Sağlık Akademisyenleri Dergisi
www.saglikakademisyenleridergisi.com

Derleme / Review Article

Sağlık kurumlarında bilgi güvenliği bağlamında biyometrik sistemler

Biometric systems in the context of information security in health institutions

Şemsettin Varol[1], Fatih Orhan[1], Selahattin Tuncer[1], Selahattin Akyüz[2]

[1]SBÜ Gülhane Sağlık Meslek Yüksek Okulu, Ankara, Türkiye.
[2]Dışkapı Yıldırım Beyazıt E.A.H. Mevki Binası, Ankara, Türkiye.

Anahtar Kelimeler:
Bilgi yönetimi, bilgi güvenliği, sağlık bilişimi, biyometrik sistemler

Key Words:
Information management, information security, health informatics, biometric systems

Yazışma Adresi/Address for correspondence:
Selahattin Tuncer,
SBÜ Gülhane Sağlık Meslek Yüksek Okulu, Ankara, Türkiye.
selahattin.tuncer@sbu.edu.tr

Gönderme Tarihi/Received Date:
December 8, 2016

Kabul Tarihi/Accepted Date:
December 18, 2016

Yayımlanma Tarihi/Published Online:
December 30, 2016

DOI:
10.5455/sad.13-1483706096

ÖZET

Bilgi, bilgi yönetimi, bilgi güvenliği ve bilgi sızıntısı gibi konular özellikle son yıllarda sağlık kurumlarında sıkça tartışılmaya başlanmıştır. Tüm bu konular temelde insan faktörü ile ilgilidir. Kurumun yıllar içerisinde kazandığı olumlu imaj atmosferi, yalnızca bir bilgi güvenliği ihmali ile anında yok olabilmektedir. Çünkü konu etik ihlalin ötesinde, temel hukuk ve sağlık hukuku kriterleri açısından çok önemli sonuçlar doğurabilir. Bu açıdan sağlık kurumlarını da kapsayan ve 2016 yılında yürürlüğe giren Kişisel Verilerin Korunması Kanunu çerçevesinde bilgi ve belge yönetimine dayanan iş ve işlemlerin belirlenmesi bir zorunluluktur. Özellikle de teknolojik gelişmeler ve yenileşim çabaları ile beraber bilgi sızıntılarının arttığı söylenebilir. Bu bağlamda bu araştırma ile bilgi güvenliği açısından sağlık bilişim sistemleri incelenmiştir. Özellikle son yıllarda ortaya çıkan inovatif biyometrik sistemler ve entegrasyonu konusu tartışılmıştır. İlgili alan yazın incelendiğinde konunun yeterince tartışılmadığı görülmüştür. Bu çalışmanın bilgi güvenliği ve sağlıkta bilişim sistemleri açısından önemli bir farkındalık oluşturabileceği değerlendirilmektedir.

ABSTRACT

Topics such as information, information management, information security and information leakage have been frequently discussed in health institutions especially in recent years. All these topics are mainly related to the human factor. The atmosphere of the positive image that the institution earns over the years can be destroyed instantaneously with only one information security omission. Because, beyond ethical violation, the matter can have very important consequences in terms of basic law and health law criteria. In this respect, it is important to determine the work and procedures based on information and document management within the framework of the Law on the Protection of Personal Data, including the health institutions, which entered into force in 2016. Especially with the technological developments and innovation efforts, it can be said that the information leakage increases. In this context, this research examines the health informatics systems in terms of information security. In particular, the topic of innovative biometric systems and integration that emerged in recent years has been discussed. When the relevant literature is examined, it has been seen that the topic has not been discussed sufficiently. It is evaluated that this study may be an important awareness in terms of information security and health information systems.

GİRİŞ

Sağlık kurumları emek yoğun olduğu kadar teknolojik gelişmeler ve yeniliklerden de en fazla etkilenen bütünleşik hizmetlerden oluşmaktadır. Bu bütünleşik hizmetler ve alt sistemlerin kurgulanması esnasında, hizmetin insana dair olmasından dolayı sıfır hata hedeflenmesi gerekir. Ayrıca oluşabilecek her bir hata etik ilkeler açısından değerlendirilebileceği gibi, tıp hukuku çerçevesinde de sonuçları itibariyle incelenmesi gerekir. Özellikle de son yıllarda sağlık kurum ve kuruluşlarının pazarlama stratejileri ve imaj oluşturma çabalarının sistematik bir şekilde ele alındığı düşünüldüğünde "sıfır hata" yaklaşımının ne denli önemli olduğu ortaya çıkmaktadır.

Sağlık kurumları geneli ve hastaneler özelinde, kalite, akreditasyon ve hasta güvenliği çabalarının da temel amacı hastalara kaliteli, etkili, etkin, verimli, kabul edilebilir ve optimum hizmeti sunma çabasıdır. Bu bağlamda Sağlıkta Akreditasyon Standartları (SAS) ve Sağlıkta Kalite Standartları (SKS) incelendiğinde, bilgi ve belge güvenliği gibi konuların rekabet avantajı yakalayabilmek için önemli bir yere sahip olduğu söylenebilir. Çünkü "hastaya ait bilgilerin sır olarak saklanması" ve "mahremiyet" etik ilkeleri gibi konular sağlık kuruluşları için en temel ve önemli alanlardandır. Bu açıdan bu araştırmada kısaca bilgi, bilgi güvenliği, bilgi sızıntısı konularına değinilerek, sağlık bilişim sistemleri ve entegrasyonu konusu ile bazı inovatif biyometrik yaklaşımlara değinilmiştir.

