ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 1 Yıl/Year : 2018 ISSN -2149-6161

Usaysad Derg, 2018; 4(1): 15 -25(Araştırma makalesi)

KURUMSAL BİLGİ KAYNAKLARINA ERİŞİMDE GÜVENLİK: HEKİMLERİN ŞİFRE YÖNETİMİNE YÖNELİK BİR ARAŞTIRMA

Yrd.Doç.Dr. Yusuf Yalçın İLERİ
Necmettin Erbakan Üniversitesi
yileri@konya.edu.tr
Makale gönderim-kabul tarihi (02.02.2018-08. 03.2018)

Özet

Kurumlarda bilgi güvenliği politikalarının oluşturulması ve uygulanmasından yöneticiler sorumlu olmak birlikte, çalışanların üzerine de önemli görevler düşmektedir. Araştırmalar, kurumlarda bilgi güvenliği tehditlerinin büyük bölümünün çalışanlardan kaynaklandığını ortaya koymaktadır. Bu çalışmanın amacı, bilgi güvenliğinin ve bilgi güvenliğini sağlamada insan faktörünün çok önem kazandığı sağlık kurumlarında, Hastane Bilgi Yönetim Sistemlerini (HBYS) kullanan hekimlerin kurumsal bilgi kaynaklarına erişimde şifre yönetimi alışkanlıklarını incelemektir. Araştırmanın örneklemini kamuya ait veya özel hastanelerde çalışmakta olan ve HBYS'ni aktif kullanan ancak kurumlarında zorunlu şifre yönetim politikası olmayan hekimler oluşturmaktadır. Basit tesadüfi yöntemle seçilen 420 hekime anket formu e-posta yoluyla gönderilmiş, sonuçlar geri dönen 203 (%49) anket formu üzerinden değerlendirilmiştir. Hekimlerin HBYS parola güvenlik seviyelerini ölçmek için TÜBİTAK BİLGEM tarafından geliştirilen parola ölçer yazılımı kullanılmıştır. Parola güvenlik seviyesi toplamda 14 aşamada incelenerek 100 tam puan üzerinden değerlendirilmiş ve "çok zayıf"-"çok güçlü" arasında beş gruptan birisine dahil edilmiştir. Araştırma sonuçlara göre; hekimlerin %35'inin kullandıkları HBYS parolaları "çok zayıf" güvenlik kategorisinde iken %56'sının kullandıkları parolalar "zayıf" güvenlik kategorisinde, sadece %9'unun kullandıkları parolalar "iyi/orta" güvenlik kategorisindedir. Bulgulara göre; çalışmaya katılan hiçbir hekim "güçlü" veya "çok güçlü" seviyesinde parola kullanmamaktadır. HBYS parola güvenlik seviyeleri "iyi/orta" kategorisinde olan ve parolaları diğerlerine göre nispeten daha güçlü olan hekimlerin tamamının 35 yaş üstünde olması dikkat çekmektedir.

Anahta Kelimeler: Bilgi Güvenliği, Şifre Güvenliği, Sağlık Yönetimi, Yönetim Bilişim Sistemleri

SECURITY IN ACCESSING ENTERPRISE INFORMATION RESOURCES: A RESEARCH ON PASSWORD MANAGEMENT OF PHYSICIANS

Abstract

In the instutitions, managers are in charge of the creation and implementation of information security policies but employees have also important responsibilities. Studies reveal that most of the information security threats in organizations come from employees. The purpose of this study is to examine the password management habits of

physicians using Hospital Information Systems (HIMS) in accessing institutional information resources in healthcare institutions where information security and human factor are of great importance in ensuring information security. The sample of the research is composed of physicians who are working in public or private hospitals and who actively use HIMS but do not have mandatory password management policy in their institutions. The questionnaire forms were sent via e-mail to 420 randomly selected physicians and analysis were implemented over 203 (%49) returned questionnaire forms. Password meter software developed by TÜBİTAK BİLGEM was used to measure the HIMS password security levels of physicians. Password security levels were evaluated totally in 14 steps and over 100 full points and included in one of five groups between "very weak" - "very strong". According to the results of the research; 35% of the physicians' HIMS passwords are in the "very weak" security category, while 56% of the passwords are in the "weak" security category and only 9% of the passwords are in the "good / medium" security category. According to the results; none of the physicians participating in the study use a password at the "strong" or "very strong" level. It is noteworthy that all of the physicians whose password security levels are in the "good / medium" category and whose passwords are relatively stronger than others are over 35 years of age.

