Yılmaz, B. ve Özdemirci, F. "Bilgi Güvenliği Yönetim Sistemi (BGYS) Sürecinde Bilgi Güvenliği Temelli EBYS Yönetimi", Bilgi Yönetimi ve Bilgi Güvenliği: eBelge-eArşiv-eDevlet-Bulut Bilişim-Büyük Veri-Yapay Zeka/ Editörler. Bahattin Yalçınkaya, M. Altay Ünal, Burcu Yılmaz, Fahrettin Özdemirci. – Ankara: Ankara Üniversitesi BİL-BEM, 2019. İçinde 45- 59.ss.

Bilgi Güvenliği Yönetim Sistemi (BGYS) Sürecinde Bilgi Güvenliği Temelli EBYS Yönetimi

Electronic Records Management Systems (ERMS) Based on Information Security in The Information Security Management System (ISMS) Process

Burcu YILMAZ
Ankara Üniversitesi BEYAS Koordinatörlüğü

Fahrettin ÖZDEMİRCİ
Ankara Üniversitesi Bilgi ve Belge Yönetimi Bölümü

Öz

Bilgi odaklı yeni toplum yapısıyla beraber bilgi, daha önce hiç olmadığı kadar değer kazanmış, birçok alanda temel güç kaynağı olarak ele alınmaya ve ekonomik bir meta olarak görülmeye başlanmıştır. Bu değişim süreci, bilginin korunması problemini ortaya çıkarmış böylece bilgi güvenliği kavramı hayatımıza girmiştir. Organizasyonlarda bilgi güvenliğinin sağlanmasına yönelik olarak birçok yöntem uygulanmaktadır. Bu yöntemlerin arasında yaygın olarak kullanılanlardan biri de Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulmasıdır. Elektronik Belge Yönetim Sistemleri (EBYS), kurumların yönetim süreçlerine dair önemli veriler içermektedir. EBYS'lerin sahip olduğu bilgi varlıkları ve bu varlıkların değeri göz önüne alındığında, bu sistemlerde bilgi güvenliğinin sağlanmasının bir zorunluluk olduğu görülmektedir. Bu çalışmada kurumsal bilgi ve belgelerin yönetildiği Elektronik Belge Yönetim Sistemleri (EBYS), bilgi güvenliği perspektifinden ele alınmış, EBYS Uygulamalarında BGYS Belgelendirme sürecinin uygun şekilde yürütülebilmesi için gerekli görülen tedbirler/çalışmalar tanımlanmıştır. Çalışmayla EBYS'lerde bilgi güvenliğinin sağlanmasının önemine yönelik farkındalık oluşturmak ve bu süreçlerden geçecek kurumlara uygulama konusunda yardımcı olmak amaçlanmıştır.

Anahtar Kelimeler: *Elektronik Belge Yönetim Sistemi, EBYS, Bilgi Güvenliği, Uygulama, Bilgi Güvenliği Yönetim Sistemi, BGYS,27001*

Abstract

With the new information-oriented social structure, information has gained value more than ever before, and in many areas it has been considered as the main source of power and seen as an economic commodity. This process of change has revealed the problem of protection of information, thus the concept of information security has entered our lives. Many methods are applied to ensure information security in organizations. One of the commonly used methods is the establishment of an Information Security Management System (ISMS). Electronic Records Management Systems (ERMS) contain important data on the management processes of the institutions. Considering the information assets and the value of these assets, it is seen that information security is a necessity in these systems. In this study, Electronic

Records Management Systems (ERMS, where corporate information and documents are managed, are handled from the information security perspective, and necessary measures / studies are deemed necessary for the proper implementation of the ISMS Certification process in the ERMS. The aim of the study was to raise awareness about the importance of providing information security in ERMS and to help implement these processes to institutions.

Keywords: *Electronic Records Management Systems, ERMS, Information Security, Implementation, Information Security Management System, ISMS, 27001*

1. Giriş

Toplumlar tarih boyunca bilgi ile gelişmiş, bilgi ise insan ile beraber var olmuş ve insanlık tarihi boyunca üretilmiştir. Günümüzde ise toplum ve bilgi arasındaki bu ilişki hiç olmadığı kadar yoğunlaşmış ve başkalaşmıştır. Bilginin ele alınma biçimi de kökten değişmiştir. Bilgi artık ekonomik bir meta olarak görülmekte, alınıp satılmaktadır. Bu değişimin temel nedeni ise bilginin taşıdığı değerdir. İçinde bulunduğumuz çağda "Bilgiyi elinde tutanlar güçlü olarak değerlendirilmekte, elindeki bilgiyi kullanarak yeni bilgiler üretenler rakiplerinin bir adım önünde bulunmaktadırlar (Atılgan, 2009)." "Bilginin değerinin olması, bu değeri elde etmek için emek ve zamanın harcanması ve kazanılan bilginin fark yaratması nedeniyle bilgi, korunması gereken bir varlık olarak görülmektedir (Brykczynski ve Small, 2003; Akt. Canbek ve Sağıroğlu, 2006)." Bilgi Güvenliği kavramı da bu değişimle beraber bilginin korunmasına yönelik olarak ortaya çıkmıştır. Gün geçtikte daha da önem kazanan bilgi güvenliği kavramı, elektronik ve basılı ortamlarda yer alan bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümü olarak ifade edilebilir. (Canbek ve Sağıroğlu, 2006)

