Ataşehir Adıgüzel MYO

Bilgisayar Programcılığı

Siber Güvenlik

Google.classroom

Sınıf kodu:xxxx

Öğr. Görevlisi Mustafa ÇORUH

I. Hafta

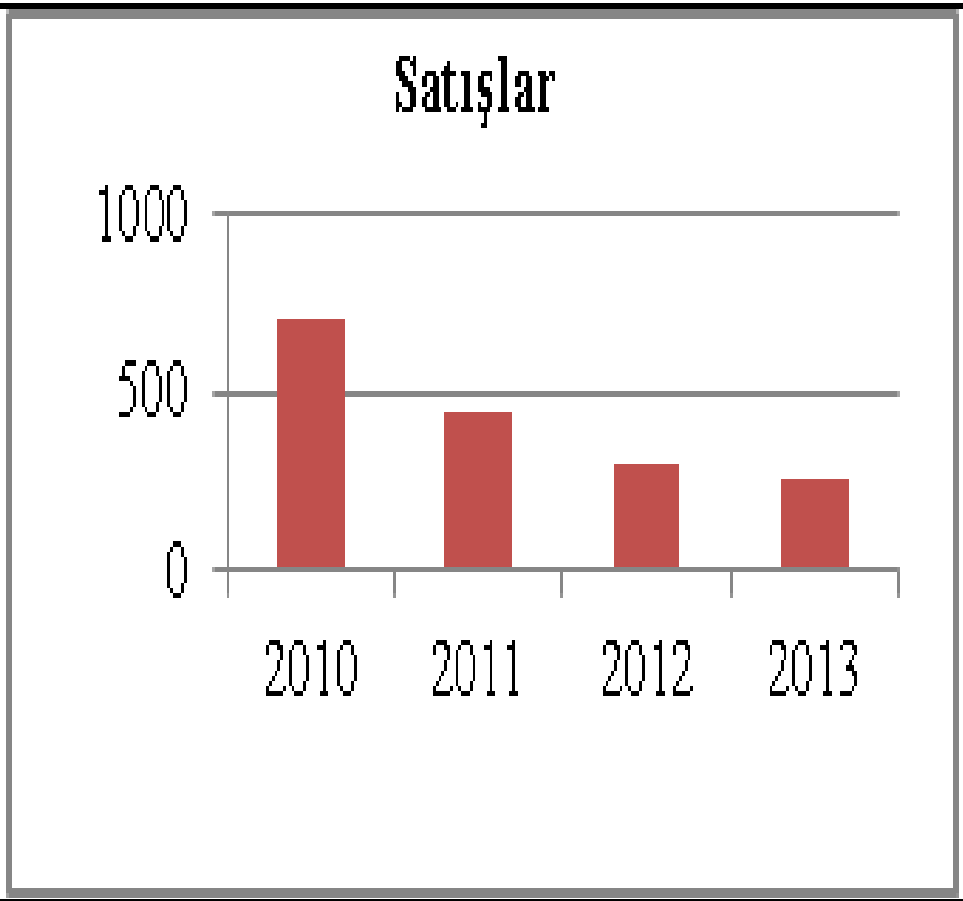
Bilişim Hiyerarşisine Giriş

Mustafa Çoruh

Veri, Enformasyon ve Bilgi

- Veri ve Enformasyon kodlanarak sayısal yazı haline getirilebilen ve dolayısıyla BT araçlarıyla işlenebilen kavramları, Bilgi ise kodlanamayan veya yazılı hale getirilemeyen, sadece insan beyninde bir anlamı olan kavramı ifade etmektedir.
- Bilgi, insanın etrafındaki dünyayı şekillendirme, onu sınıflandırma, yaşamlarındaki belirsizliği azaltma ve belirli bir biçimde dünyayı yorumlamak için veri ve enformasyon yardımıyla beyinlerinde oluşturdukları anlamlardır (Beijerse, 1999).

Şekil-2.3: Veri, Enformasyon ve Bilgi'ye Örnekler (Çoruh, 2017)

Veri	Enformasyon	Bilgi
2010 – 500 2011 – 450 2012 – 300 2013 – 250		Satışlarda düşüş var. Acilen önlem alınmalı.
05091962	05.09.1962	İşe almak için yaşlı

Tablo-2.6: Yeni Bilişim Hiyerarşisi		
Kavram	Açıklama	Örnek
İmge (Sign)	Bir dilin en küçük anlamlı birimi veya bir mananın sembolüdür.	İlköğretim
Veri (Data)	Gerçeği ifade eden yazı, kod, imge, ses vs. gibi ham veridir.	Lisans
Enformasyon (Information)	Organize edilmiş, yapısal hale getirilmiş, yorumlanmış özetlenmiş veridir.	Master
Bilgi (Knowledge)	İnsan beynindeki bir mana, durum (case), kural (rule), süreç veya modeldir.	Doktor
Uzmanlık-Anlayış (Expertise)	Anlayış, yeni bilginin sentezlenmesidir. Bilgi ile anlayış arasında bilişsel süreçlerin işin içinde olup olmaması açısından fark vardır. Bilgi ezber düzeyinde iken anlayışla bilişsel süreçlere dâhil edilerek öğrenme boyutuna varılır (Ackoff, 1989). Kişi belli bir alanda anlayışını geliştirince uzman olur. Uzmanlık ilgili faaliyetler için gerekli bilgi dağarcığına sahip olma ve olaylara çok farklı açılardan bakabilme yetisidir.	Doçent
Bilgelik (Wisdom)	Bilginin hayat için anlamını ve felsefesini kavramadır. Bilgelik, bilgiyi idrak etme, ayırt etme ve değerlendirme yanında karar verme sürecinde kullanabilme melekesidir (Uğras, 2015:18).	Profesör

