ISO 27001 Bilgi Güvenliği Yönetim Sistemi ve Ağ Yönetimi Politikası

Dr. İzzet Gökhan ÖZBİLGİN, Mustafa ÖZLÜ

***Özet* — Bilgisayar ağları dinlenme, verilerin ele geçirilmesi, zararlı kodların bulaşması gibi bir takım tehditlerle karşı karşıyadır. Ağ güvenliğini gerçekleştirmemiş kurumlar ve bireyler yetkisiz sızma, hizmet kesintisi, yasa ve yönetmeliklere uyumsuzluk gibi problemler yaşayabilirler. Tehditlerden korunmak için ağı kullanan sistemler ve uygulamalar, güvenliği sağlamak amacıyla uygun şekilde yönetilmeli, denetlenmeli ve tüm ağ hizmetlerinin güvenlik özellikleri, hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalıdır. ISO/IEC 27001 Bilgi Teknolojileri - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi - Gereksinimler Standardı (ISO 27001 BGYS) uluslar arası kabul edilmiş bir bilgi güvenliği yönetim sistemi standardı olup, bu standardın içindeki birçok kontrol ağ güvenliğini ele almaktadır. Çeşitli çalışmalarda ağ yönetimine ve güvenliğine ilişkin hususlar ele alınmış olmakla birlikte, bu çalışmada ağ yönetimindeki güvenlik gereksinimleri ISO 27001 BGYS kapsamında ele alınacak, ISO 27001 BGYS'de yer alan ağa ilişkin güvenlik kontrollerini içeren bir politikada ele alınması gereken hususlara yer verilmiştir.**

***Anahtar Kelimeler* — Ağ Güvenliği, ISO 27001, Bilgi Güvenliği**

1. GİRİŞ

Gelişen ve değişen dünyamızda bilginin önemi günden güne artmakta, artan bu önem bilgiye yönelik bir takım tehditleri de beraberinde getirmektedir. Çoğu zaman göz ardı edilen bu tehditler kişileri ve kurumları telafisi zor problemlerle karşı karşıya bırakabilmektedir. Bilgi bugün hayatımızda sadece yazılı olarak değil, çok farklı biçimlerde yer bulmaktadır. Bilginin üretilirken, saklanırken ve iletilirken farklı ortamlarda bulunması bilgiye yönelik tehditleri karmaşıklaştırmakta ve farklılaştırmaktadır.

Bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini hedefleyen tehditlerle mücadele için bilgi güvenliğinin sağlanmış olması gerekmektedir. Bilgi güvenliği; karşılaşılabilecek tehditleri, bu tehditler sonucunda riskleri belirleme, işlerin devamlılığını sağlama, yaşanabilecek problemlerde kayıpları aza indirme, problemlerden öğrenme, kurumun varlıklarının her koşulda gizliliği, erişebilirliği ve bütünlüğünü korunma amaçları taşımaktadır. Bilgi güvenliğinin sağlanması amacı doğrultusunda bilgiye sürekli erişilebilirliği, bilginin gizliliği ve bütünlüğünü korumayı amaçlayan Bilgi Güvenliği Yönetim Sistemi (BGYS) kavramı ortaya çıkmıştır.

Bir bilgisayardaki bilgilerin korunması her şeyden önce o bilgisayarın içerisinde bulunduğu ağın korunmasına bağlıdır. Bu da ağ güvenliğinin önemini ortaya çıkarmaktadır. Ağda güvenlik faaliyetlerin yürütülebilmesi için değerli bilgilerin kullanıma hazır olması ve tehditlere karşı korunması gerekmektedir. Ağ güvenliği, özellikle Internet üzerinden çalışan işletmeler için bir zorunluluğa dönüşmüştür. Müşteriler, satıcılar ve iş ortakları, işletmelerden veya kurumlardan paylaştıkları bilgilerin korunmasını bekleyecektir. Ağ güvenliği, bir işi yürütmek için bir zorunluluğa dönüşürken, birden çok şekilde kendisini amorti etmektedir[1].

Bu çalışmanın ilerleyen bölümlerinde önce uluslararası bir standart olan ISO/IEC 27001 BGYS ele alınacaktır. Ardından ISO 27001 BGYS'de yer alan ağa ilişkin kontrolleri kapsayan bir ağ yönetimi politikasına yer verilecek ve değerlendirmeler yapılacaktır.