Bu çalışmada EBYS'ler bünyesinde yer alan belgeler ve bu belgelerin değeri üzerinde durulmakta, bu değer göz önüne alınarak EBYS'ler de bilgi güvenliğinin sağlanmasının gerekliliği tanımlanmaktadır. Sonrasında bilgi güvenliği çalışmaları Elektronik Belge Yönetim Sistemleri (EBYS) perspektifinden ele alınarak, EBYS'lerde bilgi güvenliğinin sağlanması için yapılması gereken çalışmalara ve yürütülmesi gereken süreçlere değinilmektedir. Bilgi güvenliği çalışmaları belgelendirme için kullanılan ISO/IEC 27001:2017 standardı referans alınarak değerlendirilmekte, ISO/IEC 27001:2017 standardı belgelendirme sürecinde EBYS'lere özel olarak oluşturulması gerekli görülen dokümanlara dair bilgi verilmektedir. Standart kapsamında bilgi sistemlerine yönelik olarak birçok teknik gereksinim yerine getirilmelidir. Çalışmada belirtilen "Sistemsel Gereksinimler" çalışmanın 4.2.2 başlığında yer alan, EBYS'lerde idari yapılanma ve kurumsal iş süreçlerinden kaynaklanan "Süreç Gereksinimlerinin" karşılanabilmesi için yerine getirilmesi zorunlu olan teknik gerekliliklerdir. Çalışmanın sadece

ilgili süreçleri kapsaması sebebiyle Uygulanabilirlik Bildirgesi içerisinde yer alan A.13, A.14 gibi tamamen teknik altyapıya yönelik maddeler kapsam dışı bırakılmıştır. Çalışmayla EBYS'lerde bilgi güvenliğinin sağlanmasının önemine yönelik farkındalık oluşturmak ve bu süreçlerden geçecek kurumlara uygulama konusunda yardımcı olmak amaçlanmıştır.

2. Bilgi Güvenliği

20. yy sonlarına doğru, bilginin ortamının ve kullanım amaçlarının değişmesiyle beraber ortaya çıkan bilgi güvenliği kavramı 1988 yılında ilk siber casusluk girişiminin -kayıtlara geçen- gerçekleşmesiyle ele alınmaya başlanmış, daha sonra gerçekleşen casusluk girişimleriyle beraber önem kazanmıştır. Bu girişimlerin sonucunda organizasyonlar bilgi güvenliği ihlallerini önlemek adına çalışmalar yürütmüş ve 1995 yılında ilk zafiyet tarama programı olan SATAN (Security Administrator Tool for Analyzing Networks) piyasaya sürülmüştür. SATAN ile kurumların bilgi güvenliği zafiyetleri tanımlanmaya çalışılmış, ihlalleri önlemek adına zafiyetler ortadan kaldırılmaya çalışılmıştır. (Chen vd., 2005; Akt. Gülmüş, 2011). Bu yazılım ile başlayan bilgi güvenliği çalışmaları, zamanla dünya geneline yayılmıştır.

Günümüzde bilgi güvenliği konusunda çalışan çok sayıda şirket ve kurum, bilgi güvenliğinin sağlanmasına yönelik olarak birçok standart, yazılım ve program geliştirmiştir. Bunlar organizasyonlarda bilgi güvenliğinin nasıl sağlanacağı konusunda rehberlik yapmakta ve bilgi güvenliğinin sağlanabilmesi için farklı yöntemler ortaya koymaktadır.

Bilgi güvenliğine yönelik ilk standartlaşma çalışmaları İngiliz Standartları Enstitüsü (BSI) tarafından gerçekleştirilmiştir. BSI tarafından yayınlanan BS 7799 standardın ilk kısmı (BS 7799-1) 1995 yılında yayınlanmıştır. Standart, bilgi güvenliğinin sağlanmasında uygulanacak kontrolleri tanımlamaktadır. 1998 yılında yayınlanan standardın ikinci kısmı (BS 7799-2) ise bilgi güvenliği yönetim sisteminin kurulabilmesi için asgari seviyedeki gereksinimleri tanımlamaktadır. BS 7799-2 Standardı Uluslararası Standartlar Örgütü (ISO) tarafından kabul edilerek ve ISO/IEC 27001: 2005 olarak yayınlanmıştır. Bu standart bilgi güvenliği yönetim sisteminin kurulmasına yönelik olarak belgelendirme işleminin yapıldığı belgedir. BS 2299-1 Standardı ise yine ISO tarafından kabul edilerek ISO/IEC 27002: 2005 olarak yayınlanmıştır. (Dönel ve Dinçkan, 2007) Bu belge ise belgelendirme süreci için yardımcı doküman olarak kullanılmakta, rehber niteliği taşımaktadır.

ISO/IEC 27001: 2005 standardı 2013 ve son olarak 2017 yıllarında revizyona uğramış, 2017 yılı Mayıs ayı itibarıyla ISO/IEC 27001: 2017 standardı olarak adlandırılmaya başlamıştır. ISO 2005 yılı itibarıyla 27000 standartlar serisi oluşturmaya karar vermiş ve bu kapsamda günümüze dek 33 standart

oluşturulmuştur (ISO 27000 Series, 2018). Bu çalışmada belgelendirme için kullanılan ISO/IEC 27001:2017 standardı referans alınmıştır. Çalışmada ISO/IEC 27001: 2017 standardı EBYS'ler perspektifinden ele alınacaktır.

3. Elektronik Belge Yönetim Sistemleri (EBYS)

Elektronik ortama aktarılan ya da elektronik ortamda oluşturulan belgelerin; üretilmesi, işlenmesi, kullanılması ve tasfiyesini içeren bu süreci tanımlayan kavram, teknolojik gelişmelerle beraber kurumsal yapıda yaşanan değişimler sonucunda hayatımıza girmiştir. "Elektronik Belge Yönetim Sistemleri (EBYS), Avustralya Ulusal Arşivi (2005) tarafından 'İş etkinliklerini kanıtlama amacı güden elektronik olarak yaratılmış belgelerin yaratılması, kullanımı, devamlılığı ve imhasını yöneten otomatikleştirilmiş bir sistem' olarak tanımlanmıştır (Özdemirci ve diğerleri, 2013, s.14)."

