

Doküman Kodu: BGYS-0006

ERİŞİM KONTROL POLİTİKASI OLUŞTURMA KILAVUZU

SÜRÜM 1.00

19.11.2007

Hazırlayan: Dinçer Önel

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
<http://www.bilgiguvenligi.gov.tr>
bilgi@bilgiguvenligi.gov.tr

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji AraŐtırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliđi, haberleŐme ve ileri elektronik alanlarında Türkiye'nin teknolojik bađımsızlıđını sađlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüŐ altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliđi, haberleŐme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaŐılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı araŐtırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sađlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliđi Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıŐtır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu deđildir. Bu doküman UEKAE'nin izni olmadan deđiŐtirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geçen Ađ Güvenliđi personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali Dinçkan ve Dođan Eskiyörük'e teşekkürü borç biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
2. ERİŞİM KONTROLÜ	6
3. ÖN ÇALIŞMALAR.....	7
3.1 Standarda Danışma	7
3.2 Fikir Edinme	7
4. ERİŞİM KONTROL POLİTİKASININ OLUŞTURULMASI.....	8
4.1 Kapsam Belirleme	8
4.2 Nesnelerin (varlıkların) Sınıflanması	8
4.3 Öznelerin (kullanıcıların) Sınıflanması	8
4.4 Adreslenecek Erişim Türleri.....	9
4.4.1 Fiziksel Erişim	9
4.4.2 Ağ Erişimi.....	10
4.4.3 Üçüncü Taraf Erişimleri	10
4.5 Sorumluluklar	11
4.6 Uygulama ve Ceza.....	11
4.7 Gözden Geçirme ve Onay.....	12
5. ERİŞİM KONTROLÜNÜ SAĞLAMA ADIMLARI.....	12
5.1 Kimlik Tanımlama.....	12
5.2 Kimlik Doğrulama	13
5.3 Yetkilendirme	14
KAYNAKÇA	16

1. GİRİŐ

Bilgi Güvenliđi Yönetim Sistemi (BGYS) kapsamında hazırlanması gereken politikalardan bir tanesi de EriŐim Kontrol Politikasıdır. EriŐim Kontrol Politikası kuruma ait olan bilgiye erişimlerin hangi kurallar çerçevesinde olması gerektiđini ortaya koyar.

1.1 Amaç ve Kapsam

Bu doküman, bünyesinde bir Bilgi Güvenliđi Yönetim Sistemi (BGYS) hayata geçirmek isteyen kurumlara erişim kontrol politikası oluŐturma konusunda yol gösterici bilgiler vermeyi hedeflemektedir.

Bu dokümanda kurumların sahip oldukları bilgi varlıklarına fiziksel ve mantıksal erişimler ele alınmaktadır.

1.2 Hedeflenen Kitle

Bu doküman Bilgi Güvenliđi Yönetim Sistemi (BGYS) kurulumu gerçekleŐtiren kurum ve kuruluşlara yönelik olarak hazırlanmıştır.

1.3 Kısaltmalar

BGYS : Bilgi Güvenliđi Yönetim Sistemi

UEKAE : Ulusal Elektronik ve Kriptoloji AraŐtırma Enstitüsü

2. ERİŞİM KONTROLÜ

Erişim kontrolü, en basit tanımıyla, belli bir varlığa sadece yetkili kişi veya grupların tanımlanan haklar dahilinde erişebilmesini sağlama amacıyla uygulanır. Bu erişim fiziksel olabileceği gibi mantıksal bir erişim de olabilir. En genel haliyle mantıksal erişim bir bilgi varlığına bilgisayar aracılığıyla yapılan erişimleri ifade eder.

Fiziksel güvenlik kapsamında erişim kontrolü bir mülke, binaya veya odaya girişin sadece yetkili kişilere kısıtlanması olarak karşılık bulmaktadır. Fiziksel erişim kontrolü bir insan (güvenlik görevlisi, kapıcı vb.), mekanik engeller (kilit, anahtar vb.) veya teknolojik geçiş kontrol sistemleri (kart, parmak izi vb.) kullanılarak sağlanabilir.