2. ISO 27001 Bİlgİ Güvenlİğİ YönetİM Sİstemİ

Bilgi güvenliği, yazılı, sözlü, elektronik ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişebilirlik bakımından güvence altına alınması ve bu güvence durumunun sürekliliğinin sağlanmasıdır.

Bilgi güvenliği, bilginin gizliliğini, bütünlüğünün korunmasını sağlar, işin aksamamasını ve verilerin kaybolmamasını amaçlar. Bilgi güvenliği ayrıca bilgiye yetkisiz kişilerin ulaşmasını engellemeyi hedefler ve sonuç olarak kurumun çalışmalarında verim artışı sağlar.

Bilgi sistemlerinin hayata geçmesiyle ortaya çıkan depolama, işleme, bilgiye erişebilme imkânlarının artması, bilinçli veya bilinçsiz hataların çok önemli sonuçlar doğurması, izinsiz erişimler, bilginin yetkisiz imhası, yetkisiz değiştirilmesi ve yetkisiz görülmesi ihtimallerinin artması gibi problemler nedeniyle bilgi güvenliği kavramı gündeme gelmektedir.

Günümüzde ise bilgi teknolojilerinin daha çok günlük hayata girmesi, bilgi teknolojilerini daha çok kişinin

kullanması, bilgi teknolojisi ürünlerinin hızlı bir şekilde üretilmesi ve sistemlerin hızlı geliştirilmesinden kaynaklanabilecek güvenlik açıklıkları ortaya çıkmaktadır. [2]

Bilgi hangi biçime girerse girsin veya ne tür araçlarla paylaşılır veya depolanır olursa olsun, her zaman uygun bir şekilde korunmalıdır. Kurumların sahip oldukları bilgi, çok çeşitli tehditlere karşı açık durumdadır. Bu tehditler ve yol açtıkları zararın boyutları giderek artmaktadır.

Bilgi sistemlerinin çoğu, bilgi saklanırken, paylaşılırken, gönderilirken güvenlik kaygıları düşünülerek tasarlanmamıştır. Bu sistemler bu nedenle pek çok güvenlik açığı barındırmaktadırlar.

Bilgi sistemleri birçok güvenlik ihlal olayıyla karşı karşıyadır. Bilgi sistemine ve bilgiye yetkisiz erişim, kullanımda dikkatsizlik ve uygunsuzluk, kaybolma, çalınma ve servislerin kesilmesi başlıca ihlal olaylarıdır. BGYS, bilgi güvenliği ihlali ve buradan doğacak kayıpların riskini minimize etmek için kurulur. BGYS, bilgi güvenliğini kurmak, işletmek, izlemek ve geliştirmek için iş riski yaklaşımına dayalı, dokümante edilmiş, işlerliği ve sürekliliği garanti altına alınmış bir yönetim sistemidir.

BGYS kurumunuzdaki tüm bilgi varlıklarının değerlendirilmesi ve bu varlıkların sahip oldukları zayıflıkları ve karşı karşıya oldukları tehditleri göz önüne alan bir risk analizi yapılmasını gerektirir [3].

BGYS, bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir. BGYS'nin ihtiyaç duyduğu gereksinimlere cevap vermek için çok sayıda standart vardır. Bunların en önde geleni ISO 27001 standardıdır.

2.1. PUKÖ Modeli

ISO 27001 kurumların bilgi güvenliği yönetim sistemi kurmaları için gereklilikleri tanımlayan tek denetlenebilir BGYS standardıdır. ISO 27001 ülkelere göre özel tanımlar içermeyen, genel tanımların bulunduğu uluslararası standardıdır. ISO 27001 standardı; kuruluşların kendi bilgi güvenlik sistemlerini sağlamasını mümkün kılan teknoloji tarafsız, satıcı-tarafsız yönetim sistemleri için bir çerçeve sağlar.