BİLGİ GÜVENLİĞİ İLE İLGİLİ TEMEL YAKLAŞIMLAR

Bilgi güvenliği konusu global açıdan incelendiğinde ilk akla gelen kuruluşların başında InfoWatch Analytical Center gelmektedir. Bu merkez kurum ve şirketlerde veri kaybı önleme/koruma, entelektüel sermayenin korunması ve risk yönetimi gibi konularda öncü ve yenilikçi bir teknoloji şirket grubu olarak görev yapmaktadır. InfoWatch tarafından 2014 yılının başında, 2013 Dünya Bilgi Sızıntı Raporu yayınlanmıştır. 2013 yılında, InfoWatch Analytical Center 1143 gizli belge ve bilginin kurum dışına sızma vakasını tespit etmiştir. Bu sayının 2012 yılındaki rakamlarla kıyaslandığında %22 oranında bir yükselme gösterdiği görülmüştür. 2013 yılında sızan belgeler personel şahsi bilgileri ve finansal bilgileri dâhil olmak üzere toplam 561 milyon belgeden oluşmaktadır. Küresel bir karşılaştırma yapılacak olursa 679 bilgi sızıntı vakası ile Amerika ilk sırada yer alırken (%59,41), Rusya 134 bilgi sızıntı vakası ile ikinci sırada yer almaktadır. Bunun yanında Kanada 33, Almanya 48 ve İngiltere 80. sırada yer almaktadır(InfoWatch Analytical Labs, 2014; Yıldız, 2014).

Yakın tarihlerde Amerika Birleşik Devletlerinde yaşanan ve tüm dünyaya mal olan Julian Assange önderliğindeki WikiLeaks organizasyonu ve Edward Joseph Snowden'in Amerikan Ulusal Güvenlik Dairesi'ne (NSA) ait gizli belgeleri ifşa ederek ABD tarihindeki en önemli sızıntıya imza atması gibi olaylar bilgi güvenliği konusunun ulusal değil uluslararası düzeyde önem arz eden bir konu olduğunu da bir kez daha ispatlamıştır.

Konu mikro planda incelendiğinde ise daha çok bu konunun güvenlik departmanları ve finans şirketleri esaslı olarak incelendiği görülmektedir. Ancak yapılan araştırmalar kamu kurum ve kuruluşları ile beraber kamu hastanelerinin de kişisel veri sızıntı vakalarının olduğu yerlerin başında gelmekte olduğunu ve bilgi sızıntılarının büyük çoğunluğunun %85 ile kişisel verilerden kaynaklandığını ortaya koymaktadır (Yıldız, 2014).

Bu bağlamda yapılacak tüm teknolojik altyapı ve sağlık bilişimi sistemi entegrasyonu çok önemlidir. Son yıllarda tüm sektörlerde olduğu gibi sağlık kurumlarında da bilgi güvenliği konusu, değerlerin ve deneyimlerin, amaca yönelik enformasyonun ve uzmanlık görüşünün, yeni deneyimlerin ve enformasyonun bir araya getirilip değerlendirilmesi için bir çerçeve oluşturan esnek bir bileşimidir. İşletmelerde genellikle rutin çalışmalarda, süreçlerde, uygulamalarda ve normlarda kendini gösterir (Davenport ve Prusak, 2001: 27). Bu açıdan bilgiyi sistematik bir şekilde yönetebilmek tüm kuruluşları başarıya götürebilecek en temel ve kestirme yol olarak karşımıza çıkmaktadır. Zaten bilgi yönetiminin nihai amacı, entelektüel sermayeden yararlanmak, spesifik olarak bilgi transferini teşvik etmek ve bilgi paylaşımını sağlamaktır (Duffy, 2001: 59).

Alavi'ye göre (1997) bilgi yönetimi süreci, bilginin yaratılmasından bilginin kullanılmasına kadar birbirini takip eden bilginin yaratılması/elde edilmesi, bilginin saklanması/organize edilmesi, bilginin yayılması/dağıtılması ve bilginin kullanılması/uygulanması gibi aşamalardan oluşmaktadır. Bilgiyi yönetirken karşımıza çıkabilecek en önemli sorun alanı ise bu bilginin güvenliğinin sağlanamamasıdır. Bu durumda kurumu finansal ve hukuki açıdan zora sokabilecek birçok durumla karşılaşılabilmektedir.

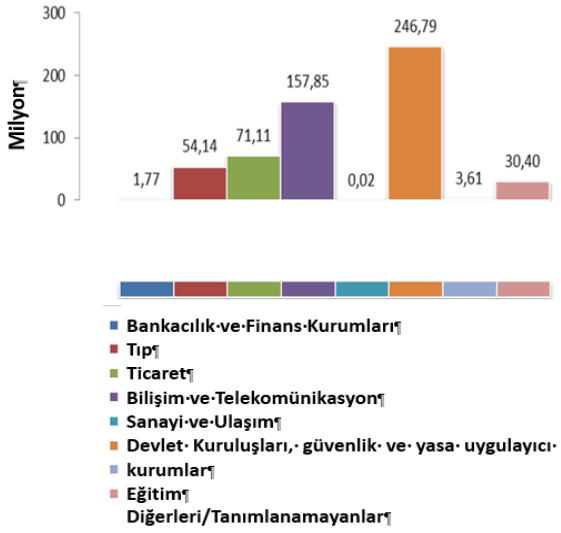
Canbek ve Sağıroğlu'na göre (2006) ise bilgi güvenliği, bilginin oluşabilecek ihmallerden korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemek olarak tanımlanır. Özellikle sağlık kurumları gibi teknoloji yoğun ve bilgisayar teknolojilerinde güvenliğin amacı ise, kişi ve kurumların bu teknolojilerini kullanırken karşılaşabilecekleri tehdit ve tehlikelerin analizlerinin yapılarak gerekli önlemlerin önceden alınması ve hastaya ait bilgilerin korunması şeklindedir.