Kurumlar için hayati öneme sahip olan EBYS'ler bünyesinde;

- Kurum personelinin kişisel bilgilerini,
- Kurumun idari yapılanmasına dair bilgileri,
- Kurum tarafından yürütülen iş süreçlerini,
- Kurum tarafından üretilen güncel ve geriye dönük belgeleri,
- Kurumun paydaşlarının bilgilerini barındırmaktadır.

"Genel bir ifadeyle EBYS'ler kuruma ait bilgiyi barındırır. Kurumun bilgi birikimi, bir başka deyişle kurumun belleği, o kurumun aynı zamanda geçmişten geleceğe taşınan gücünü belirleyen ve konumunu simgeleyen temel unsurdur" (Özdemirci ve diğerleri, 2013). Kurumsal bilginin taşıdığı değer göz önüne alındığında EBYS'lerin yönetiminin ne denli mühim olduğu ortaya çıkmaktadır. Temelde belgelerin yönetilmesi için oluşturulmuş olan sistem, iş akışı yönetimi, rapor yönetimi, doküman yönetimi, duyuru ve mesaj yönetimi gibi farklı bileşenlere sahiptir. Elbette tüm bileşenler ve sistem tek bir amaca hizmet etmektedir. Bu da kurumsal bilgilerin verimli bir şekilde yönetilmesidir.

Kurumsal bilgilerin yönetilmesi kadar bu yönetim işleminin güvenli ortamlarda yapılması da önem arz etmektedir. "Unutulmamalıdır ki, kurumsal yapılarda bilgi ve bilgi sistemlerine dönük temel beklentilerden birisi de güvenliktir (Külcü, 2018)." "Kurumsal bilginin rekabeti körükleyici, itici, üretken gücünü doğru ve yerinde kullanan kurumlar dünyanın her bölgesinde rekabet edecek duruma gelebilmektedirler (Odabaş, 2005). " Kurumsal bilgi yönetiminin bu derece önemli olduğu günümüzde kurumsal bilgilerin güvende olması ve güvenli şekillerde taşınması çok önemlidir.

Ayrıca en son Ekim 2015 yılında revize edilen TS 13298 Elektronik Belge ve Arşiv Yönetim Sistemi Standardında "Elektronik Doküman ve Belge Yönetim Sistemi, TSE-CCCS-PP-003 numaralı Koruma Profili uyumlu TS

ISO/IEC 15408: Ortak Kriterler standardından EAL 2 seviyesinde veya Temel Seviye Güvenlik Kriterinden belge almış olmalıdır. Eğer başvurulan ürüne ait belge yoksa ürün, ISO 17025 akreditasyonuna sahip veya Belgelendirme Kuruluşundan lisanslı Yazılım Test Laboratuvarları tarafından yapılan Temel Seviye Güvenlik Kriteri Değerlendirmesinden ""Başarılı"" olarak geçmiş olmalıdır" ifadesi yer almaktadır. Bu revizyon ile beraber standartta EBYS'lerde güvenlik tedbirleri zorunlu tutulmuştur. Çalışmanın bundan sonraki kısmında ISO/IEC 27001: 2017 standardı belgelendirme sürecinde EBYS'lere özel olarak oluşturulması gerekli görülen dokümanlara dair bilgi verilecektir.

4. EBYS'lerde Bilgi Güvenliği Yönetim Sistemi Kurma Çalışmaları

Bir kurumda ISO/IEC 27001:2017 standardı kapsamında BGYS kurulması sürecinin en önemli noktası, üst yönetimin desteğidir. Kurumda sürecin etkin ve verimli şekilde yürütülebilmesi üst yönetimin desteğine bağlıdır. Bunun için yöneticiler bilgi güvenliği kavramına dair bilinçlendirilmeli ve yöneticilerde konuya dair farkındalık oluşturulmalıdır. Sonrasında üst yönetim kurum içerisinde süreci yürütecek ekibi oluşturmalıdır. Kurumun BGYS Ekibi içinde EBYS yöneticisi ve çalışanları mutlaka yer almalıdır. Bu ekip içinde bilgi güvenliği sorumlulukları tanımlanmalı ve tahsis edilmelidir. Daha sonra oluşturulan bu ekip ile beraber kurum için bilgi güvenliği politikaları ve ilgili dokümantasyon hazırlanmaya başlanabilir.

4.1. Sistemsel Gereksinimler

Bilgi güvenliği çalışmaları genelde ilk olarak varlık envanterinin çıkarılmasıyla başlamaktadır. Fakat söz konusu EBYS'ler olduğunda dokümantasyona başlamadan önce yerine getirilmesi gereken bazı sistemsel gereksinimler bulunmaktadır. Bilgi Güvenliği Yönetim Sistemi kurulumu için önce aşağıda yer alan sistem gereksinimlerinin karşılanıp karşılanmadığı kontrol edilmelidir. Uygulanabilirlik Bildirgesi kapsamında ele alınan sistemlerde aşağıda yer alan maddeler uygun şekilde yerine getirilmelidir. (Tablo 1) Bu gereksinimlerin karşılanmaması sertifika denetimi sırasında uygunsuzluk verilmesine sebep olabilir.

Konu Başlığı	**Sistemsel Gereksinimler**		
Sisteme Giriş	9.3.1	Gizli kimlik doğrulama bilgisinin kullanımı	Kullanıcıların, gizli kimlik doğrulama bilgisinin kullanımında kurumsal uygulamalara uymaları şart koşulmalıdır.
	9.4.3	Parola yönetim sistemi	Parola yönetim sistemleri etkileşimli olmalı ve yeterli güvenlik seviyesine sahip parolaları temin etmelidir.