Key Words: Information Security, Password Security, Health Management, Management Information Systems

GİRİŞ

Günümüzde, bilgi güvenliği ile ilgili riskler birçok organizasyon için büyük sorunlar oluşturmaktadır. Çünkü bu riskler kurumlar için doğrudan yükümlülük doğuran, kurumsal sorumluluk ve güvenilirliği zedeleyen ve maddi ve manevi kayıplara yol açabilen önemli olgulardır (Cavusoglu vd., 2004). Bu nedenle, bilgi güvenliğinin sağlanması birçok organizasyonda üst yöneticilerin önceliklerinden biri haline gelmiştir (Ransbotham ve Mitra, 2009). Bilgi güvenliği risklerini azaltmak için, kuruluşlar genellikle teknoloji tabanlı çözümlere güvenmektedirler (Ernst ve Young, 2008; Vroblefski vd., 2007; Fernandez vd., 2006). Ancak, teknoloji tabanlı çözümler kurumsal bilgi güvenliğine katkıda bulunsada her zaman yeterli olmayabilmektedir. Çünkü bilgi güvenliği açıklarını oluşturan en önemli etmen çalışanların kendisidir. Bu nedenle kurumların hem güvenlik teknolojilerine hem de çalışanlarının bilgi güvenliği noktasında kültür ve bilişsel ve davranışsal özelliklerine yatırım yapmaları gerekmektedir. Bilgi güvenliğinde odak nokta bireysel ve örgütsel bakış açısına doğru kaymalı ve çalışanların bilgi güvenliği politikalarına uyumu anahtar bir sosyo-örgütsel durum olarak incelenmelidir (Boss ve Kirsch 2007).

Kuruluşlar, işlerini südürürken kullandıkları bilgi sistemlerinin güvenliğini nasıl sağlayacaklarını ve çalışanların bu hedefe uymak için hangi yönergeleri takip edeceklerini belirlemek amacıyla bilgi güvenliği yönetim politikalarını oluştururlar. Çalışmalar göstermiştir ki; kurumsal bilgi kaynaklarını zafiyete uğratmak, kurumlara doğrudan veya dolaylı olarak zarar vermek, sistemlere izinsiz girerek işleyişlerini aksattırmak, durdurmak, çökertmek gibi kötü niyetle yapılan tüm saldırı girişimleri ile ticari sırların çalınması, finansal kayıplar, itibar kayıpları, hizmetlerin sunulamaması veya aksaması gibi tehlikelere karşı yöneticilerin en güçlü silahları bilgi güvenliği yönetim sistemlerini tüm iş süreçlerine entegre etmek ve kurumsal bilgi güvenliği kültürünün oluşmasını sağlamak olacaktır (Canbek ve Sağıroğlu, 2006; Eminağaoğlu ve Gökşen, 2009; Tekerek, 2008; Vural ve Sağıroğlu, 2007).

Güvenlik bilinci veya kültürü, çalışanların örgütlerinin bilgi güvenliği hedeflerinin farkında oldukları, hedeflere ulaşmak için izlemeleri gereken prosedürleri anladıkları, riskli veya beklenilmeyen

durumlarda uygulamaları gereken süreçleri bildikleri durumdur. Çalışanlar kurumların bilgi güvenliğini doğrudan veya dolaylı olarak artırabilme kapasitesine de sahiptir. Ancak sadece bilgi güvenliği politikalarının varlığı çalışanlarda istenen ve beklenen davranışların ortaya çıkmasını sağlayamaz, bunu gerçekleştirmek için gerekli motivasyonu oluşturmak önem arz etmektedir (Stanton vd., 2005). Kurumlarda çalışanların bilgi güvenliğini önemsemeleri noktasında ilgili motivasyonel faktörler ve uyum davranışlarını inceleyen sınırlı sayıda çalışma bulunmaktadır (Pahnila vd., 2007; Herath ve Rao, 2009).

Mishra ve Dhillon'a göre; kurum içi çalışanların ihmali ve uyumsuzluğu kuruluşlara milyonlarca dolar zarar vermektedir, ayrıca, son kullanıcı uyumsuzluğundan kaynaklanan güvenlik ihlallerini önlemede veya en düşük seviyeye indirmedeki başarısızlığın, bilgi güvenliği yönetim politikalarındaki teşvik etme araçlarında ele alınmayan göstergeler olduğunu ileri sürmektedirler (Mishra ve Dhillon, 2006). Hangi faktörlerin çalışanları kurumlarının kurallarıyla uyumlu şekilde motive edeceği konusu kurumların bilgi güvenliği yönetimi politikalarında aranmalıdır. Bu politikalar doğru şekilde oluşturulur ve izlenebilirse; yöneticilere bilgi güvenliğindeki eksiklikleri teşhis edebilme olanağı sağlar, davranışsal sorunların bulunması ve sorunları çözmek için gerekli yolların takip edilmesi sürecine ışık tutar (İleri, 2017).

