BİLGİ GÜVENLİĞİ DERSİ
2. HAFTA

TEMEL BİLGİ GÜVENLİĞİ UNSURLARI

DR. ÖĞR. ÜYESİ FURKAN ATLAN

Veri

İnsanların anlayabileceği ve kullanabileceği şekle dönüştürülmemiş ham gerçeklerdir.

Veri

Bilgi işleme sürecinin temel girdisi olarak çeşitli sembol, harf, rakam ve işaretlerle temsil edilebilen, işlenmeye hazır izlenimlerdir.

BÜYÜK VERİ (BIG DATA)

Büyük veri (big data), hacmi çok büyük, karmaşık ve hızlı bir şekilde artan veri kümelerini tanımlamak için kullanılan bir terimdir. Bu veri kümeleri genellikle geleneksel veri tabanı araçları ile işlenmesi zor veya imkansız olan yapılandırılmamış verilerden oluşur.

Enformasyon

Bir amacı ve önemi olan veridir.

«Belli bir şekle sokulmuş, anlamlı ve insanlara faydalı olabilecek veridir» (Laudon)

Big data içerisinde yer alan yapılandırılmış veriler olarak düşünülebilir.

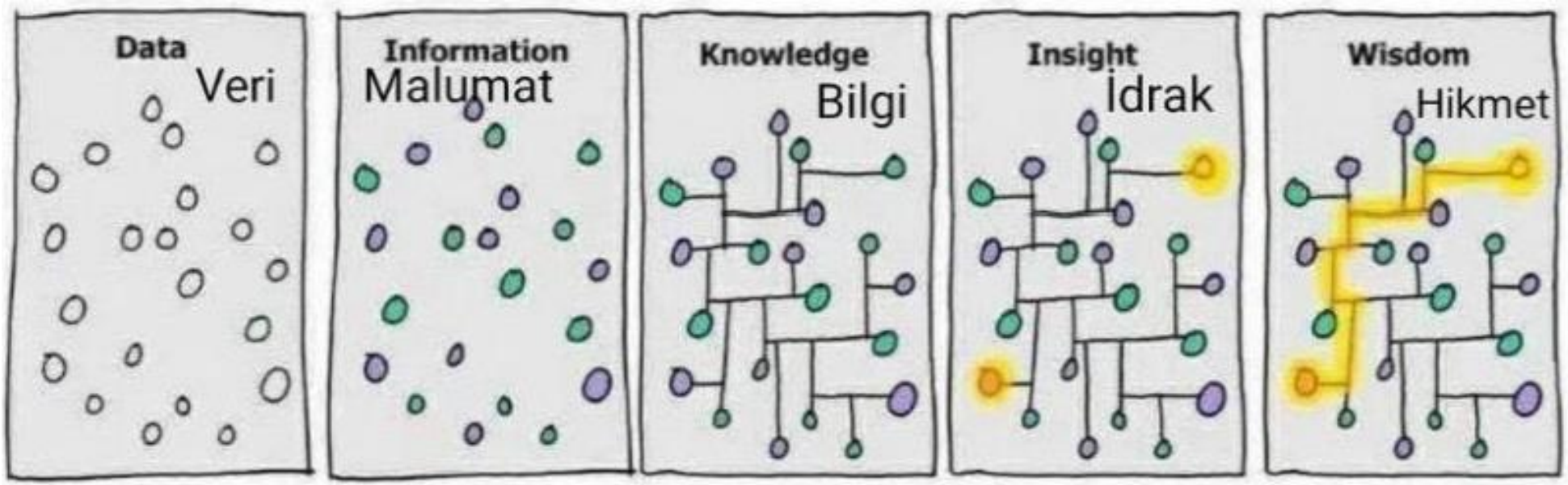
BİLGİ

«Düşünme, yargılama, akıl yürütme, araştırma, gözlem ve denge sonucunda elde edilen düşünsel ürün»

«Sistemli bir şekilde iletişim araçlarıyla başkalarına aktarılan, mantıklı bir hükme veya tecrübeye dayanan, sonucu gösteren gerçekler ve sistemli ifadeler bütünüdür»

«Bilgi bir bina, enformasyon ise yapı malzemesidir»

Enformasyon-Bilgi İlişkisi



BİLGİ GÜVENLİĞİ

Bilginin bir varlık olarak tehdit ve tehlikelerden korunmasıdır.