	9.4.2	Güvenli oturum açma prosedürleri	Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.
Erişim Hakları	9.4.1	Bilgiye erişimin kısıtlanması	Bilgi ve uygulama sistem fonksiyonlarına erişim, erişim kontrol politikası doğrultusunda kısıtlanmalıdır.
Kayıtların Tutulması	12.3.1	Bilgi yedekleme	Bilgi, yazılım ve sistem imajlarının yedekleme kopyaları alınmalı ve üzerinde anlaşılmış bir yedekleme politikası doğrultusunda düzenli olarak test edilmelidir.
	12.4.1	Olay kaydetme	Kullanıcı işlemleri, kural dışılıklar, hatalar ve bilgi güvenliği olaylarını kaydeden olay kayıtları üretilmeli, saklanmalı ve düzenli olarak gözden geçirilmelidir.
	12.4.2	Kayıt bilgisinin korunması	Kaydetme olanakları ve kayıt bilgileri kurcalama ve yetkisiz erişime karşı korunmalıdır.
	12.4.3	Yönetici ve operatör kayıtları	Sistem yöneticileri ve sistem operatörlerinin işlemleri kayıt altına alınmalı, kayıtlar korunmalı ve düzenli olarak gözden geçirilmelidir.
	18.1.3	Kayıtların korunması	Kayıtlar kaybedilmeye, yok edilmeye, sahteciliğe, yetkisiz erişime ve yetkisiz yayımlamaya karşı yasal, düzenleyici, sözleşmeden doğan şartlar ve iş şartlarına uygun olarak korunmalıdır.
	18.1.4	Kişi tespit bilgisinin gizliliği ve korunması	Kişiyi tespit bilgisinin gizliliği ve korunması uygulanabilen yerlerde ilgili yasa ve düzenlemeler ile sağlanmalıdır.
Test Ortamı	12.1.4	Geliştirme, test ve işletim ortamların birbirinden ayrılması	Geliştirme, test ve işletim ortamlar, yetkisiz erişim veya işletim ortamlarında değişiklik risklerinin azaltılması için birbirinden ayrılmalıdır.
	14.3.1	Test verisinin korunması	Test verisi dikkatli bir şekilde seçilmeli, korunmalı ve kontrol edilmelidir.

Tablo 1: Sistem Gereksinimleri

Sisteme Giriş: Bir EBYS'de bilgi güvenliğinin sağlanması için öncelikle uygun bir kimlik doğrulama mekanizması kullanılmalıdır. Belgeleri oluşturan, üzerinde iz bırakan kişilerin yaptıkları işlemlerin ve sistem içerisinde tüm hareketlerinin izlenebilmesi için ön koşul olan bu işlem, sistemde bilgi güvenliğinin sağlanabilmesi için ilk adımdır. Uygun bir kimlik

doğrulama mekanizması kullanılmalı, kullanıcı adı ve şifre doğrulamaları; SMS, mobil uygulamalar, e-imza vb. yöntemler aracılığı ile yapılmalıdır. Ayrıca parola yönetimi etkileşimli olmalı, parola oluşturma ya da sıfırlama işlemleri kişinin kendisi tarafından yapılmalıdır. Parolalar en az 8 karakterden oluşmalı, büyük ve küçük harfler, rakam ve "?, @, !, #, %, +" gibi özel karakterler içermelidir. Sistem bu parola politikasına uyumu kullanıcıya zorunlu tutmalıdır.

Erişim Hakları: Bir diğer önemli konu ise erişim hakları yönetimidir. Bu işlemler kurumsal verilerin kendi içinde mahremiyeti olduğu göz önüne alınarak, idari süreçlere uygun şekilde yürütülmelidir. Sistem içerisinde kuruma dair bilgi ve belgelerin yer alması sebebiyle, kullanıcı erişimleri sınırlandırılmalı, her kullanıcı sadece tanımlı olduğu birimde işlem yapabilmeli ve sadece o birimin belgelerini görebilmelidir. Sistem mimarisinin buna uygun şekilde yapılandırılmış olması gerekmektedir.

Kayıtların Tutulması: Kullanıcıların sistem içerisindeki hareketlerinin kayıt altına alınmasını konu alır. Bu işlem kısaca sisteme ait log kayıtlarının tutulması olarak ifade edilebilir. Log kayıtları, sistem içerisinde tanımlı olan tüm kullanıcıların hareketlerinin izlenmesi işlemidir. Bu kayıtlar bilgi güvenliği açısından tüm bilgi sistemlerinde olduğu gibi EBYS'ler için de hayati bir öneme sahiptir. "Sistem içerisindeki tüm olaylar kayıt altına alınmalı, kayıtlar korunmalı ve güvenlik açıklarının tespit edilebilmesi ve olay sonrası gerekli kanıtların oluşturulabilmesi için belirli aralıklarla gözden geçirilmelidir" (Koruma Profili, 2004). Kayıtlar hiçbir şekilde silinememeli, sistem yöneticileri de dâhil kimse tarafından değiştirilememelidir. Log kayıtları sistem içerisinde yürütülen süreçlerin delilidir. 6698 sayılı Kişisel Verilerin Korunması Kanunu uyarınca bilgi içeren tüm sistemlerin log kayıtlarının tutulması yasal olarak zorunlu hale gelmiştir. (Kişisel Veri Güvenliği, 2018) Bunlara ek olarak olası bir saldırı ya da afet durumunda sistem sürekliliğinin sağlanması ve işleyişin devam edebilmesi için tüm bu bilgiler yedeklenmelidir. Yedekleme işlemi bilgi içeren tüm sistemlerde hayati öneme sahiptir. Sistemin bunlara uygun şekilde yapılandırılmış olması gerekmektedir.