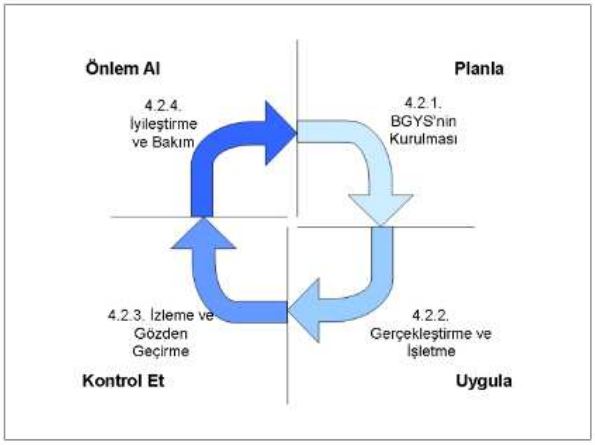
ISO 27001, kuruma uygun politikalar, prosedürler ve kılavuzlar oluşturmaya yol gösteren uluslar arası kabul görmüş yapısal bir metodoloji sunar. ISO 27001 sertifikası, kurumların güvenlik seviyesine ve kurumun konuya ciddi yaklaşımına ilişkin bir göstergedir.

Bilgi güvenliği yönetimi konusunda ilk standart British Standard Institute (BSI) tarafından geliştirilen BS 7799'dur. BS 7799 "Pratik Kurallar" ve "BGYS Gerekleri" başlıklı iki kısımdan oluşmaktaydı. BS 7799 birinci kısım daha sonra ISO tarafından 2000 yılında "ISO 17799" olarak kabul edilmiştir. 2002'de BSI; BS 7799-2'yi çıkartmıştır. ISO, 2005 yılında ISO/IEC 1799:2005'i ve BS 7799-2'nin yeni hali olan ISO/IEC 27001:2005'i yayınlamıştır. ISO 27001, 2005 yılında yayınlanmasıyla yürürlüğe girmiş ve ISO/IEC 27000 standart serisi altında yerini almıştır.

Türkiye'de ise, ISO tarafından kabul edilen, ISO/IEC 27001:2005 standart esas alınarak, TSE Bilgi Teknolojileri ve İletişim İhtisas Grubunca hazırlanmış ve TSE Teknik Kurulu'nun 2 Mart 2006 tarihli toplantısında Türk Standardı olarak kabul edilerek, "TS ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimleri" adıyla yayınlanmıştır[4].

ISO 27001 yaşayan, dolayısı ile tehdit ve saldırılara reaksiyon gösteren ve kendini yenileyen bir bilgi güvenliği sisteminde yer alması gereken öğeleri tanımlamaktadır [5]. ISO 27001, BGYS'yi kurmak, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için standart proses yaklaşımını benimsemiştir. Bu proses yaklaşımı güvenlik önlemlerinin belirlenip kurulması, uygulanması, etkinliğinin gözden geçirilmesi ve iyileştirilmesi süreçlerini ve bu süreçlerin sürekli olarak tekrarlanmasını içerir. Bu süreçler Planla, Uygula, Kontrol et, Önlem al (PUKÖ) döngüsünden oluşan bir model olarak da ortaya konmuştur.

BGYS'de kurum kendine bir risk yönetimi metodu seçmeli ve risk işleme için bir plan hazırlamalıdır. Risk işleme için standardda öngörülen kontrol hedefleri ve kontrollerden seçimler yapılmalı ve uygulanmalıdır. Şekil 1'de gösterilen PUKÖ Modeli uyarınca risk yönetimi faaliyetlerini yürütmeli ve varlığın risk seviyesi kabul edilebilir bir seviyeye geriletilene kadar çalışmayı sürdürmelidir [2].