Bilgi Güvenliğinde Tehdit

Bilgi güvenliğini tehlikeye atan olası olayların veya durumların genel kavramıdır.

Örneğin; bir şirketin çalışanının içeriden bilgi sızdırması bir tehdittir.

Bilgi Güvenliğinde Tehlike

Belirli bir tehdidin gerçekleşmesi durumunda ortaya çıkacak olası zarar veya kayıpları ifade eder. Tehlikeler, bir tehdidin gerçekleşmesinin potansiyel sonuçlarıdır.

Örnek: Bilgisayar korsanlığı tehdidi, veri sızıntısı, itibar kaybı, hukuki sorunlar ve finansal kayıplar gibi çeşitli tehlikeleri beraberinde getirebilir. Örneğin, bir şirketin müşteri verileri sızdırıldığında, bu durum hem müşterilerin güvenini sarsabilir hem de şirketin itibarını ciddi şekilde etkileyebilir.

BİLGİ GÜVENLİĞİ TEMEL UNSURLARI

Bilgi güvenliği, bilgi varlıklarını korumayı amaçlayan 3 temel unsurdan oluşur.

Bunların tek bir amacı vardır: Güvenli bir şekilde sistemin devamlılığının sağlanması.

Confidentiality

Integrity

Availability

BİLGİ GÜVENLİĞİ TEMEL UNSURLARI

Gizlilik (Confidentiality): Bilginin, yetkili olmayan kişilerin eline geçmesini engellemeyi amaçlar.

Bütünlük (Integrity): Bilginin yetkisiz kişiler tarafından değiştirilmesinin, silinmesinin engellenmesini ve bilginin bütünlüğünün korunmasını amaçlar.

Erişilebilirlik (Availability): Bilginin, yetkili kişilerce ihtiyaç duyulduğu her an erişilebilir olmasını amaçlar.

BİLGİ GÜVENLİĞİNDE SORUMLULUKLAR

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 yapılabilir.

Bilginin Korunmasında Bizim Sorumluluklarımız

- Bilgiler korunmasız bırakılmamalıdır (Örneğin; bilgisayarınızı bir yerde kapalı şekilde olsa bile bırakmazsınız. Sonradan açılma ihtimaline karşı.)
- Veriler paylaşılmamalı ya da güvenli ve sınırlı bir şekilde paylaşılmalıdır. (Form doldurulurken «zorunlu olmayan alanların» boş bırakılması)
- Şirketin «bilgi güvenliği politikasına» uyulmalıdır (ip adreslerine filtre konulduğu zaman devre dışı bırakacak işlemlerin yapılmaması)

Bilginin Korunmasında Bizim Sorumluluklarımız

- Şüpheli durumlarda ilgili kurumlar ve yetkililer ile iletişime geçilmelidir (kredi kartının kaybolması durumunda bankanın aranması ya da şirket içerisinde bir olay olması durumunda üst yönetime haber verilmesi)
- Farkındalık için bilgiler her zaman güncel tutulmalıdır (zero day)
- Her zaman şüpheli yaklaşım tarzı benimsenmeli (Bu bilgiyi neden soruyorsun? Ya da dosyalar açılırken güvenli bir ortamda açılmalı)

BİLGİ GÜVENLİĞİNDE RİSKLİ DAVRANIŞLARIMIZ

- Uygulama indirirken verdiğimiz izinler (her uygulamaya her izin verilmeyebilir. Sadece uygulama kullanılacağı zaman izin verilebilir)

- Bilgisayar ekranını kilitlemeden yanından ayrılmak

- Kullanıcı ya da kart bilgilerini kaydetmek

BİLGİ GÜVENLİĞİNDE RİSKLİ DAVRANIŞLARIMIZ

- Güncellemeleri görmezden gelmek
- Farklı sitelere sosyal medya hesaplarımız ile kaydolmak
- Talep edilen her bilgiyi yanıtlamak ya da form doldururken bu bilgileri paylaşmak

BİLGİ GÜVENLİĞİNDE RİSKLİ DAVRANIŞLARIMIZ

- İlginç başlıklar görünce göz atmak (Twitter ya da instagram'da çıkan banka hesaplarının «iade ücretlerinin ödenmesine dair m

BİLGİ GÜVENLİĞİ OLAYI NEDİR?