Test Ortamı: EBYS'lerde geliştirme amacıyla yapılan testlerin hangi koşullarda yapılması gerektiğini belirtir. Bir EBYS'nin versiyon testlerinin "canlı" sunucular üzerinde değil, farklı bir sunucu üzerinden yapılması gerekmektedir. Test verileri gerçeği yansıtması amacıyla "canlı" versiyonundan kopyalanabilir. Bu kopyalama işlemi EBYS içerisinde yer alan tüm verileri test sunucularına aktaracağından bu sunuculara erişim de kısıtlanmalıdır. Aynı şekilde bu verilerin korunması da en az canlı sunucularda yer alan verilerin korunması kadar önemlidir. Bu sebeple kopyalama işlemi çeşitli önlemler alınarak yapılmalıdır. Test için kullanılan veriler; maskeleme, şifreleme vb. uygun yöntemlerle korunarak kullanılmalı ve güvenliği sağlanmalıdır. (Çek, 2017)

4.2. EBYS'lerde İdari Süreçler Kapsamında Yapılması Gerekenler

EBYS'lerde Bilgi Güvenliği sürecinin yürütülebilmesi için gerekli teknik tedbirler alındıktan sonra BGYS kurulum süreci başlatılabilir. Öncelikle sisteme dair bir varlık envanteri çıkarılmalı, sahip olunan kişisel ve kurumsal bilgiler ortaya konulmalıdır. Sistemde, bilgi güvenliğini sağlanmanın amacının bu bilgilerin korunması olduğu gerçeği göz önüne alınarak, envanter formu içerisinde yer alan tüm varlıkların "varlık sahibi" ve "varlık sorumlusu" belirlenmelidir. Bu çalışmada EBYS içerisinde yer alan bilgi varlıkları da işlenmelidir. Resmi yazılar, formlar, kullanıcı bilgileri gibi bilgi varlıkları, envanter formunda değerlendirilmelidir. Envanterde yer alan varlıklar birbiri ile ilişkilendirilerek gruplandırılmalıdır. Sonrasında bir risk analizi dokümanı oluşturularak bu gruplar gizlilik, bütünlük ve erişilebilirlik unsurlarına göre derecelendirilmeli, varlık değerleri hesaplanmalı ve yüksek risk içeren bilgi varlıkları tespit edilmelidir. EBYS içerisinde yer alan bilgi varlıklarının yanında, kuruma verilen hizmet kapsamında EBYS yazılımı ve bu yazılımın temin edildiği firma/kuruluş da burada değerlendirilmelidir. Risk analizi sonucunda yüksek risk grubunda yer alan bilgi varlıklarına yönelik kalıcı ve iyileştirmeye yönelik tedbirler alınmalı ve sonuçlar sürekli olarak gözden geçirilmelidir.

Konu Başlığı	**Süreç Gereksinimleri**		
Sisteme Giriş	9.2.4	Kullanıcılara ait gizli kimlik doğrulama bilgilerinin yönetimi	Gizli kimlik doğrulama bilgisinin tahsis edilmesi, resmi bir yönetim prosesi yoluyla kontrol edilmelidir.
	9.4.2	Güvenli oturum açma prosedürleri	Erişim kontrol politikası tarafından şart koşulduğu yerlerde, sistem ve uygulamalara erişim güvenli bir oturum açma prosedürü tarafından kontrol edilmelidir.
Erişim Hakları	9.1.1	Erişim kontrolü politikası	Bir erişim kontrol politikası, iş ve bilgi güvenliği şartları temelinde oluşturulmalı, yazılı hale getirilmeli ve gözden geçirilmelidir.
	9.2.1	Kullanıcı kaydetme ve kayıt silme	Erişim haklarının atanmasını sağlamak için, resmi bir kullanıcı kaydetme ve kayıt silme prosesi uygulanmalıdır.
	9.2.2	Kullanıcı erişimine izin verme	Tüm kullanıcı türlerine tüm sistemler ve hizmetlere erişim haklarının atanması veya iptal edilmesi için resmi bir kullanıcı erişim izin prosesi uygulanmalıdır.

	9.2.3	Ayrıcalıklı erişim haklarının yönetimi	Ayrıcalıklı erişim haklarının tahsis edilmesi ve kullanımı kısıtlanmalı ve kontrol edilmelidir.
	9.2.5	Kullanıcı erişim haklarının gözden geçirilmesi	Varlık sahipleri kullanıcıların erişim haklarını düzenli aralıklarla gözden geçirmelidir.
	9.2.6	Erişim haklarının kaldırılması veya düzenlenmesi	Tüm çalışanların ve dış taraf kullanıcılarının bilgi ve bilgi işleme olanaklarına erişim yetkileri, istihdamları, sözleşmeleri veya anlaşmaları sona erdirildiğinde kaldırılmalı veya bunlardaki değişiklik üzerine düzenlenmelidir.

Tablo 2: Süreç Gereksinimleri-1

Envanter ve risk analizi dokümanı oluşturulduktan sonra süreçle ilgili diğer dokümantasyon işlemleri başlatılabilir (Tablo 2). Bilgi güvenliği söz konusu olduğunda her insanın sisteme açılan birer kapı olduğu gerçeği göz önünde bulundurularak sisteme giriş ile ilgili dokümantasyona öncelik verilmelidir. Sisteme giriş için kullanılan parola politikası ve bu parolaların kullanıcılara nasıl iletileceği tanımlanmalıdır. İlk parola verme, parola güncelleme gibi işlemler tüm aşamalarıyla ve anlaşılır biçimde tanımlanmalıdır. Kayıt işlemi sırasında kişisel bilgilerin işlenmesi sebebiyle veri işleyen pozisyonunda olan personel için sorumluluk yükleyici bir sözleşme hazırlanmalı ve ıslak imzalı nüshaları saklanmalıdır. Ayrıca kullanıcılara yönelik olarak güvenli oturum açma prosedürü/politikası hazırlanmalıdır. Bu doküman içerisinde kullanıcıların sisteme giriş için kullanabileceği tüm yöntemler tanımlanmalı ve uygun kullanım şekli adım adım aktarılmalıdır.