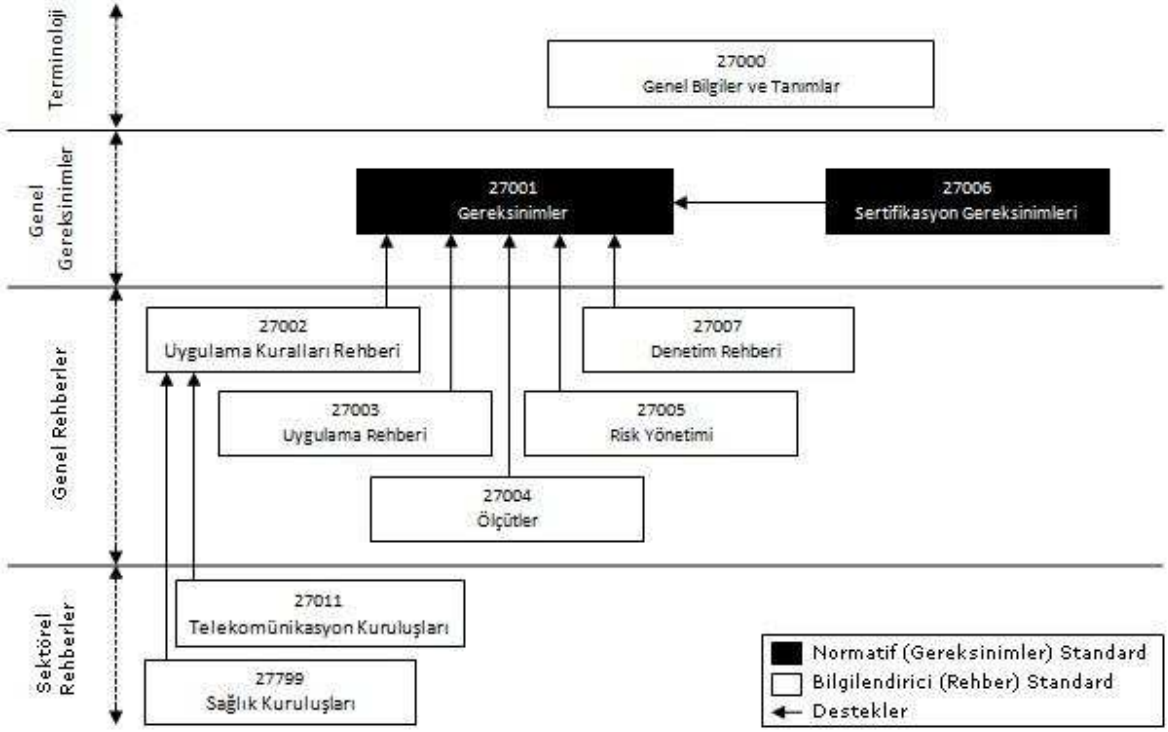


Şekil 1- BGYS'nin PUKÖ Modeli [9]

PUKÖ Model'inin süreçleri aşağıdaki gibidir;

Planla: BGYS'nin kurulması : Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin kurulması.

Uygula: BGYS'nin gerçekleştirilmesi ve işletilmesi: BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi.
Kontrol Et: BGYS'nin izlenmesi ve gözden geçirilmesi: BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.
Önlem Al: BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi: BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi [6].



Şekil 2- ISO 27000 Standart Ailesi [6]

2.2. ISO 27000 Ailesi

Bilgi güvenliği ile ilgili olarak ISO 27000 serisi güvenlik standartları, (Şekil 2) kullanıcıların bilinçlenmesi, güvenlik risklerinin azaltılması ve de güvenlik açıklarıyla karşılaşıldığında alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır. Bu standartlar temel ISO'nun 9000 kalite ve 14000 çevresel yönetim standartlarıyla da ilgilidir. [6]

ISO 27000 standardı, ISO 27000 standartlar ailesi ile ilgili kavramların açıklanmasını sağlayan ve bilgi güvenliği yönetimine yönelik temel bilgileri içeren bir standarttır. ISO 27000 standartlarının büyük bir çoğunluğu bilenen, diğerleri ise basım aşamasında olan standartlar olarak verilebilir.

ISO/IEC 27000 standart serisi altında yer alan ve ISO 27001 için gereken güvenlik kontrollerini içeren standart; ISO/IEC 27002:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzu'dur. Bu standardın önceki adı ISO/IEC 17799:2005'dir. 1 Temmuz 2007 tarihinde, ISO tarafından yapılan teknik bir düzenlemeyle ISO/IEC 17799:2005 standardının adı, ISO/IEC 27002:2005 (ISO 27002) olarak değiştirilmiştir. [4]

ISO 27000	BGYS ile ilgili olarak genel bilgiler verilmekte, bu sistemde kullanılan kavramlar tanımlanmaktadır. 2009 yılında yürürlüğe girmiştir.
ISO 27001	BGYS ile ilgili **gereksinimler** belirtilmektedir. Bu standart BGYS kuracak kuruluşların uyum göstereceği standarttır. 2005 yılında yürürlüğe girmiştir.
ISO 27002	BYGS ile ilgili gereksinimlerin karşılanması konusunda **rehberlik** eden, en iyi uygulamaları içeren standarttır. 2005 yılında yürürlüğe girmiştir.
ISO 27003	BGYS sisteminin uygulanmasıyla ilgili **rehberlik** yapmayı amaçlayan standarttır. 2009 yılında yürürlüğe girmiştir.
ISO 27004	BGYS'nin ölçümü ile ilgili kriterler açısından **rehber** standarttır. 2009 yılında yürürlüğe girmiştir.
ISO 27005	BGYS'nin önemli bir süreci olan risk yönetimi ile ilgili **rehber** standarttır. 2008 yılında yürürlüğe girmiştir.
ISO 27006	BGYS sertifikasyonu ve denetimi ile ilgili **gereksinimlerin** belirtildiği standarttır. 2007 yılında yürürlüğe girmiştir.

