YMT 311-Bilgi Sistemleri ve Güvenliği

Ders hakkında Bilgilendirme ve temel kavramlar

Ders Hakkında Temel Bilgilendirme

Ders Sorumlusu: Dr. Muhammet BAYKARA

Ders. Lab. Yardımcısı : Arş. Gör. Fırat Artuğer

Ders Saatleri : 3 saat teori, **2 saat laboratuar**

Dersler A405'te uygulamalar ise laboratuar ortamında yapılacaktır.

Devam / Devamsızlık Durumu : Teori : **%30** – Uygulama : **%20**

Dersin Amacı : Bu derste; bilgi ve bilgisayar güvenliği konuları, unsurları ve süreçleri üzerinde durulacak ve yüksek derecede bir güvenlik için uygulanması gerekenler anlatılacaktır. Bilgi ve bilgisayar güvenliğine neden önem verilmesi gerektiği ve bilgi güvenliğinin en temel anlamda nasıl oluşturulabileceği gibi sorulara kapsamlı cevaplar aranmaya çalışılacak, bu kapsamda bilgi güvenliği yazılımları ve proje uygulamaları ortaya konulacaktır.

Dersin İşleniş Biçimi & Nasıl Geçerim!?

- Teorik anlatım
- Haftalık Ödevler
- Dönemlik araştırma ve uygulama projesi
  - Raporlama + Sunum
- Ara sınav, Final Sınavı ve Quizler
- Ders Geçme Notu = (Ara sınav(%33) + Haftalık Ödevler(%33) + Quizler(%34)) *0,4 + ((Final+Proje)/2)*0,6

Dersin Amacı

- Bilgi güvenliği konularında farkındalık ve temel düzeyde teorik ve pratik bilgiler öğrenmenizi sağlamak
- Bilgi güvenliği temel kavram, standart, metodoloji, yöntem ve stratejilerini öğrenmenizi sağlamak
- Araştırma yeteneğinizi geliştirmek
- Kişisel ve kurumsal bilgi güvenliğinin sağlanması konusunda fikir sahibi olmanızı sağlamak

Temel Kaynaklar

1. Kamil Burlu, ***Bilişimin Karanlık Yüzü*** , Nirvana yayınları, 3.baskı, 2010.
2. G. Canbek, Ş. Sağıroğlu, ***Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri***, Grafiker Ltd. Şti. Aralık 2006.
3. Türkay HENKOĞLU, ***Adli Bilişim : Dijital Delillerin Elde Edilmesi ve Analizi,*** Pusula Yayınları, 2011.
4. ***Veri ve Ağ Güvenliği Ders Notları***, İ.Soğukpınar, G.Y.T.E.Bilg.Müh.Bölümü
5. Hamza Elbahadır, ***Hacking Interface***, Kodlab Yayınları, 2010.
6. Bünyamin Demir, Dikeyeksen Yayınları, ***Yazılım Güvenliği Saldırı ve Savunma, 2013.***
7. Ömer Çıtak, Level Yayınları, ***Ethical Hacking*****, 2016.**
8. Kevin D. Mitnick, Çevirmen(Nejat Eralp Tezcan) ***Aldatma Sanatı***
9. Canan Çimen, Sedat Akleylek, Ersan Akyıldız, ***Şifrelerin Matematiği: Kriptoğrafi***, ODTU Yayınları, Ankara.
10. ***Computer and Information Security*** - Handbook
11. ***Elements of Computer Security Book***
12. ***Cryptography And Network Security Principles And Practices***" Stallings Will, Prentice Hall, 2003.
13. ***Security Engineering***, R. Anderson, Wiley, New York, 2001.

