Bilişim Güvenliği Tedbirleri ve TKDK Kurumunda Uygulama Örneği

Emine TUĞ İLÇİN[1], Ş. Feyza ADAK[2], Hüseyin ÇAKIR[3]

[1]Adli Bilimler Enstitüsü, Ankara Üniversitesi, Ankara, Türkiye
[2]Bilişim Sistemleri, Gazi Üniversitesi, Ankara, Türkiye
[3]Bilgisayar ve Öğretim Teknolojileri Eğitimi, Gazi Üniversitesi, Ankara, Türkiye
emine.tugilcin@tkdk.gov.tr, sehbalfeyza@gmail.com, hcakir@gazi.edu.tr
(Geliş/Received: 30.01.2013; Kabul/Accepted: 13.04.2014)

DOI: 10.12973/bid.2012

Özet— Veri, tek başına hiçbir anlam ifade etmeyen işlenmemiş bilgidir. Verilerin anlamlı olarak işlenmesiyle bilgi oluşur. Bilgi güvenliği, elektronik ortamlarda tutulan bilgi ve verilerin yetkisiz kişiler tarafından ele geçirilmemesi ile oluşabilecek maddi ve manevi zararlardan korunmak için alınan tedbirler bütünüdür. Bilişim ve sistem güvenliği, kurumların sahip olduğu bilgi kaynaklarının korunmasına yönelik güvenlik tedbirlerini kapsar. Bir kurumun sahip olduğu maddi varlıklar yanında kurumun bilgisi de değeri olan ve korunması gereken bir varlıktır. Bilişim sistemlerinin kullanımının artmasıyla bilişim ve sistem güvenliğinin önemi de gün geçtikçe artmaktadır. Kurumlarda saldırılar en çok kurum çalışanları tarafından yapılmaktadır. Bu saldırıları kurumla ilgisi olmayan üçüncü şahıslar ve en son olarak da eski çalışanlar izlemektedir. Mevcut çalışan personelin tehditleri, bilgi ve tecrübesizlikten kaynaklanan kötü niyetli olmayan tehditlerdir. Kurumlar en çok personelin eğitimsizliğinden dolayı zarar görmektedir. Bu çalışmada bilişim ve sistem güvenliği prensip ve pratiklerinden bahsedilecek; bilgi, bilişim ve sistem güvenliğinin sağlanması için gerekli olan tedbirler ele alınacaktır. Son olarak, Tarım ve Kırsal Kalkınmayı Destekleme Kurumunda (TKDK) bilişim ve sistem güvenliği uygulama örneği verilecektir.

Anahtar Kelimeler- bilişim güvenliği, sistem güvenliği, bilgi güvenliği, güvenlik tedbirleri

Informatic Security Measures And Application Example In ARDSI

Abstract— Data is raw information that does not mean anything by itself. The information consist of the data processing significantly. Information security is measures to protect data and information held in electronic media from unauthorized persons accesving. Informatic and system security include security measures for protection of information sources of institutions. Information of institution together with its real assets must be protected. With increasing of informatic systems usage, importance of informatic and system security is increasing. Most of the attacks carried out by the employees of the institutions. Attacks made by third persons and former employees have fallowed these attacks. The threats of current employee are non-malicious threats because of inexperience. Institutions are damaged due to lack of education of its employees. In these study, informatic and system security principles and practices are mentioned and measures to ensure information, informatic and system security are discussed. Finally, an application example for informatic and system security in ARDSI is given.

Keywords- informatic security, system security, information security, security measures

1. GİRİŞ (INTRODUCTION)

Bilgi ve iletişim teknolojilerinin gelişimine paralel olarak bilişim aygıtları ve sistemleri hayatın vazgeçilmez bir parçası olmuşlardır. Teknoloji kullanımındaki hızlı artış ile birlikte bilgi sistemlerine yönelik saldırılarda büyük ölçüde artmıştır. Ağ teknolojileri ve internet sayesinde bilişim sistemleri hem bir saldırı aracı hem de açık birer hedef konumundadır.

Bilişim ve sistem güvenliği, kurumların sahip olduğu bilgi kaynaklarının korunmasına yönelik güvenlik tedbirlerini kapsar. Kurumun sahip olduğu maddi varlıklar yanında kurumun bilgisi de değeri olan ve korunması gereken bir varlıktır.

Güvenlik açıkları, başarılı bilişim saldırıları ve bilgi kayıpları kurumların itibarlarını zedelemekte, güvenilirliklerini azaltmakta, pazar ve müşteri kayıplarına

neden olabilmektedir. Bu saldırıların sonuçlarının getirdiği riskler göz önüne alındığında, bir kurum için bilgi güvenliğinin sağlanması hayati önem taşımaktadır.

Bilişim ve sistem güvenliği konusu oldukça dinamik bir kavramdır. Bilgi güvenliğini sağlamaya yönelik güvenlik tedbirleri tek başlarına etki olmaz, bu tedbirlerin birbirleri ile etkileşimli çalışması gerekir. Aynı zamanda tedbirlerin izlenmesi, gerektiğinde güncellenmesi önemlidir.