Çalışanların kurumların bilgi ve teknoloji kaynaklarını sahiplenmelerini sağlayabilmek önemlidir. Çünkü onların cehaleti, hataları veya kasıtlı eylemleri bilgi güvenliğini tehlikeye atabilmektedir (Durgin, 2007). Çalışanların kurumun ne istediğini bilmesi, amaçları anlaması, bilgi kaynaklarının neden korumak gerektğini özümsemesi, yani bilgi ve bilinç seviyesinin yükselmesi hizmet verirken daha dikkatli olmalarına ve ilgili prosedürlere daha bağlı şekilde iş yapmalarına imkan verebilecektir. Kurumlarda bilgi güvenliği yöneticilerinin, önemli noktaları vurgulamak için çalışanlarla ikna edici iletişim kanalları kurmaları, güvenlik eğitimi ve farkındalık programları oluşturmaları, kurumsal bilgi güvenliği politikalarının doğru hedeflere odaklanıp odaklanmadıklarını değerlendirmek için çalışanları motive eden ödüllendirme sistemleri kullanması faydalı olabilecektir.
Arzulanan davranışları teşvik etmek için kullanılan ödüller ve istenmeyen davranışları caydırmak için kullanılan cezalar harici motivasyonlar sağlamakla birlikte, bir çalışanın özündeki arzular kuralları ve düzenlemeleri takip etmek veya etmemek için iç motivasyon sağlamaktadır (Tyler ve Blader, 2005; Garoupa, 2000). Bu noktada bilgi güvenliği politikasına eklenebilecek uygun bir ceza ve ödüllendirme sistemi faydalı olabilecek, çalışanların bilgi güvenliğini sağlama motivasyonu üzerinde etkili olabilecektir. Literatür, cezanın ciddiyetini dikkate alarak, cezanın seviyesi arttıkça bireyin kural dışı bir fiil yürütme eğiliminde olma ihtimalinin daha düşük olduğunu ileri sürmektedir. Ceza şiddetinin, çalışanların bilgi güvenliği tutumlarıyla anlamlı derecede ilişkili olduğu sonucuna varan çalışmalar da mevcuttur (Peace vd.,2003).

Çalışanlar örgüt için bir bağlılık hissettikleri ve örgütsel sonuçlarını geliştireceğine inandıkları için organizasyona yararlı faaliyetlerde bulunurlar. Bilgi güvenliği bağlamında, çalışanlar, yöneticilerin, BT personelinin ya da iş arkadaşlarının kendisinden bilgi güvenliği politikası uyumu beklediğine inanırsa, bilgi güvenliği prosedürlerine uyma ihtimali daha yüksektir. Yani herkes yapıyorsa, özellikle de yöneticiler katı şekilde uyuyorsa, bu demekki gerekli ve yapılmalıdır anlayışı gelişebilir. Bu noktada, kuruluşlardaki güvenlik politikası uyumluluğu bağlamında, çalışanlar eylemlerinin farklılık yaratabileceğini ve genel kurumsal bilgi güvenliği hedefini etkileyebileceğini düşünüyorsa, güvenlik davranışlarını yerine getirme olasılığı daha yüksektir (Anderson, 2005).

Çalışmalar göstermiştir ki; kurumlarda bilgi güvenliği politika ve prosedürlerinin yürürlükte olduğu kurumlarda bile, birçok çalışan onları görmezden gelmektedirler (CERTC, 2004). SANS Enstitüsü'nün raporuna göre; kuruluşlar, çalışanlardan kaynaklanan tehdidinin önemini kabul etmekte hatta içeriden gelen tehdidi tehdit ortamlarının en zararlı bileşeni olarak görmektedir. İlginçtir ki, çoğu organizasyonun bilgi güvenliği bütçesi ve personel eğitimi noktasında, bu tehdit algılamasına rağmen herhangibir düzenleme yapmamakta, gerekli önlemleri almamaktadır. Ankete katılanların %45'i olayla ilişkili finansal kayıpların potansiyelini bilmediğini,% 33'ünün de kayıplara bir değer biçemediğini belirtmiştir. Kurumların sadece %18'I içeriden kaynaklanan saldırılara karşı çözümler içeren resmi bir bilgi güvenliği planına sahipken, % 49'u bu tür programları geliştirmeye yeni başladıklarını belirtmişlerdir. Kurumların %40' kötü niyetli çalışanları karşılaştıkları en zararlı tehdit vektörü olarak değerlendirirken, kaza sonucu zarar veren ya da ihmalkar çalışanları kurumsal bilgi güvenliğine en çok zarar verici etmen olarak tanımlayanların oranı %36'dır (Cole, 2017).

Kurumsal bilgi güvenliğinde, örgütsel güvenlik politikalarına uyup uymama veya yok sayma sorumluluğu çalışanlara devredilmektedir. Çalışanlar, güvenlik politikalarını kötü amaçlı olarak kırmayı veya güvenlik politikalarından yalnızca kolaylık sağlamak için kaçmayı seçebilir. Çalışmalara göre, çalışanlar, daha yüksek bilgi güvenliği seviyesinin esnek çalışma usullerini takip etme ve bunları karşı üretken olarak algılama yeteneklerini kısıtladığına inanmaktadır (Post ve Kagan, 2007). Bu sonuç çalışanların bilgi güvenliği eğitimlerine katılmalarının ve bu konuda bilinçlenmelerinin önemini vurgular niteliktedir. Literaürde, çalışanlara bilgi güvenliği farkındalığı eğitimlerinin verilmesinin (Furnell vd., 2002; Hentea, 2005; Puhakainen, 2006) faydalı olacağı sonucuna varan birçok çalışma bulunmaktadır. Bu çalışmalar, kullanıcıların, karşı önlemlere ilişkin farkındalıklarının, örgütsel yaptırımlara ilişkin algılarını etkilediğini ve bunun da, kullanıcıların yanlış kullanım niyetlerini azalttığını göstermişlerdir.