Konu Başlıkları

- Bilgi ve bilgisayar güvenliğine giriş, temel kavramlar
- Siber bilgi güvenliği, güvenlik ve hacking kavramları
- Ağ güvenliği
- Şifreleme teknikleri
- Steganografi
- Yazılım güvenliği, bilgi güvenliği yönetimi ve ilgili mevzuatlar
- Sızma belirleme, Saldırı tespit ve engelleme sistemleri
- Bilgi güvenliğinde kullanılan temel araçlar
- Biyometrik güvenlik sistem ve araçları
- Bir siber saldırının senaryosu

Temel Kavramlar

- Bilgi Güvenliği Sistemleri: Information Security Systems
- Bilgisayar Güvenliği: Computer Security
- Saldırı, Sızma, Atak: Attack, Intrusion, Hack
- Saldırgan: Attacker, Hacker, Intruder
- Güvenlik Açığı, Açıklık: Vulnerability
- Bilgi: Information, Öz Bilgi: Knowledge
- Hikmet: Wisdom
- Saldırı Tespit Sistemleri: Intrusion Detection Systems
- Saldırı Önleme Sistemleri: Intrusion Prevention Systems
- Gizlilik: Confidentiality
- Bütünlük Doğruluk: Integrity
- Kullanılabilirlik, erişilebilirlik: Availabilty

Temel Kavramlar

- Sosyal Mühendislik: Social Engineering
- Şifreleme: Cryptology
- Bilgi Gizleme: Steganography
- Klavye dinleme sistemi: Keylogger
- Kötücül yazılım (analizi): Malware (analysis)
- Kaynak kod istismarı-korunmasızlık sömürücü: exploit
- Arka kapılar: backdoor
- Hizmet aksattırma saldırısı: DoS(Denial of the Service)
- Dağıtık hizmet aksattırma: DDoS
- Sağanak: spam
- Casus yazılım: spyware
- Solucan :worm
- Truva atı: trojan horse
- Kök kullanıcı takımı: rootkit
- Koklayıcı, ağ izleyici: sniffer

Temel Kavramlar

- Bilgi Güvenliğinin temel amacı, elektronik veya diğer ortamlarda bulunan her türlü bilgi için,

  - Gizlilik (Confidentiality)
  - Bütünlük (Integrity)
  - Kullanılabilirlik (Availability)…

temel özelliklerini sürekli olarak sağlamaktır.

Temel Kavramlar

Temel Kavramlar- Bilgi Güvenliği

Bilgi Güvenliği Temel Unsurları

- Gizlilik : Bilginin yetkisiz kişilerin eline geçmemesidir.
- Bütünlük : Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.
- Erişilebilirlik : Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Temel Kavramlar- Standartlar

- **TS ISO IEC 27001** Bilgi Güvenliği Yönetim Sistemi
- UEKAE BGYS-0001 Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzuna bilgiguvenligi.gov.tr den ulaşılabilir.

Bilgi Güvenliği - Kim Sorumlu?

- Bilgi güvenliğinin sağlanmasından **herkes sorumludur**.
- Bu sorumluluklar yasal olarak da ifade edilmiş ve **5651 sayılı kanun** *"İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla işlenen suçlarla mücadele edilmesi"* amacı ile düzenlenmiştir.

Bilgi Güvenliği – Kim Sorumlu?

- Herhangi bir bilgi sisteminde aşağıdaki konumlardan **herhangi birisinde iseniz sorumluluğunuz var** demektir.
  - Bilginin sahibi
  - Bilgiyi kullanan
  - Bilgi sistemini yöneten
- Bu durum çok geniş bir kitleyi içerdiğinden *"bilgi güvenliğinin sağlanmasından herkes sorumludur"* diye genelleme yapmakta bir sakınca yoktur.

Bilgi

- 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 beklentileriniz doğrultusunda çalışıyorsa güvenlidir (Practical UNIX and Internet Security)
- Güvenlik, bulunurluk, kararlılık, erişim denetimi, veri bütünlüğü ve doğrulamadır.