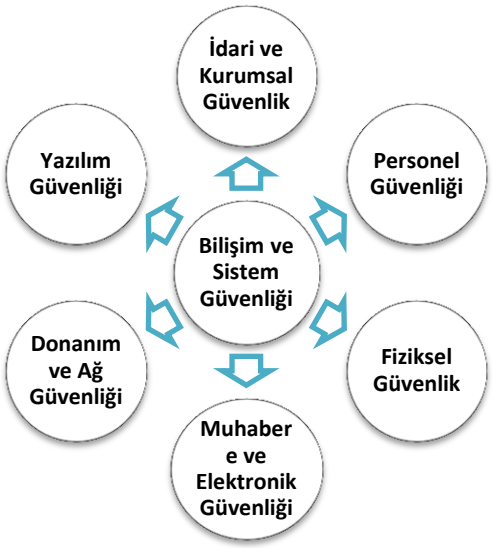
Bu çalışmada genel olarak, bilişim ve sistem güvenliğine yönelik uygulanabilecek güvenlik tedbirleri incelenmiştir.

2. BİLİŞİM VE SİSTEM GÜVENLİĞİ (INFORMATION AND SYSTEM SECURITY)

Bilgi güvenliği diskte, iletişim ağında, yedekleme ünitelerinde ya da başka bir yerde tutulan verilerin, programların ve her türlü bilginin korunmasıdır. Bilişim güvenliğinin temel amaçları Gizlilik, Bütünlük, Erişebilirlik, İnkâr edememe ve İzleme olarak verilebilir [1].

Gizlilik, bir bilgiye erişim hakkı olan kişileri belirlemek ve diğer kişilerin bilgiye ulaşmasını engellemek; Bütünlük, bir bilginin hiçbir şekilde değiştirilmemiş olması; Erişebilirlik, bir bilgiye ulaşmaya yetkili olan herkesin gerektiğinde o bilgiye erişiminin mümkün olması; İzleme, bir bilginin oluşmasından bu yana ne tür değişikliklerin olduğu, bu bilgiye kimlerin ne zaman ulaştığı, kimlere nasıl, ne zaman ve kim tarafından gönderildiği gibi tüm verilerin izlenebilmesidir.

Bilgi teknolojileri açısından bakıldığı zaman güvenlik konuları fiziksel güvenlik, iletişim güvenliği ve bilgisayar güvenliği olarak sınıflandırılabilir [1].



Şekil 2.1. Bilişim ve Sistem Güvenliği (Information and System Security)

2.1. *İdari ve Kurumsal Güvenlik (Administrative and Enterprise Security)*

Kurumsal bilgi güvenliği, kurumların bilgi varlıklarının tespit edilerek zafiyetlerinin belirlenmesi ve istenmeyen tehdit ve tehlikelerden korunması amacıyla gerekli güvenlik analizlerinin yapılarak önlemlerin alınmasıdır [2].

TBD (2006)'ye göre kurumlardaki bazı güvenlik açıkları; hatalı yapılandırılmış sanal özel ağ (VPN) sunucuları, web uygulamalarında SQL sorgularının değiştirilmesi, web uygulamalarında başka siteden kod çalıştırma, kolay tahmin edilebilir şifrelere sahip kullanıcı hesapları, SNMP servisi kullanımı, güncellemeleri yapılmamış web sunucuları, işletim sistemi ve uygulamaların standartlara uygun şekilde kurulmaması, hatalı yapılandırılmış saldırı tespit sistemleri, güvenlik duvarı tarafından korunmayan sistemlerdir.

Kurumsal güvenliğin sağlanabilmesi için, üst yönetimin katılımı ile kurumda bilişim güvenliği programının çerçevesini oluşturacak bir Kurumsal Güvenlik Politikası oluşturulmalıdır. Bu politikanın oluşturulması ve uygulanması idari bir süreçtir. Oluşturulacak güvenlik politikası kurumun tüm bilişim faaliyetlerini kapsamalı, aynı zamanda uygulanacak güvenlik faaliyetlerinde de yönlendirici olmalıdır.

2.2. *Personel Güvenliği (Personal Security)*

Kurum içi personel güvenliği, kurumun kendi personeli, geçici çalışanlar, danışmanlar, alt yüklenicilerin personeli, ortak çalışılan kurum ve kuruluşların çalışanları ve son kullanıcıya kadar tüm kişileri kapsar. Güvenliğin en önemli zaaflarından biri de insan davranışlarıdır. Bu nedenle güvenlik politikaları oluşturulurken kurum personeli bilinçlendirilmeli, olası personel hatalarına veya personelin kasıtlı davranışlarına karşı gerekli tedbirler alınmalıdır.

Personel güvenliği, personelin işe alım sürecinde yapılan araştırmalar, kritik önceliğe sahip iş ve işlemlerde gizlilik anlaşmalarının devreye alınması, çeşitli zamanlarda görev değişikleri, belirli zamanlarda personelin zorunlu izne ayrılması ve güvenlik olaylarının raporlanması gibi birçok tedbiri kapsar.