EBYS'lerde bilgi güvenliğini sağlamanın en temel yolu, yetkisiz kişilerin erişimlerini engellemek ve yetkisi olan kişilerin erişimlerini de ihtiyaca göre kısıtlamaktır (Erişim Kontrol Politikası, 2019)**.** EBYS'lerde bilgi güvenliğinin sağlanması söz konusu olduğunda Erişim Hakları Yönetimi büyük önem taşımaktadır. Erişim hakları ile ilgili teknik gereksinimlerin karşılanması bir EBYS'de bilgi güvenliğinin sağlanması için yeterli değildir. Teknik gereksinimlerin karşılanması ve akabinde süreç yönetiminin doğru bir şekilde yürütülmesi gerekmektedir. Erişim haklarının yönetimi özellikle büyük ve karmaşık yapıya sahip organizasyonlar için zorlu olabilmektedir. Bu sebeple sistem üzerinde yürütülen erişim hakları yönetiminin, organizasyonun özüne sadık olması, gerçek iş süreçlerini yansıtması gerekmektedir. Sürecin sadece

dokümante edilmesi bilgi güvenliğinin sağlanması için yeterli değildir. Sürecin kendisinin de bilgi güvenliği unsurlarına dikkat edilerek yürütülüyor olması gerekmektedir.

Bilgi güvenliği yönetim sistemi kurma çalışmaları kapsamında; kullanıcı hesaplarının yönetilmesi, kullanıcıların erişim izinleri, ayrıcalıklı erişim haklarının yönetimi, erişim haklarının gözden geçirilmesi, düzenlenmesi veya kaldırılması ve bilgiye erişimin kısıtlanması gibi süreçler tanımlanmalı ve dokümante edilmelidir. Bu kapsamda öncelikle Erişim Hakları Yönetim Politikası/Prosedürü oluşturulmalıdır. Bu dokümanda sisteme kayıt, güncelleme, pasif etme ve silme işlemlerinin nasıl yapıldığı, kullanıcılara nasıl ve hangi yollarla iletildiği tanımlanmalı ve ayrıntılı olarak açıklanmalıdır. Kullanıcı hesaplarının yönetimi tanımlandıktan sonra, süreç "kullanıcıların erişim hakları hangi ölçütlere göre belirleniyor, erişim izinleri nasıl veriliyor, hangi yöntemlerle iletiliyor" gibi sorulara cevap verecek şekilde ayrıntılarıyla aktarılmalıdır.

Erişim hakları EBYS'lerde roller ve rollere atanan aksiyonlar aracılığı ile yönetilmektedir. Roller ve rollere atanan aksiyonlar sistem üzerinde bilgi ve belgelere yetkisiz erişimi ve işlem yapmayı engellediği için bilgi güvenliği açısından büyük önem taşır. Bu sebeple sistem içerisinde hangi rol hangi kullanıcıya ne sebeple veriliyor, rolün verilmesi için hangi koşullar yerine getirilmeli gibi bilgiler de dokümante edilmelidir.

Sistem içerisinde hangi rolün hangi aksiyona sahip olduğu bilgisi de bilgi güvenliği için önemli noktalardan birisidir. Bu sebeple tüm rollerin sahip olduğu aksiyonlar tanımlanmalı, hangi rolün hangi işlem için verildiği ve sistem içerisinde hangi alanları görüp işlem yapabildiği açıklanmalı ve dokümante edilmelidir.

Kişilerin sistem içerisinde yapabildikleri işlemler, roller ve rollere atanan/tanımlanan aksiyonlar aracılığı ile sınırlandırılabilir fakat erişim söz konusu olduğunda roller bilgi güvenliğini tam anlamıyla sağlayamaz. Kullanıcıların birim bazında da sınırlandırılması gerekmektedir. Tüm kullanıcılar sadece görevli oldukları birimlerin belgelerini görebilmeli, sadece o birimlerde işlem yapabilmelidir. Bu sebeple kullanıcı tanımlama işlemleri tüm bu dinamikler göz önüne alınarak yapılmalı ve sonrasında dokümante edilmelidir.

Organizasyonlarda bazı kullanıcılara ayrıcalıklı haklar verilmektedir. Bunlar kişilerin görevleri sebebiyle diğer kullanıcılardan daha fazla işlem yapmasını ya da daha fazla alan görmesini sağlayan roller ya da erişim izinleri olabilir.

Ayrıcalıklı erişim haklarının yönetimi de bilgi güvenlinin sağlanması konusunda dikkat edilmesi gerekli olan noktalardan biridir. Sistem içerisinde bu hakların ne olduğu ve kimlere verildiği açıklanmalı, ayrıcalıklı haklara sahip kullanıcılar listelenmeli ve görevli personel tarafından kurumun belirlediği uygun zaman aralıklarıyla takip edilmelidir.

Kullanıcı erişim hakları bilgi güvenliğinin sağlanmasında temel yapıtaşlarından biridir. Bu sebeple erişim haklarının gözden geçirilmesi, düzenlenmesi veya kaldırılması işlemleri düzenli aralıklar ile kontrol edilmeli, kurumdan/birimden ayrılan personelin ilgili rolleri ve birimleri pasif edilmelidir. Bu işlemin hatasız yürütülmesi ve düzenli olarak takip edilmesi gerekmektedir. Bu sebeple pasif edilme işlemlerinin takip edildiği ayrı bir doküman hazırlanmalı ve belirli aralıklarla ilgili personel tarafından kontrol edilmelidir. Erişim haklarının düzenlenmesi ve dokümante edilmesinden sonra diğer gereksinimler için çalışmalar yürütülebilir (Tablo 3).

BGYS Süreci Yürütülürken Dikkat Edilmesi Gereken Noktalar (Dokümantasyon ve Eğitimler)	
7.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	Kuruluştaki tüm çalışanlar ve ilgili olduğu durumda, yükleniciler, kendi iş fonksiyonları ile ilgili, kurumsal politika ve prosedürlere ilişkin uygun farkındalık eğitim ve öğretimini ve bunların düzenli güncellemelerini almalıdırlar.
7.3.1 İstihdam sorumluluklarının sonlandırılması veya değiştirilmesi	İstihdamın sonlandırılması veya değiştirilmesinden sonra geçerli olan bilgi güvenliği sorumlulukları ve görevleri tanımlanmalı, çalışan veya yükleniciye bildirilmeli ve yürürlüğe konulmalıdır.
11.2.9 Temiz masa temiz ekran politikası	Kâğıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.
17.1.2 Bilgi güvenliği sürekliliğinin uygulanması	Kuruluş, olumsuz bir olay süresince bilgi güvenliği için istenen düzeyde sürekliliğin sağlanması için prosesleri, prosedürleri ve kontrolleri kurmalı, yazılı hale getirmeli, uygulamalı ve sürdürmelidir.