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

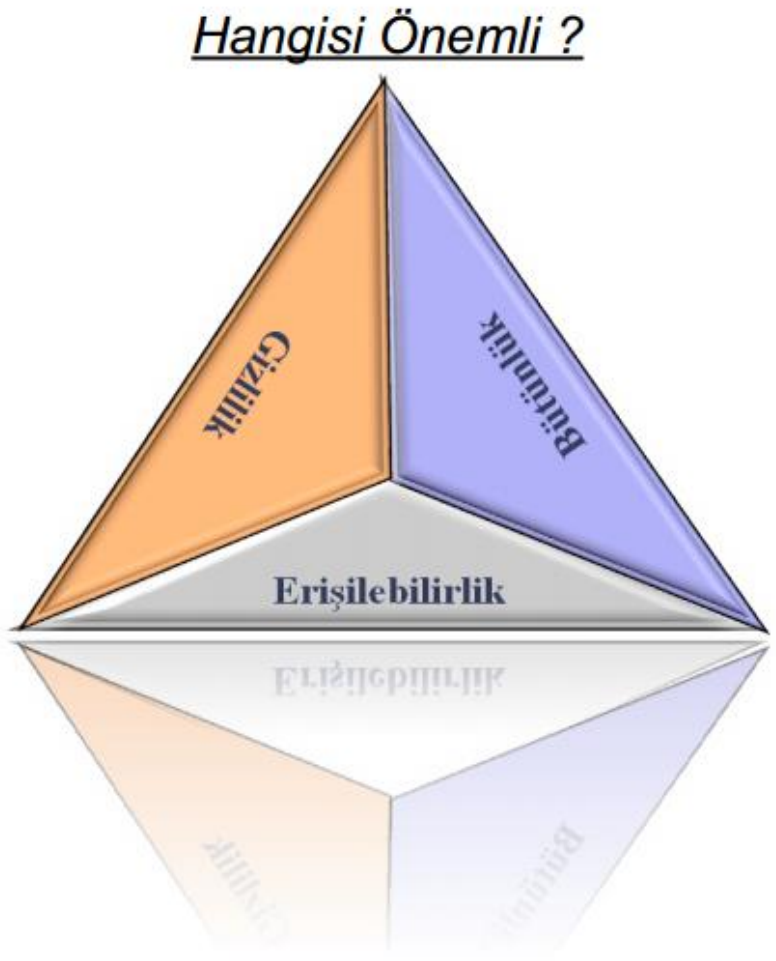
“Eğer teknolojinin tek başına güvenlik probleminizi çözebileceğini düşünüyorsanız, güvenlik probleminiz ve güvenlik teknolojileri tam anlaşılmamış demektir.”

(Bruce Schneier – Şifreleme Uzmanı)

Güvenlik Yönetim Pratikleri

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

Gizlilik, bütünlük, erişilebilirlik



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 kaynakların 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