Bilgi güvenliği kapsamında ise erişim kontrolü kimlik doğrulama (*authentication*), yetkilendirme (*authorization*) ve izlenebilirlik (*accountability*) kavramlarını içine almaktadır. Erişim kontrol modelinde varlıklara erişenler ve sistemde aktif halde olanlara özne (*subject*), erişilen kaynaklara ise nesne (*object*) denilir. Bir erişim kontrol sisteminin sağladığı temel servisler şunlardır:

- Kimlik doğrulama ile sisteme hangi öznelerin giriş yapabileceğinin belirlenmesi
- Yetkilendirme ile öznelerin hangi işlemleri yapmaya veya hangi nesnelere erişmeye yetkili olduğunun belirlenmesi
- İzlenebilirlik ile öznelerin sistemde hangi işlemleri yaptıklarının veya hangi nesnelere eriştiklerinin bilinmesi ve gözlenebilmesi

Bilinen 2 tür erişim kontrol tekniği mevcuttur. Bunlar:

- İsteğe bağlı erişim kontrol (Discretionary Access Control)
- Zorunlu erişim kontrol (Mandatory Access Control)

İsteğe bağlı erişim kontrolde varlığa kimlerin veya hangi öznelerin, hangi yetkiler dahilinde erişebileceğini o varlığın sahibi belirler. Zorunlu erişim kontrol tekniğinde ise erişim yetkileri sistem tarafından tanımlanır, varlığın (bilginin) sahibi tarafından değil. Zorunlu erişim kontrolünde, nesnelerin içerdiği bilginin etiketle belirtilen hassasiyet derecesine ve erişimde bulunacak öznelerin sahip olduğu resmi yetkilendirmeye (klerans) bağlı olarak erişim kısıtlanır.

Erişim kontrolü konusunda bilinmesi gereken önemli bir prensip bulunmaktadır. “En düşük erişim hakkı”, veya diğer bir tabirle “Mümkün olan en az yetki”, (*least privilege*) prensibince erişimde bulunan özneye kendisine atanmış olan görevlerini gerçekleştirmelerine yetecek en düşük seviyede erişim hakkı verilmelidir. Örneğin veritabanından raporlama amacıyla okuma yapan bir programa sadece gerekli tablolardan okuma yapmasına izin verilmelidir. Bu programın başka tablolardan okuma yapabilmesi veya yazma işlemi gerçekleştirmesi en düşük erişim hakkı ilkesine aykırıdır. Bu prensip ayrıca bilmesi gereken ilkesi (*need-to-know principle*) olarak da bilinir.

Erişim kontrol politikası kurumun bilgi varlıklarına hangi kurallar ve şartlar dahilinde, kimlerin (hangi öznelere), hangi yetki ve imtiyazlarla erişebileceğini kurallar dahilinde belirleyen dokümandır.

3. ÖN ÇALIŞMALAR

3.1 Standarda Danışma

Bilgi güvenliğinin tesis edilmesinde erişim kontrolü önemli bir yer tutmaktadır. Türk Standartları Enstitüsü tarafından yayınlanan “TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri” isimli dokümanda erişim kontrolü (denetimi) konusu detaylı bir şekilde işlenmiştir. TS ISO/IEC 17799 standardı kurumların iş ve güvenlik ihtiyaçlarını temel alarak bir erişim kontrol politikası oluşturması, doküman etmesi ve gözden geçirmesi gerektiğini ifade eder. Erişim kontrol politikası hazırlamadan önce bilgi edinmek amacıyla bu dokümanın incelenmesi tavsiye edilmektedir.

3.2 Fikir Edinme

Fikir edinme amacıyla aynı veya benzer alanda faaliyet gösteren başka kurumların erişim kontrol politikaları gözden geçirilebilir. Biçim, kullanılan dil ve kapsanan konular açısından başka örneklerin incelenmesi fayda sağlayabilir. Öte yandan bu tip bir çalışmanın olası zararlarından da kaçınmak gerekir. Fikir edinme amacıyla yapılan bir çalışma başka kuruma ait bir politikanın birebir veya büyük oranda kopya edilmesi ile de sonuçlanabilir. Bu şekilde oluşturulan bir politikanın fayda getirmeyeceği baştan kavranmalıdır. Hazırlanacak erişim kontrol politikası kurumun kendi güvenlik ihtiyaçlarına yönelik bir belge olmalıdır. Her erişim kontrol politikasının kuruma özel bir belge olduğu unutulmamalıdır. Başka politikaların incelenmesi fikir edinmeden öteye geçmemelidir.

