

BTRisk



KİŞİSEL VERİLERİN KORUNMASI

Hasta Hakları
Açısından Mahremiyetin
Önemi

Fatih Emiral CISSP, CISA, CEH, CIA
6 Mart 2009

İçindekiler

- I. Kişisel Verilerin Korunma İhtiyacı
- II. Kişisel ve Kritik Kurumsal Veriler Nelerdir?
- III. Kişisel Verilerin Korunmasına İlişkin Genel Prensipler
- IV. Hasta Haklarının Korunmasına İlişkin Prensipler
- V. Türkiye İçin Ulusal Düzenleme Taslağı
- VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı

I. Kişisel Verilerin Korunma İhtiyacı Günlük Yaşantımızdan Örnekler

687 bin öğretmenin bilgileri çalındı

687 bin öğretmenin okul ve kimlik numaralarının da yer aldığı bilgilerin çalınarak internete yüklendiği ortaya çıktı. Milli Eğitim Bakanlığı, inceleme başlattı.

NTV
Güncelleme: 21:29 TSİ 13 Şubat 2009 Cuma

ANKARA - Hırsızlık olayı, İl ve ilçe Milli Eğitim Müdürlükleri Yönetim Bilgi Sistemi'nde (İLSİS) gerçekleşti. Sistemdeki öğretmen bilgilerinin paylaşım sitesi Rapidshare'e yüklendiği ortaya çıktı.



Muhtarın bilgisayarını çalındı kayıtlar yok oldu

Aydın'ın Nazilli ilçesinde, Sümer Mahallesi Muhtarlığı'nın korkuluklarını keserek giren hırsızlar, 5 bin kişinin kaydının bulunduğu bilgisayarını çaldı. Muhtar Erdoğan Dilbaz, 10 yıldır muhtarlık yaptığını, ilk kez böyle bir olayla karşılaştığını söyledi. Bilgisayarda 5 bin kişinin kaydının bulunduğunu

aktaran Dilbaz, bu kayıtlar için 10 ay emek verdiğini ifade etti. Bilgilerin yedeğinin ise bulunmadığı belirtildi.

8.5 milyon kişinin bilgileri internete düştü

KEY ödemesinden yararlanacak vatandaşların kimlik numaraları ve sosyal güvenlik numaraları internete düştü 8.5 milyon kişiyi ilgilendiren sorun yeni bir güvenlik tartışması yarattı.

ABD, güvenlik nedeniyle Bush'un idrarını bile saklarken
Erdoğan'ın kan tahlil sonuçlarını tüm dünyaya ifşa etti.

İnternethaber'in haberine göre dün [redacted] açılışını yapan Başbakan Erdoğan, gazetecilere göstereceği kartla kendi kartını karıştırınca [redacted] kurtulamadı. Gazete, tele-objektife Erdoğan'ın gazetecilere gösterdiği "sağlık kartının" üzerindeki sağlık numarasını okuyarak, internetten Erdoğan'ın tüm sağlık bilgilerine ulaştı. [redacted] bu büyük ayıbı, bugünkü gazete manşetine, "10 yıldır şeker hastasıymış" başlığıyla yansıdı ve tüm dünyaya Erdoğan'ın üreden kolesterol oranına kadar tüm biyokimya ve hematoloji tahlil sonuçlarını yayınladı.

I. Kişisel Verilerin Korunma İhtiyacı Neden Kişisel Bilgiler Tehdide Açık?

- Kişisel verinin tanımı belli mi?
- Kişisel verilerimiz kaç kurum / kuruluşta mevcuttur biz veya bir kamu otoritesi bunu biliyor muyuz?
- Kişisel verilerimize sahip çıkılıyor mu?
- Kişisel verilerimize kendimiz sahip çıkabilmek için hukuki bir dayanağımız mevcut mu?
- Kişisel verilerimize sahip çıkıldığından emin olmak için kamu yönetimi veya kurum ve kuruluşlar tarafından işletilen bir güvence mekanizması var mı?
- Kişisel verilerimize sahip kurum / kuruluşlar (ve onların personeli) tek başına önemsiz gibi görünen kişisel verileri herkesle paylaşırken birden fazla verinin bir araya getirilmesi nedeniyle bireyin ciddi zarar göreceğinin farkında mı?
- Kişisel bilgilerimizin güvenliği ile ilgili bir zarara uğradığımızda başvurabileceğimiz bir merci var mı?

