar, siteler, ağlar veya kuruluşlar grubu
Olay	Bilgisayar güvenlik ilkelerinin, kabul edilebilir kullanım ilkelerinin veya standart güvenlik uygulamalarının ihlali veya yakın ihlali tehdidi
Triyaj	Uygun şekilde işlenmesini kolaylaştırmak için bilginin alınması, ilk sıralanması ve önceliklendirilmesi süreci.
Güvenlik açığı	Bir güvenlik olayı gerçekleştirmek için kullanılabilecek bir teknoloji parçasının özelliği. Örneğin, bir program istemeden sıradan kullanıcıların ayrıcalıklı modda rastgele işletim sistemi komutları yürütmesine izin verdiyse, bu "özellik" bir güvenlik açığı olacaktır

Olayları Tespit Etme

- Olaylar, kullanıcılar veya yönetim personeli tarafından tespit edilebilir
  - Personel, sistem arızalarını veya anormal davranışları rapor etmeye teşvik edilmelidir.
- Otomatik araçlar
  - Sistem bütünlüğü doğrulama araçları
  - Günlük analiz araçları
  - Ağ ve ana bilgisayar saldırı tespit sistemleri (IDS)
  - Saldırı önleme sistemleri

Triyaj Fonksiyonu

Hedef:

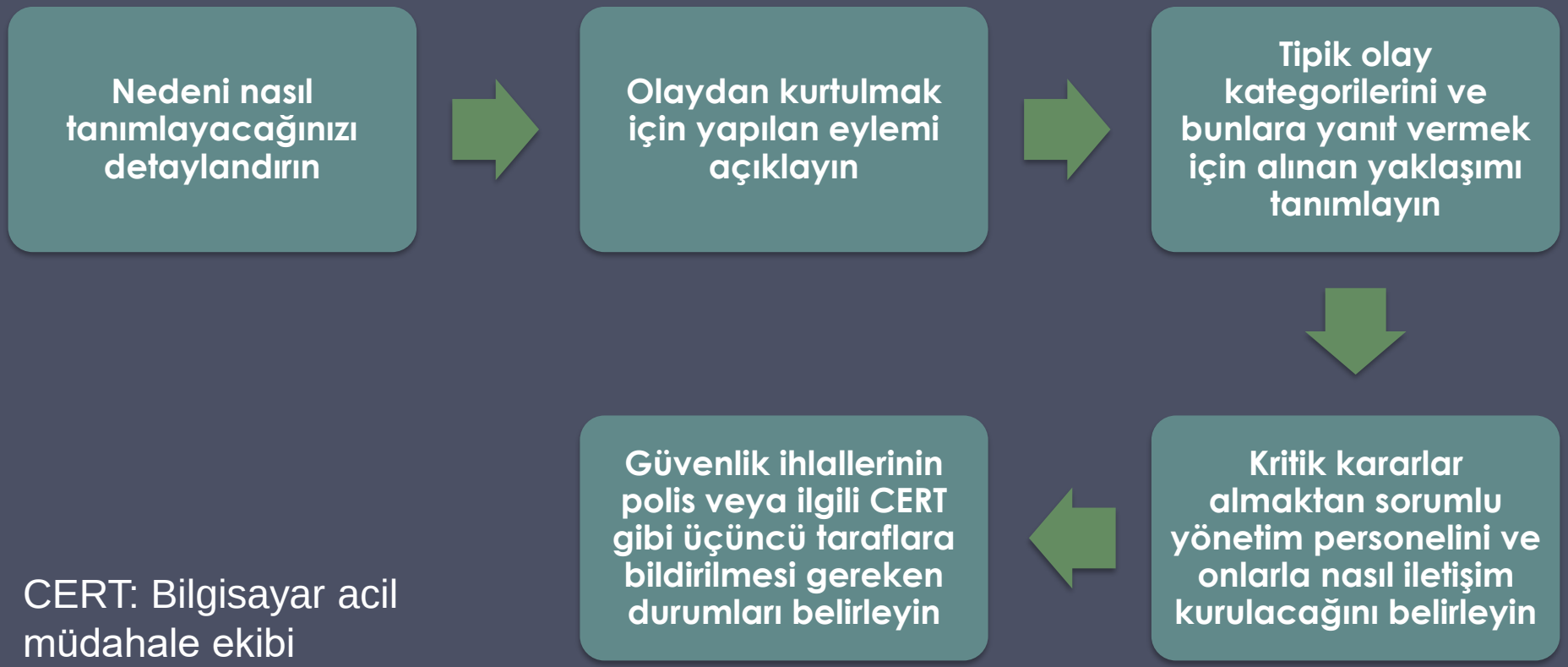
- **Olay işleme hizmetine yönelik tüm bilgilerin tek bir odak noktası üzerinden kanalize edilmesini sağlamak**
- **Genel olarak, tüm olay işleme hizmeti için tek temas noktası olarak triyaj işlevini tanıtarak elde edilir**