Personel güvenliğinde alınabilecek tedbirler şunlardır [3-6]:

- Bilgisayar sistemlerinin yönetim merkezlerinde ve kritik yerlerde çalıştırılacak personelin güvenlik tahkikatı yaptırılmalı ve bu personele düzenli olarak güvenlik brifingi verilmelidir,
- Bilgisayar sistemlerinin kullanıcıları, bilgi sistemleri güvenliği konusunda eğitime tabi tutulmalı ve güvenlik bilinci geliştirilmelidir,
- Kurum personeli, yetkileri ve görevleri gereğince kendilerine tanımlanan parola ve şifreleri kimseyle paylaşmamalıdır,

- Kurum personeli, bilgisayar sistemleri üzerinde dosya paylaşımı ve yetkilendirme konularında bilgi sahibi olmalıdır,
- Kurum personeli, bilgisayar sisteminde alınması gereken fiziki ve işlemsel güvenlik tedbirlerini bilmeli ve en üst seviyede uygulamalıdır,
- Kurum personeli, sisteme yetkisiz müdahale edenlerin kimler olduğunu, bunların yeteneklerini, yapabileceklerinin neler olduğunu ve verebilecekleri zararların boyutlarını bilmelidir,
- Kurum personeli, temel bilişim suçlarının neler olduğunu, bunların nasıl işlenebileceğini ve bunlar hakkındaki yasal mevzuatı bilmeli ve buna göre belirlenmiş tedbirleri uygulamalıdır,
- Bilgisayar sistemlerinde kullanılan anti-virüs ve firewall (ateş duvarı) yazılımlarını, her seviyedeki kullanıcı çok iyi bilmeli, bu yazılımları kullanarak virüslerden ve saldırılardan korunabilmelidir,
- Kurum personeli, olası saldırılara karşı hazırlıklı olmalıdır,
- İlgili personel, oluşan saldırıları ve kaynaklarını tespit edebilmelidir,
- İlgili personel, işin sürekliliği için, olası hasar ve kayıpları en aza indirebilmeli ve en kısa sürede olumsuz etkileri giderebilmelidir,
- İlgili personel, bilgi sistemlerinin güvenliği için gerekli politikaları belirleyip, uygulama ve stratejik planlama yapabilecek yetkinlikte olmalıdır.

2.3. Fiziksel Güvenlik (Physical Security)

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır [7].

Fiziksel güvenlik, bir işletmenin kaynaklarına ve hassas bilgilerine yönelik tehditler ve güvenlik açıklarını fiziksel açıdan önlemeye yönelik fiziksel ve çevresel tedbirleri ifade eder. Bu kaynaklar, işletmenin çalışanları, verisi, ekipmanları, altyapısı, destek sistemleri ve faydalanılan her türlü araç-gereç olabilir.

Fiziksel güvenliğin sağlanması için gerekli tedbirler şunlardır [7-9]:

- Temiz masa ve temiz ekran politikası, belgelere, çalışma ortamına ve bilgi işleme araçlarına yetkisiz erişim veya hasar risklerini azaltmak için tavsiye edilmektedir.
- Fiziki giriş denetimleri kullanılarak güvenli alanlara sadece yetkili personelin erişimine izin verilmelidir. Biyometrik giriş sistemleri, kartlı okuyucular, parmak izi, retina tanıma ile kimlik kontrolleri gibi çözümler mevcuttur.
- Güvenli alanlarda ziyaretçilere eşlik edilmeli, gerekirse üstleri aranmalı ve giriş ve çıkış tarihleri ve saatleri not edilmelidir. Ziyaretçilerin sadece belirli, yetkili amaçlar çerçevesinde güvenli alanlara erişimlerine izin verilmeli ve güvenlik direktifleriyle ve acil durum yöntemleriyle ilgili bilgilendirilmelidirler.
- Hassas bilgilere ve bilgi işleme araçlarına erişim, denetlenmeli ve sadece yetkili kullanıcılarla sınırlı olmalıdır. Kimlik doğrulama denetimleri, (örneğin giriş kartı ve parola) tüm erişimleri yetkilendirmek ve geçerli kılmak için kullanılmalıdır. Tüm erişimlerin bir kontrol zinciri güvenli olarak korunmalıdır.
- Tüm personelden, görünür biçimde kimlik kartı taşımaları istenmelidir ve eşlik edilmeyen bir yabancıya veya kimlik kartı taşımayan birine rastlanıldığında hemen bildirmeleri teşvik edilmelidir.
- Güvenli alanlara erişim hakları düzenli aralıklarla gözden geçirilmeli ve güncellenmelidir.
- Tesisin konumu, yangın, sel, patlama, askeri saldırı ve diğer biçimdeki doğal veya insan yapımı afetlerden meydana gelebilecek hasar ihtimallerine göre seçilmelidir.
- Tesis, insanların, park alanlarının ve bina girişlerinin görünürlüğünü maksimize eden mimari özellikle olmalıdır.
- Tesiste özel ve kamusal alanların birbirinden ayrılması (çitler, ağ geçitleri, peyzaj, vb) sağlanmalıdır.
- Kritik veri içeren araçlar yetkisiz kişiler tarafından gözlenemeyecek şekilde yerleştirilmelidir.
- Tesiste yetkisiz erişimleri engellemeye yönelik mimari unsurlar (kapı kilitleri, pencere kilitleri, iç kapı menteşeleri, vb.) kullanılmalıdır.
- Tehlikeli ve patlamaya hazır maddeler, güvenli alandan uygun bir uzaklıkta güvenli bir şekilde toplanmalıdır.
- Yakın çevrede oluşan felaketler, örneğin komşu binada çıkan bir yangın, çatıdan akan veya zemin kat seviyesinden aşağıdaki katlara akan su veya caddede olan bir patlama göz önünde bulundurulmalıdır.
- Teçhizatlar, güç kaynağı bozulmalarından veya diğer olağan dışı elektriksel olaylardan korunmalıdır. Donanım üreticisinin belirttiği özelliklere uygun elektrik kaynağı sağlamalıdır.
- Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve haberleşme kabloları, durdurmalardan veya hasarlardan korunmalıdır.
- Teçhizatların, elverişliliğinin ve güvenilirliğinin garanti edilmesi için doğru bir biçimde bakımı yapılmalıdır.
- Elektrik, su, kanalizasyon ve iklimlendirme sistemleri destekledikleri bilgi işlem dairesi için yeterli düzeyde olmalıdır.
- Elektrik şebekesine yedekli bağlantı, kesintisiz güç kaynağı gibi önlemler ile ekipmanları elektrik arızalarından koruyacak tedbirler alınmış olmalıdır.
- Yedek jeneratör ve jeneratör için yeterli düzeyde yakıt bulundurulmalıdır.