- 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

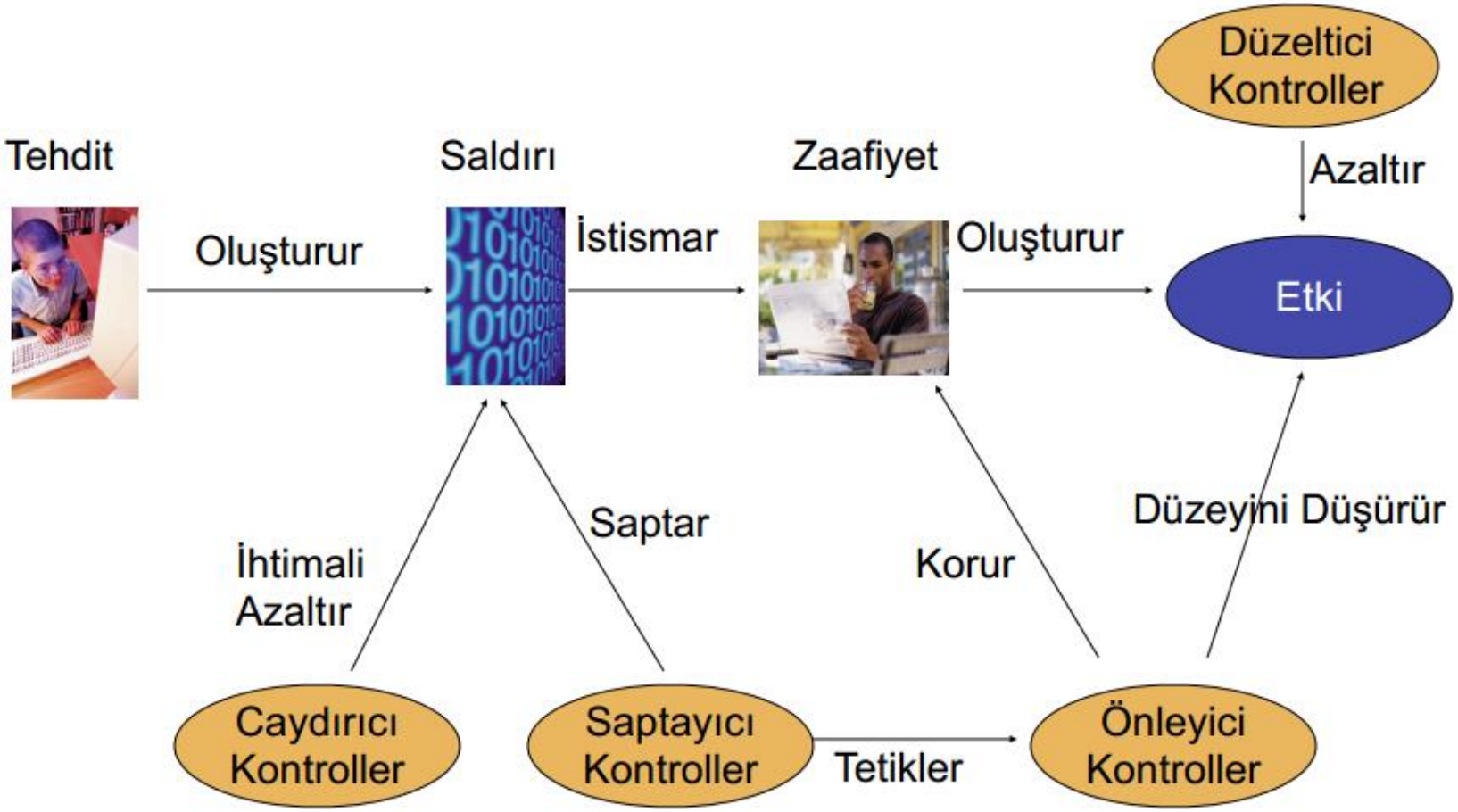
– Caydırıcı Kontroller

– Saptayıcı Kontroller

– Önleyici Kontroller

– Düzeltici Kontroller

Risk Yönetimi Kontrolleri



Risk Yönetimi 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 Engelleme

  -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 yangın söndürme sistemi	İnsan hayatı kaybı
Dış Kaynaklı İnsan Yapımı	Virüs	Güncellenmemiş anti-virüs sistemi	İş devamlılığının aksaması
Teknik İç Tehdit	Sabit Disk Bozulması	Veri yedeği alınmaması	Veri kaybı, çok miktarda iş kaybı

Varlıkların Değerlerinin Belirlenmesi

- 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 görülmelidir.

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 kavramlar 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 olmayacaktır, 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 (National Institue of Standarts and Technology)

(Security Self-Assessment Guide for Information Technology Systems)

Riske Karşı Davranış 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

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 karşılanmayan beklentilerin sonuçlarını açıkça ifade etmelidir.

Politika Türleri

- **Duyuru Politikaları**

–Çalışanların, davranışlarının sonuçlarını bildiğinden emin olunması hedeflenmektedir.

- **Bilgilendirici Politikalar**

–Çalışanların bilgilendirilmesini ve eğitilmesini sağlayarak, görevlerinin ve beklentilerin bilincinde olmaları hedeflenmektedir.

- **Yasal Politikalar**

–Organizasyonun attığı adımların, yasal ve sektörel sorumluluklar ile uyumlu olmasının sağlanması hedeflenmektedir.