**Yukarıdaki sorulara verilen olumsuz yanıtların olumlu yanıtlara oranı
tehdide açıklığın oranına işaret eder**

I. Kişisel Verilerin Korunma İhtiyacı Neden Kritik (Kurumsal) Veriler Tehdide Açık?

- Verinin (gerçekten) sahibi var mı, veri sahibi sahipliğinin ve sahip olduğu verinin farkında mı?
- Verilerin nereden geldiği, nerelerden geçtiği, nasıl işlendiği, nerede ve hangi formlarda (evrak üstünde, sabit diskte, taşınabilir medya üzerinde, vd.) bulunduğu, nasıl yok edildiği biliniyor mu?
- Verilerin değerleri biliniyor mu?
- Verilerin karşı karşıya oldukları riskler ve bunlara karşı uygulanan kontroller incelenmiş mi?
- Verilere erişim, işleme ve saklama kuralları belirlenmiş mi?
- Verilerin nasıl kullanılması ve korunması gerektiği personele, iş ortaklarına ve müşterilere anlatılmış mı?
- Veri korunmasına ilişkin ihlaller tespit ediliyor/edilebiliyor mu?

**Yukarıdaki sorulara verilen olumsuz yanıtların olumlu yanıtlara oranı
tehdide açıklığın oranına işaret eder**

I. Kişisel Verilerin Korunma İhtiyacı Kişisel Veriler ile Kritik (Kurumsal) Veriler Arasındaki İlişki

- Gelişmiş ülkelerde toplumsal yaşamın bilgi sistemleri kullanımına erken geçmiş olması nedeniyle son 10 ila 25 yıl arasında değişen süreler için kişisel verilere yönelik tehditler anlaşılmış ve bu konuda ulusal ve sektörel düzenlemeler yapılmıştır.
- Ciddi yaptırımları içeren mahremiyet (privacy) düzenlemeleri nedeniyle kişisel bilgiler aynı zamanda kritik (kurumsal) veriler arasında en hassas seviyede yer almaktadır.
- Kritik kurumsal verilerinin güvenliğine ilişkin bir program yürütmeyen bir kurumun kişisel bilgilerin güvenliği açısından gerekli faaliyetleri gerçekleştirmesini beklemek çok da gerçekçi değildir.

II. Kişisel Veriler ve Kritik Kurumsal Veriler Nelerdir?

- Kişisel verilerin neler olduğunun genel tanımı “Kişisel Verilerin Korunması Kanun Taslağı”nda şu şekilde yapılmıştır:

– **Kişisel Veri: Belirli veya kimliği belirlenebilir bir kişiye ilişkin bütün bilgilerdir.**

- 1995 yılında yayınlanmış olan Directive 95/46/EC numaralı Avrupa Birliği direktifi kişisel verinin (personal data) tanımını şu şekilde yapmaktadır:

– **Kişisel Veri: Kim olduğu belli veya belirlenebilen bir gerçek kişiye ait tüm bilgilerdir. Belirlenebilen bir kişi doğrudan veya dolaylı olarak bir kimlik numarası referansından veya kişiye ait fiziksel, psikolojik, ekonomik, kültürel veya sosyal bilgilerden yola çıkarak tesbit edilebilen bir kişidir.**