- Su bağlantısı, iklimlendirme ve yangın söndürme sistemlerini destekleyecek düzeyde olmalıdır.
- Acil durumlarda iletişimin kesilmemesi için servis sağlayıcıdan iki bağımsız hat alınmış olmalıdır.
- Kurum, fiziksel güvenlik konusunda yasal yükümlülüklerini yerine getirmelidir.

2.4. *Muhabere ve Elektronik Güvenliği (Communications and Electronical Security)*

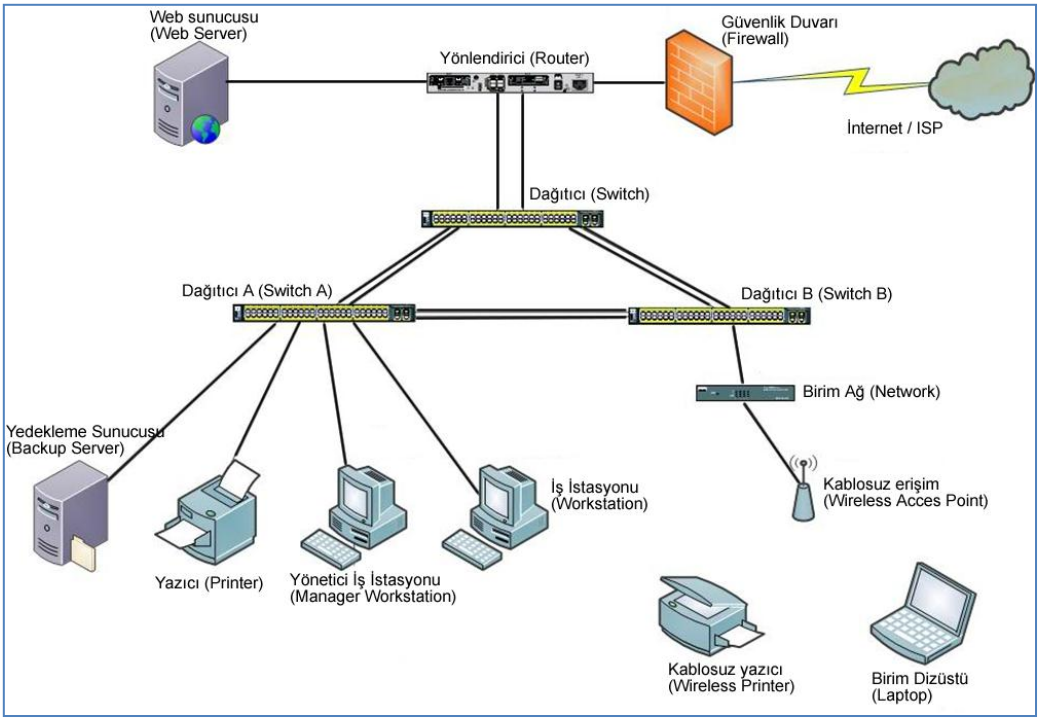
Elektronik cihazlar çalışırken anlamlı sinyaller üretirler. Üretilen sinyaller bazı özel cihazlar kullanılarak yeniden veriye dönüştürülebilir. Yazıcıdan alınan veriler, bilgisayarların ekran görüntüleri, klavyeler, ses kayıtları gibi veriler çeşitli yöntemler kullanılarak yeniden elde edilebilir. Sinyallerden elde edilen verilerin üçüncü kişiler tarafından ele geçirilmemesi için alınan bilgi güvenliği önlemlerine, muhabere ve elektronik güvenliği denir. En çok askeri alanda kullanılır.