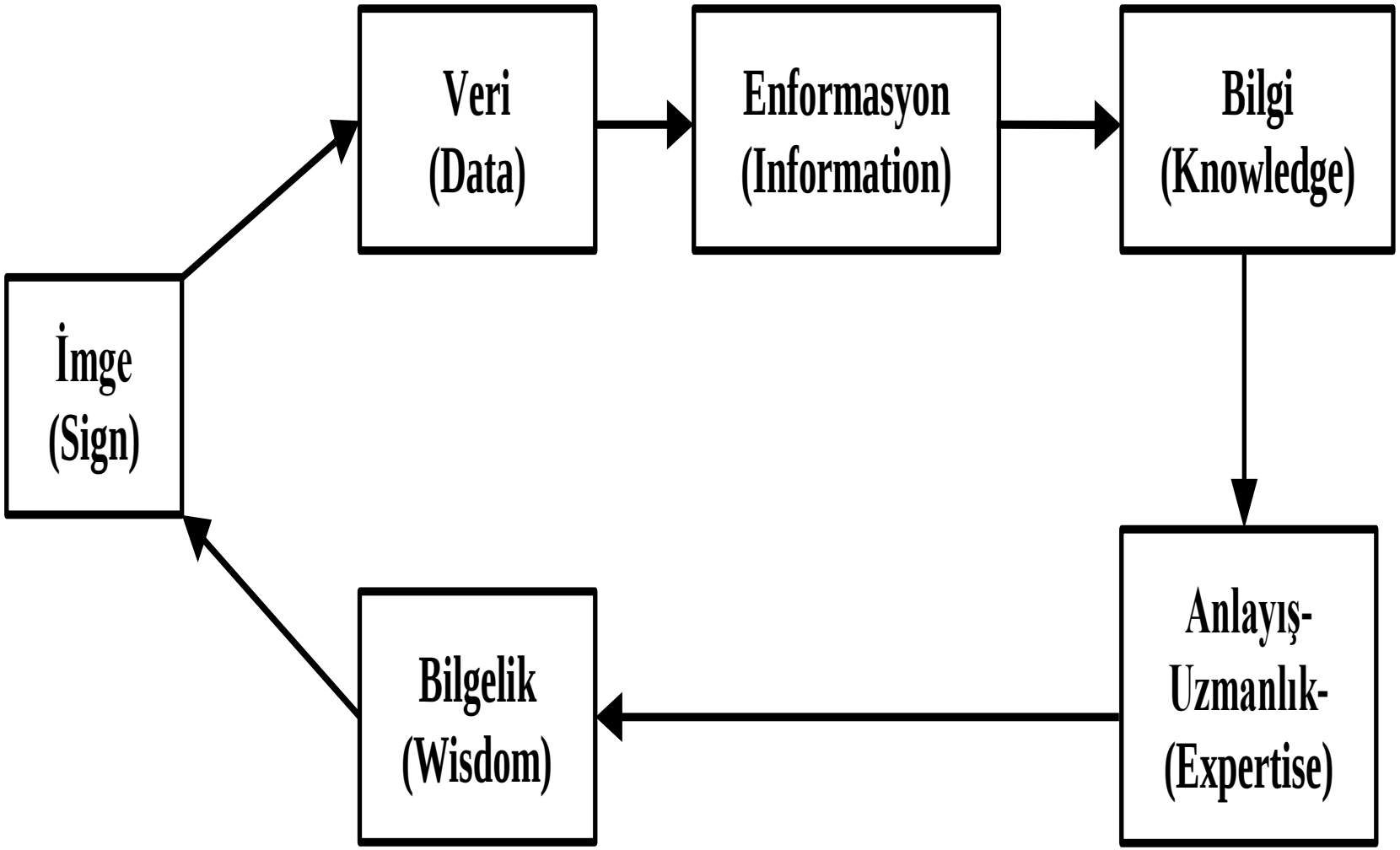
Veri, Enformasyon ve Bilgi

- Bilginin değeri güncel olmayan veya yetersiz bilgiyle alınan kararların verdiği zararın ölçüsüyle ters orantılıdır.
- Veri ve Enformasyon kodlanarak sayısal yazı haline getirilebilen ve dolayısıyla VT'lerde işlenebilen kavramları ifade etmektedir. Bilgi ise kodlanamayan veya yazılı hale getirilemeyen, sadece insan beyninde bir anlamı olan kavramı ifade etmektedir. Ancak zaman içinde geliştirilen teknolojilerle (Uzman sistemler gibi) bugün insan beynindeki bazı örtük bilgiler kayıt altına alınarak enformasyon haline getirilebilmektedir. Bu işlemin son noktası insan beyninin kopyalanmasıyla sağlanabilecektir. Bu kopyalamayı sağlayacak teknolojiye "Bilgi Teknolojisi" denebilir.
- BS Bölümünün misyonu, "diğer bölümler için enformasyon üretmektir."

