Kimlik Yönetim Sistemi Merkezli Bütünsel Bilgi Güvenliği

Yılmaz Çankaya [1],

[1] TÜBİTAK-UEKAE, Gebze/Kocaeli

[1] e-mail: yilmaz.cankaya@uekae.tubitak.gov.tr

Abstract

Although the term *Identity Management* (IdM) has not been recently added to our informatics dictionary, it could not gain the importance deserved and moreover, mostly misinterpreted as a set of managerial business processes causing increase in workload. Centralized identity management not only addresses the security needs on application layer, but on the network layer, on operation system level, database level and storage device level as well. Having accomplished the security and control of all data access processes through the management of identities those accessing any form of protected data, with some additional complementary but crucial security measures, in a holistic approach we may talk about the overall security of the information system. A successful implementation of an IdM system, due to the centralization of data access rules, policies and flows through out the ecosystem, should provide a managable and auditable information system that also complies with regulatory measures and standards.

Keywords: Identity Management, Enterprise Information Security, Authentication, Authorization, OS Security, Database Security, Application Security

1. Giriş

Bilgi işleyen tüm sistemlerin en temel amacı verilerin saklanması, işlenmesi ya da görüntülenmesinin sağlanmasıdır. Bu temel amaca ek olarak, verilere erişim kontrolü yapmayan bir sistemin güvenliği, o sistemin ya da uygulamanın varlığından haberdar olmakla eşdeğerdir. Bilgisayar sistemlerinin yaygın olarak kullanılmaya başlanmasıyla birlikte bu uygulamalar için kimlik doğrulaması, yetkilendirme, izleme, süreklilik gibi temel güvenlik fonksiyonların uygulamalara eklenmesine karşın, çok sayıda varlığı ve uygulamayı barındıran karmaşık sistemlerde bu güvenlik mekanizmalarını yönetmek kolay olmamaktadır. Herhangi karmaşık bir sistemde bulunan bu varlık ve uygulamalara kullanıcıların etkin olarak erişimini kontrol etmek için kimlik yönetim sistemlerine ihtiyaç duyulmaktadır.

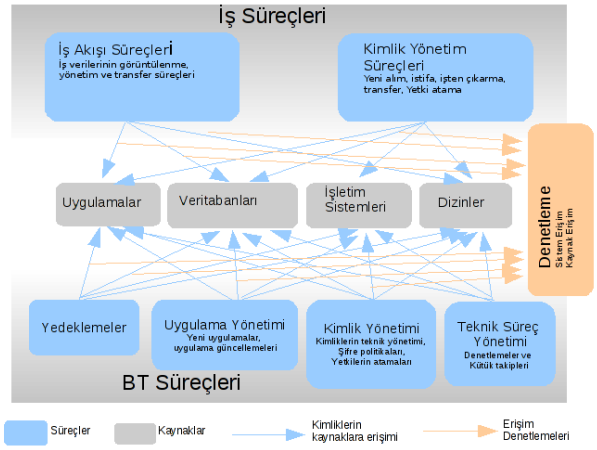
Güvenlik söz konusu olduğunda, ister fiziksel ister sayısal güvenlikten bahsediyor olalım, *tanımlama* (identification) ve *erişim* (access) açıklayıcı terimler olacaktır. İş yeri girişinde güvenlik görevlilerinin kimliğinizi kontrol etmesi tanımlama, size verilen giriş kartı ile belli kısımlara giriş izninin verilmesi ise erişim olarak tanımlanabilir. Doğruluğunu elinizdeki bilgiler ile sağlayabildiğiniz *tanımlama* kimlik doğrulama ve doğruluğundan emin olduğunuz bir *tanımlama* ise güçlü kimlik doğrulamadır [12],[7],[6].

Kimlik yönetimi penceresinden bakıldığında, kurumsal bilgi güvenliğinin sağlanması çalışmalarında en büyük engel, uygulama geliştirme ve analiz aşamasında bilgi güvenliğinin bütünsel ve kurumsal olarak göz önünde bulundurulmadan uygulamaların geliştirilmiş olmasıdır. Bir diğer ifadeyle, uygulamanın nasıl çalışacağı, neler yapabileceği ve kimin neye erişebileceğinin belirlendiği iş süreçlerine tamamlayıcı olarak, uygulamayı kullanacak kimliklerin bütün organizasyon ile ilişkisi olduğu gerçeği ihmal edilmiştir. Kurum ya da kuruluşun bünyesinde barındırdığı uygulamalarda

- Bir kişinin aynı anda birkaç uygulamayı kullanabiliyor olması
- Erişim kontrol noktalarının atomik yapıda olması
- Müşteri (B2C) ve tedarikçilerin (B2B) de kısıtlı yetkilendirmeler ile sisteme katılıyor olması
- Uygulamaların sanal kimlikler üzerinden birbiri ile iletişim içinde bulunması
- BT (Bilişim Teknolojileri) çalışanlarının veriye arka kapılardan erişebiliyor olması
- Kimlik doğrulama ve yetkilendirme kontrollerinin, yetkili kullanıcılar tarafından atlatılabiliyor olması

gibi zorluklar kimlik doğrulama, yetkilendirme (erişim) ve izleme yönetiminin kurumsal bazda ele alınması ve bilgi güvenliğini sağlama çalışmalarının merkezinde oturması gerektiğini işaret etmektedir.