Muhabere ve elektronik güvenliği için alınacak tedbirler şunlardır [10-14]:

- Ağ ve telefon hatlarında korumalı kablolar (shielded) (örneğin CAT6 yada CAT7) kullanılmalı yada fiber optik kablo tercih edilmelidir.
- Elektrik alt yapısı şebeke toprağı dışında ayrıca topraklanmalıdır.
- Zırhlama yöntemi, özellikle çok gizli evrakların bulunduğu askeri ve diplomatik alanlarda, en güvenli yöntemdir. Zırhlama yönteminde bilgisayarların bulunduğu odalar tamamen iletken(örneğin kurşun) bir maddeyle kaplanarak elektromanyetik yayılımları durdurucu Faraday Kafesi oluşturulur. Odaların havalandırma girişlerine dalga kırıcı yansıtıcılar yerleştirilir. Elektrik şebekesine frekansları kesen filtreler aracılığıyla bağlantılar yapılır.
- Elektromanyetik dalgalara gürültü ekleme yöntemi ile sinyallere gürültü eklemek suretiyle elektromanyetik veriyi algılayan cihazda parazit oluşturarak yayılan dalgalar anlaşılmaz hale getirilmektedir.
- Cihazların pozisyonları da oldukça önemlidir. Monitör kesinlikle pencereye çevrilmemelidir. Bu durum elektromanyetik sinyallerin çok net bir şekilde yayılmasını sağlar. Bilgisayarların metal dolapların, kalorifer peteklerinin ya da borularının yakınında olması sinyallerin yayılımlarını kolaylaştırır. Çünkü iletken metaller elektromanyetik dalgaların yayılımı güçlendirir.

2.5. *Donanım ve Ağ Güvenliği (Hardware and Network Security)*

Donanım güvenliği bir bilişim sisteminde bulunan her türlü donanım ve ağ bileşeninin korunmasına ve uygun kullanılmasına yönelik güvenlik tedbirlerini kapsar. Donanım güvenliği de diğer güvenlik politikası kategorileri ile iç içe geçmiştir. Bir donanım, fiziki güvenlik veya personel güvenliği politikaları ile korunabileceği gibi salt donanımsal güvenlik politikaları da uygulanabilir.



Şekil 2.2. Donanım ve Ağlar (Hardware and Networks) [18]

Donanım güvenliğini sağlamak için yapılması gerekenler şunlardır [3, 7, 15, 16]:

- Aktif ağ elemanlarını besleyen elektrik alt yapısının sağlam ve sorunsuz olması sağlanmalıdır. Ağ cihazlarına ayrı ve adanmış sigortalardan hat çekilmeli, mümkünse UPS ile sistem desteklenmelidir. Sigortalı ve topraklı prizler kullanılmalıdır. Gelen elektrik hattının topraklama değerinin mümkün olduğunca sıfıra yakın olmasına önem verilmelidir. UPS'in kısa süreli bir çözüm olduğu unutulmamalı ve kritik önem taşıyan yerler ve merkez bilgi işlem için UPS'in yanı sıra jeneratör sistemi kullanılmalıdır,
- Data kablosu, sonlandırma ve aktarma işlemlerinde kullanılan bütün bileşenlerin (patch panel, data prizi, patch ve drop kabloların) EIA/TIA-568B yapısal kablolama standartlarına uygun olması sağlanmalıdır. Kaliteli malzeme için; kablo üreticilerinin ürünleri ISO 9000 standardına uygun olmalı, kablo üreticisi sadece kablo değil, bütün tamamlayıcı bileşenleri üretiyor olmalıdır,
- Elektrikle çalışan bütün cihazların en büyük düşmanı toz ve sıcaktır. Aktif cihazların tozdan uzak tutulması için kabinetlerde tutulması, kabinetlerin hava akımını sağlayacak yapıda olmaları (fan) gerekmektedir,
- Sistem odalarında yangın (örn. otomatik yangın söndürme sistemi) ve fiziksel güvenlik önlemlerinin (şifreli kapı sistemleri, kamera takip sistemi) olması gerekmektedir,
- Özel koruma gerektiren donanım izole edilmiş olmalıdır,
- Nem ve sıcaklık gibi parametreler izlenmelidir,
- Hırsızlık, yangın, duman, patlayıcılar, su, toz, sarsıntı, kimyasallar, elektromanyetik radyasyon, sel gibi potansiyel tehditlerden kaynaklanan riskleri düşürücü kontroller uygulanmalıdır,
- Paratoner kullanılmalıdır,
- Bilgi işlem araçlarının yakınında yeme, içme ve sigara içme konularını düzenleyen kurallar olmalıdır,
- Bilgisayar sistemleri ile birlikte kullanılan disket, CD, taşınabilir disk ve dokümanlar kullanılmadıkları zaman kesinlikle açıkta veya sistemlerin üzerinde bırakılmamalı, kilitli bir dolap yada bölmede muhafaza edilmelidir,
- Bilgisayar sistemleri kullanılmadıkları zaman kesinlikle gözetimsiz bırakılmamalıdırlar. Sistem kullanılmadığı zaman açma-kapama anahtarı ile kapatılmalı ve diğer sistemlerle olan tüm irtibatları (network, internet vb.) kesilmeli, elektrik fişi çekilmelidir,
- Bilgisayar sistemlerinin arızalanması durumunda firmada yapılacak onarımlarda, bilgisayar sisteminin sabit diskleri sökülmeli veya içindeki bilgilere ulaşılmaması için formatlanmalıdır,
- Bilgisayar sistemleri ışıma-yayılma yoluyla bilgi kaçağına sebebiyet vermektedir. Bunu engellemek için sistemlerin yanında yansıtma özelliği bulunan malzemeler bulunmamalıdır,
- Bilgisayar sistemlerinde kullanılan orijinal yazılım ve programlar yetkisiz kopyalama ve çoğaltılmalarına engel olmak amacıyla mutlaka kilit altına alınmalıdırlar

2.6. Yazılım Güvenliği (Software Security)

Yazılım güvenliği genel olarak; yazılımların tersine mühendislik yöntemleri ve araçları ile (debugger, disassembler, vb.)algoritmalarının ortaya çıkartılması veya değiştirilmesini engellemeyi amaçlayan yöntemler bütünüdür. Yazılım güvenliğinin ele aldığı temel sorunlar, kodların açığa çıkmasını ve değiştirilmesini (debugging, tracing ya da disassembly ile) ve tersine mühendislik araçlarını (debugger, disassembler, vb.) engellemek şeklinde özetlenebilir [17].