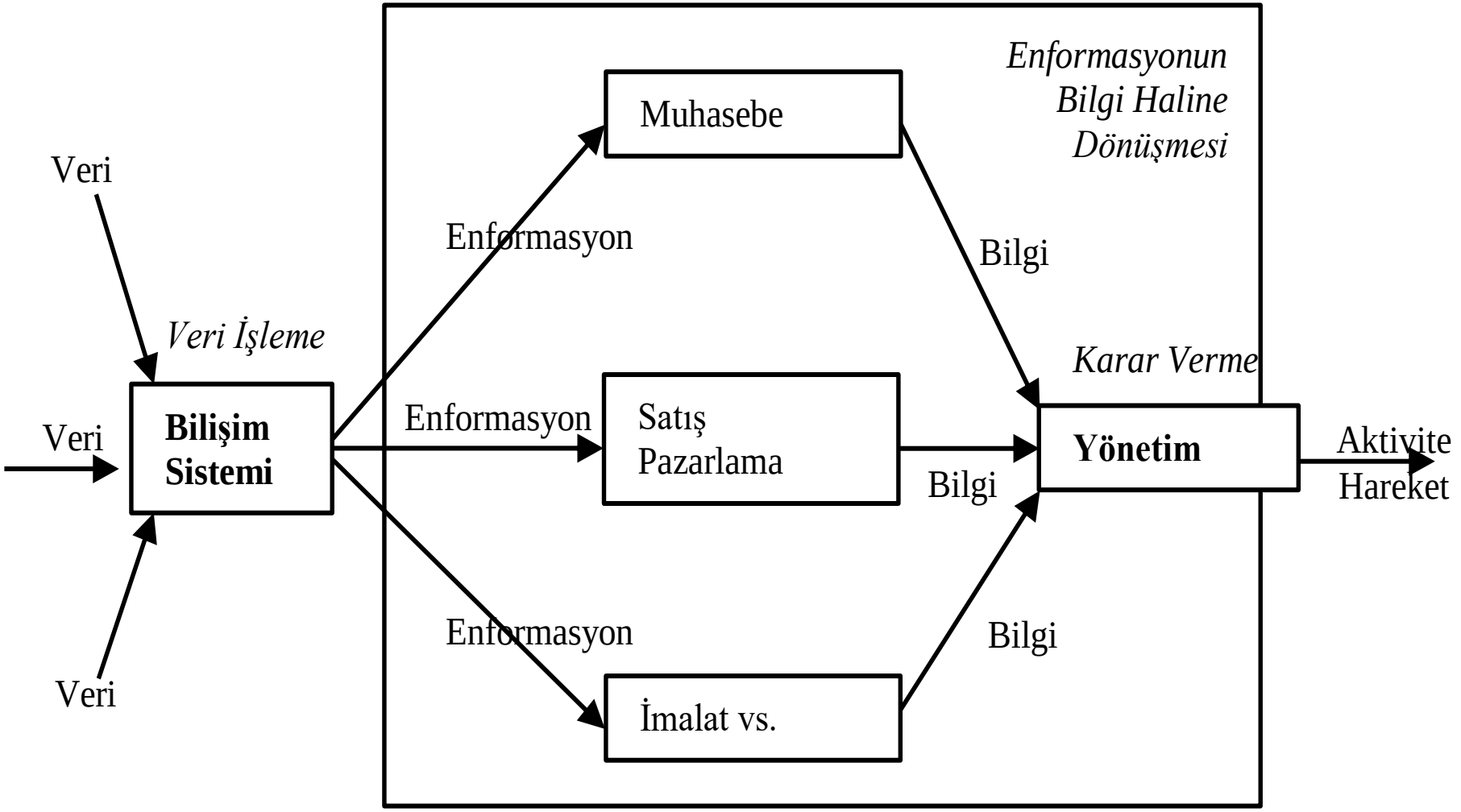
Uzmanlık ve Bilgelik

- Uzmanlık, Larousse'nin yaptığı tanıma uygun olarak düşünme, araştırma, gözlem, deney, akıl yürütme sonucunda elde edilen düşünsel ürünün organize hale getirilmiş biçimi olarak tarif edilebilir (Tutar, 2010:53). Kısacası insan beynindeki bilginin organize olmuş halidir.
- Bilginin felsefi manasını kavramak ise bilgeliktir.
- Ayrıca bilgelik aşamasına kadar doğru yapmak olgusu baskın iken bilgelik aşamasında artık doğru şeyi yapmak olgusu öne çıkmaktadır.

Şekil-2.2: İmgeden İmgeye Bilişim Döngüsü (Tutar, 2010:53)



Şekil-1.3: Kurumlarda Bilgi Üretim Modeli (Çoruh, 2015:21)



Veri İşleme: Veriyi enformasyon haline getirme işlemi

Karar Verme: Bilgiyi hareket (aktivite) haline getirme işlemi.

Tablo-3.8: Tarihsel Sıraya Göre Veri İşleme Araçları	
Yazının Bulunması	MÖ 5000-6000 yıllarında yazının Mezopotamya da bulunmasıyla nesiller arası bilgi aktarımı başlatıldı.
Kitabın İcadı	MÖ 1300 de Çin'de ve 500'de Atina'da Homeros'un destanlarının yazıya dökülmesi için kitap icat edildi.
Matbaanın İcat Edilmesi	1500 de Gutenberg'in matbaayı icat etmesiyle kitaplar kolayca basılıp çoğaltılabildi. Bu sayede Avrupa'da Reform ve Rönesans için altyapı oluşturuldu.
Bilgisayarın İcadı	1946 yılında ENIAC adlı ilk bilgisayarın icat edilmesiyle dijital veri ve enformasyon işlemenin yolları açıldı.
Kelime İşlemcinin İcadı	1976'da Word Star'la dijital kelime işlemcisinin üretilmesiyle bilgisayarda yazı yazmak ve yazıların kolayca düzenlenmesi gerçekleştirildi.
İnternet'in Yayılması	1995'den sonra internetin yayılmasıyla Dünya'da enformasyonun, tecrübenin, fikirlerin, haberlerin ve icatların paylaşılmasının önündeki tüm engeller ortadan kalkmış oldu.
Mobil Teknolojilerin Kullanımı	Özellikle 2000 yılından sonra iletişim ve veri işleme teknolojilerinin akıllı telefonlar yardımıyla gelişmesiyle mobilazasyon artmıştır.

Tablo-2.12: Enformasyon Miktarındaki Değişim	
Yıl	Enformasyon Miktarı (Birim)
1920	1
1940	2
1960	4
1980	8
2000	16
2020	32

BS alt yapısını oluşturan BT'ler

- Bilgisayarlar (Donanım),
- Paket veya özel yazılımlar,
- Veritabanları,
- Bilgisayar ağları (şebeke),
- İletişim teknolojileri,
- İnternet ve Web Teknolojileri,
- Mobil teknolojiler,
- Bulut bilişim.