Tablo 3: Süreç Gereksinimleri- 2

EBYS içerisinde kullanıcıların kabul edilebilir kullanımının nasıl olduğu tanımlanmalıdır. Bu işlem EBYS özelinde bir "Kabul edilebilir kullanım dokümanı" oluşturmak şeklinde ya da genel olarak hazırlanan dokümanın içerisinde EBYS'ler için özel maddeler eklemek şeklinde olabilir. Bu doküman içerisinde EBYS ile ilgili tüm program, yazılım ya da araçların kabul edilebilir kullanımları tanımlanmalıdır.

Bilgi güvenliği devamlılık gerektiren bir süreçtir. Sistem her daim canlı kalmalı, bilgi güvenliğini sağlamaya yönelik çalışmalar sürekli olarak yürütülmelidir. Tüm bunlara ek olarak insan faktörü de unutulmamalıdır.

EBYS'leri yöneten ve kullanan tüm kullanıcılar bilgi güvenliği perspektifinde sisteme açılan birer kapıdır. Bu sebeple güvenliğin sağlanması için öncelikle personel bilinçlendirilmeli, farkındalık eğitimleri verilmelidir. Farkındalık eğitimleri içerisinde kurumun sahip olduğu EBYS'nin güvenliğinin sağlanmasının ne derece mühim olduğu vurgulanmalı, kullanıcı bilgilerinin kesinlikle paylaşmaması gerektiğinin altı çizilmelidir. Temiz masa temiz ekran politikası ile beraber EBYS'ye giriş için kullanılan parolaların ekran ya da masa üzerinde tutulmaması gerektiği hatırlatılmalıdır. Ayrıca istihdamın sonlanması durumunda personelin ilişiğinin kesilebilmesi için EBYS üzerindeki tüm erişim haklarının pasif edildiğine dair bir belge oluşturulmalı ve tüm personel buna uygun hareket etmelidir.

Bilgi güvenliğinde sürekliliğin sağlanması EBYS'ler söz konusu olduğunda hayati öneme sahiptir. Sürecin sekteye uğraması, belgelerin kısa bir süreyle ulaşılmaz olması ya da yetkisiz kişilerce erişime açılması bilgi güvenliğinin sağlanması kapsamında yapılan tüm çalışmaları işlevsiz kılabilir. Kurumun sahip olduğu bilgi varlıkları ve değeri göz önüne alındığında BGYS'nin sürekliliğinin sağlanmaması kurum adına kötü sonuçlar doğurabilir. Bu sebeple süreklilik konusunda gerekli testler yapılmalı ve konuyla ilgili görevli/yetkili kişiler belirlenmelidir. Olası bir olumsuz durumda neler yapılacağı, kimlerin müdahale edeceği gibi kritik noktalar saptanmalı ve süreç ayrıntılı şekilde dokümante edilmelidir.

Tüm bu çalışmalar sonucunda etkin bir BGYS kuran kurumların, EBYS özelinde aşağıda yer alan konularda dokümanlarının olması ve bunların bilgi güvenliği esasına uygun şekilde yürütülüyor olması beklenir. Bunlar;

- Kullanıcı Erişim Hakları Yönetimi,
    - Kullanıcı Hesaplarının Yönetimi,
    - Kullanıcılara Ait Gizli Kimlik Doğrulama Bilgilerinin Yönetimi,
    - Erişim Haklarının Gözden Geçirilmesi, Düzenlenmesi veya Kaldırılması,
    - Bilgiye Erişimin Kısıtlanması,
- Ayrıcalıklı Erişim Haklarının Yönetimi,
- Erişim Kontrol ve Takip Listesi,
- Güvenli Oturum Açma Parola Yönetim Sistemi,
- Kabul Edilebilir Kullanım Koşulları,
- Rol - Aksiyon Tablosu,
- Veri İşleyen Pozisyonundaki Personelin Sorumluluk Sözleşmesi.

Kurumlarda yürütülen Bilgi Güvenliği Yönetim Sistemi kurma çalışmaları neticesinde birçok doküman oluşturulur. Bazı dokümanlar direkt olarak Elektronik Belge Yönetim Sistemleri için oluşturulmasa bile EBYS'lere dair

bilgiler içerebilir. Bu sebeple BGYS kurma çalışmaları sonucunda oluşturulan tüm dokümanlar personel ile paylaşılmalı ve personelin bundan haberdar olması sağlanmalıdır.

5. Sonuç

Ele alınan tüm bu tedbirler etkin bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmak için yeterli olabilir fakat bilgi güvenliği devamlılık gerektiren bir süreçtir. (Canbek ve Sağıroğlu, 2006). Bu sürecin yürütülebilmesi için gerekli teknik tedbirler sağlandıktan sonra bilgi güvenliği politikaları, prosedürleri, talimatları ve formları oluşturulmalı, risk analizleri gerçekleştirilmeli, bu riskleri önlemek adına tedbirler alınmalı ve tüm bunlar sürekli gözden geçirilmelidir. Sistem her daim canlı kalmalı, bilgi güvenliğini sağlamaya yönelik çalışmalar sürekli olarak yürütülmelidir. Tüm bunlara ek olarak insan faktörü de unutulmamalıdır. "Bilginin korunmasına çalışıldığı ilk günden itibaren güvenlik zincirinin en zayıf halkasını her zaman insanlar oluşturmuşlardır. Birçok teknik veya teknik olmayan güvenlik kontrolleri uygulansa dahi bu kontroller saldırganlar tarafından en zayıf halka olan insan faktörü kullanılarak çeşitli yöntemlerle aşılabilmektedir" (Barrett, 2003; Akt. Vural ve Sağıroğlu, 2008). İnsan faktörüne bağlı oluşabilecek güvenlik riskleri hiçbir zaman tamamen ortadan kaldırılamamaktadır. Bu etkenlerin tamamının bilgi güvenliği söz konusu olduğunda birbirlerini tamamlayıcı özellikte olduğu unutulmamalıdır. Kurumlar bilgilerinin güvenliğini ancak tüm bu etkenleri göz önüne alarak planlama yaptıkları takdirde sağlamaya çalışabilirler.