Her an yeni bir kötü amaçlı yazılımın (virüs, solucan, truva atı, uygulama yazılımlarındaki arka kapılar, vb.) üretildiği ve hızla yayıldığı ağ ortamında bu tür saldırılara hazırlıklı olmak son derece önemlidir. Kötü amaçlı yazılımlar en çok kullanıcı bilgisayarlarına zarar verir ve bu bilgisayarlardan ağa yayılırlar. Dolayısıyla, her kullanıcının makinasında bir *antivirüs yazılımı* bulunmalıdır. Kullanıcıların antivirüs yazılımlarını kullanmalarını zorunlu hale getirmek için kurumsal antivirüs çözümü kullanmaları sağlanmalı, düzenli aralıklarla bu yazılımların otomatik güncelleştirmeleri yapılmalıdır.

Kurumun tüm iş bilgileri, verileri ve yazılımlarının yedekleme kopyaları düzenli olarak alınmalıdır. Yedekler, bir felaket ya da ortamın zarar görmesi sonrasında sistemin en son çalışır durumuna geri getirilmesini sağlar. Yedeklemede amaç, bilgi işlem ve iletişim hizmetlerinin kullanılabilirliğinin ve bütünlüğünün sürdürülmesidir. Yedekleme ve geri yükleme süreç ve sorumlulukları, güvenilir yedeklerin alınması ve gerektiğinde sistemin eski haline getirilmesi için iyi tanımlanmalı, tüm süreçler düzenli olarak test edilmelidir.

2.7. İşlem Güvenliği (Process Security)

İşlem güvenliği, bilişim sistemlerinde verilerin işlenmesine ait gerekli önlemleri kapsar [10]. İşlem güvenliğini sağlamaya yönelik en çok rol tabanlı güvenlik çözümleri kullanılır. Bu yapıda, kullanıcıların kurum içerisindeki görev ve sorumluluklarına göre roller tanımlanır. Kullanıcılar kendilerine atanan roller sayesinde ilgili yetkilere sahip olurlar. Roller bilgi sistemi uzmanları aracılığıyla merkezi bir şekilde kullanıcılara verildiği için kurumsal güvenlik politikalarının uygulanması da mümkün hale gelir.

İşlem güvenliğinin sağlanması için alınacak tedbirler şunlardır:

- Bilgisayarda mutlaka lisanslı yazılımlar kullanılmalıdır. Crack yazılımlar virüs içerebilir, açık kapı bırakabilir,
- Bilgisayarlar açılırken parola ile açılmalıdır, parola kolay tahmin edilecek bir şey olmamalıdır. Ayrıca bilgisayar başından kalkıldığı zaman ekran koruyucu devreye girmeli ve tekrar masaüstüne dönmek için şifre korumalı olmalıdır.
- Lisanslı bir antivirüs programı olmalıdır. Lisanslı olmayan antivirüsler bilgisayarı gerçek anlamda korumamaktadır.
- Eğer bilgisayarda kullanıcı sayısı birden fazla ise, kullanıcıların kullanabileceği dosya ve programlar belirlenmeli, gizli ve önemli belgelere erişim yetkileri iyi tanımlanmalıdır.
- Ağ paylaşımı yapılıyor ise, hangi dosyalara kimin ulaşabileceği ve dosya üzerinde ne tür değişiklikler yapılabileceği belirlenmelidir,
- Güvenlik duvarı kapatılmamalıdır,
- Bilgisayarda Log kayıtları tutulabilir. Bu şekilde eğer bilgisayara bir saldırı yapılıyorsa tespit edilmesi kolaylaşacaktır.

3. TKDK KURUMUNDA BİLGİ GÜVENLİĞİ TEDBİRLERİ (INFORMATION SECURITY AT TKDK)

Bu bölümde, bilişim ve sistem güvenliğini sağlamaya yönelik bir örnek olarak Tarım ve Kırsal Kalkınmayı Destekleme Kurumu'nda (TKDK) gerçekleştirilen uygulamalardan bahsedilmiştir.

TKDK, kırsal kalkınma alanında Avrupa Birliği(AB) ve diğer uluslararası kuruluşlardan sağlanan mali fonlardan faydalanabilmek için 2007 yılında kurulmuştur. Kurum, ülkemizde kırsal kalkınma programlarının uygulanmasına yönelik faaliyetlerde bulunmaktadır. Ankara merkezli olan kurumun 42 adet ilde birimleri mevcuttur.