Isaca'ya göre (2009) ise bilgi güvenliği, yetkisiz erişimlerden bilgiyi koruyarak gizliliğini sağlamak, bilginin bozulmadan bütünlük ve doğruluğunu sağlamak ve istenildiği zaman erişilebilirliğini garanti etmektir. Bilgi güvenliği denilince gizlilik, bütünlük ve erişilebilirlik kavramları ön plana çıkmaktadır. Bilginin gizliliği kavramı ile kastedilen, bilgiye sadece o bilgiye erişmesi gereken kişi ya da kişilerin erişimine izin verilmesidir. Bilginin bütünlüğü kavramı ile kastedilen, bilginin tahrif edilmeden, orijinal yapısı bozulmadan olduğu gibi korunmasının sağlanmasıdır. Bilginin erişilebilirliği kavramı ile kastedilen ise, bilgiye istenilen ve makul olan bir zamanda erişilmesi ve bilginin kullanılmasıdır (Baykara ve diğ, 2013). Özellikle son yıllarda tıbbi hatalı uygulama (malpraktis) vakaları ve hastaya ait bilgilerin ifşa edilmesi gibi sebeplerle hastane ve sağlık personeli aleyhine açılan birçok dava bulunmaktadır. Örneğin gazete sayfaları karıştırıldığında, hasta bilgilerin karıştırılması sonucu yaşanan birçok olumsuz olay, çocuk kaçırılma hadiseleri (pembe kod), kimliklendirme hataları, yanlış ilaç uygulamaları ve yanlış taraf cerrahisi gibi hasta güvenliği ihlalleri görülebilmektedir.

Günümüzde bilişimde yaşanan müthiş gelişim hızı ile beraber kişiler ve kurumlar; yazılımlar ve bilgisayarların kullanılmasıyla yapılan sahtekârlıklar, bilgi hırsızlığı,

bilgisayar korsanları, elektronik saldırılar, bilgi sızdırma ve ilgili kuruluşların kendi çalışanlarınca oluşturulabilecek potansiyel iç saldırılar (Rost ve Glass, 2011), sağlık kurum ve kuruluşları açısından da büyük bir tehlike ve tehdit unsuru olabilmektedir.

Sektör bazında kişisel verilerin sızdığı sektörler ve sızan belge miktarı Grafik 1'de gösterilmiştir. 246,79 milyon belge ile devlet kuruluşları, savunma ve yasa uygulayıcı kurumların ilk sırada olduğu gözükmektedir. Bilişim ve telekomünikasyon sektörü 157,85 milyon belge ile ikinci sırada yer alırken, tıp sektörü ise 54,14 milyon belge ile dördüncü sırada yer almaktadır(Yıldız, 2014). Bu durum bize sağlık sektörü açısından önemli bazı önlemlerin alınması gerektiği ve bu konunun iyileştirilmeye açık bir alan olduğu gerçeğini bize göstermektedir.



Grafik 1. Sektör Bazında Kişisel Verilerin Sızdığı Sektörler ve Sızan Belge Miktarı

Kaynak: Yıldız, 2014 (InfoWatch Analytical Center, Global Data Leakage Report 2013, https://infowatch.com/analytics/reports/3641

SAĞLIK BİLGİ SİSTEMİ

Son yıllarda ülkemizdeki hastane işletmeciliğindeki gelişmelere paralel olarak, çağdaş işletmeciliğin bilgisayar yardımı olmadan yapılamayacağı hemen herkes tarafından kabul edilmektedir. Bilgisayarların etkin bir şekilde kullanıldığı gelişmiş ülkelerde de diğer sektörlere göre daha yavaş gelişen sağlık sektöründe bilgisayar kullanımı, ülkemizde de aynı çizgiyi göstermektedir. Hastanelerde bilgi işlem, öncelikle "teşhis ve tedavi" de yardımcı olacak bir çalışma alanı olarak düşünülmekte ve bu öncelikle olaya bakılarak alınan kararlarla içinden çıkılamaz yanlışlara varılmaktadır. Elbette ki bilgisayar, bir hastanede teşhis ve tedavi için çok önemli ve hâlihazırda hemen hemen tüm tıbbi aletlerde kullanılan bir araçtır ama konuya tüm hastanenin bilgi işlem otomasyonu olarak bakıldığında önceliğin bir işletmenin kurulu alt sistemlerinin iyi yürütülmesinde yardımcı olmak olduğu ve buna bağlı olarak, iyi kurulmuş bir işletme zinciriyle birlikte, tıbbi kararlara destek verecek halkalar olabileceği görülmektedir.

Bilgi işlem, en basit anlatımı ile bilginin optimum koşullarda saklanması ve işlenmesidir. Bu depolama ve işleme, işletmenin türü ve yapısına göre kurulmuş donanım (üzerinde çalışılacak bilgisayar parkı -hardware-) ve onun üzerinde çalışacak yazılım (kullanılacak uygulama programları- software-) olarak çok farklılıklar gösterebilecektir. Özellikle hastane gibi işletmelerde tüm tıbbi cihazların artık bilgisayar desteği ile çalıştığını düşünürsek, bilgi işlem, işletmeyi yönlendiren bilgisayarla tıbbi aletlerin entegre (otomatik bilgi alış verişi) edilebileceği bir otomasyona dönüşecektir. Hastanelerde kullanılan yazılım paketlerinde baz alınan program grubu Hastane Bilgi Sistemi adı altında yürütülerek, hastanın tıbbi ve finansal kayıtlarının ana hatları ile tutulması işlemidir. Bu ana sisteme bağlı olarak (entegre çalışan) diğer departmanın işletimine özgü çalışma kurallarını içeren diğer programlar dizisi bu çalışmaları bir bütün haline getirir (Binbaşıoğlu, 1988).