Bilgi güvenliğinin sağlanması kurumlara birçok avantaj sağlar. EBYS'ler özelinde bakıldığında bu avantajlardan en büyüğü elbette kurumun belleğinin koruma altına alınması, süreçlerin güven içinde yürütülmesidir.

Bunlara ek olarak,

- Bilgi güvenliği sürecinde, EBYS içerisinde yer alan bilgi varlıkları tanımlanır, bu sayede kurum sahip olduğu bilgi varlıklarının ve bunların değerinin farkına varır,
- Bilgi güvenliği ihlali durumlarında sistemi koruyarak kurumun prestij kaybının önüne geçer,
- Sisteme dair riskler analiz edilir ve işlenerek etkileri azaltılır,
- Sürecin yürütülmesiyle beraber sistem performansı izlenir ve geliştirilir, sürekli iyileştirme yapabilmek için imkân verir,
- Her türlü veri kaybı ihtimallerini minimize eder,
- Yedekleme ve diğer bilgi güvenliği tedbirleri ile beraber EBYS'lerde iş sürekliliği sağlanır, kurumsal süreçlerin aksamasının önüne geçilir.
- Personel ve kurumun tüm paydaşlarına güven verir,
- Yasal tepkileri önler, uyumluluk sağlar.

Bulunduğumuz çağa da ismini veren bilginin, artık ekonomik bir meta olarak görüldüğü, bilgiyi elinde tutanların güçlü olarak değerlendirildiği unutulmamalıdır. EBYS'lerin içerdiği kurumsal bilginin önemi ve değeri, olası olumsuz durumlarda kurumun yaşayacağı prestij kaybı göz önüne alındığında EBYS'lerde bilgi güvenliğinin sağlanmasının ne denli mühim olduğu anlaşılmaktadır.

Kaynakça

Atılgan, D. (2009). Bilgi yönetimi kavramı ve gelişimi. Türk Kütüphaneciliği, 23(1), 201-212. Erişim adresi: http://www.tk.org.tr/index.php/TK/article/view/467

Başaranoğlu, E. (2016). Bilgi Güvenliği Unsurları. Erişim adresi: https://www.siberportal.org/blue-team/securing-information/concepts-of-information-security/

Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. Politeknik Dergisi, 9(3). Erişim adresi: https://dergipark.org.tr/download/article-file/384578

Çek, E. (2017). Kurumsal bilgi güvenliği yönetişimi ve bilgi güvenliği için insan faktörünün önemi (Doctoral dissertation, İstanbul Bilgi Üniversitesi).

Elektronik Doküman ve Belge Yönetim Sistemi Koruma Profili (Sürüm 1.3.1). (2014). Türk Standardları Enstitüsü (TSE). Erişim adresi: https://statik.tse.org.tr/upload//tr/dosya/icerikyonetimi/2231/09012015111018-3.pdf

Elektronik İmza Kanunu. (2004). Kanun no: 5070. T.C. Resmî Gazete, 15.01.2004. Erişim adresi: http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5070.pdf

Erişim Kontrol Politikası. (2019). *BGYS Politikaları içinde.* BEYAS Koordinatörlüğü.

Gülmüş, M. (2010) Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. (Yüksek Lisans Tezi). Erişim adresi: http://dspace.yildiz.edu.tr/xmlui/bitstream/handle/1/7782/0047315.pdf?sequence=1&isAllowed=y

ISO 27000 Series of Standards. (2018). IT Governance. Erişim adresi: https://www.itgovernance.co.uk/iso27000-family

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı. (2013). Ankara: Türk Standardları Enstitüsü (TSE).

Kişisel Veri Güvenliği Rehberi. (2018). Kişisel Verileri Koruma Kurumu. Ankara: KVKK Yayınları. Erişim adresi: https://www.kvkk.gov.tr/yayinlar/veri_guvenligi_rehberi.pdf

Külcü, Ö. (2018). Kurumsal Bilgi Yönetimi ve Belge Yönetimi: Organizasyonlarda Bilgi ve Belge Yönetimi Sistemlerinin Temel İlkeleri. İstanbul: Hiperlink Yayınları

Odabaş, Hüseyin. (2005). "Bilgi Yönetimi Sistemi". Bilgi Çağı, Bilgi Yönetimi ve Bilgi Sistemleri. Ed.: Coşkun Can Aktan ve İstiklal Y. Vural. Konya: Çizgi Kitabevi.

Önel, D. ve Dinçkan, A. (2007). Bilgi Güvenliği Yönetim Sistemi Kurulumu. Kocaeli: Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü.

Özdemirci, F., Bayram, Ö. G., Torunlar, M., Saraç, S. ve Yalçınkaya, B. (2013). Elektronik belge yönetimi ve arşivleme sistemi: Geçiş süreci ve uygulama yönetimi.

TS ISO/IEC 27001 Bilgi güvenliği yönetim sistemleri- Gereksinimler. (2013). Ankara: Türk Standardları Enstitüsü.

Vural, Y., ve Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23(2). Erişim adresi: https://dergipark.org.tr/download/article-file/757