Önemli Notlar

- Teknoloji kendi kendine gelişmiyor. Birileri tarafından rekabet avantajı sağlamak için geliştiriliyor.
- Bilim ve Teknolojinin ahlakı yoktur. İyi veya kötü değildir. Bunları kullanan insanlar iyi veya kötüdür.
- Atom bombasıyla yüzbinlerce kişiyi bir anda öldüren çiftçiler, işçiler, şoförler değildir. Kimler?
- Eğer bir şeyin bir amacı varsa bir tasarlayıcısı vardır.
- Öğretimden amaç sağlanan veri ve enformasyonla (malumat) öğrencinin kendi bilgisini oluşturmasını sağlamaktır.

II. Hafta Bilişim Güvenliği

https://docs.google.com/viewerng/viewer?url=http://www.siberguvenlik.xyz/ders/Siber2.pdf

Mustafa Çoruh

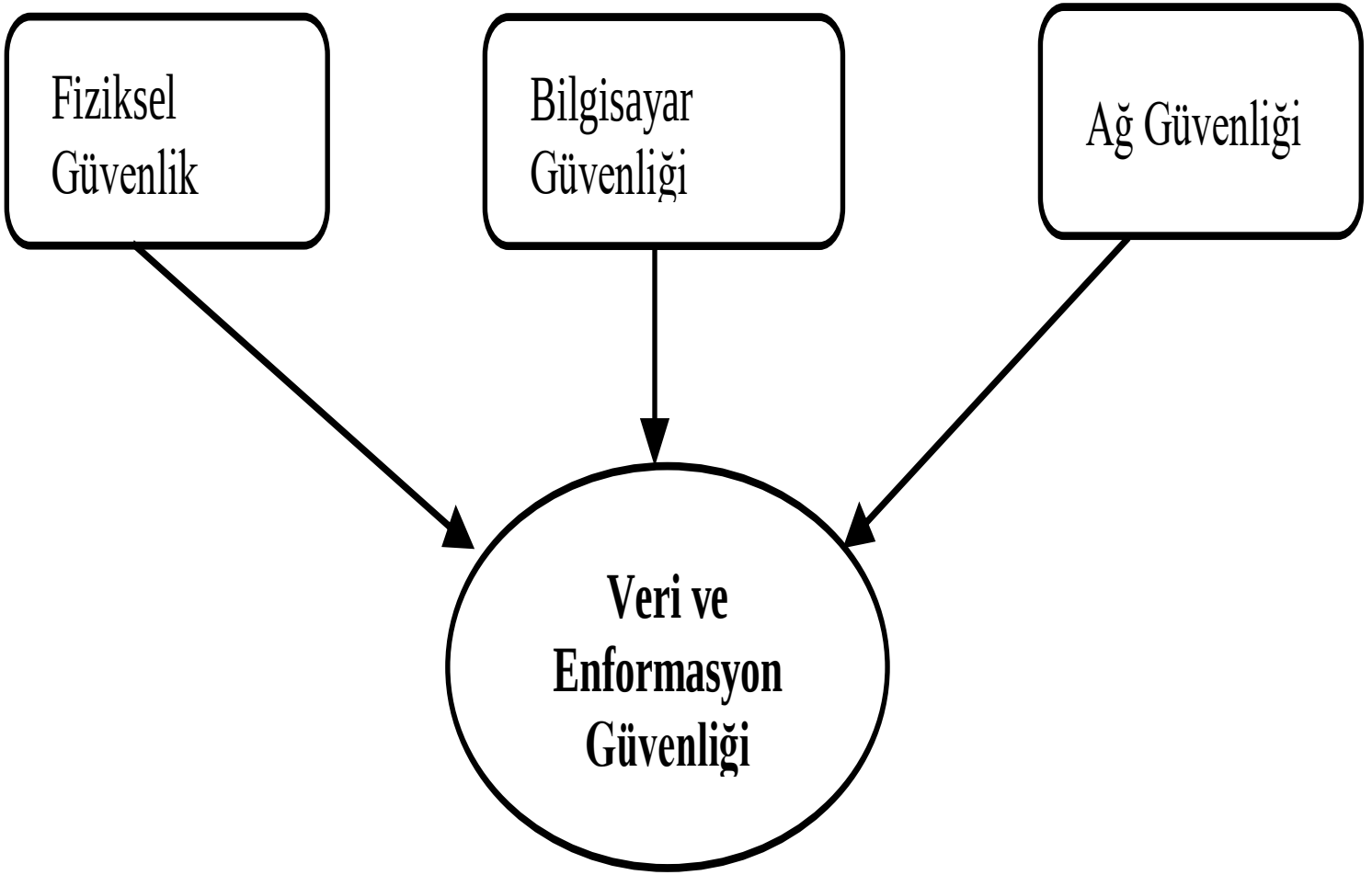
Kurumlarda Bilişim Güvenliğinin Amaçları (Oz, 2006 aktaran Cura, 2009:186):

- BS ve organizasyon işlemlerinin durma riskini azaltmak,
- Enformasyon ve veri gizliliğini sağlamak,
- Veri kaynaklarının güvenilirliğini ve bütünlüğünü sağlamak,
- Veri kaynaklarının ve çevrimiçi işlemlerin kesintisizliğini sağlamak,
- Gizlilik ve güvenliğe saygı göstererek anlaşmalar ve kanunlara uyulmasını sağlamak.