Bir hastane, birbirinin müşterisi olan çok sayıda fonksiyonel alt sistemlerden oluşan ve üst düzeyde profesyonel standartlar gerektiren, karmaşık bir hizmet kuruluşudur. Bu nedenle hastane fonksiyonel alt sistemleri hem iç hem de dış müşterilere hizmet verme durumundadır. Modern bir hastane, her biri son derece profesyonel süreçler ile yüksek kalitede hizmet üreten 30 ile 100 arasında alt sistem (object) den oluşmaktadır. Hastane otomasyonu projesi minimum 30 alt sistemi entegre olarak birbirine bağlayacak ve kaliteli hizmet vermelerine olanak sağlayacak, bilgisayar ve haberleşme teknolojilerinin etkin bir şekilde sentezinden oluşan bir yüksek teknoloji uygulamasıdır (Güleş ve Özata, 2005).

Hastane bilgi sistemi, bir hastanedeki tüm tıbbi ve idari işlemlerin bilgisayar ortamında yapılması, her türlü verinin birbirine entegre (bütünleşik) olarak çalışan çeşitli modüller yardımıyla, farklı kullanıcılar vasıtasıyla ana bir veri tabanına girilmesi ve gerekli olan tüm çıktıların/verilerin bu veri tabanından tekrar anlamlı bir şekilde geri alınmasını sağlayan, hastanelere zaman, işgücü kazancı, maddi kazanç ve en önemlisi düzgün ve güvenilir istatistiki veri/bilgi sağlayan bir yazılımlar bütünü olarak tanımlanabilir (Suntay, 2010).

HASTANE BİLGİ SİSTEMLERİNDE DONANIM, YAZILIM VE KULLANIM

Bütün Otomasyon Projeleri temel olarak Donanım (Hardware), Yazılım (Software) ve Kullanım (Orgware) olarak bilinen üç temel bileşenin seçimi ve uygulanması ile oluşturulan bir On-Line Transaction Platformudur (Merih, 2001). Yeni teknoloji ile birlikte özellikle wireless sistemler de sisteme entegre edilmişlerdir. Dijital hastane uygulamaları ve fijital inovasyon çalışmaları çerçevesinde aşağıda çok temel bileşenleri verilen donanımsal ve yazılımsal birçok bileşenin değişmesine yol açmaktadır. DaVinci robotları, sanal gerçeklik ve artırılmış gerçeklik uygulamaları da bilişim sistemine adapte edilmesi gereken geleceğin konularıdır. Ama çok temel olarak bu üç alt bileşen aşağıdaki bölümlerden oluşmaktadır:

I - Donanım (Hardware)

- Kablolama
- Server(ler)
- Terminaller
- Yazıcılar

II- Yazılım (Software)

- İşletim sistemi (Unix,Netware,Windows NT.)
- Veritabanı (Oracle,Clipper vs.)
- Uygulama Modülleri
- Network yönetim sistemi

III-Kullanım (Orgware)

- İşleyişler (Prosedürler)
- Veri
- Raporlama
- Faturalama
- Defter tutma

Bir otomasyon projesinin başarıya ulaşabilmesi için bu temel bileşenler stratejik bir perspektif içinde birbirleri ile uyumlu olarak seçilmeli ve hastanelerde hızla artan işlem (transaction) yoğunluğunu uzun bir dönemde kaldıracak esneklikte ve 7 gün 24 saat çalışacak bir güvenirlilik düzeyinde bakım yapılabilmelidir.

Bir Otomasyon projesinin Donanım (Hardware), Yazılım (Software) ve Kullanım (Orgware) bileşenlerinde aşağıdaki kurallara özellikle uyum gösterilmelidir (Merih, 2000).

1- Hastaneler çok sayıda otonom çalışan profesyonel alt sistemlerden oluşmaktadır. Otomasyon açısından bakıldığında bütün hastaneler Klinik, Poliklinik, Acil Hizmetler ve İdari/Mali İşlemler olmak üzere dört temel alt sistemin bileşimidir.

2- Bu alt sistemlerin enformatik özellikleri birbirinden farklıdır ve özgün olarak tasarlanmalıdır.

3- Hastane otomasyonu kesinlikle birbirinden ayrı ve bağımsız olarak tasarımlanan, gerektiğinde entegre edilebilen dört ayrı klinik (yatan hasta), poliklinik (ayaktan hasta), acil hizmetler ve idari ve mali işlemler otomasyon projesi olarak tasarlanmalı ve her biri için bağımsız serverlere bağlı bir network kullanılmalıdır.

4- Hastane otomasyonunu oluşturan dört ayrı otomasyon projesi, kendilerine özgü veri bankaları kullanmalı ve bunlar sisteme entegre yedek serverler ile yedeklenmelidir. Yedek serverler sistemde On-Line olarak bulunmalı ve arıza durumlarında On-Line olarak devreye girebilmelidir.

5- Hastane otomasyonu projelerinin stratejik önceliğini "Network Kablolaması" teknolojisi uygulaması taşımaktadır. Bu uygulama, otomasyon projesinde maliyetin %10'u, başarının ise %80-90 ağırlığını taşır.

6- Bir otomasyon sisteminin kalbini serverler (ana bilgisayarlar) oluşturur. Dağıtılmış Bilgi İşlem tasarımı kullanıldığında bunların çok güçlü, çok hızlı ve çok pahalı olmaları gerekmez. Disklerin yüksek kaliteli ve hızlı seçilmesi öncelik taşır.