II. Kişisel Veriler ve Kritik Kurumsal Veriler Nelerdir?

- **Kişisel Veriler:** Genel yaşam ve sektörel mahremiyet ihtiyaçlarından yola çıkılarak aşağıdaki veriler kişisel veri olarak değerlendirilebilecek verilere örnektir:
 - Yaşam şekline ilişkin kişisel veriler: Ayrımcılığa uğramamak ve haysiyetin korunmasıyla ilişkili olarak dinsel inanç, cinsel tercih, etnik köken, suç geçmişi, politik eğilimler ve kişisel özel aktivitelere ilişkin bilgiler hassas bilgilerdir.
 - Finansal kişisel veriler: Suçlular tarafından suistimale ve kimlik hırsızlığına hedef olmamak için kişinin mali varlığı, sahip olduğu hisse ve hesaplar, borçları yaptığı alışverişler, kredi kartları'na ilişkin veriler kritiktir. Ayrıca bu bilgiler kişinin nerede ve kimlerle bulunduğu, sağlık bilgilerine ilişkin bilgiler de ortaya çıkarabileceğinden ve varlık bilgisinin toplumsal açıdan da özel sayılmasından dolayı hassastır.
 - İnternet kullanımına ilişkin kişisel veriler: e-posta'lar, internet siteleri ile paylaşılan kişisel veriler mahrem olarak değerlendirilebilir. Ayrıca internet kullanımından kaynaklanan saldırı yüzeyi sosyal paylaşım siteleri, dosya saklama hizmeti, internet erişimine ilişkin iz kayıtlarının hizmet sağlayıcı ve sunucu sahipleri tarafından tutulabiliyor olması nedenleriyle artmaktadır.
 - Sağlıkla ilgili kişisel veriler: Sağlık verileri kişilerin iş güvenliğini, toplum içindeki statüsünü ve sigorta kapsamını etkileyebileceğinden hassas verilerdir. Ayrıca sağlık verileri kişilerin sosyal yaşantısı ve psikolojik durumları hakkında bilgi edinilmesine neden olabilir. Biyometrik veriler de kişisel veriler arasındadır.
 - Politik kişisel veriler: Toplum barışı ve seçme özgürlüğü açılarından politik veriler mahrem verilerdir.

II. Kişisel Veriler ve Kritik Kurumsal Veriler Nelerdir?

- **Kritik Kurumsal Veriler:** Söz konusu kurumun faaliyet alanı ve faaliyet gösterdiği ortama göre kurumsal verilerin kritiklik derecesi değişebilmekle birlikte aşağıdaki verilerin kurumlar açısından genel olarak kritik olduklarını söyleyebiliriz:
 - Stratejik Planlar: Rekabet açısından kritik olabilecek stratejik yatırım, ürün, ya da faaliyet değişimi planları hassas olabilir.
 - Mali Bilgiler: Özellikle halka açık şirketlerde pay sahipleri ve kamunun eşit bilgi alma hakkı dolayısıyla mali bilgilerin kontrollü biçimde oluşturulması ve yayınlanması gerekmektedir. Özel kurumlarda bu bilgiler rekabet açısından kritik olabilir.
 - Personel Bilgisi: Hem kişisel verilerin korunmasına ilişkin düzenlemeler hem de rekabet veya kurumu hedef alabilecek sosyal mühendislik saldırılarına karşı personel bilgileri ve iletişim bilgileri hassastır. Ayrıca maaş bilgileri de kurum içi huzurun ve kişisel mahremiyetin sağlanması için kritiktir.
 - Müşteri Bilgileri: Özellikle denetim, sağlık, telekomünikasyon, finans hizmeti veren kurumlar için müşteri bilgileri hem kişisel bilgilerin korunmasına ilişkin kanunlar hem de sektörel düzenlemeler nedeniyle son derece hassastır. Bu bilgilerin korunmasında gösterilecek yetersizlik ayrıca kuruma ticari olarak da olumsuz etki yapacaktır.
 - Kritik Sistem, Prosedür ve Erişim Bilgileri: Kurumu hedef alan taraflara yardımcı olabilecek kritik altyapı ve prosedür bilgileri hassastır.