Bir kişiye veya kuruma ait verilere veya cihazlara yetkisiz erişim gerçekleşmesi, verilerin çalınması veya kullanılması durumlarıdır.

NELER BİLGİ GÜVENLİĞİ OLAYIDIR?

- Bilgisayarınızın ya da cep telefonunuzun çalınması
- Bir e-posta içerisindeki zararlı bir bağlantıya tıklamak ya da zararlı bir dosya indirmek (çözüm için https://www.virustotal.com/gui/home/upload)
- Şüpheli bir mesaj, arama ya da e-posta almak
- Bir kişinin veri sızıntısı yaptığına ya da destek sağladığına tanık olmak

Örnek bir Bilgi Güvenliği Olayı

Arkadaşlarınız ile bir restorana gittiniz. Menüler QR kod tarayıcısı ile görüntüleniyor. Menüyü seçtiniz ve ödemeyi de yaptınız. Ancak, o QR kodu bir saldırgan tarafından yerleştirilen zararlı bir bağlantı içeriyordu. Kişisel bilgileriniz ve kredi kartı bilgilerinizi girdiniz.

Garson, size hesabı getirdiğinde dolandırıldığınızı anladınız. NE YAPARDINIZ?

Örnek olay için olay anında yapılacaklar

Şüphelenme ve ihbar: «Neden hesabı şimdi ödüyorum?» Restoranın gerçek web sitesini kontrol edin (çoğu zaman sahtesi de buna göre düzenlenmiştir zaten). Her iki QR kodun adresini ve sonucunu karşılaştırın. Durumu restoran yetkililerine bildirin.

Örnek olay için sonrasında yapılacaklar

Önlemler:

- Kredi kartını iptal etmek için bankayı arayın
- Parola bilgisi girdiyseniz ve aynı parolayı kullanan kartlarınız varsa onları da iptal edin (hatta ardışık olarak kullandığınız parolaları bile iptal edin)
- Telefona bir dosya indirdiyseniz dosyayı silin. Daha sonra antivirüs taraması başlatın.
- QR kod kullanacağınız zaman siteyi manuel olarak yazın

KVKK

Kişisel verilerin korunmasını sağlamak amacıyla yürürlüğe konmuş bir kanundur.

Bu kanun sayesinde her bir bireyin kendisi ile ilgili verilerin 3. bir kişinin eline geçmemesi konusunda gerekli tedbirlerin alınmasını isteme hakkı vardır.

Kişisel Veri

Kimliği belli ya da belirlenebilir gerçek kişiye ilişkin her türlü bilgidir.

- Ad-Soyad
- Adres
- TC Kimlik Numarası
- Plaka Numarası
- Doğum Tarihi

Özel Nitelikli Kişisel Veri

Öğrenildiği zaman kişinin mağdur edilmesine ya da ayrımcılığa tâbi tutulmasına sebebiyet verecek nitelikteki verilerdir.

- Sağlık Verileri
- Kılık-kıyafet tercihi
- Dernek, vakıf, sendika üyeliği
- Ceza Mahkumiyeti

Haklarımız Nelerdir?

KVKK'nın 2. maddesinde kişilerin hakları belirlenmiştir.

- Kişisel veri işlenip işlenmediğini öğrenme
- Kişisel veri işlenmişse buna ilişkin bilgi talep etme
- Yurt içinde ya da yurt dışında kişisel verilerin aktarıldığı üçüncü kişileri öğrenme
- Kişisel verilerin kanuna aykırı bir şekilde işlenmesinden dolayı uğranılan zararın tazminini talep etme