7- Sistemi çalıştıracak olan İşletim Sistemi (Operating System) stratejik bir önem taşımaktadır. Bu nedenle seçilen işletim sisteminin otomasyon projelerinde uzun yıllar denenmiş ve güvenilirliğini kanıtlamış teknolojiler olması stratejik bir önem taşımaktadır.

8- Hastane otomasyonu "Bilgi İşlem" ağırlıklı bir uygulamadır ve stratejik öncelik "Sistem Güvenilirliği" (Reliability) üzerinedir. Bu nedenle henüz güvenilirliğini kanıtlamamış olan uygulamalardan ve teknolojilerinden uzak durulmalıdır.

9- Otomasyon sistemlerinde önemli bir stratejik tercih verileri üreten, kaydeden, depolayan ve raporlayan "Databankası Yönetim Sistemi" (Database Management System) nin seçimidir. Hastane otomasyonunda databankaların On-Line olarak yedeklenmesi ve yedeklerin On-Line olarak devreye girmesi stratejik bir önem taşır. Bu nedenle databankalarının yedeklenmesi de On-Line olarak çalışan yedek serverler tarafından yapılmalıdır.

10- Hastane otomasyonu modüllerinin bir takım hevesli amatörler tarafından değil, network sistemleri üzerinde kilitlenmeyen modüller yazmakta beceri ve deneyim kazanmış programcı ustalar tarafından geliştirilmesi gerekmektedir.

11- Hastane otomasyonu sisteminin arkasında, gerekli bakımı verebilecek, deneyimli ve profesyonel bir uzman kadronun olması gerekmektedir.

12- Bir hastane otomasyonu projesinde en stratejik bileşen Kullanım (Orgware) olarak görülmektedir. Bu hastaneye özel prosedürleri etkin ve kapsamlı bir şekilde bilgi sistemlerine aktarmak, düzenli çalışmasını sağlamak, sistemin hastane çalışmalarını aksatmaması için bakımını sağlamak, otomasyonda maksimum yararı sağlayacak kullanıcıları temin etmek ve eğitmek önemlidir (Bars, 2002).

4. Hastane Bilgi Sistemi Yazılım Seçiminde Dikkat Edilmesi Gerekenler

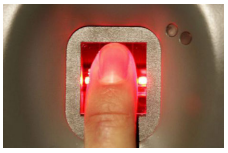
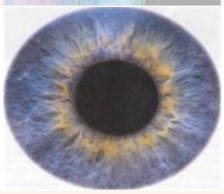
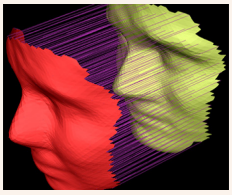
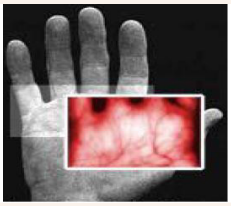
Hastane bilgi sisteminde yazılım alınırken bazı temel hususlara dikkat etmek gerekmektedir ki bu hususlar zaman, teknolojik gelişim, yasal mevzuat ve fayda-maliyet açısından değişebilmektedir (Güçbilmez, 2000; Dikmetaş, 2000; T C. Sağlık Bakanlığı, 1997; Merih, 2000):

- Hastane bilgi sistemini üreten firmalarla görüşülmelidir,
- Firmaların teknolojik altyapısı, uzmanlığı, bilgi birikimi, problem çözme becerisi, desteği dikkate alınmalıdır,
- Ürünün gelişime açık olması, değişken tüm bilgilerin yetkili kullanıcılar tarafından güncellenebiliyor olması, internet üstünden veri alışverişi yapılabiliyor olması, dinamik raporlama, sorgulama ve istatistik becerisi göz önünde bulundurulmalıdır,
- Demo sırasında yazılımın belirlenen ihtiyaçları karşılama ölçüsüne bakılmalı, bu konuda firmanın çözüm önerileri değerlendirilmelidir,
- Firmalar ile görüşülürken eğitim, destek hizmetleri, yerinde uygulama hakkındaki yaklaşımları sorulmalıdır,
- Yazılımı kullanan siteler ziyaret edilmeli, kullanıcılarla görüşülmelidir,
- Donanım, bilgi sistemleri seçildikten sonra alınmalıdır,
- Ağ altyapısı firma kontrolünde kurulmalıdır,
- Hastane otomasyon sisteminin arkasında, gereken bakımı verebilecek, profesyonel ve uzman kadro bulunmalıdır,
- Hastane alt sistemleri (klinik, poliklinik, acil hizmetler, idari / mali işlemler), enformatik özelliklerinin farklı olmasından dolayı özgün olarak tasarlanmalıdır ve her bir alt sistem için bağımsız anabilgisayarlara bağlı ağ kullanılmalıdır,
- Hastane otomasyonu sistem güvenirliliği dikkate alınmalıdır,
- Hastane bilgi sistemi yazılımında veri girişleri uygun kodlarla yapılmalıdır,
- Geçerli hastalık, malzeme vb. kodlama sistemlerini içermelidir,
- Sistem genelinde, kullanıcı, işlem ve bilgi düzeylerinde bilgilerin gizliliğini ve güvenliğini sağlamalıdır,
- Yeni modüllerin sistemle bütünleştirilmesine olanak sağlamalıdır,
- Uyarlanabilir olmalıdır. Hastanede açılabilecek yeni bir birim, sunulabilecek yeni bir hizmet kullanıcılar tarafından yetkileri çerçevesinde kolaylıkla sisteme dâhil olabilmelidir.
- Tüm sıralamalar ve karşılaştırmalar ulusal dile uygun olmalıdır,
- Yazılımın donanım ve işletim sisteminden bağımsız olması, değişik platformlarda çalışabilmesi tercih edilmelidir,
- Yazılımın etkin kullanımını sağlamak için kullanıcı kılavuzları ve eğitim el kitapları bulunmalıdır
- Tıbbi uygulamalara adapte edilmiş olmalıdır,
- Tüm birimler arasında daha kolay haberleşme sağlamalıdır.