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

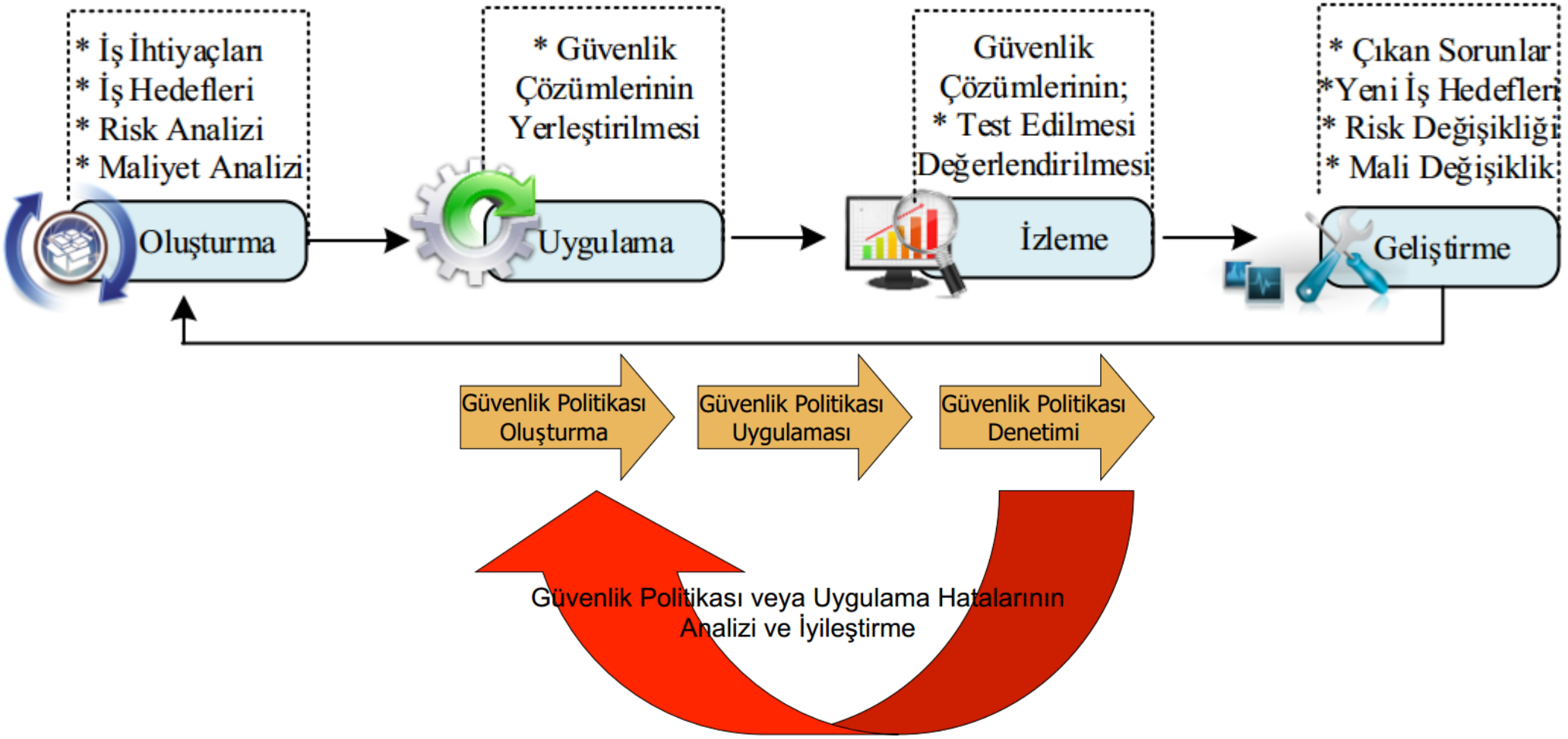
Eğitim

- 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.