Örgütsel güvenlik uygulamalarını ve etkinliklerini değerlendiren birçok çalışma bulunmakla birlikte, bu çalışmalarda katılımcılar genellikle BT yöneticileri veya üst düzey yöneticiler seviyesinde kalmaktadır (Dhillon ve Torkzadeh, 2006; Ma ve Pearson, 2005) ve çalışanların bilgi güvenliği noktasında nasıl davrandıklarına fazla önem verilmemektedir. Ancak; etkin organizasyonel bilgi güvenliği üç bileşene, yani: kişi, süreçler ve teknolojiye bağlıdır (Hamil, 2005). Güvenlik yönetiminin davranışsal yönlerinin amacı, çalışanların kurallara ve politikalara uyduklarından emin olunmasını sağlamaktır (Solms ve Solms, 2004). Son zamanlarda, davranışsal bilgi güvenliği araştırmaları, çalışanların güvenlik politikalarını takip etme niyetlerine dikkat etmeye başlamıştır (Pahnila vd., 2007; Chan vd., 2005).

Tüm örgütlerde çalışanların kurumsal bilgi güvenliği üzerindeki etkisi yadsınamayacak seviyede olmakla birlikte, hizmet odaklı olan, çok farklı disiplinlerden uzmanların beraber iş yaptığı, yoğun bilgi erişimi gerektiren sağlık kurumlarında bilgi güvenliğini sağlamada insan boyutu fazlaca önem kazanmaktadır. Sağlık kurumlarında çalışanların bilgi güvenliği algısı noktasında çalışmalar bulunmakla birlikte, bilgi kaynaklarına erişimde sağlık çalışanlarının şifre güvenliği yönetimleri üzerine literatürde çok kısıtlı sayıda çalışma bulunmaktadır. Bu çalışmanın amacı, bilgi güvenliğinin ve bilgi güvenliğini sağlamada insan faktörünün çok önem kazandığı sağlık kurumlarında, hastane bilgi yönetim sistemlerini kullanan hekimlerin kurumsal bilgi kaynaklarına erişimde şifre yönetimi noktasında alışkanlıklarını belirlemektir.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 1 Yıl/Year : 2018 ISSN -2149-6161

GEREÇ VE YÖNTEM

Araştırmanın örneklemini kamuya ait veya özel hastanelerde çalışmakta olan ve Hastane Bilgi Yönetim Sistemi'ni aktif kullanan ancak kurumlarında zorunlu şifre yönetim politikası olmayan hekimler oluşturmaktadır. Basit tesadüfi yöntemle seçilen 420 hekime anket formu e-posta yoluyla gönderilmiş, geri dönen 217 (%52) anket formundan 14'ü kurumlarında zorunlu şifre yönetim politikası bulunduğunu beyan ettiklerinden değerlendirmeden çıkarılmış, 203 (%49) anket formu üzerinden veriler değerlendirilmiştir. Ankete katılım tamamen isteğe bağlı olup, hiç kimse katılıma zorlanmamıştır ve araştırmaya katılım için sadece bir kez e-posta gönderilmiştir.

Araştırmada, veri toplama aracı iki bölümden oluşmaktadır. Birinci bölümde, cinsiyet, yaş, eğitim durumu vb. demografik sorular ile ikinci bölümde ise hekimlerin şifre güvenliği ile ilgili değerlendirmelerini içeren sorular bulunmaktadır. İkinci bölümde yer alan "Kurumunuzda zorunlu şifre yönetim politikası bulunmakta mıdır?" sorusuna "hayır" yanıtını veren hekimler değerlendirmeye alınmıştır. Zorunlu şifre yönetim politikası bulunan kurumlarda, kullanıcılar genellikle en az 8 karakterden oluşan, harf, rakam ve özel karakterlerin aynı anda kullanımının zorunlu olduğu, tekrar içermeyen yüksek güvenlikli şifreler oluşturmak zorundadırlar. Bu nedenle bu kurumlarda çalışanların şifre güvenliği zaten yüksektir ve herhangibir ölçüme gerek yoktur. Anket içerisinde katılımcılara şifrelerini TÜBİTAK BİLGEM'in geliştirdiği parola ölçer (bilgimikoruyorum.org) ile en son kullandıkları otomasyon şifresine benzer özellikler içeren ancak aynı olmayan bir şifreyi güvenlik seviyesi bakımından test etmeleri istenmiş ve sadece şifrenin güvenlik testi sonucunu (çok zayıf-çok güçlü) yanıt olarak yazmaları talep edilmiştir. Araştırmanın yapılabilmesi için ilgili Bilimsel Araştırma ve Yayın Etiği Kurulu Başkanlığı'ndan Etik Kurul Onayı alınmıştır.

Araştırmanın Sınırlılıkları

Çalışmanın, sadece Konya ilinde yapılmış olması araştırmanın temel kısıtlılığını oluşturmaktadır. Çalışmanın sadece uzman ve pratisyen hekimlere yönelik olması ise diğer bir kısıttır.

Parola Güvenlik Ölçer

Kurumlarda parola güvenliğini sağlamak amacı ile parola oluşturma ve değiştirme politikaları geliştirilmektedir. Bu politikalara uygun hareket etmek tüm kurum çalışanlarının sorumluluğudur. Parola güvenlik politikası olmayan kurumlarda ise çalışanlar istedikleri şekilde bir parola belirlemekte özgürdürler. Ancak bu durum bilgi güvenliği zafiyetlerine sıklıkla yol açabilmektedir.