GÜVENLİK DUVARI VE BİYOMETRİK SİSTEMLER

Sağlık kuruluşları açısından yukarıda anlatılan temel bilgi güvenliği uygulamaları açısından en önemli konulardan birisi de proaktif ve reaktif risk yönetimi uygulamalarının kurumsal açıdan kullanılmasıdır. Hata türü ve etkileri analizi (FMEA) Olay Ağacı Analizi, Hata Ağacı Analizi ve Papyon (BowTie) Modeli gibi uygulamalarla bilgi güvenliği ihlalleri oluşturulabilecek güvenlik bariyerleriyle engellenebilir ya da minimize edilebilir (Aksay ve Orhan, 2013). Kurumsal güvenlik ve hacker saldırılarından korunmak için de bazı teknolojik bariyerler zorunlu hale gelmiştir. Örneğin güvenlik duvarı dışarıdan gelebilecek tehditlere karşı koruma sağlayarak yetkisiz kişilerin bilgisayarlara erişmesini engellemektedir. Güvenlik duvarı, kurulduğu konumda gelen ve giden ağ trafiğini kontrol bilgisayar ya da bilgisayar ağlarına yetkisiz veya istenmeyen kişilerin çeşitli yollardan erişim sağlamasını engellemeye yarayan yazılım veya donanımdır. Güvenlik duvarları ev ve küçük ofislerde

Çizelge 1. Sağlık Bilgi Sistemleri Güvenliği

S.No	Güvenlik Uygulaması	Resim	Açıklama
1	Güvenlik Duvarı (Firewall)		Güvenlik duvarı dışarıdan gelebilecek tehditlere karşı koruma sağlayarak yetkisiz kişilerin bilgisayarınıza erişmesini engeller. Firewall internet ağından yerel ağı korumanın çeşitli yollarından birisidir.
2	Biyometrik Sistemler		Biyometrik insan tanımlamadır. Uygulamalarda alınan sonuçlar güvenilirliğin %100'e yakın olduğunu göstermektedir.
3	Parmak İzi ile Kimlik Tespiti		Parmak izi tanıma sistemleri günümüzde en yaygın kullanılan biyometrik tanıma sistemidir. Parmak izi taranırken iki tipte tarayıcı kullanılır. İlki normal optik tarayıcılardır. Bu tarayıcılar parmakta bulunan çukurlar ve çıkıntıları görüntüler. Diğer tip tarayıcılar ise yalnızca parmaktaki izleri taramakla kalmaz aynı zamanda parmaktaki statik etkileri ölçerek taranan parmağın canlı bir parmak olup olmadığını tarar.
4	Göz Retinası ile Kimlik Tespiti		Tarayıcı cihaz tarama sırasında yaklaşık altı tur döner ve her turda yaklaşık 700 kadar noktayı kaydeder. Daha sonra bu bilgiler dijitalleştirilerek kaydedilir. Retina oldukça güvenilir bir biyometri olmasına karşın tarama sırasında gözün tarayıcıya fiziksel teması, gözde oluşabilecek ve retina yapısına zarar verebilecek travmaların olması, tarama işleminin oldukça zahmetli olması gibi olumsuz yönleri de bulunmaktadır.
5	İris Tarama ile Kimlik Tespiti		İris tarama biyometrik taramalar içerisinde en basit olanlarından biridir. Sıradan bir CCD kamera kullanılarak yaklaşık 15–20 cm uzaklıktan tarama yapılır. Kullanıcı ile tarayıcı arasında fiziksel temas olmasına gerek yoktur. Gözlükle bile kullanılabilmesi, sistemlere kolay entegre olabilmesi ve iris deseninin en güvenilir desenlerden biri olması iris tarama sistemlerini daha çok tercih edilir hâle getirmiştir.
6	Yüz Taraması ile Kimlik Tespiti		Yüz tanıma sistemleri yüzde bulunan yaklaşık 50 kadar noktayı analiz eder. Yüz karakteristiği tanımlanırken göz çukurlarının saptanması, elmacık kemiğini çevreleyen bölgelerin taranması, ağız kenarlarının belirlenmesi, kulak memesinin analizi gibi çeşitli metotlar kullanılır. Birçok yüz tanıma sisteminde saç stili, saçın uzunluğu veya kısalığı gibi belirleyicilere dikkat edilmez. Diğer biyometrik sistemler de olduğu gibi yüz tanıma sisteminde de işlem 4 aşamada gerçekleşir. Bunlar, örnek imaj oluşturma, karakteristiklerin saptanması, dijital ortama aktarım ve karşılaştırmadır.
7	El Geometrisi ile Kimlik Tespiti		El geometrisi aynı zamanda el taraması (damar tanıma) olarak da bilinir. Bu sistemde el üç boyutlu olarak taranarak elin ve parmakların fiziksel karakteristikleri analiz edilir. Tarama sırasında parmakların uzunluğu, birleşme noktaları arasındaki uzaklıklar, parmaklardaki oynak yerlerinin geometrisi gibi noktalara dikkat edilir.
8	Ses Taraması ile Kimlik Tespiti		Ses tanıma biyometrik sistemlerde oldukça sık kullanılan bir tanıma şeklidir. Diğer biyometrik sistemlere göre daha kolay uygulanır. Sistem kişilerin seslerine ait akustik seslerin kaydedilip dijital ortama dönüştürür. Kullanıcı önce sistemin önceden belirlediği birkaç sözcükten oluşan metni okuyarak sesini sisteme tanıtır. Kaydedilen ses spektral analizler kullanılarak dijitalleştirilir. Kullanıcı daha sonra aynı metni kullanarak sisteme girer. Ses tanıma sistemleri telefon üzerinden bir sisteme ulaşım için daha uygun bir yapıdadır.