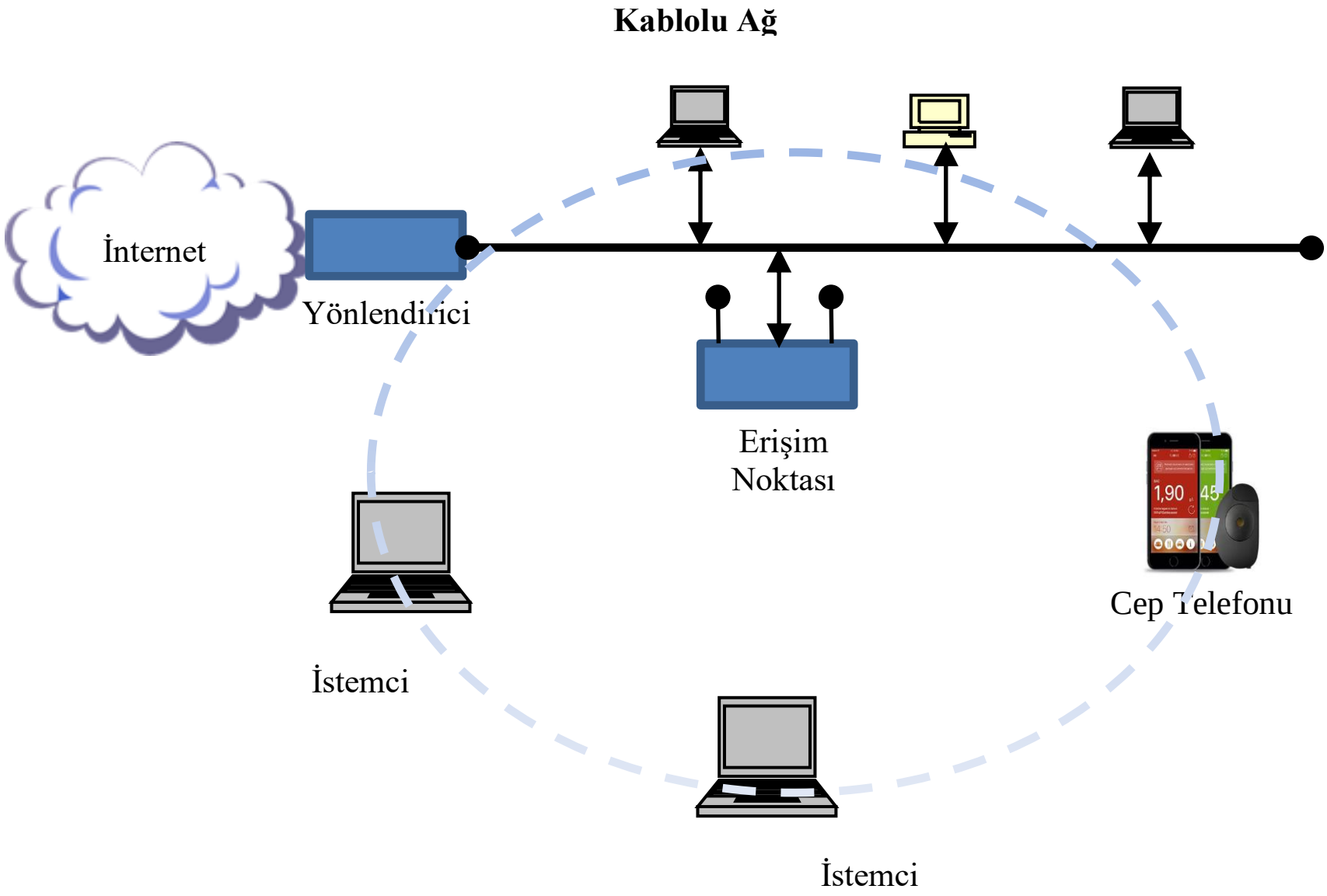
Bilişim Sistemi Güvenliği

- Sözlük anlamıyla BS güvenliği, doğal afetler, sabotaj, suç, saldırı veya veri kaçırmaya karşı korunmaktır.
- BS güvenliği = Gizlilik + Erişebilirlik + Bütünlük şeklinde formülleştirilmektedir. Bu ana öğelerden "Bütünlük" ise kimlik doğrulama, yetkilendirme ve inkâr edememe alt ilkelerinden oluşmaktadır (Graham, Howard, Olson, 2011 & Canavan, 2001).
- BS'lerin güvenliği, Şekil-11.6'da görüldüğü gibi fiziksel, ağ ve bilgisayar güvenliği olmak üzere üç temel başlık altında incelenebilir. Bu üç güvenlik yani BS güvenliği aslında sistemdeki veri ve enformasyonun güvenliğini sağlamak için yapılmaktadır.
- BS'lerin veya Bilgisayarların fiziksel güvenliği denince; yangın, su basması, deprem gibi doğal afetlere karşı BT/BS'leri korumaya yönelik tedbirler akla gelmektedir.
- Bilgisayar güvenliği; işletim sistemi güvenliği, veri (data) güvenliği ve veritabanı (database) güvenliği gibi kavramları içeren genel bir kavramdır (Tutar, 2010:139).
- BS içinde Bilgisayar Ağı veya şebeke güvenliği, kullanıcılara tüm bilgisayar kaynakları ve hizmetlerini bir bütün olarak ve gizliliği koruyarak sunmaktır (Tutar, 2010:140).
- BS güvenliği işgören odaklıdır ve çalışanların çok iyi eğitilmesini zorunlu kılmaktadır (Sipior, 2008:54).