Güvenlik Yönetim Süreci



Bilgi Güvenliği - Sertifikasyon

- CISA,
- CISSP,
- ISO 27001 LA,
- CEH

Bilgi Güvenliği Alanındaki Güncel Meslekler

- #1 Information Security Crime Investigator/Forensics Expert
- #2 System, Network, and/or Web Penetration Tester
- #3 Forensic Analyst
- #4 Incident Responder
- #5 Security Architect
- #6 Malware Analyst
- #7 Network Security Engineer
- #8 Security Analyst
- #9 Computer Crime Investigator
- #10 CISO/ISO or Director of Security
- #11 Application Penetration Tester
- #12 Security Operations Center Analyst
- #13 Prosecutor Specializing in Information Security Crime
- #14 Technical Director and Deputy CISO
- #15 Intrusion Analyst
- #16 Vulnerability Researcher/ Exploit Developer
- #17 Security Auditor
- #18 Security-savvy Software Developer
- #19 Security Maven in an Application Developer Organization
- #20 Disaster Recovery/Business Continuity Analyst/Manager

Bazı Kaynaklar

- http://muhammetbaykara.com/
- http://www.nsa.gov/
- http://www.bilgiguvenligi.gov.tr/
- http://www.bga.com.tr/
- http://www.cehturkiye.com/
- http://www.iso27001bilgiguvenligi.com/
- http://www.bilgimikoruyorum.org.tr/

  http://www.bilgiguvenligi.org.tr/

Nasıl Bir Proje Gerçekleştirebilirim?

- Kurumsal Bilgi Güvenliği açısından ülkelerin geliştirdiği stratejilerin ve ülkelerin bilgi güvenliğine bakış açılarının değerlendirilmesi. (Model, yazılım, strateji, istatistik vb.)
- Saldırı Tespit Sistemlerinin incelenmesi ve geliştirilmesi.
- Snort, ossec, pokemon, bro, firestorm vb. incelenmesi ve olası yeni alanlara uyarlanması
- Anomali temelli saldırı tespit sistemi geliştirilmesi.mpute
- Verilerin güvenli bir şekilde iletilmesine yönelik olarak kripto-steganografi uygulamaları.
- Xss, sql injection açıklıklarının tespitine yönelik uygulamalar.
- Sosyal Mühendislik maillerinin tespit edilmesine yönelik uygulamalar.
- Spam maillere yönelik olarak spamsavar.
- Web loglarının incelenmesiyle saldırı analizi uygulaması.
- DOS, syn flood saldırılarının analiz ve tespiti için çeşitli uygulamalar

Nasıl Bir Proje Gerçekleştirebilirim?

- Web güvenliğini sağlamak amaçlı uygulamalar (CAPTCHA, vb…).
- Biyometrik güvenlik sistemleri, iris tanıma, parmak izi tanıma vb. sistem güvenliği yazılımları
- Tek kullanımlık şifre üretimi ve uygulamaları
- E ticaret güvenliğinin sağlanmasına yönelik geliştirmeler
- Yazılım güvenliği, güvenli kod çalışmaları ve uygulamalar
- Windows azure ile güvenli bir bulut bilişim uygulamaları
- Yazılım Tanımlamalı Ağlarda güvenlik uygulamaları
- Mobil yazılımlarda güvenlik açıklarını önleme-mobil güvenlik.
- Mobil Bulut Bilişim uygulamaları (MCC)
- Veri merkezi-bulut yapısı: Data center networking
- Kötücül yazılım tespitlerine yönelik uygulamalar-Antimalware

Nasıl Bir Proje Gerçekleştirebilirim?

- Güvenlik duvarı uygulamaları
- Antivirüs, antimalware, antispyware uygulamaları
- Web uygulama güvenlik duvarı uygulamaları
- Veritabanı güvenlik duvarı uygulamaları
- E-posta güvenliğinin sağlanmasına yönelik uygulamalar
- Zaafiyet tarama sistemleri
- Kayıt toplama ve korelasyon sistemleri- SIEM
- Sıfırgün zararlı yazılım tespit sistemleri- zeroday
- Ağ izleme, performans analizi ve veri kaçakları önleme sistemleri

Tubitak Yarışmaları ve Destekleri-Yönlendirme

- **DETAYLAR İÇİN RESİMLERİ TIKLAYINIZ**