Kaynak: http://www.guvenlikdanismanlik.com/biyometrik-tanima-sistemleri.htm
http://www.firewallmerkezi.com/fortigate-fortinetfirewallnedir.php
http://bilgimikoruyorum.org.tr/?b414_guvenlik-duvari-nasil-yapilandirilir

internet güvenliğini sağlamak amacı ile kullanılırken, kurumsal olarak da bilgisayar ağına erişim kontrolü amacı ile kullanılmaktadır(http://bilgimikoruyorum.org.tr/).

Firewall internet ağından yerel ağı korumanın çeşitli yollarından birisidir. Genel olarak iki türlü firewall yapısından bahsedebiliriz; veri trafiğini engelleyen türler ve veri trafiğine izin veren türler. Bazı firewall tiplerinde veri akışının engellenmesi esas iken bazılarında da veri trafiğini düzenlemek ve sınırlamak önem kazanır. Genellikle firewalllar dışarıdan ağa yetkisiz erişimleri engellemek için düzenlenir. Ağdan dışarıya erişim serbest iken dışarıdan ağa erişim kısıtlanır.

Firewallun esas amacı ağa zarar vermek ya da sızmak isteyenleri engellemektir. Genel olarak şirketler ve veri merkezleri için firewall sıkça kullanılan bir güvenlik metodudur. Firewalllar güvenlik ve denetim için bir tür geçit noktası oluşturur (http://www.firewallmerkezi.com).

Günümüzde güvenliğin her geçen gün daha ön plan çıkması, kişinin çok daha fazla şifreyi aklında tutmak zorunda kalması ve daha fazla kartın yanında bulundurulması gerekliliğini ortaya çıkarmıştır. Bu yaklaşımların giderek pratiklikten ve güvenilirlikten uzaklaşması biyometrik sistemlere ait tekniklere olan ilgiyi de artırmıştır.

Biyometrik kısaca insan tanımlamadır. Kişinin sadece kendisinin sahip olduğu, kendisi olduğunu kanıtlamaya yarayan, değiştiremediği ve diğerlerinden ayırt edici olan fizyolojik özelliklerin tanınması prensipleri ile çalışır. Parmak izi, el, yüz, iris, retina, ses tanıma gibi biyometrik teknikler üzerine çok kapsamlı çalışmalar yapılmış, çeşitli sistemler geliştirilmiş ve bu sistemler denenerek bazı sonuçlar elde edilmiştir.

Bu uygulamalarda alınan sonuçlar güvenilirliğin %100'e yakın olduğunu göstermektedir. Şirketlerin kaynaklarını ve değerli bilgilerini tehdit eden güvenlik açıkları ulusal güvenliği tehdit eden terörist saldırıları, giriş için kullanılan şifre ve kart gibi tanıtıcıların unutulması, kaybolması ve çalınması risklerinin olması özellikle havaalanı ve şirket binalarının girişlerinde biyometrik sistemlerin kullanımına olan talebi artırmıştır.

Biyometrik sistemler kullanıcının fizik ve davranış özelliklerini tanıyarak bilgisayar kontrollü kimlik saptamak üzere geliştirilmiş otomatik sistemler için kullanılan genel bir terimdir. Şifreler veya pin numaraları, ağ korsanları tarafından yardımcı programlar kullanılarak kırılabileceği için ya da kullanıcılar tarafından sık sık unutulabildiklerinden dolayı yerlerini akıllı kartlar ve biyometrik cihazlar gibi yeni teknolojilere bırakmaktadırlar. Mesela, ses, parmak izi, yüz, iris, kızıl ötesi yüz ve el damar termogramı, retinal tarama, el ve parmak geometrisi gibi fiziksel karakteristikler çok çeşitli sistemlerden bazıları olup, bu sistemler Çizelge 1'de kısaca açıklanmıştır.

Çizelge 1'de belirtilen güvenlik bariyerleri ve biyometrik sistemler, öncelikle kişinin doğrulanması ve tespiti şeklinde kendini göstermektedir. Ancak bu sistemler geri ödeme sistemleri ve sağlık sigortacılığı yaklaşımıyla ele alındığında, sağlık ekonomisi açısından da incelenmesi gereken bir husustur. Bu bağlamda bu sistemlerin sağlık sistemi açısından entegrasyonu konusu birçok farklı alanı ilgilendiren ve multidisipliner şekilde değerlendirilmesi gereken bir konudur. Bu açıdan teknolojik yeniliklerin hastane bilgi güvenlik sistemi açısından da takip ve kontrolü ilgililer ve yöneticiler açısından kaçınılmazdır. Ayrıca kurumsal ve kişisel bilgi güvenliği uygulamalarının kurumsal bir kültür haline getirilebildiği ve teknolojik alt yapının oluşturulabildiği hastane sistemlerinin rekabet avantajı yakalayabileceği gerçeği de göz ardı edilmemelidir.