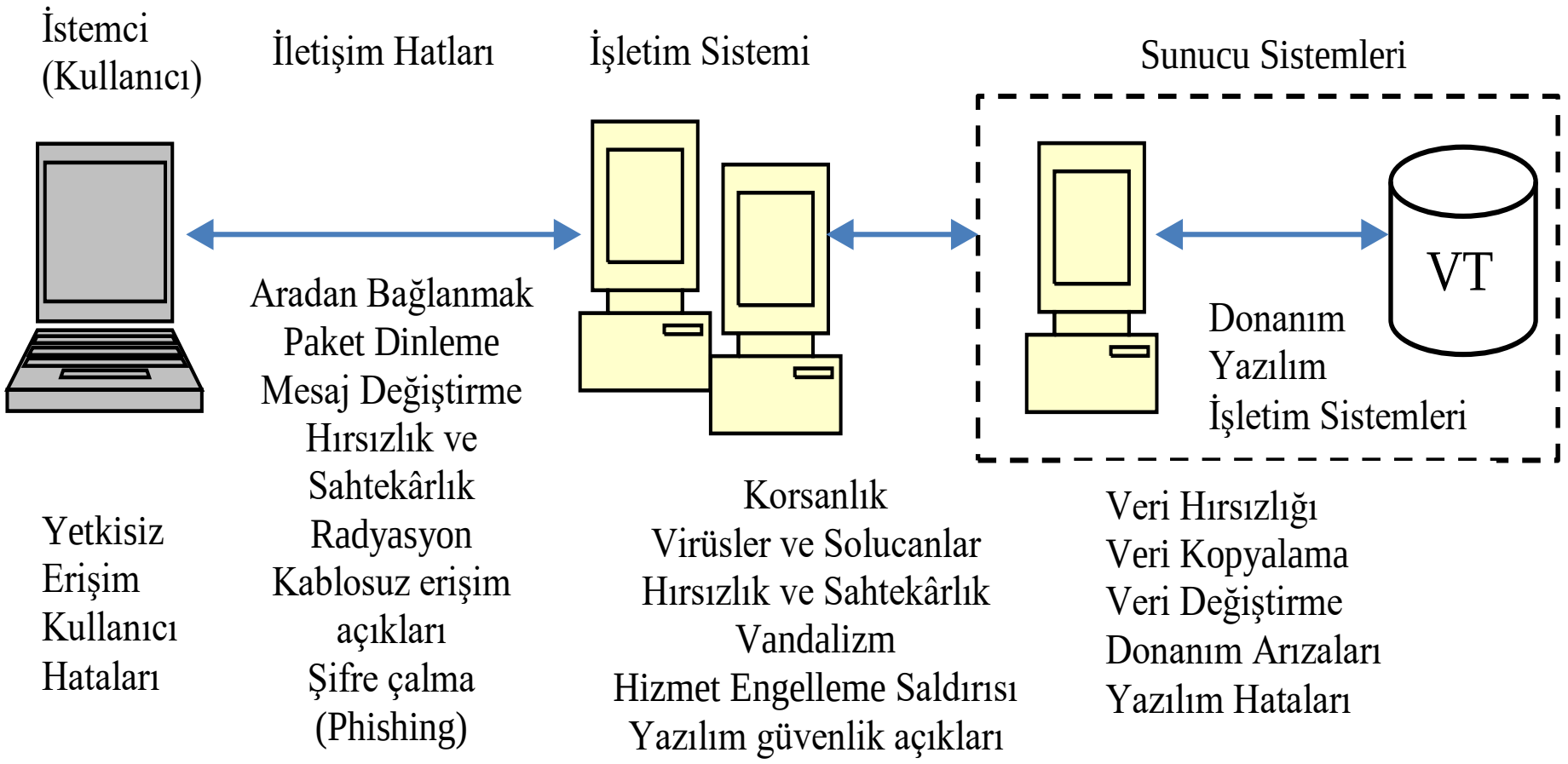
Şekil-2.6: Bilişim Güvenliğini Etkileyen Unsurlar (Çınar-Dondurmacı, 2014:210)



Şekil-3.7: Kablosuz Bilgisayar Ağ (Network) Sistemi (Laudon, 2014:278)



Şekil-2.7: Kurumlarda BS Ağ Güvenlik Sistemi Zayıflıkları (Laudon, 2014:293)



Veri ve Enformasyon Güvenliği

- Enformasyon: Bir kurumun kuruluşun veya organizasyonun faaliyetlerini yürütmekte kullandıkları verilerin anlam kazanmış haline denir.
- Veri Güvenliği: Öneme sahip bilginin korunması, bütünlüğünün sağlanması, erişebilir ve ulaşabilir olmasının sağlanması için alınan gerekli, önemler ve tedbirlerdir.
- Veri Güvenliği Yönetim Sistemi Standardı (ISO 27001).

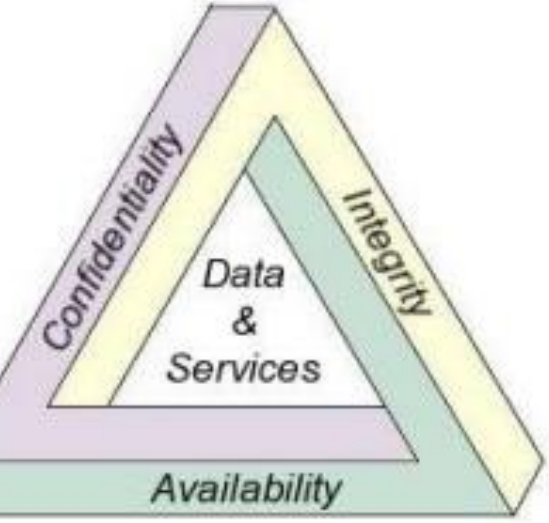
- Bilişim güvenliği ve siber güvenlik çoğu zaman birbirleri yerine kullanılan ancak birbirlerinden farklı olgulardır. Veri ve enformasyon güvenliği verinin bütünlüğünün, güvenliğinin ve gizliliğinin korunması olarak tanımlanır ve ISO 27001, ITIL, COBIT gibi global çapta kabul görmüş standartlarla sınırları çizilmiştir. Ancak alt yapısı bilişim sistemleri olan bilgi güvenliğini de kapsayan çok daha geniş bir kavramdır (https://berqnet.com/blog/siber-guvenlik-nedir).

CIA Üçlüsü (CIA Triad)

Confidentiality - Gizlilik

Integrity - Bütünlük

Availability - Erişilebilirlik
(Kullanılabilirlik)



Veri ve Enformasyon Güvenliği

- Gizlilik: Verilerin yetkisiz erişime karşı korunması
- Bütünlük: Verilerin eksiksiz, tam, tutarlı ve doğru olması
- Erişilebilirlik: Verilerin yetkililerce ihtiyaç duyulduğunda erişilebilir olması

Veri ve Enformasyon Güvenliği

- Gizlilik – Confidentiality: Herşeyi herkesten gizlemek değil, veriye/bilgiye sadece yetkisi onların ulaşılabilmesini sağlamak. Şifreleme gibi..
- Bütünlük – Integrity: Yetkisiz ve izinsiz değişikliklerin engellenmesi, verinin amacına uygun derecede doğru olması.
- Erişilebilirlik – Availability: Veriyi iletmek, depolamak ve işlemekten sorumlu hizmetlerin devamlılığının sağlanması.