Gelen bilgilere şu şekilde yanıt verir::

- **Olayı kategorize etmek için ek bilgi talep eder**
- **Kuruluşun veya sorumluluk bölgesinin çeşitli bölümlerine güvenlik açığı hakkında bilgi verir ve güvenlik açığının nasıl düzeltileceği veya azaltılacağına ilişkin bilgileri paylaşır**
- **Olayı yeni veya devam eden bir olayın parçası olarak tanımlar ve bu bilgiyi olay işleme müdahale işlevine iletir**

Olaylara Müdahale

- Olaylara müdahale etmek için belgelenmiş prosedürlere ihtiyaç vardır
- Prosedürler:



CERT: Bilgisayar acil müdahale ekibi

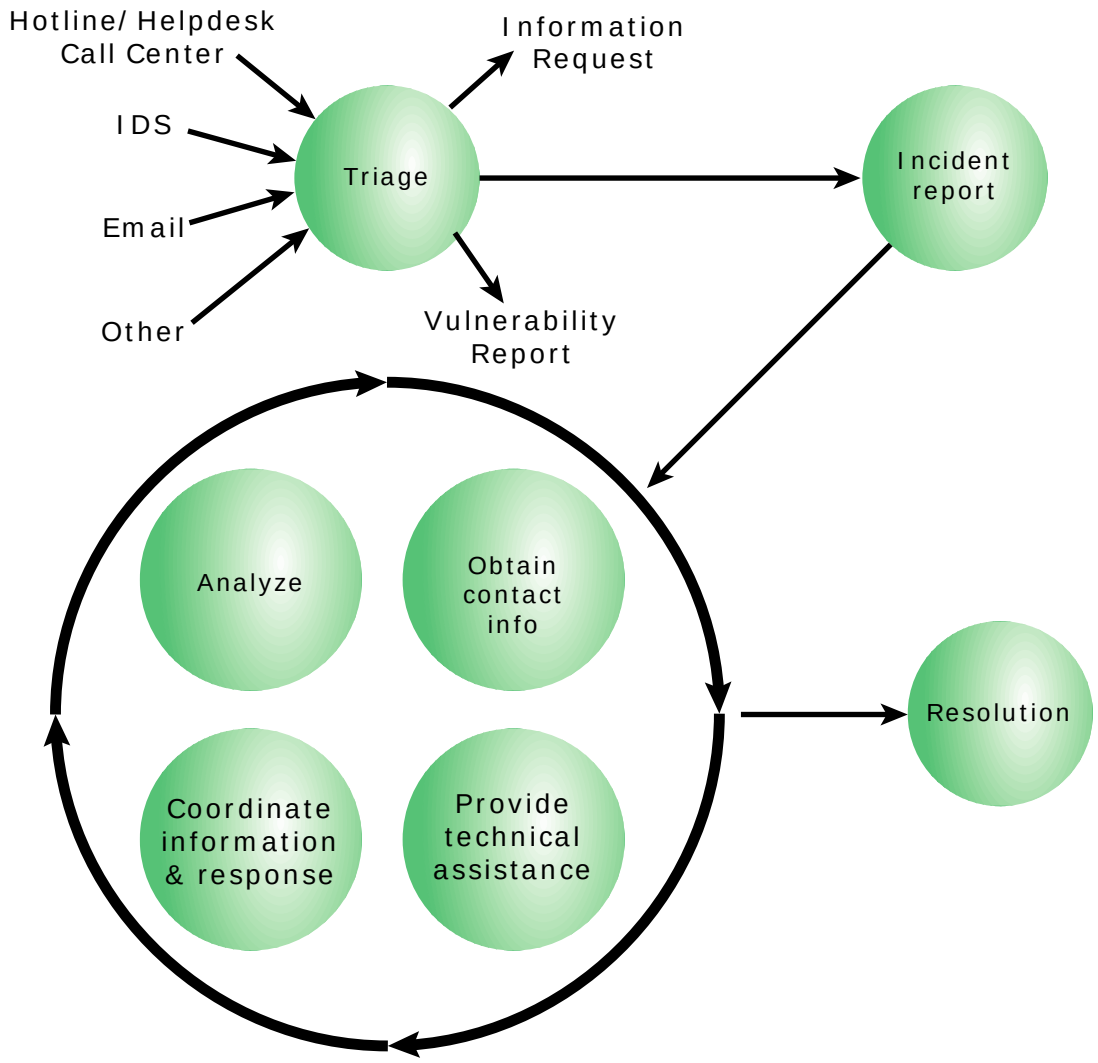


Figure 17.2 Incident Handling Life Cycle

Olayları Belgelemek

- Bir olaya verilen yanıttan hemen sonra yapılacaklar
  - Hangi güvenlik açığının ortaya çıkmasına neden olduğunu belirleyin
  - Gelecekte olayı önlemek için bunun nasıl ele alınabileceği tanımlayın
  - Olayı ve verilen cevapları detaylandırın
  - Kuruluşun sistemleri ve risk profili üzerindeki etkisini tespit edin

Olay İşleme Hizmetin(e/den) Olası Bilgi Akışı Örnekleri

Hizmet Adı	Olay işleme yönüne bilgi akışı	Olay işlemeden gelen bilgi akışı
Duyurular	Mevcut saldırı senaryosu uyarısı	İstatistikler veya durum raporu Göz önünde bulundurulması veya araştırılması gereken yeni saldırı profilleri