Bu çalışmada; TÜBİTAK BİLGEM tarafından geliştirilen parola ölçer yazılımı kullanılmıştır. Parola ölçer yazılımı; (1) kritik özellikler, (2) karakter sayısı, (3) önerilen karakter sayısı, (4) küçük harf kullanımı, (5) büyük harf kullanımı, (6) rakam kullanımı, (7) sembol kullanımı, (8) rakamların aralarda kullanımı, (9) sembollerin aralarda kullanımı, (10) ardışık harf kullanımı, (11) ardışık rakam kullanımı, (12) klavye kalıpları kullanımı, (13) tekrarlanan kısımların varlığı, (14) tersten yazılan kısımlar varlığı gibi toplamda 14 alanda incelenmekte ve alınan puanlara göre "çok zayıf" – "çok güçlü" aralığında 5 farklı seviyede parolalara güvenlik seviyesi atamaktadır. Tahmin edilmesi kolay olmayan ya da deneme yanılma yolu ile ele geçirilmesi oldukça zor olan parolalar "güçlü", kolayca tahmin edilebilecek, az sayıda ve benzer veya sıralı karakterden oluşan parolalar ise "zayıf" olarak değerlendirilmektedir. Tablo 1'de TÜBİTAK'ın geliştirdiği parola güvenlik ölçer yazılımının gözönüne aldığı parola güvenlik seviyeleri ve her seviyenin 100 toplam puan üzerinden karşılığı yer almaktadır.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 1 Yıl/Year : 2018 ISSN -2149-6161

Tablo 1: Parola Güvenlik Seviyeleri

Parola Güvenlik Seviyesi	Toplam Puan
Çok Güçlü	80 - 100
Güçlü	60 - 80
İyi / Ortalama	40 - 60
Zayıf	20 - 40
Çok Zayıf	0 - 20

Kaynak: TÜBİTAK BİLGEM

Parola ölçerin 14 temel kriteri aşağıda kısaca açıklanmıştır.

(1) Kritik Özellikler: * ile işaretlenmiş tüm kriterlerden alınan toplam puanı gösterir. Belirli sayıda puan karşılandığında puan alınmakta, aksi durumda puan kaybedilmektedir.

(2) Karakter Sayısı: Paroladaki karakter sayısının artması parolayı güçlü hale getirir. Karakter sayısı 5'den az ise 10 ceza puanı alınır. Karakter sayısı beş ve fazla ise toplam puana katkı yapmaya başlar.

(3) Önerilen Karakter Sayısı: Sekiz ve üstü karakter sayısına sahip parolalar fazladan puan alır.

(4) Küçük Harf Kullanımı: Parolada küçük harf kullanımı çeşitlilik sağlayarak güçlendirir.

(5) Büyük Harf Kullanımı: Parolada büyük harf kullanımı çeşitlilik sağlayarak güçlendirir.

(6) Rakam Kullanımı: Parolada rakam kullanımı çeşitlilik sağlayarak güçlendirir.

(7) Sembol Kullanımı: Parolada sembol kullanımı alfabe boyutunu artırır ve kelime kalıplarının dışına çıkartır, parolayı kuvvetlendirir.

(8) Rakamların Arada Kullanımı: Rakamlar parolalarda genellikle sona eklenmektedir. Aralarda rakam kullanımı parolayı kuvvetlendirir.

(9) Sembollerin Arada Kullanımı: Aralarda sembol kullanımı parolanın ele geçirilmesini çok zorlaştırır, parolayı kuvvetlendirir.

(10) Ardışık Harf Kullanımı: Ardışık harf kullanımı (abc, xyz vb.) parola güvenliğini azaltır. Ceza puanı uygulanır.

(11) Ardışık Rakam kullanımı: Ardışık rakam kullanımı (123 vb.) parola güvenliğini azaltır. Ceza puanı uygulanır.

(12) Klavye kalıpları kullanımı: Klavye üzerinde yakın yerleştirilmiş tuşların beraber kullanımı parola güvenliğini azaltır. Ceza puanı uygulanır.

(13) Tekrarlanan Kısımların Olması: Aynı kalıp yada bölümlerin tekrar kullanılması parola güvenliğini azaltır. Ceza puanı uygulanır.

ULUSLARARASI SAĞLIK YÖNETİMİ VE STRATEJİLERİ ARAŞTIRMA DERGİSİ
INTERNATIONAL JOURNAL OF HEALTH MANAGEMENT AND STRATEGIES RESEARCH
Cilt/Volume : 4 Sayı/Issue : 1 Yıl/Year : 2018 ISSN -2149-6161

(14) Tersten Yazılan Kısımların Olması: Parola içindeki bir bölüm yada bloğun tersten yazılması parola güvenliğini azaltır. Ceza puanı uygulanır.

BULGULAR

Çalışmada elde edilen bulgular aşağıdaki tablolarda özetlenmiştir.