- Veri güvenliğinin sağlanmasından herkes sorumludur. (Bilginin sahibi, kullanan, sistemi yöneten, vb..)
- Yetki paylaşılır, sorumluluk paylaşılmaz. Bilgi ise paylaşıldıkça artar.

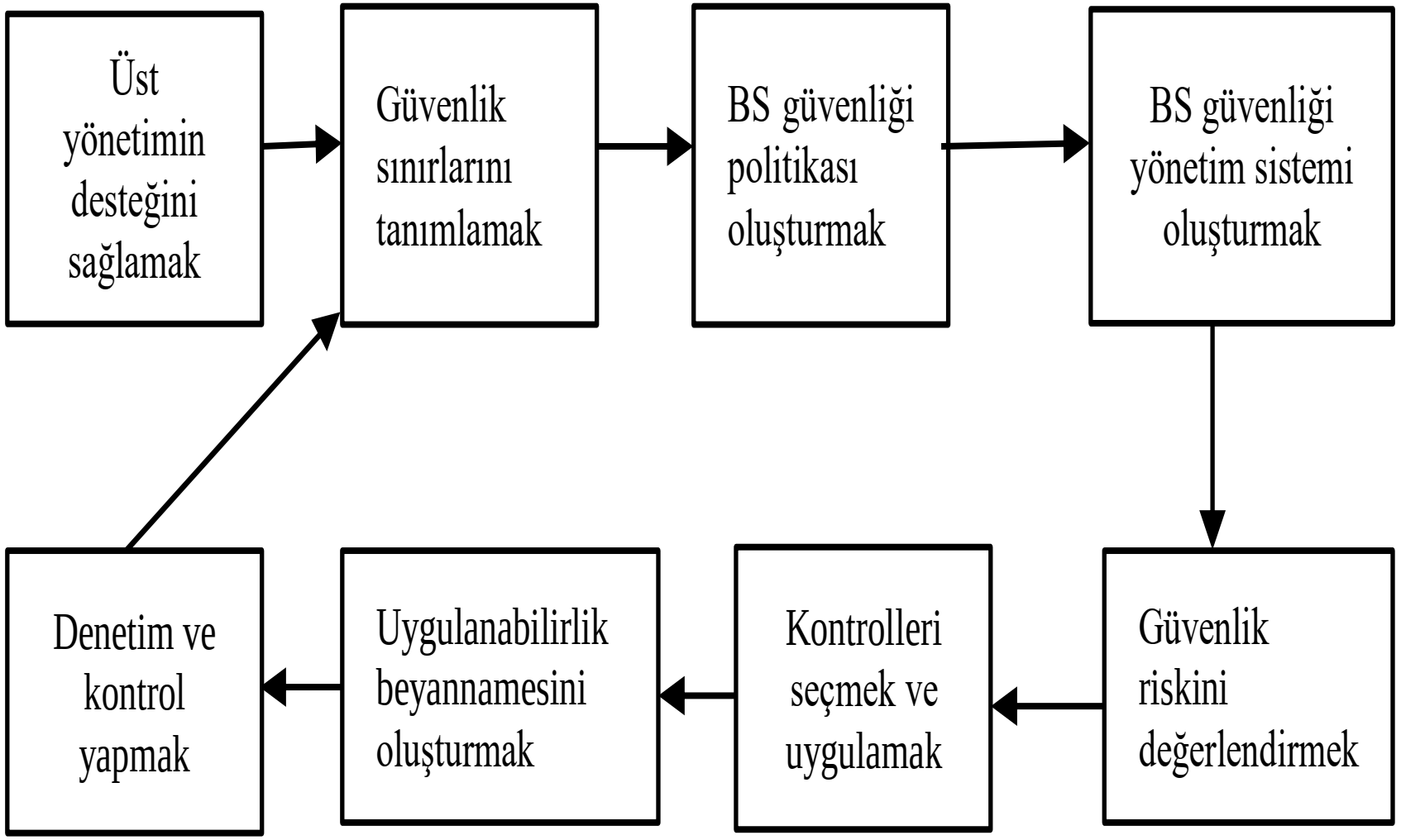
Veri ve Enformasyon Güvenliği Kategorileri

- Ağ güvenliği (Network security)
- Uç/Son nokta veya Kullanıcı güvenliği (Endpoint security)
- Veri güvenliği (Data security)
- Uygulama güvenliği (Application security)
- Kimlik ve Erişim Yönetimi (Identity and access management)
- Güvenlik yönetimi (Security management)
- Sanallaştırma ve bulut (Virtualization and cloud)

Bilişim Güvencesi (Information Assurance, IA)

- Bilişim sistemlerinin ;
- • Kullanılabilirliğini,
- • Bütünlüğünü,
- • Doğrulanmasını,
- • Gizliliğini ve
- • İnkar edememe
- Özelliğini sağlar. Veri güvenliğini de içine alır.

Şekil-11.8: Bilişim Sistem Güvenliği Yönetim Süreci (McFadzean & Ezingeard & Birchall, 2007:622)



BT/BS'lerin Güvenliği İlgili Kanunlar

- İlgili standartların son halleri https://webstore.ansi.org/ adresinden takip edilebilir:
- ISO/IEC 27001 / ISO/IEC 27002 / ISO/IEC 27017 - IT Security Control Code of Practice Package (Bilişim Sistemleri güvenliği),
- ISO 27799 / ISO/IEC 27001 / ISO/IEC 27002 - Protected Health Information Security Management Package (Sağlık Bilişim Sistemleri güvenliği),
- ISO/IEC 27018 / ISO/IEC 29100 / ISO/IEC 27001 - Public Clouds Privacy Framework Package (Bulut Bilişim Sistemleri güvenliği)

III. Hafta

Siber Güvenliğe Giriş

https://docs.google.com/viewerng/viewer?url=http://www.siberguvenlik.xyz/ders/Siber2.pdf

Mustafa Çoruh

Siber Güvenlik (Cyber Security)

- Siber uzayda organizasyon ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünüdür.
- Kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon
- sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır.