ISO 27007	BGYS denetimlerine yönelik **rehber** standarttır. Hala geliştirilme aşamasındadır.
ISO 27011	Telekomünikasyon kuruluşları açısından BGYS'nin uygulanışına yönelik rehber standarttır.
ISO 27799	Sağlık kuruluşları açısından BGYS'nin uygulanışına yönelik rehber standarttır. 2008 yılında yürürlüğe girmiştir.

Tablo 1- ISO 27000 Standart Ailesi

2.3. Güvenlik Kontrol Alanları

ISO 27001 BGYS standardı 39 kontrol hedefi ve 133 kontrol içeren toplam 11 güvenlik kontrol alanından oluşmaktadır. Burada geçen "kontrol"den kasıt politika, prosedür, rehber, pratikler veya organizasyon yapısı gibi risk yönetim araçları ve "kontrol amacı" ise kontrollerin uygulanması sonucu elde edilecek durumdur [7]. Aşağıda kısaca açıklanan bu alanların her birinin kurumlara nasıl uygulanacağına yönelik rehber bilgiler ise ISO 27002 standardında ele alınmaktadır:

1- Güvenlik Politikası: Bilgi güvenliği için yönetimin desteğini ve katılımını sağlamak, bilgi güvenliğinin önemini vurgulamak

2- Bilgi Güvenliği Organizasyonu: Bilgi güvenliğinin koordinasyonu ve yönetimi için bir yönetim çerçevesi geliştirmek, bilgi güvenliği için sorumlulukları tahsis etmek

3- Varlık Yönetimi: Tüm kritik veya hassas varlıklar için uygun bir koruma düzeyi belirlemek

4- İnsan Kaynakları Güvenliği: Kullanıcı eğitimini ve bilincini teşvik ederek hırsızlık, dolandırıcılık veya bilgisayar kaynaklarının kötüye kullanılma riskini azaltmak

5- Fiziksel ve Çevresel Güvenlik: Kuruluşun tesislerindeki bilgi işlem olanaklarına yetkisiz erişimi önlemek ve bilgilerin zarar görmesini engellemek

6- Haberleşme ve İşletim Yönetimi: Bilgi işlem tesislerinin uygun ve güvenli kullanımını sağlamak ve olay müdahale prosedürleri geliştirerek riski ve sonuçlarını azaltmak

7- Erişim Kontrolü: Yetkisiz erişimlerin tespiti ve ağ sistemlerinin korunması için gerekli kontrol faaliyetlerini sağlamak

8- Bilgi Sistemleri Edinim, Geliştirme ve Bakımı: İşletim sistemleri ve uygulama yazılımlarını bilgi kaybına karşı güncellemek ve kayıpları engellemek

9- Bilgi Güvenliği İhlal Olayı Yönetimi: Etkin bir bilgi güvenliği sağlamak için olayların zamanında tespit etmek ve gerekli önlemleri almak

10- İş Sürekliliği Yönetimi: Kritik arızalar, olaylar, doğal afetler, felaketlerden kaynaklanan kesintilere karşı hızla müdahale edilebilmek için kapasite geliştirme faaliyetleri gerçekleştirmek

11- Uyum: Mevcut güvenlik politikalarının tüm yasalara ve yönetmeliklere uygun olduğundan ve üst yönetim onayından geçtiğinden emin olmak [8]

3. ISO 27001 VE AĞ YÖNETİMİ POLİTİKASI

Dokümante edilmiş bir BGYS hedefleyen ISO 27001 BGYS, Ağ Yönetimi Politikası (AYP)'nın yazılı hale getirilmesini, ilgili tüm taraflara duyurulmasını ve kurum içinde kullanılabilir hale getirilmesini beklemektedir. AYP, kısaca bilgisayar ağının güvenliğini ilgilendiren her türlü bileşenin yönetimi ile ilgili stratejinin resmi şekilde yazılı olarak ifade edilmesi olarak tanımlanabilir [9]. Ne kadar iyi teknik önlemler alınmış olursa olsun, AYP hazırlanmamış bir kurumda güvenliğin temel ilkeleri olan gizlilik, erişebilirlik ve bütünlüğün tam olarak sağlandığını söylemek mümkün değildir. Buna en kolay örnek bilgisayar ağlarını tasarlarken ya da yönetirken her zaman önleyici kontrollerin hesaba katılması, fakat tehditler gerçekleştiğinde bununla ilgili neler yapılacağının, kimlerin yapacağının veya yaşanan bu olayların kayıt altına alınarak ders çıkarılmasının tam olarak sağlanmamasıdır.