TKDK'da temel bilgi güvenliği ilkeleri olan gizlilik, bütünlük ve erişilebilirliğin garanti edilmesi için Bilgi Güvenliği Yönetim Sistemi kurulması çalışması gerçekleştirilmiştir. Bu çalışmada gerekli prosedürler oluşturulmuş, personel bilinçlendirmeye yönelik farkındalık eğitimleri gerçekleştirilmiş ve bilgi güvenliğine yönelik kabul edilebilir risk seviyeleri belirlenmiştir.

Bilgi güvenliği yönetim sistemi kurulumuna yönelik diğer bölümlerde vurgulanan tedbirleri sağlayacak uygulama örnekleri aşağıda sıralanmıştır.

3.1. İdari ve Kurumsal Güvenlik Tedbirleri (Administrative and Enterprise Security Measures)

TKDK'da idari ve kurumsal güvenliği sağlamaya yönelik ISO 27001 standardı uygulanmaktadır. Bu standart kapsamında kurum bilgi varlıkları belirlenmiş, bilgi süreçleri modellenmiş ve bilginin yönetimine dair prosedürler oluşturulmuştur.

Kurum içi bilgi güvenliği prosedürleri hazırlanması ve uygulanması sürecinde korunacak nesneleri belirlemek amacıyla varlık envanterleri hazırlanmış, varlıklara kimlerin hangi düzeyde erişeceği ve bilgiye erişim sorumlulukları belirlenmiş, verilerin yedekleme süreçleri modellenmiş ve kabul edilebilir risk seviyeleri belirlenmiştir.

Oluşturulan prosedürler üst yönetimin de onayı ile uygulanmaktadır. Dolayısıyla kurum içerisinde bilgi kaynaklarının idari yönetimi bu prosedürler uyarınca gerçekleştirilmektedir.

3.2. Personel Güvenliği Tedbirleri (Personal Security Measures)

TKDK'da personel güvenliğini sağlamaya yönelik olarak bir personel işe başladığında personele Bilgi Güvenliği Sözleşmesi imzalatılmaktadır. Bu sözleşme bilgi güvenliği açısından personelin yetki ve sorumluluklarını belirlemektedir.

Kurumda, yeni kurum personeline işe başladıkları sürede, eski personele ise dönemsel olarak bilgi güvenliği farkındalık eğitimi verilmektedir. Bu eğitimde personele, temel bilgi kavramları, bilginin bulunduğu ortamlar, güncel tehditler ve saldırılar, sosyal mühendislik, fiziksel güvenlik, şifre güveliği, yasal düzenlemeler, bilgi güvenliği prosedürleri ve personelin sorumlulukları konularında en güncel bilgi verilmektedir. TKDK'da ayrıca temiz masa temiz ekran kuralı uygulanmaktadır.

3.3. Fiziksel Güvenlik Tedbirleri (Physical Security Measures)

TKDK'da bütün birimlere giriş ve çıkışlar kartlı geçiş sistemi ile sağlanmaktadır. Bir personel giriş yetkisi olmayan bir birime geçiş yapamamaktadır. Personelin kimlik kartı taşıması zorunludur.

Bina girişlerinde fiziki güvenliği sağlamaya yönelik güvenlik personeli görev yapmaktadır. Ayrıca tüm koridorlar, birim girişleri ve hassas bölgeler güvenlik kameraları ile izlenmektedir. Ayrıca gerekli kısımlarda yangın/duman algılama sistemleri, yangın söndürücüler ve güç kaynakları bulunmaktadır.

Kurum merkezinde olası herhangi bir felaket anında devreye girecek bir felaket kurtarma merkezi kurulmuştur.

3.4. Muharebe – Elektronik Güvenliği Tedbirleri (Communications - Electronical Security Measures)

TKDK'da elektronik güvenliğini sağlamaya yönelik özel bir altyapı mevcut değildir. Ancak veri iletişiminde kablolu ağ bağlantısı tercih edilmektedir.

3.5. Donanım ve Ağ Güvenliği Tedbirleri (Hardware and Network Security Measures)

TKDK'da donanımların ve ağın güvenliğini sağlamaya yönelik, güç kaynakları kullanılmakta, dış ağa erişimler güvenlik duvarı aracılığıyla sağlanmakta, ihtiyaç halinde kurum dışı erişimler için personele VPN bağlantısı sağlanmaktadır.

Kurumda 5651 sayılı "İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun" uyarınca IP ve erişim log kayıtları saklanmakta, yasaklı sitelere ve bilgiye erişim engellenmektedir.

3.6. Yazılım Güvenliği Tedbirleri (Software Security Measures)

TKDK'da yazılım güvenliğini sağlamaya yönelik kurumsal antivürüs yazılımları tercih edilmektedir. Kurum sunucu bilgisayarları bilgi güvenliği prosedürleri uyarınca düzenli olarak yedeklenmekte, yazılımlar için yazılım versiyonları tutulmaktadır. Kurum yazılımcıları, ihtiyaç halinde olası yazılım saldırılarına karşı güncel eğitimler almaktadır.

3.7. İşlem Güvenliği Tedbirleri (Process Security Measures)

TKDK'da kurumsal yazılımlar için ortak bir yetki kontrolü yazılımı kullanılmaktadır. Bu yazılım sayesinde personelin hangi yazılıma hangi yetki seviyesi ile erişeceği belirlenmektedir. Yazılımlara *single sign on* kuralı ile erişilmektedir. Bir kullanıcı ağ üzerinde bir bilgisayarda oturum açtığında tekrar yetki kontrolü yapılmamakta sistem kullanıcıyı otomatik olarak tanımaktadır.