Güvenlik Açığı İşleme	Belirli güvenlik açıklarının kötüye kullanılmasına karşı nasıl korunursunuz?	Yeni güvenlik açıklarının olası varlığı
Kötü Amaçlı Yazılım İşleme	Belirli kötü amaçlı yazılım kullanımının nasıl tanınacağına ilişkin bilgiler Kötü amaçlı yazılım etkisi/tehdidi hakkında bilgi	Vakalarda kötü amaçlı yazılımların tanımlanmasına ilişkin istatistikler Yeni kötü amaçlı yazılım örneği
Eğitim/Öğretim	-	Pratik örnekler ve motivasyon bilgisi
Saldırı Tespit Hizmetleri	Yeni olay raporu	Kontrol edilecek yeni saldırı profili
Güvenlik Denetimi veya Değerlendirmeleri	Sızma testi başlangıç ve bitiş programlarının bildirilmesi	Yaygın saldırı senaryoları
Güvenlik Danışmanlığı	Sık karşılaşılan tuzaklar ve tehditlerin büyüklüğü hakkında bilgi	Pratik örnekler/deneyimler
Risk Analizi	Sık karşılaşılan tuzaklar ve tehditlerin büyüklüğü hakkında bilgi	İstatistikler veya kayıp senaryoları
Teknoloji Takibi	Gelecekteki olası saldırı senaryolarına karşı uyarı Yeni araç dağıtımına ilişkin uyarı	İstatistikler veya durum raporu Göz önünde bulundurulması veya araştırılması gereken yeni saldırı profilleri
Güvenlik Araçlarının Geliştirilmesi	Sorumluluk bölgesi kullanımı için yeni araçların mevcudiyeti	Ürünler için ihtiyaç Mevcut uygulamaların görünümünü sağlama