Tablo 2: Katılımcıların Cinsiyet Değişkenleri

CİNSİYET	Erkek		Kadın		Toplam	
	N	(%)	N	(%)	N	(%)
Pratisyen Hekim	72	%59	49	%41	121	%58
Uzman Hekim	54	%62	32	%38	86	%42
Toplam	126	%60	81	%40	207	%100

Tablo 2'den de görüldüğü gibi araştırmaya toplamda 207 hekim katılmıştır. Bunların %59'u pratisyen hekim, %41'I ise uzman hekimdir. Katılımcıların 126'sı (%60) erkek, 81'I (%40) ise kadındır.

Tablo 3: Katılımcıların Yaş Değişkenleri

YAŞ	25 Yaş Altı		25-30		31-35		35 Yaş Üstü		Toplam	
	N	(%)	N	(%)	N	(%)	N	(%)	N	(%)
Pratisyen Hekim	21	%18	17	%14	66	%54	17	%14	121	%100
Uzman Hekim	0	%0	42	%48	33	%38	11	%14	86	%100
Toplam	21	%10	59	%29	99	%47	28	%14	207	%100

Tablo 3'de gösterildiği gibi; çalışmaya dahil olan hekimlerin ortalama %10'u 25 yaş altında iken, %29'u 25-30 yaş aralığında, %47'si 31-35 yaş aralığında ve %14'ü ise 35 yaşın üstündedir. 25 yaş altı uzman hekim olmaması, tıpta uzmanlık eğitiminin fazladan 4 yıl gerektirmesidir.

Tablo 4: Katılımcıların Şifre Güvenlik Seviyesi Değişkenleri

Şifre Güvenlik Seviyesi	Çok Zayıf		Zayıf		İyi /Orta		Güçlü		Çok Güçlü	
	N	(%)	N	(%)	N	(%)	N	(%)	N	(%)
Pratisyen Hekim	45	%37	65	%53	11	%10	0	%0	0	%0
Uzman Hekim	27	%32	51	%59	8	%9	0	%0	0	%0
Toplam	72	%35	116	%56	19	%9	0	%0	0	%0

Tablo 4'de hekimlerin parolalarının TÜBİTAK parola güvenlik ölçer yazılımı ile test ettikten sonra bildirdikleri güvenlik seviyeleri görülmektedir. Sonuçlara göre; hekimlerin %35 'inin kullandıkları parolalar "çok zayıf" güvenlik kategorisinde iken (TÜBİTAK parola ölçer puanı 0-20 arası), %56'sının kullandıkları parolalar "zayıf" güvenlik kategorisinde (TÜBİTAK parola ölçer puanı 20-40 arası), sadece %9'unun kullandıkları parolalar "iyi/orta" güvenlik kategorisindedir (TÜBİTAK parola ölçer puanı 40-60 arası). Eldeki sonuçlara göre; çalışmaya katılan hiçbir hekim "güçlü" veya "çok

güçlü" seviyesinde parola kullanmamaktadır. Bunun yanında, hekimlerin %91'i "çok zayıf" veya "zayıf" güvenlik kategorisinde parola kullanmaktadır.

Sonuçlara göre; parola güvenlik seviyeleri "iyi/orta" kategorisinde olan, yani parolaları diğerlerine göre nispeten daha güçlü olan hekimlerin tamamının 35 yaş üstünde olması dikkat çekmektedir. Bu sonuca göre; hekimlerin yaşları ilerledikçe parola güvenliğine verdikleri önem artmaktadır. Parola güvenlik seviyelerinin dağılım gösterdiği, "çok zayıf","zayıf","iyi/orta" güvenlik kategorilerinde pratisyen hekim ve uzman hekimlerin yüzdesel oranları birbirine çok yakın olduğu görülmektedir. Örneğin; "iyi/orta" güvenlik kategorisindeki uzman hekim oranı %9 iken, pratisyen hekim oranı %10 seviyesi ile uzman hekim oranına çok yakındır. Benzer şekilde "çok zayıf" güvenlik kategorisindeki uzman hekim oranı %32 iken pratisyen hekim oranı %37'dir. Bu sonuçlara göre, parola güvenliğine verilen önem açısından uzman hekimler ile pratisyen hekimler arasında önemli bir fark bulunmamaktadır.

SONUÇ VE TARTIŞMA

Günümüz sağlık kuruluşları, sağlık çalışanlarına bilgiye erişim özgürlüğü verebilmek ve onların teknolojiden mümkün olan en fazla katkının alınabileceği, kullanıcı dostu, esnek ve çevik sistemlerle çalışabilmeleri için önemli yatırımlar yapmaktadır. Bu yatırımlar sayesinde, tüm tahlil, tetkik sonuçları ve diğer hasta verilerine bulundukları her yerden ulaşabilen sağlık çalışanları hizmetlerini çok daha hızlı ve kaliteli verebilme imkanı bulmakta, özellikle hekimler hastaların geçmiş tıbbi verilerine de ulaşabildiklerinden hastalık teşhis ve tedavisinde çok daha iyi sonuçlar alabilmektedirler.