- Siber güvenlik, kurum, kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlamaktadır.

- Kaynak: Uluslararası Telekomünikasyon Birliği (ITU)

Siber Güvenlik Terimleri

- Hack : Kırmak, Küçük parçalar koparmak, Açık yönlerini ortaya çıkarmak, ve Açıklığı kullanmak Anlamlarında kullanılır.
- Hacking : Sistem veya programın açığından yararlanıp erişim sağlamak, değiştirmek veya silmek. Açıklığı kullanma işlemidir.

Hacker

- Sistemlere sızabilme yeteneğine sahip, programlama bilgisi üst düzeyde olan ağ ve sistemlerin işleyişini iyi bilen, gerektiğinde sosyal mühendislik yapabilen, hacking araçlarını tanıyan ve bunları gerektiği zaman geliştirebilen kişilerdir.

Hacker’ın Yapabildikleri

- Siber korsan,
- İnternet ve ağ alt yapısı bilgisine sahip,
- Programlama dili bilen,
- Ağ veya sisteme sızmayı başarabilen,
- Verilere-bilgilere ulaşabilen,
- Tüm işlemleri fark edilmeden yapabilen,
- İleri düzey bilgiye sahip kişidir.

Siber Korsanlar

- Etik, kültür, etnik veya siyasi özelliklerine göre farklılar göstermektedir.
- Siyah Şapkalı Hacker,
- Gri Şapkalı Hacker,
- Beyaz Şapkalı Hacker,
- Haktivist,
- Cracker,
- Phreaker,
- Lamer,
- Script Kiddie

Hackerlar ve Şapkaları

- Amaç ve faaliyetlerine göre; Siyah Şapkalı, Gri Şapkalı ve Beyaz Şapkalıdır.
- Siyah Şapkalı Hacker:
  - Kötü amaçlı, zarar vermek veya para odaklı,
  - Sistemleri ele geçirmek veya yok etmek için,
  - Saldırı gerçekleştiren, tehlikeli bilgisayar korsanıdır.
  - Sisteme erişimi engelleme, bilgi değiştirme, gizli bilgi çalma gibi faaliyetlerde bulunurlar.
- Beyaz Şapkalı Hacker
  - Etik hacker,
  - Aynı bilgi ve beceriye sahip, İyi niyetli,
  - Açıklığı tespit eden, uyaran veya önleyen,
  - Sistem güvenliğinden sorumlu personel,
  - Ahlaklı siber korsandır.

Gri Şapkalı Hacker

- Sistemlere sızma ve giriş yapan,
- Kötü amaç olmayıp, merak için,
- Yasallık sınırlarında saldırganlık faaliyeti olan,
- Zaman zaman tehlikeli faaliyetler içerisinde,
- Yaptıkları hukuk karşısında suç teşkil eden,
- (Sisteme sızma, girme vb.) Siber korsanlardır.

Cracker

- Bilgisayar programlarının kopya korumalarını kırarak, bu programların izinsiz olarak dağıtımına imkan veren veya bu yolda çıkar sağlayan kişilere denir. (Yazılım korsanı)
- Lisansların iptali veya serial-key temini,

Hacktivistler

- Hacker + Aktivist = Hacktivist
- Kendilerine göre, toplumsal sorun veya yanlış politik durum olarak gördükleri konulara dikkat çekmek için sistemlere saldıran kişi veya gruplardır. (sanal protestocu)
- – Wikileaks,
- – Anonymous,
- – RedHack,
- – Cyber-Warrior,
- – Ayyıldız Tim,
- – SEA vb.

Lamer

- Başkalarının önceden yazdığı betik(script) kodları veya programları çalıştırır, övünür,
- Ağ, sistem, yazılım, programlama gibi konularda bir bilgiye sahip olmadan, Atak yapmaya çalışan kişilerdir.
- (Lamer: Özenti, basit)

Script Kiddie

- Yeterli bilgisi olmadan hazır araçlarla saldırı düzenleyen (genelde genç yaşta-çocuk) kişilere verilen isimdir. (Betikçiler-BetikKerataları)
- Tıpkı lamer'lar gibi ama bir miktar bilgi sahibi,
- Kötü niyetli, zarar verme amaçlı,
- Teknik detay ve programın nasıl çalıştığını bilmez, ama kullanımını bilenlerdir.

Phreaker

- Telefon iletişim hatlarına erişip,
- Uzun süreli Ücretsiz görüşme, vb. amaçlı,
- Telefon kırıcılardır.

NewBie

- Çaylak, okula yeni başlayan,
- Bilişimde veya programla da yenilere denilir,
- Betik keratalarından bir basamak üstte,
- Kendini öğrenmeye adamış bilişim korsanı adaylarıdır.

Script Kiddie

- Yeterli bilgisi olmadan hazır araçlarla saldırı düzenleyen (genelde genç yaşta-çocuk) kişilere verilen isimdir. (Betikçiler-BetikKerataları)
- Tıpkı lamer'lar gibi ama bir miktar bilgi sahibi,
- Kötü niyetli, zarar verme amaçlı,
- Teknik detay ve programın nasıl çalıştığını bilmez, ama kullanımını bilenlerdir.

Script Kiddie

- Yeterli bilgisi olmadan hazır araçlarla saldırı düzenleyen (genelde genç yaşta-çocuk) kişilere verilen isimdir. (Betikçiler-BetikKerataları)
- Tıpkı lamer'lar gibi ama bir miktar bilgi sahibi,
- Kötü niyetli, zarar verme amaçlı,
- Teknik detay ve programın nasıl çalıştığını bilmez, ama kullanımını bilenlerdir.