4. ERİŞİM KONTROL POLİTİKASININ OLUŞTURULMASI

4.1 Kapsam Belirleme

Erişim kontrol politikası oluştururken ilk yapılması gereken kapsamın belirlenmesidir. Politikanın kurallarının kimlere ve hangi bilgi varlıklarına uygulanacağı baştan belirlenmelidir. Kontrole tabi olacak erişimde bulunan özneler (*subject*) ile erişilen bilgi kaynağı olan nesnelere (*object*) açık bir şekilde tanımlanmalıdır.

4.2 Nesnelere (varlıkların) Sınıflandırılması

Kurum için değer ifade eden ve bu sebeple korunması gereken unsurların tamamı varlık kategorisine girmektedir. Bilgi güvenliği kapsamında en temel varlık bilgisidir. Bilgi pek çok farklı yerde farklı biçimlerde bulunabilir. Etkin bir erişim kontrol politikasının hazırlanabilmesi için kurum varlıklarının listelenmesi ve sınıflandırılması gerekli bir önkoşuldur (bkz. Varlık Envanteri Oluşturma ve Sınıflandırma Rehberi). Varlık envanteri erişim kontrolünün uygulanacağı nesnelere (*object*) ayrıntılı dökümünü ve bunların değerlerini verir. Bu sayede hangi varlığın ne seviyede bir korumaya gerek duyduğu bilinmiş olur.

Varlık envanterinde bulunabilecek bilgi varlıkları;

- Veritabanları, veri dosyaları, arşivlenmiş bilgiler, sistem belgeleri, süreklilik planları
- Uygulama yazılımları, sistem yazılımları, geliştirme araçları
- Bilgisayar bileşenleri, donanımlar, aktif cihazlar, optik ve manyetik ortamlar

olabilir.

Erişim kontrol politikası hazırlanması sürecinde ayrıca risk analizi sonuçlarından da faydalanmak hazırlanacak politikanın etkinliğini önemli ölçüde etkiler. Varlık envanteri oluşturma süreci sonrasında kurum içinde uygulanacak bir risk analizi hangi varlıkların öncelikli olarak ve daha sıkı bir şekilde korunması gerektiğini ortaya koyar. Bu sebeple risk analizi sonuçlarından yola çıkarak uygun kontrollere erişim kontrol politikasında yer verilmelidir.

4.3 Öznelerin (kullanıcıların) Sınıflandırılması

Kurumun bilgisine pek çok farklı sınıfta özne erişebilir. Özneler bilgiye erişimde bulunan aktif unsurlardır. Bunlar kullanıcılar, programlar, program süreçleri, kurum dışı kullanıcılar

olabilir. Özneler farklı erişim seviyelerine sahip gruplar veya roller kullanılarak sınıflandırılabilir. Tanımlanan rollere erişim hakları verilerek nesnelere erişim daha rahat ve etkin bir şekilde denetim altında tutulabilir. Bu roller kurum içinde üstlenilen görev ve sorumluluklara göre oluşturulabileceği gibi erişilen bilgi varlığının sınıfına göre de olabilir.

Erişimde bulunan öznelerin sahip olabileceği roller;

- Yöneticiler
- Departman yöneticileri
- Sistem yöneticileri
- Kullanıcılar
- XYZ projesi çalışanları
- Kurum dışı kullanıcılar

olabilir.

4.4 Adreslenecek Erişim Türleri

Bilgiye veya bilgi kaynaklarına erişim farklı yollardan olabilir. Bilgiye fiziksel yollarla doğrudan ulaşmak mümkün olduğu gibi bir bilgi ağı üzerinden de erişilebilir. Oluşturulan erişim kontrol politikası bu erişim türlerini kapsamalıdır. Ayrıca kurum dışından olan kullanıcıların ihtiyaç halinde kurumun bilgi kaynaklarını kullanması da erişim kontrol politikası ile denetime tabi tutulmalıdır.