Bilişim sistemlerinin sağlık kurumlarında bu kadar yoğun kullanımı beraberinde teknolojiye bağımlılık , bilgi kaynaklarının güvenliği ve erişim denetimi gibi problemler ortaya çıkarmaktadır. Hastane bilgi kaynaklarına en sık şekilde erişim gerçekleştiren ve lokasyon olarak çok farklı yerlerden sisteme bağlanan hekimlerin şifre güvenliği yönetimine verdikleri önem, sağlık kurumlarının bilgi kaynaklarının güvenliğini doğrudan ilgilendirmektedir. Ancak, bu çalışmada elde edilen sonuçlar göstermiştirki hekimler otomasyon şifrelerinin güvenlik derecesine önem vermemektedir. Hekimlerin %91'i şifrelerinin "çok zayıf" veya "zayıf" olduğunu kabul etmektedir. Bilgi güvenliğine erişimde en önemli koruma olan şifre yönetiminde bu seviyede yüksek umursamazlık, kaçınılmaz olarak bilgi kaynaklarının yetkisiz kişilerce ele geçirilmesine neden olacaktır. Hastane otomasyon sistemlerinin günümüzde birçok hastane tarafından en az on yıldır kullanıldığı düşünüldüğünde, kaybedilebilecek veya yetkisiz kişilerce görüntülebilinecek verilerin büyüklüğü noktasında bir fikir verebilecektir.

Çalışma sonuçları göstermiştirki; sağlık kurumlarında son kullanıcıların güvenlik davranışlarını denetlemek için denetleme mekanizmaları acilen kurulmalıdır. Bilgi güvenliği eğitimleri tüm sağlık çalışanlarına zorunlu olacak şekilde verilmeli, bilgi güvenliğinin sağlanmasının neden kritik önemde olduğu etkili şekilde anlatılmalıdır. Bir çalışanın eğitim ve teknoloji bilgisinin düzeyi, çalıştığı kuruluşun büyüklüğü, hizmet verdiği sektör ve sektördeki enformasyon yoğunluğu uyumluluk davranışını etkileyebilmektedir. Bu nedenle eğitimlerin konunun uzmanları tarafından verilmesi, çalışanların eğitim düzeyi, mesleği, bilgi kaynaklarına erişim yoğunluğu vb. özellikleri gözönüne alınarak gruplara ayrılması daha verimli sonuçlar elde edilmesini sağlayabilecektir.

Çalışanların kurumun bilgi güvenliği amaçlarını anlaması, bilgi kaynaklarının neden korumak gerektğini özümsemesi ve bu noktada bilgi ve bilinç seviyesinin yükseltilmesi hizmet verirken daha dikkatli olmalarına ve ilgili prosedürlere daha bağlı şekilde iş yapmalarına imkan verebilecektir. Kurumlarda bilgi güvenliği yöneticilerinin, çalışanlarla ikna edici iletişim kanalları kurmaları, bilgi

güvenliği eğitimlerinde farkındalık oluşturmaları, çalışanları motive eden ödüllendirme sistemleri kullanması faydalı olabilecektir.

Yöneticilerin, kuruluşlardaki uygun bilgi güvenliğini iklimini oluşturarak güvenlik politikalarına uyumu geliştirmesi kritik önemdedir. Çalışanlar, eylemlerinin bilgi güvenliğini artırmada bir fark yarattığını ve yardım sağladığını algılarlarsa, güvenlik politikalarına olan inançları artacak ve bu politika ve prosedürlere uyma olasılıkları yükselecektir. Güvenlik politikalarına uyan çalışan sayısının artması, diğer çalışanların bilgi güvenliği politikalarına uyma niyetlerine ve algılarına katkıda bulunmaktadır. Çalışanların herhangibir bilgi güvenliği zaafiyeti ortaya çıktığında buna neden olan etmen veya personelin belirleneceğini bilmesi de önemlidir. Yöneticilerin, çalışanlarının güvenlik performansını araştırmak ve değerlendirmek için gerekli mekanizmaları kullanmaları ve bunu çalışanlara açıkça göstermeleri uygun bir yol olacaktır.

Çalışma sonuçları göstermiştirki, sağlık kurumlarında bilgi kaynakları çalışanlar nedeniyle tehditlere açık durumdadır. Birçok çalışma çalışanların kurumlarda en önemli güvenlik tehditlerinden sorumlu olduklarını göstermiştir. Bu noktada yöneticiler, bilgi güvenliği polotika ve prosedürlerini kurumlarında hızla faaliyete geçirmeli ancak insan hatasını en aza indiriecek önlemleri de almalıdır. Günümüzde iş ortamlarının teknolojiye bağımlılığı gözönüne alındığında, zorunlu yüksek güvenlikli şifre politikası olmayan hiçbir kurumun bilgi kaynakları güven altında değildir.

ÖNERİLER

Son kullanıcı davranışlarını etkileyen ve yönlendiren bilgi güvenliği yönetiminin önemi uygulayıcılar tarafından vurgulanmış olmasına rağmen, davranışsal bilgi güvenliği noktasında çok sınırlı sayıda çalışma bulunmaktadır. Davranışsal bilgi güvenliğinin özellikle sosyal baskı, algılanan fayda, caydırıcı ve destekleyici önlemler, örgütsel vatandaşlık boyutu alanlarında incelenmesi literature önemli katkı sağlayacaktır.