SONUÇ VE ÖNERİLER

Sağlık kurumları açısından bilgi ve belge güvenliği konusu çok büyük bir öneme sahiptir. Devletler bazında yöneticileri koltuğundan edebilecek sonuçları olan bilgi güvenliği ve bilgi sızıntısı konusu hastaneler özelinde hastaya ait bilgilerin ifşa edilmesi, kimliklendirme hataları, ilaç güvenliği ihlalleri vs. şeklinde kendini gösterebilmektedir. Bu durum hastane için hem büyük bir imaj kaybı, hem de etik ve hukuki yaptırımları olan bir sürecin başlangıcı olmaktadır. Bu açıdan gerek kalite ve akreditasyon uygulamaları, gerekse hasta güvenliği kriterleri yönüyle sağlık bilişimi sistemlerinin entegrasyonu kurumlar için hayati öneme sahiptir. Teknolojiyi takip edebilen ve inovatif uygulamaları risk yönetimi kriterleri çerçevesinde kurum kültürü ile özdeşleştirebilen işletmeler diğerlerine göre rekabet üstünlüğü yakalayabileceklerdir. Bu açıdan güvenlik duvarı uygulamaları ve biyometrik sistemler sağlık kurumları içinde vazgeçilmez olacağı fikrini ön plana çıkarmıştır. Sosyal güvenlik sistemi anlaşmaları ile hasta muayenelerinde avuç içi okuma ve hasta doğrulama bu örneklerden sadece bir tanesidir. Konunun politik, ekonomik, demografik ve teknolojik çevre açısından başka araştırmalarla desteklenmesi önemlidir. Çünkü konu ile ilgili alan yazında yapılmış çok az sayıda araştırma mevcuttur. Bu bağlamda çalışmanın alan yazına katkı sağlayacağı ve sektörel açıdan paydaş farkındalığını artıracağı değerlendirilmektedir.

KAYNAKÇA

1. Alavi, M. (1997). "Knowledge Management and Knowledge Management Systems", December, http://www.rhsmith.umd.edu/is/malavi/icis–97KMS/sld018.htm, 12.05.2011.
2. Aksay, K. ve Orhan, F.. "Hastanelerde İnovasyon Sürecinin Risk Yönetimi Bağlamında Değerlendirilmesi: Bir Model Önerisi", Diyarbakır:Dicle Üniversitesi İİBF Dergisi, 2(3), 2013.
3. Baykara M., DAŞ R. ve KARADOĞAN İ. "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", 1st International Symposium on Digital Forensics and Security 20-21 May 2013
4. Bars, M., Hastane Bilgi Sistemleri Ve Dicle Üniversitesi Araştırma Hastanesi İle İlgili Bir Uygulama, Dicle Üniversitesi Sağlık Bilimleri Enstitüsü Biyoistatistik Anabilim Dalı, Yüksek Lisans Tezi, Diyarbakır, 2002.
5. Binbaşıoğlu, C., Eğitim Yöneticiliği, Binbaşıoğlu Yayınevi, 4. Baskı, Ankara, 1988.
6. Canbek G. ve Ş. Sağıroğlu Ş. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3):69-72. S.165-174, 2006
7. Dikmetaş, E., Hacettepe Üniversitesi Hastanelerinde Mevcut Bilgi Sisteminin Değerlendirilmesi, Geçilmesi Düşünülen Elektronik Hastane Bilgi Sisteminde Mevcut Ve Oluşabilecek Sorunların Tespiti Ve Çözüm Önerileri, Hacettepe Üniversitesi Sağlık Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, 2000.
8. Davenport, Thomas H. ve Prusak L. İş Dünyasında Bilgi Yönetimi: Kuruluşlar Ellerindeki Bilgiyi Nasıl Yönetirler. (Çev. Günhan Günay). İstanbul: Rota Yayınları, 2001
9. Duffy, J. "Knowledge Management And its Influence on the Records and Information, Manager', Information Management Journal, Praide Village, July, 2001
10. Güleş K. H., Özata M., Sağlık Bilişim Sistemleri, Nobel, Yayın Dağıtım, Eylül 2005
11. Güçbilmez, B., Hastane Bilgi Sistemi Temel Özellikleri Seçim Kriterleri ve Adaptasyon Süreci, Modern Hastane Yönetim Dergisi, Cilt: 4, Sayı: 2, 2000.
12. http://www.guvenlikdanismanlik.com/biyometrik-tanima-sistemleri.htm (Erişim Tarihi: 01.08.2016)
13. http://www.firewallmerkezi.com/fortigate-fortinetfirewallnedir.php (Erişim Tarihi: 07.09.2016
14. http://bilgimikoruyorum.org.tr/?b414_guvenlik-duvari-nasil-yapilandirilir (Erişim Tarihi: 23.11.2016)
15. InfoWatch Analytical Center, Global Data Leakage Report, 2013, https://infowatch.com/analytics/reports/3641)
16. Merih, K., Hastanelerde On-Line Otomasyon Stratejileri, www.merih.com, 22/10/2001.
17. Merih, K, Hastane Otomasyonu Projelerinde Yanılsama ve Gerçek, Modern Hastane Yönetimi Dergisi, Cilt: 4, Sayı: 2, 2000.
18. Isaca, Cisa Review Manual, Isaca Press, Rolling Meadows, 2009
19. Rost, J., Glass, R. L., The Dark Side of Software Engineering, Evil on Computing Projects. IEEE Computer Society, John Wiley & Sons, Inc.,Hoboken, New Jersey, USA. 2011.
20. Suntay, Y., Hastane Bilgi Sistemleri'nde Entegrasyon Sorunları Ve Çözüm Önerileri, Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü, Yüksek Lisans Tezi, Kocaeli – 2010.
21. T. C. Sağlık Bakanlığı Sağlık Projesi Genel Koordinatörlüğü, Hastane Bilgi Sistemleri Alımı Çerçeve İlkeleri, 1997.
22. Yıldız, Müslüm, "Bowtie tekniği ile bilgi yönetiminde sızıntıların önlenmesine yönelik bir model önerisi" Dicle Üniversitesi SBE Yüksek Lisans Tezi, Diyarbakır, 2014