4. SONUÇ VE ÖNERİLER (CONCLUSIONS AND SUGGESTIONS)

Bilişim teknolojileri alanındaki gelişmelere paralel olarak artık bilginin önemi kadar bilginin korunması da büyük önem arz etmektedir. Özellikle kamu kurumları hem hizmet kalitesini artırmak hem de kesintisiz hizmet sağlayabilmek için bilgi sistemlerini daha aktif kullanmaktadır.

Bilgi sistemlerine gerçekleştirilebilecek olası saldırılara karşı her zaman hazırlıklı olabilmek için sistemin sürekli kontrol edilmesi, düzeltici ve önleyici faaliyetlerin gerçekleştirilmesi, bilişim ve sistem güvenliği risklerinin iyi yönetilmesi gerekir. Tüm bunları sağlayabilmek için özellikle kamu kurumlarının bilgi güvenliği yönetim sistemlerine ihtiyacı vardır. Bilgi güvenliği yönetim sistemleri, kurumların sahip olduğu hassas bilgileri koruyabilmek ve yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır.

Bu çalışmada bilişim ve sistem güvenliğinin önemi açıklanmış, uygulanabilecek güvenlik tedbirleri sunulmuş ve ISO 27000 bilgi güvenliği yönetim sistemine sahip bir kamu kurumu olan Tarım ve Kırsal Kalkınmayı Destekleme Kurumu'nda sunulan bu güvenlik tedbirlerinin nasıl uygulandığı örneklenmiştir.

KAYNAKLAR (REFERENCES)

[1] Türkiye Bilişim Derneği (TBD)., *Bilişim Sistemler Güvenliği El Kitabı*.Sürüm1.0.Ankara: TBD.(2006).

[2] Y. Vural, Ş. Sağıroğlu, *Kurumsal Bilgi Güvenliği: Güncel Gelişmeler*. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Kongresi. Ankara. (2007).

[3] Tulum, İ., **Bilişim Suçları ile Mücadele.** Yüksek Lisans Tezi. Süleyman Demirel Üniversitesi Sosyal Bilimler Üniversitesi. Isparta. (2006).

[4] A. Bequai, A Guide to Cyber Crime Investigations. *Computers and Security* 17.(1998).

[5] N. Nykodym ve R. Taylor, Control of Cyber Crime:The World's Current Legislative Efforts Against Cyber Crime, *Computer Law and Security Report*, Vol.20, No.5, University of Toledo. (2004).

[6] S. Atay, Bilgi Sistemleri Güvenliğinde Çalışan Personelin Sertifikasyonu. İzmir İleri teknoloji Üniversitesi, Mühendislik Fakültesi, İzmir. (2005).

[7] M. Nazlı, Fiziksel ve Çevresel Güvenlik.(http://mikailnazli.blogspot.com/2010/01/bilgi-guvenligi-fiziksel-ve-cevresel.html) 03.01.2013

[8] S. Kahraman, Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi ve Aselsan A.Ş.'de Uygulaması, Yayınlanmamış Yüksek Lisans Tezi. Anadolu Üniversitesi Sosyal Bilimler Enstitüsü. Eskişehir. (2006).

[9] A. Ouyang, CISSP - Common Body of Knowledge Review: Physical (Environmental) Security Domain, Version: 5.9. USA. (2012).http://opensecuritytraining.info/CISSP-8-AC_files/8-Access_Control.pdf

[10] B. Alaca, Ülkemizde Bilişim Suçları ve İnternetin Suça Etkisi (Antropolojik ve Hukuki Boyutları İle. Yayınlanmamış Yüksek Lisans Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü. Ankara. (2008).

[11] Elektromanyetik casusluk ve Tempest. http://www.turkboard.com/elektromanyetik - casusluk - ve- tempest - vt219869.html. (20.12.2012).

[12] Tempest (Elektromanyetik Dinleme). http://www.adlibilirkisi.org/index.php?sayfa=makaleoku&kategori=1&id=233 (20.12.2012).

[13] Tempest ve Tempest Önlemleri. http://www.serhatakinci.com/index.php/tempest-ve-tempest-guvenligi.html. (20.12.2012).

[14] Tempest Nedir? Tempest için korunma yolları nelerdir?http://blog.aytacengin. com/tempest-nedir

[15] E. Karaarslan, *Kampüs ağ Yönetimi.* Ege Üniversitesi Bitam Kampüs Network Yönetim Grubu, İzmir. (2006).

[16] Y. Uzunay, *Dijital Delil Araştırma Süreci*. 2.Polis Bilişim Sempozyumu, Ankara Emniyet Müdürlüğü Bilgi İşlem Şube Müdürlüğü, Ankara. (2005).

[17] E. Demirkan, *Yazılım Güvenliğine Genel Bakış ve Yazılım Güvenliğinin Önemi*. (2012). (http://www.bilgiguvenligi.gov.tr/yazilim-guvenligi/yazilim-guvenligine-genel-bakis-ve-yazilim-guvenliginin-onemi.html). 03.12.2012.

[18]http:img.photobucket.com/albums/v47/Silent54/real/network.jpg (2014).