Bilgi güvenliği yönetim sisteminin önemli hususlarından biri kurum için kritik olan bilginin yol aldığı cihazların, yolların, yazılımların ve kullanıcıların kısaca bu bilgilerin aktığı ağın güvenliğini sağlamaktır. ISO 27001 BGYS standardı bu kapsamda ağ güvenliğinin sağlanması ve yönetilmesine yönelik olarak çeşitli kontrol amaçları ve kontroller tanımlanmıştır.

Bilgi Güvenliği Organizasyonu, Varlık Yönetimi, Fiziksel ve Çevresel Güvenlik gibi farklı güvenlik alanlarında bilgisayar ağlarının güvenliği ve yönetimi ile ilgili dolaylı hususlar yer almakla beraber asıl olarak Tablo 2'de gösterildiği üzere, **A.10. Haberleşme ve İşletim Yönetimi** ile **A.11 Erişim Kontrolü** alanları ise bilgisayar ağlarının güvenliğine yönelik kontrolleri içermektedir.

A.10 Haberleşme ve İşletim Yönetimi		
	A.10.6 Ağ Güvenliği Yönetimi	A.10.6.1 Ağ kontrolleri
		A.10.6.2 Ağ hizmetleri güvenliği
A.11 Erişim Kontrolü		
	A.11.4 Ağ erişim kontrolü	A.11.4.1 Ağ hizmetleri kullanım politikası
		A.11.4.2 Dış bağlantılar için kullanıcı kimlik doğrulama
		A.11.4.3 Ağlardaki cihazları tanımlanma
		A.11.4.4 Uzaktan tanımlama ve konfigürasyon portunun korunması

		A.11.4.5 Ağlarda ayrım
		A.11.4.6 Ağ bağlantısı kontrolü
		A.11.4.7 Ağ yönlendirme kontrolü

Tablo 2- Ağ Güvenliği ve ISO 27001 Kontrol Maddeleri

Kontrol alanlarından "Haberleşme ve İşletim Yönetimi" ile ilgili güvenlik alanı bilgi işleme sırasında kullanılan varlıkların uygun ve güvenli kullanımına yönelik hususları belirtmektedir. Bu alanda yer alan "Ağ Güvenliği Yönetimi" kontrol amacı ile ağdaki bilginin ve destekleyici altyapının korunmasını sağlamak amaçlanmış, bu amaçla ilgili *ağ kontrolleri* ve *ağ hizmetleri güvenliği* olmak üzere 2 kontrol belirlenmiştir. Bu kapsamda

- ağlara yönelik tehditlerden korunmak için gerekli güvenlik önlemlerinin alınması, ağların uygun şekilde yönetilmesi ve izlenmesi,
- ister kuruluş içinden ister kuruluş dışından sağlanmış olsun ağ hizmetlerinin güvenlik özelliklerinin, hizmet seviyelerinin, yönetim gereksinimlerinin hizmet seviyesi anlaşmalarında bulunması gerektiği

tanımlanmıştır.

ISO 27001 BGYS standardında belirtilen "Erişim Kontrolü" güvenlik alanı ise bilgi güvenliği ile ilgili erişim hususlarını tanımlamaktadır. Erişim kontrolünün en önemli bölümlerinden biri de ağlara yapılan erişimlerin kontrol edilmesidir. Bu kapsamda "Ağ Erişim Kontrolü" kontrol amacı ile ağdaki servislere yapılacak yetkisiz erişimlerin engellenmesini amaçlamaktadır. Standart bu kontrol amacı ile ilgili olarak 7 kontrol belirlemiştir. Bu kontrol maddeleri ile temel olarak