III. Kişisel Verilerin Korunmasına İlişkin Genel Prensipler

- Düzenlemeler dolayısıyla uluslararası iş yapış şekillerindeki uyumsuzlukları da azatmayı da hedefleyen çerçevenin (US-EU Safe Harbor) bir parçası olan temel mahremiyet prensipleri şunlardır:
 - Bilgilendirme: Kişiler verilerinin toplandığı ve hangi amaçla kullanılacağı hakkında bilgilendirilmelidir.
 - Seçim Hakkı: Kişiler verilerinin toplanıp toplanmaması ve üçüncü taraflara iletilip iletilmemesi konularında seçim hakkına sahip olmalıdır.
 - Üçüncü Taraflara Transfer: Üçüncü taraflara veri transferi ancak iletilen tarafın da uygun veri koruma prensiplerini uygulaması durumunda söz konusu olabilir.
 - Güvenlik: Toplanan veriye yönelik güvenlik tehditlerine karşı mümkün olan gerekli güvenlik önlemleri alınmalı ve işletilmelidir.
 - Veri Bütünlüğü: Veriler toplanma amacıyla ilgili ve doğrulukları sürdürülerek tutulmalıdır.
 - Erişim Hakkı: Kişiler kendileriyle ilgili bilgilere erişme, eğer doğru değilse bu bilgileri düzeltme ve silme hakkına sahip olmalıdır.
 - İcra Gücü: Yukarıdaki prensiplere ilişkin kuralları uygulamaya yönelik yeterli icra gücü bulunmalıdır.
- Bize ait kanun taslağında “**Güvenlik**” prensibi dışında yukarıdaki prensiplere ilişkin uygulama kurallarının tanımlandığı görülmektedir.

IV. Hasta Haklarının Korunmasına İlişkin Prensipler

- Kişisel veriler açısından önemli olan sektörlerden sağlık sektöründe uygulanan prensipler de genel prensiplerle paraleldir. Bu alanda geliştirilmiş pek çok rehber ve düzenleme mevcuttur. Bunlardan "European Guidance for Healthcare Professionals on Confidentiality and Privacy in Healthcare" rehberinde değinilen başlıklardan bazıları şunlardır:
 - Madde 10. Hastanın bilgilendirilmesi: Bu madde içinde belirtilen hasta bilgilendirme ihtiyaçlarından birisi de hasta bilgilerinin ifşa edilmemesi için uygulanan kontrollerin hastaya anlatılmasıdır.
 - Madde 17. İkincil kullanım için hasta onayının alınması: Hasta bilgisinin tedavi dışında ikincil amaçlar için kullanılabilmesi için hasta veya hukuki temsilcisinden onay alınmalıdır.
 - Madde 18. Hasta kimliğinin gizlenmesi ve Madde 19. Anonimleştirme: Hasta bilgisi sadece kullanım amacı hasta kimliğiyle eşleştirme gerektirdiği durumlarda kimlik bilgisini içermelidir. Bunun dışındaki durumlarda hasta kimlik bilgisinin korunması için gerekli önlemler alınmalıdır.
 - Madde 21. Bilgi açıklamasını gerektiren durumlar: Sağlık sektörü çalışanları bilginin açıklanması gerekleri (ki bu gerekler hasta'nın sağlığının iyileştirilmesi ile de ilgili olabilir) ile hasta hakları arasındaki dengeyi değerlendirebilmek için ulusal düzenleme ve hukuki gerekler hakkında bilgi sahibi olmalıdır.
 - Madde 25. Güvenlik: Sağlık personeli gerekli politika ve protokolleri uygulayarak hasta bilgilerinin gizliliğini sağlamalıdır. Ayrıca sağlık personeli telefon, e-posta ve faks gibi kanallarla hasta bilgilerini hastalara, onların refakatçilerine ve hukuki temsilcilerine, meslektaşlarına hasta bilgisi aktarırken mahremiyet ihtiyaçlarını göz önünde bulundurarak dikkatli hareket etmelidir.