4.4.1 Fiziksel Erişim

Bilgi varlıklarının bulunduğu fiziksel ortamlara erişim, Erişim Kontrol Politikasında ele alınmalıdır. Fiziksel erişim kontrolü kapsamında politikada düzenlenebilecek bazı örnek kontroller şunlar olabilir:

- Kritik varlıkların bulunduğu fiziksel ortamlara (örneğin sistem odası) girişlerin güçlü kimlik doğrulama ve kimlik tanımlama metotları ile kontrol edilmesi
- Bilgi sistem aygıtları ve bilgi içeren her türlü ekipmanlara fiziksel erişimin kullanıcı başında bulunmadığı zaman zarfında kontrol altına alınması
- Sistem odasına girmeye yetkili olmayan ama bakım/onarım, danışmanlık v.b gibi amaçlarla sistem odasında çalışma ihtiyacı olan kişilerin uygun kontroller altında çalışması

4.4.2 Ağ Erişimi

Günümüzde bilgiye erişimlerin büyük kısmı bilgisayar ağları üzerinden gerçekleşmektedir. Kullanıcılar istemciler vasıtasıyla ağ üzerinden sunumcular üzerindeki bilgilere erişerek işlerini yerine getirmektedirler. Bu erişimler yerel ağlar üzerinden olabildiği gibi internet benzeri geniş ağlar üzerinden de olabilmektedir. Ağ erişim kontrolünde temel amaç ağ üzerinden ulaşılabilecek bilgilere yetkisiz erişimleri engellemektir. Yetkisiz erişimlerin önüne geçmek için uygun kimlik doğrulama mekanizmalarının uygulanmış olması gerekmektedir. Ağ erişimi kontrolü kapsamında politikada düzenlenebilecek bazı örnek kontroller şunlar olabilir:

- Kullanıcıların kurum tarafından sağlanan İnternet çıkışı dışında başka yollar (modem, kablosuz ağ, GSM bağlantıları v.b) üzerinden İnternet'e erişimlerinin kontrol edilmesi
- Kullanıcıların İnternet üzerindeki erişebileceği servislerin tanımlanması (http, https ve smtp gibi) ve söz konusu servisler dışındaki başka servislere erişim taleplerinin yetkili birimlerce denetlenmesi ve onaylanması
- Kurum dışından kurumun bilgi ağı servislerine yapılacak bağlantıların yetkisiz erişimlere izin vermeyecek şekilde denetlenmesi ve kontrol altına alınması
- Kurum içinde gizlilik seviyelerine uygun bilgi ağlarının kurulması ve kritik bilgi içeren ağların uygun kontrollerle (kimlik doğrulama, yetkilendirme, sınır koruma vb.) korunması
- Yönlendirici ve anahtar gibi aktif cihazlar üzerinde yetkisiz erişimi engelleyecek yönlendirme kurallarının tanımlanması

4.4.3 Üçüncü Taraf Erişimleri

Günümüz iş dünyasında kurumlar ihtiyaç gereği sıklıkla dışarıdan farklı alanlarda hizmet alımına gitmektedirler. Bu durum kurum dışı üçüncü taraf kişilerin kurum içinde çalışması veya kurum bilgisine erişmesi ihtiyacını doğurmaktadır. Kurum bilgisini koruma amacıyla kurum dışı kullanıcılara daha farklı bir erişim kontrolü uygulanmalıdır. Bilmesi gereken ilkesi gereğince üçüncü taraf erişimleri bu kullanıcıların sadece görevlerini yerine getirmeye yetecek kadar olmalıdır. Ayrıca üçüncü taraf erişimleri mutlaka denetlenmeli, herhangi bir yetkisiz erişim girişimi olup olmadığı sürekli kontrol edilmelidir. Üçüncü taraf erişim kontrolü kapsamında politikada düzenlenebilecek bazı örnek kontroller şunlar olabilir:

- Üçüncü tarafa ait şirketler/kurumlar/kuruluşların kurum dahilinde herhangi bir hizmet

kapsamında kurumun bilgilerine ve bilgi sistemlerine erişim izni verilmeden önce risk analizi yapılması

- Kurum dışı kullanıcılara risk analizi sonuçlarına göre erişim izinleri verilmesi
- Üçüncü tarafa ait şirketler/kurumlar/kuruluşların erişecekleri varlıkların sahiplerinin söz konusu erişimlerin güvenliğinin sağlanması adına gerekli tedbirleri alınmasından sorumlu tutulması

4.5 Sorumluluklar

Erişim kontrol politikası ile ilgili sorumlulukların belirlenmesi gerekmektedir. Erişim kontrol politikasının geliştirilmesinden, gözden geçirilmesinden, uygulanmasından ve güncellenmesinden kurum içinde sorumlu kişi veya gruplar belirlenmelidir.

Erişim kontrol politikasının kullanıcılar tarafından bilinmesini ve anlaşılmasını sağlamaktan, diğer tüm politika ve prosedürlerin bu politika ile tutarlı olmasından üst yönetim sorumlu olmalıdır.

Kurumun yapısına ve güvenlik ihtiyacına uygun olarak, varlıklara erişim için gerekli yetkilendirme veya yetkilendirme isteğini onaylamak varlık sahibinin sorumluluğunda olabileceği gibi merkezi bir üst kurulda da olabilir. Her iki durumda da ilgili sorumlu belirli ve tanımlı olmalıdır.

Kullanıcılar erişim kontrol politikası ile beraber

- ilgili politika ve prosedürdeki kuralları bilmekten ve bu kurallara uymaktan
- bilgi varlıklarına erişim hakkı istemek için kurum tarafından onaylanmış süreç ve prosedürleri kullanmaktan
- şifre, akıllı kart gibi kimlik doğrulama bilgilerini korumaktan
- bilgi kendi kullanımlarındayken bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini varlık sahibi tarafından belirlenen önlemlere uygun olarak korumaktan

sorumlu olmalıdırlar.

4.6 Uygulama ve Ceza

Erişim kontrol politikası tarafından düzenlenen kurallara uymayanlara uygulanacak yaptırım ve cezalar politika içinde açık ve net bir şekilde ifade edilmelidir. Bu yaptırımlar politikayı ihlal edenler hakkında disiplin süreci başlatılması veya gerekli yasal işlem başlatılması gibi

uygulamalar olabilir. Kullanıcılar erişim kontrol politikasına uyulmadığı zaman ne gibi yaptırımlara maruz kalacağını baştan bilmelidirler.

4.7 Gözden Geçirme ve Onay

Erişim kontrol politikası hazırlandıktan sonra gözden geçirilmeli ve gerek duyulursa değişiklikler uygulanmalıdır. Kurum içinde yayınlanmadan önce politika üst yönetim tarafından onaylanmalıdır. Erişim kontrol politikasının gözden geçirilmesi ve onaylanması kurum tarafından belirlenecek düzenli zaman aralıklarında (altı ayda bir gibi) tekrarlanmalıdır.

5. ERİŞİM KONTROLÜNÜ SAĞLAMA ADIMLARI

5.1 Kimlik Tanımlama

Kimlik tanımlama (*identification*) kullanıcının kimliğini bilgi sistemine beyan etmesidir. Bu beyan kullanıcı adı, akıllı kart, manyetik kart, biyometrik özellikler (parmak izi, iris, ses vb.) aracılığıyla olabilir. Gerçek kişiler dışında bilgisayarların, uygulamaların ve program süreçlerinin de tanınabilecek kimlikleri olmalıdır. Bilgi sistemine erişimde bulunan her öznenin sisteme girişte kimliğini doğru şekilde beyan etmesi erişim kontrol politikasıyla düzenlenmelidir. Bu kimliklerin güvenliği erişim kontrolünün sağlanması açısından önemlidir. Kullanıcılar kendilerine ait kimlikleri korumaları konusunda sorumlu tutulmalıdırlar. Bir başkasına ait kimliği kullanarak yapılacak erişimler önlenmeli ve izlenmelidir. Başkasına ait kimlikle yapılacak erişim teşebbüslerinin ne gibi yaptırımlarla cezalandırılacağı açık bir şekilde belirtilmelidir. Kimlik tanımlama ile ilgili olarak erişim kontrol politikasında düzenlenebilecek bazı örnek kontroller şunlar olabilir:

- Her kullanıcının kendine ait ve kendisini benzersiz olarak tanımlayan bir kullanıcı hesabının olması
- Kullanıcıların kullanıcı hesaplarını paylaşarak bilgi kaynaklarına erişmemesi, aksi takdirde yaptırımların uygulanması
- Kullanıcıların kullanıcı hesaplarını ve parolalarını başkalarıyla paylaşmaması, aksi takdirde kullanıcı hesabıyla yapılan tüm işlemlerden kullanıcı hesap sahibinin sorumlu tutulması
- Kurumla ilişkisi kesilen kişilerin kullanıcı hesaplarının belli bir süre içinde devre dışı bırakılması

- Kurumda görev değiştiren kullanıcının, iş gereksinimi yoksa kullanıcı hesabının silinmesi, iş gereksinimi varsa söz konusu gereksinime göre erişim haklarının yeniden düzenlenmesi
- Belli bir süre zarfında kullanılmayan kullanıcı hesaplarının devre dışı bırakılması
- Belli bir süre zarfında devre dışı kalmış kullanıcı hesaplarının silinmesi
- Geçici kullanıcıların (test amaçlı kullanılan, yarı zamanlı kullanıcılar, stajyerler vb.) tahmini iş bitiş tarihlerine göre kullanıcı hesaplarına son kullanım tarihi verilmesi

5.2 Kimlik Doğrulama

Kimlik doğrulama (*authentication*), kullanıcının beyan ettiği kişi olduğunu ispatlamasıdır. Kimlik doğrulama amacıyla en yaygın olarak kullanılan yöntem parola kullanımınıdır. Kimlik doğrulama yöntemleri üç temel gruba ayrılır:

- Bilinen bir şey ile
- Sahip olunan bir şey ile
- Biyolojik bir özellik ile

Parola ile sisteme giriş bilinen bir şey ile kimlik doğrulama yöntemidir. Akıllı kartlar, tek seferlik parola, manyetik kartlar vb. gibi kullanıcıya tahsis edilen cihazlarla sisteme giriş sahip olunan bir şey ile kimlik doğrulama yöntemidir. Retina, iris, parmak izi, el ayası, ses, yüz şekli gibi kullanıcının biyolojik özelliklerinin önceden kaydedilerek sisteme girişte kaydedilen örnekle karşılaştırılması ise biyolojik bir özellik ile kimlik doğrulama yöntemidir. Bu yöntemlerden sadece birinin kullanılması zayıf kimlik doğrulama olarak bilinir. Bu yöntemlerden en az ikisinin beraber kullanılması güçlü kimlik doğrulama olarak adlandırılır.

Erişim kontrol politikasında kurum içinde hangi kimlik doğrulama yöntemlerinin kullanılacağı ve bunların doğru kullanımının ne şekilde olacağı açıkça belirtmelidir. Kullanıcıların sahip oldukları parola, akıllı kart, manyetik kart vb. gibi gizlilik ihtiva eden bilgilerin güvenliğinden sorumlu olduğu ifade edilmelidir. Bilgi sisteminde bulunması gereken, bu gizli kimlik bilgilerinin korunmasını ve sadece sahip olan kişi veya öznelere kullanılmasını sağlayan güvenlik ayarları erişim kontrol politikasında belirtilmelidir. Kimlik doğrulama mekanizmalarını yanıltmaya veya geçersiz kılmaya yönelik yetkisiz erişim teşebbüslerinin cezalandırma anlamında sonuçlarından bahsedilmelidir.