- ağ kullanıcılarına sadece yetkili oldukları servislere erişebilecek şekilde erişim haklarının verilmesi
- uzaktan erişim sağlayan kullanıcılara yönelik olarak uygun kimlik doğrulama metotlarının kullanılması
- konfigürasyon yapmak amaçlı kullanılan portlara yapılabilecek fiziksel ve mantıksal erişimlerin kontrol edilmesi
- kullanıcı, servis ve bilgi sistemleri gruplarının ağlar üzerinde ayrılması
- ortak kullanılan ağlarda (özellikle kuruluş sınırlarını aşan ortak ağlarda) kullanıcıların bu ağlardaki yetenekleri erişim kontrol politikasına ve işin gereksinimlerine uygun olarak sınırlanması
- bilgisayar bağlantıları ve bilgi akışı için uygun yönlendirmelerin yapılması ve bu yönlendirmelere yönelik kontrollerin gerçekleştirilmesi

belirtilmiştir [10].

Belirtilen bu kontrollerin dışında daha önce de belirtildiği gibi ISO 27001 BGYS Ek A'da ağ yönetimini dolaylı olarak ilgilendiren diğer kontroller de bulunmaktadır. Bu kontrolleri de içine alan ve kurumlar için bir başlangıç olarak kullanılabilecek örnek bir AYP ekte sunulmaktadır. Aslında standardın ekinde yer alan tüm bu kontroller listesi ağ yöneticileri tarafından önemli bir kontrol seçeneğini gözden kaçırmamak amacıyla ele almalı [6], gerekirse yeni kontroller eklenmelidir.

4. SONUC

Kurumların güvenli bir ortamda faaliyet gösterebilmeleri için dokümante edilmiş bir BGYS'yi hayata geçirmeleri gerekmektedir. Bu kapsamda ISO 27001 standardı tüm dünyada kabul görmüş ve en iyi uygulamaları bir araya getiren bir modeldir. Standart bu yönetim sistemini oluştururken ele aldığı önemli alanlardan biri de bilgisayar ağlarının güvenliğinin sağlanması ve buna ilişkin olarak ağ güvenliği politikasının oluşturulmasıdır. Bilgisayar ağlarında güvenlik politikasının uygulanması kritik önem taşımakta ve kurumsal güvenlik için öncelikle yazılı olarak kurallar belirlenmelidir. Etkin bir BGYS kurmaya çalışan ve bunu ISO 27001 standardına uyumlu yapmak isteyen tüm kurumların oluşturacağı bu politikada belli kontrol maddeleri asgari olarak yer almalıdır. Ayrıca kurumlar bu ağ yönetimi politikasına uygun olarak BGYS'nin diğer alt dokümanlarını (prosedür, talimat, formlar vb.) oluşturmalı ve ilgili kullanılar tarafından uygulanmasını başarmalıdır.

KAYNAKLAR

[1] İnternet: http://www.cisco.com/web/TR/solutions/smb/products/security/security_primer.html, Cisco Website

[2] Bilgi Güvenliği Yönetim Sistemi ISO 27001, CIO Club Dergisi, Mart 2009, Cengiz İdris ALPAR

[3] Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması, Akademik Bilişim 2008, Mehtap Çetinkaya

[4] Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005, TBD Kamu-BİB Kamu Bilişim Platformu X Çalışma Grubu Raporu

[5] İnternet: http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html?Itemid=6, Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri, Fikret Öttekin

[6] International Standard, **"ISO/IEC 27001:2005: Information technology – Security techniques – Information security management systems – Requirements**", First Edition, 15.10.2009.

[7] International Standard, **ISO/IEC 27000:2009: Information technology – Security techniques – Information security management systems – Overview and vocabulary**, First Edition, 01.05.2009.

[8] Rene Saint German, "Information Security Management Best Practice Based on ISO/IEC 17799", The Information Management Journal, July/August 2005

[9] Enis Karaaslan, Abdullah Teke, Halil Şengoca, "Bilgisayar Ağlarında Güvenlik Politikasının Uygulanması"

[10] Timothy P. Layton, "**Information Security: Design, Implementation, Measurement and Compliance"**, Auerbach Publications, New York, 2007.

[11] Alan Calder, Jan Van Bon, **"Implementing Information Security based on ISO 27001/ISO 17799 - A Management Guide",** Van Haren Publishing, 2006 ISBN: 9789077212783.

[12] Ted Humpreys, **"State of the art information security management systems with ISO/IEC 27001:2005",** ISO Management Systems, 2006.