V. Türkiye İçin Ulusal Düzenleme Taslağı

- “Kişisel Verilerin Korunması Kanunu Tasarısı” Haziran 2004’te Başbakanlığa sevk edilmiştir.
- Kanun söz konusu kanunun gereklerini yerine getirmek ve gerekli yönetmelikleri düzenlemek amacıyla “Kişisel Verileri Koruma Kurumu”nun kurulmasını öngörmektedir.
- Ayrıca kişisel bilgi verisi toplayan ve saklayan kurum ve kuruluşların (kanundaki tanımıyla Veri Kütüğü Sistemi Sahipleri’nin) Kişisel Verileri Koruma Kurumu tarafından tutulan Kişisel Veri Kütüğü Sistemi Sicili’ne kaydolmasını şart koşturmaktadır.
- Aradan geçen zamanda bu konuda bir ilerleme gerçekleşmemesiyle birlikte kanun tasarısının bazı maddeleri aşağıdaki gibidir:
 - Madde 6. İlgili kişilerin bilgilendirilmesi
 - Madde 7. Başvuru ve bilgi edinme hakkı
 - Madde 12. Sicil, tarife hazırlanması: Kurum tarafından bir Kişisel Veri Kütüğü Sistemi Sicili tutulur. Kişisel verileri işleme tâbi tutan kamu kurum veya kuruluşları ile gerçek ve özel hukuk tüzelkişileri, Sicile kaydolmak zorundadır.
 - Madde 15. Kişisel verilerin üçüncü kişiler tarafından işlenmesi
 - Madde 17. Kamu kurum ve kuruluşları tarafından kişisel verilerin üçüncü kişilere aktarılması
 - Madde 18. Verilerin kişisel olmaktan çıkarılması, silinmesi, yok edilmesi

V. Türkiye İin Ulusal Dzenleme Taslađı

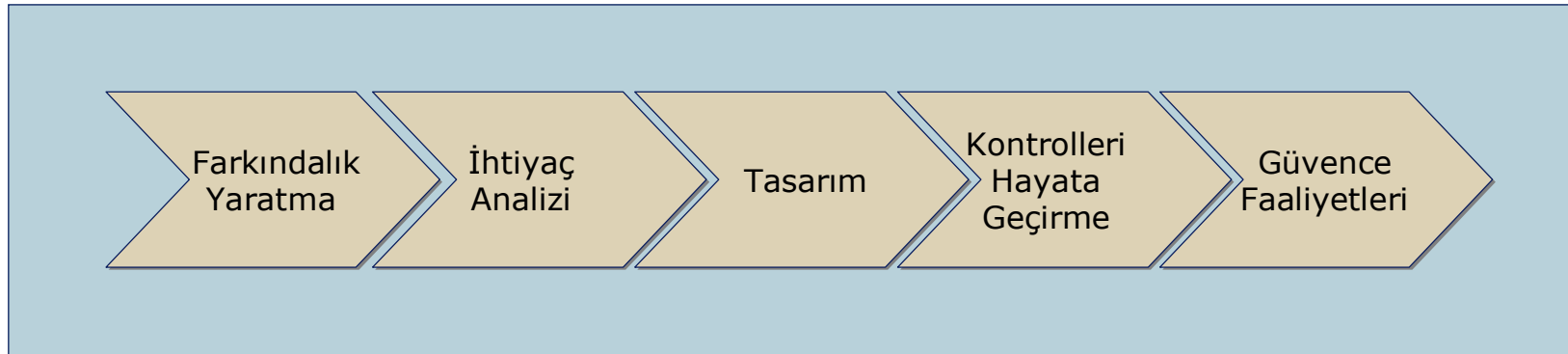
- Ayrıca kanun tasarısı arařtırma amalı sađlık verilerinin toplanması ile iliřkilendirilebilecek řu maddeye de sahiptir:

Verilerin bilimsel arařtırma, istatistik ve planlama amacıyla kullanılması

Madde 19- Kiřisel veriler, bilimsel arařtırma, istatistik ve plânlama gibi kamuya ynelik amalarla iřlenebilir. Ancak, iřleme tâbi tutulan veriler ve elde edilen sonular kiřinin tanınmasına yol amayacak řekilde nc kiřilere aktarılabilir veya yayımlanabilir.

VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı

- Düzenlemelere uyum ihtiyacı olan ve kritik verilerini korumak isteyen kurumlar bir veri koruma programı uygulamak zorundadırlar.
- Bu program “program” tanımından da anlaşılacağı üzere sürekliliği olan bir süreç olup, ihtiyaç analizlerinin, eğitim ve kontrol faaliyetlerinin, kontrol etkinliklerinin ölçümlenmesinin düzenli biçimde tekrar edilmesini gerektirmektedir.
- Veri koruma programının hayata geçirilmesi için izlenebilecek adımlar aşağıdaki gibidir:



VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı



- İlk adım olarak organizasyonun genelini ve kritik veri koruma görevi olanları kapsayan ve programın devamında desteklerini almayı sağlayacak eğitim ihtiyaçlarının tespiti ve uygulanması gerçekleştirilir. Bu amaçla aşağıdaki alt adımlar izlenir:
 - Organizasyonun mevcut veri koruma farkındalık seviyesinin tespiti
 - Kritik veri kullanan tarafların (personel veya iş ortağı) belirlenmesi
 - Üçüncü taraflardaki mevcut veri koruma farkındalık seviyesinin tespiti
 - Organizasyona en uygun farkındalık eğitim programının belirlenmesi
 - Veritabanı yöneticileri, sistem yöneticileri gibi özel alanlarda çalışan personele yönelik özel eğitim programı belirlenmesi
 - Veri akış analizine ve kurumsal ihtiyaçlara uygun olarak eğitim modüllerinin geliştirilmesi
 - Eğitim programının uygulanması

VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı



- Veri koruma program kontrollerine yönelik ihtiyaç analizi safhasında aşağıdaki adımlar izlenir:
 - Toplanan, iletilen, saklanan ve işlenen verilerin ilk elde edilme anlarından imha edildikleri noktaya kadar tespiti
 - Organizasyonun iş stratejilerinin ve veri koruma ihtiyaçları ile ilişkilerinin analizi
 - Veri sahiplerinin belirlenmesi
 - Varolan veri koruma kontrol ve prosedürlerinin belirlenmesi
 - Organizasyonun mahremiyet açısından açıklık ve risklerinin belirlenmesi
 - Veri koruma düzenlemelerine uyum seviyesinin belirlenmesi
 - Uluslararası veri transferlerinin belirlenmesi
 - Uygulanması gereken veri koruma kontrollerinin belirlenmesi

VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı



- Belirlenen kontrollerin geliştirilmesi ve kontrol yetersizliklerinin giderilmesi için aşağıdaki kontrol ve çözümler tasarlanır:
 - Veri koruma faaliyetlerini yönetecek ve uygulayacak organizasyon yapısı
 - Veri koruma stratejisi, politika ve prosedürleri
 - Veri koruma eğitim ve farkındalık programı
 - Teknik veri koruma kontrolleri (veritabanı, uygulama, ağ erişim kontrolleri, kriptolama, vd.)
 - Develop a system to handle the new policy/notice
 - Mahremiyet ihlalleri tespit ve yanıt verme süreci
 - Kişisel ve kritik verinin istenmeyen ve kasıtlı sızmasına karşı veri sızma teknolojisi isterleri

VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı



- Tasarım aşamasında planlanan kontroller hayata geçirilir:
 - Veri koruma organizasyonu oluşturulur, gerekli teknik eğitimleri ve bütçesi sağlanır
 - Veri koruma stratejisi, politika ve prosedürleri uygulamaya alınır, personel ve üçüncü taraflarla iletişimi yapılır
 - Erişim kontrolleri ve kriptolama kontrolleri veri akışının gerektirdiği noktalarda uygulanır
 - Veri sızma engelleme teknolojisi uygulanır
 - Personelin tümüne ve görevi gereği hassas veriye ulaşan personele yönelik eğitim programları uygulanır
 - Mahremiyet ihlal ve yanıt verme süreci işletilir
 - Organizasyonun faaliyetlerini etkileyen veri koruma düzenlemeleri izlenir ve gerekli uyum süreci işletilir

VI. Kişisel ve Kritik Veri Koruma Program Yaklaşımı



- Program yönetiminin etkinliği aşağıdaki açılardan izlenir ve denetlenir:
 - Kurumsal ihtiyaçlar ve düzenlemelere uyumlu ihtiyaç analizlerinin gerçekleştirildiğinin denetimi
 - Farkındalık seviyesi ve teknik veri koruma eğitimlerinin gerçekleştirildiğinin denetimi
 - Kontrollerde tespit edilen yetersizliklerin giderilmesi için yapılan planların uygulandığının denetimi
- Uygulanan veri koruma kontrollerinin etkinliği izlenir ve denetlenir.

BTRisk