KAYNAKLAR

Anderson, C. (2005). Creating Conscientious Cybercitizen: An Examination of Home Computer User Attitudes and Intentions Towards Security, presented at Conference on Information Systems Technology (CIST)/INFORMS, San Francisco, California.

Boss, S. R., Kirsch, L. J. (2007). "The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness," in Proceedings of the 28th International Conference on Information Systems, Montreal, December 9-12.

Canbek, G., Sağıroğlu, Ş. (2006). "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Politeknik Dergisi, 9(3), 165-174.

Cavusoglu, H., Cavusoglu, H., Raghunathan, S. (2004). "Economics of IT Security Management: Four Improvements to Current Security Practices", Communications of the Association for Information Systems (14), 65-75.

CERTC (2004), E-Crime Watch Survey Summary of Findings, Computer Emergency Response Team Coordination Center (CERT/CC).

Chan, M., Woon, I., Kankanhalli, A. (2005). "Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior", Journal of Information Privacy and Security, 1-3.

Cole, E. (2017). Defending Against the Wrong Enemy: 2017 SANS Insider Threat Survey, SANS Enstitüsü.

Dhillon, G.,Torkzadeh, G. (2006). "Value-focused assessment of information system security in organizations", Information Systems Journal, 16(3), 1-8.

Durgin, M. (2007). "Understanding the Importance of and Implementing Internal Security Measures," SANS Institute Reading Room. 22.01.2018 tarihinde https://www2.sans.org adresinden alınmıştır.

Eminağaoğlu, M., Gökşen, Y., (2009). "Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri", Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11 (4), 1-15.

Ernst, Young. (2008). "Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey". 22.01.2018 tarihinde http://www.ey.com/Publication adresinden alınmıştır.

Fernandez, E.M., Trujillo, J., Villarroel, R., Piattini, M. (2006). "Access control and audit model for the multidimensional modeling of data warehouses", Decision Support Systems, 42.

Furnell, S. M., Gennatou, M., Dowland, P. S. (2002). "A Prototype Tool for Information Security Awareness and Training", Logistics Information Management, 15(5), 352-357.

Garoupa, N. (2000). "Corporate Criminal Law and Organization Incentives: A Managerial Perspective", Managerial and Decision Economics, 21.
Hamill, J.T.R., Deckro, F. (2005). "Evaluating information assurance strategies", Decision Support Systems, 39.

Hentea, M. (2005). "A Perspective on Achieving Information Security Awareness," in The Information Universe: Issues in Informing Science and Information, E. Cohen (ed.), Santa Rosa, CA: Informing Science Institute, 2,169-178.

Herath, T., Rao, H.G. (2009). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", European Journal of Information Systems,18(2),106-125.

İleri, Y.Y. (2017). "Örgütlerde Bilgi Güvenliği Yönetimi, Kurumsal Entegrasyon Süreci ve Örnek Bir Uygulama", Anadolu Üniversitesi Sosyal Bilimler Dergisi, 17(4), 55-72.

Ma, Q., Pearson, J.M. (2005). "ISO 17799:Best Practices In Information Security Management? ", Communications of the Association for Information Systems, 15.

Mishra, S., Dhillon, G. (2006). "Information Systems Security Governance Research: A Behavioral Perspective", in Proceedings of the 1st Annual Symposium on Information Assurance, Academic track of 9th Annual NYS Cyber Security Conference, New York, USA.

Pahnila, S., Siponen, M., Mahmood, A. (2007). "Employees' Behavior towards IS Security Policy Compliance," in Proceedings of the 40th Hawaii International Conference on System Sciences, Los Alamitos, CA: IEEE Computer Society Press,156-166.

Pahnila, S., Siponen,M., Mahmood, A. (2007). "Employees' Behavior Towards IS Security Policy Compliance", in Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS 07). Hawaii, USA.

Peace, A. G., Galletta, D., Thong, J. (2003). "Software Piracy in the Workplace: A Model and Empirical Test", Journal of Management Information Systems, 20, 1.

Post, G.V., Kagan, A. (2007). "Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks", Computers & Security, 26, 229-237.

Puhakainen, P. (2006). "A Design Theory for Information Security Awareness," working paper, Faculty of Science, University of Oulu, Finland.

Ransbotham, S., Mitra, S. (2009). "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise," Information Systems Research, 20(1), 121-139.

Solms, R.V., Solms, B.V. (2004). "From Policies to Culture", Computers & Security, 23.

Stanton, J. M., Stam, K. R., Mastrangelo, P., Jolton, J. (2005). "Analysis of End User Security Behaviors", Computers and Security, 24(2),124-133.

Tekerek, M. (2008). "Bilgi Güvenliği Yönetimi", KSÜ Fen ve Mühendislik Dergisi, 11(1), 132-137.
TUBİTAK, BİLGEM, www.bilgimikoruyorum.org, Erişim: 05.01.2018.

Tyler, T.R., Blader, S.L. (2005). "Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings", Academy of Management Journal, 48(6), 1143-1158.

Vroblefski, M., Chen, A., Shao, B., Swinarski, M. (2007). "Managing user relationships in hierarchies for information system security", Decision Support Systems, 4.

Vural, Y., Sağıroğlu, Ş. (2007). "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", ISO Turkey, Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı, 13-14 Aralık, Ankara, Türkiye.