Kimlik doğrulama ile ilgili olarak erişim kontrol politikasında düzenlenebilecek bazı örnek kontroller şunlar olabilir:

- Tüm kullanıcı hesaplarına ait bir parolanın olması
- Yeni kullanıcı hesaplarına ait parolaların ilk kez giriş yapılırken kullanıcı tarafından değiştirilmesi
- Kimlik doğrulama bilgilerinin sahipleri dışında hiç kimse tarafından kullanılmaması
- Kullanıcı hesaplarına ait parolaların uyması gereken kuralların belirtilmesi (en az 8 karakter olması, içermesi gerek zorunlu karakterler, belli aralıklarla değiştirilmesi, başarısız parola denemelerinin belli bir sayıyla sınırlandırılması gibi)
- Bilgi kaynaklarına başarısız erişimlerin tarih, zaman ve erişilen kaynağın detayı ile ilgili bilgilerinin kaydının tutulması
- Kullanıcıların kimlik doğrulaması yaparak oturum açtıkları sistemlerin başından ayrıldıklarında sistemi kilitlemesi
- Halka açık veya paylaşılan ağlardan iletilen kimlik bilgilerinin güçlü şifreleme metotları ile korunması
- Başkaları tarafından öğrenildiğinden şüphelenilen parolaların hemen değiştirilmesi

5.3 Yetkilendirme

Yetkilendirme (*authorization*) kullanıcıların hangi yetkilere sahip olduğunun, hangi bilgi varlıklarına hangi yetkilerle erişeceğinin belirlenmesidir. Genel tanımla yetkilendirme öznelerin nesnelere üzerindeki erişim izinlerinin tanımlanmasıdır. Yetkilendirme amacıyla kullanılacak iki yöntem mevcuttur:

- İsteğe bağlı erişim kontrol (Discretionary Access Control)
- Zorunlu erişim kontrol (Mandatory Access Control)

Giriş bölümünde bu yöntemler açıklanmaktadır. Erişim kontrol politikasında kurum içinde kullanılacak yetkilendirme yönteminin ne olacağı belirtilmelidir. Erişim kontrol politikası kullanıcılara erişim izinlerinin bilmesi gereken ilkesine uygun şekilde verilmesini sağlamalıdır. Kurum için kritik derecede hassas bilgi varlıklarına erişim uygun bir şekilde kısıtlanmalıdır.

Yetkilendirme ile ilgili olarak erişim kontrol politikasında düzenlenebilecek bazı örnek kontroller Őunlar olabilir:

- Özel olarak yetkilendirme yapılmadıđı sürece tüm bilgi varlıklarına erişimin yasaklanması
- Kullanıcılara sadece iş sorumluluklarını veya iş gereksinimlerini yerine getirmelerine yetecek kadar izin verilmesi
- Herhangi bir şekilde fazla yetkiye sahip kullanıcıların bu yetkiyi kullanarak iş sorumluluklarının veya iş gereksinimlerinin dışında bilgiye ulaşmasının yasaklanması
- Fazla/gereksiz yetkinin anlaşılması durumunda yetkilendirmeden sorumlu kişilere ve varlık sahibine haber verilmesi
- Dosya, dizin ve diđer objelere erişim izinlerinin gruplara verilmesi, gerekmediđi sürüce kişilere özel izin verilmesinden kaçınılması
- Bir kullanıcının sisteme aynı anda birden çok kez girme sayısının iş gereksinimlerine göre kısıtlanması
- Yönetim yetkilerinin sadece özel olarak bu yetkilere ihtiyaç duyanlara verilmesi
- Yönetim işlemlerini gerçekleőtiren kişilerin sadece yönetimsel haklar gerektiren işler için yönetim hesaplarını kullanması
- Yetkilendirmelerin belirli aralıklarla gözden geçirilmesi, gereksinimi kalmamış yetkilerin geri alınması.

KAYNAKÇA

- [1]. ISO/IEC 27002:2005, Information technology -- Security techniques -- Code of practice for information security management standard
- [2]. NIST Special Publication 800-100 “Information Security Handbook: A Guide for Managers”
- [3]. NIST Special Publication 800-115 “Technical Guide to Information Security Testing”
- [4]. Alan Calder, Steve Watkins, “IT Governance – A manager’s guide to data security and ISO 17799”,2005, Cambridge University Press