Yukarıdaki örnekte verilen kimlik yönetim sistemini yine • yukarıda listelenen ve sayısal güvenliği, fiziksel güvenlikten ayıran farklar da göz önünde bulundurularak, kurumsal sayısal güvenlik yapısına uyarlanırsa, önümüze çok karmaşık ve yönetilmesi çok zor bir yapının çıkacağı söylenebilir. İş süreçleri (iş verisinin yönetimi ve işe alma, istifa, transfer, kiralama gibi kimlik yönetim süreçleri) uygulamalar aracılığı ile ya da doğrudan kimliklerin yetkileri çerçevesinde kaynaklara erişimi ve veri üzerindeki eylemler ile gerçekleşirler. Aynı kaynaklara BT çalışanları uygulamalar üzerinden ya da arka kapılardan çoğunlukla yüksek yetkiler ile erişebilirler. Müşteriler ve tedarikçiler de kurum tarafından atanan yetkiler ile verilere ulaşabilir ve iş süreçlerine dahil olabilirler. Farklı kaynaklara farklı kimlikler ile ulaşılmaya çalışıldığında, hatta aynı kaynağa farklı kimlikler ile ulaşmak mümkün ise, kişi-kimlik-kaynak matrisinin ne kadar karmaşık olacağı ve denetiminin zorlaşacağı Şekil 1'de gösterilmiştir.



Şekil 1 - KYS'siz kurumsal süreçler

Tümden gelim yöntemi kullanılarak;

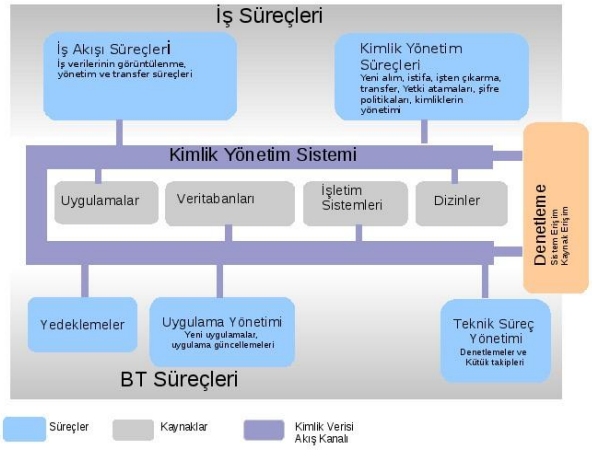
- Güvenliğin organizasyon bazında ele alınması,
- Kimlik yönetim süreçlerin belirlenmesi,
- Kişi-kimlik-kaynak matrisinin oluşturulması
- Bilgi sistemi katılımcılarının (müşteri, tedarikçi, çalışan, BT personeli, sanal kimlikler) kaynaklara erişiminin sağlıklı bir şekilde denetlenmesi

gibi konular da göz önünde bulundurularak, güvenilir, sürekli ve değişikliklere hızlı uyum sağlayan bir bilgi güvenliği yapısının oluşturulması, kimlik yönetim sistemi çıkış noktalı bir yapının kurulması ile mümkündür. Böyle bir yapı, tamamlayıcı güvenlik önlemleri ile birlikte *KYS Merkezli Bütünsel Bilgi Güvenliği Modeli* gerçekleyebilecek ve Şekil 1 - *KYS'siz kurumsal* 'de gösterilen karmaşıklığın da çözümü olacaktır.

Kimlik yönetimine tümden gelim yönetimi ile bakıldığında, bilgi güvenliğine ait bütün parçaların daha sağlam yerine oturduğu ve her bakımdan kontrolü kolay bir bilgi güvenliği sisteminin oluştuğu görülecektir. Bunu sağlayan faktör kimlik yönetiminin merkezileştirilmesi değil, daha çok müşteri, tedarikçi ve çalışanlarıyla iş süreçlerinin organizasyon bazında ele alınması ve fiziksel olarak tekil olan kişilerin, sayısal sistemlerde de tek bir kimlikle sisteme dahil olmasının sağlanmasıdır. Bir diğer ifadeyle, uygulamaların kimlik yönetiminin sağlanması yerine kurumsal kimlik yönetiminin sağlanması esastır.

2. KYS Merkezli Bütünsel Bilgi Güvenliği Modeli

KYS merkezli bütünsel bilgi güvenliği modeli, daha önce anlatılan klasik kimlik doğrulama, yetkilendirme ve izleme tabanlı güvenlik sisteminin oluşturduğu sorunun ve karmaşık yapının çözümü için sunulan bir sistem önerisidir. Kimlik yönetim sistemi bu sistemin omurgasını oluşturmaktadır. Bütünsel bilgi güvenliği modeli, kimlik yönetim sistemi merkezli, kaynakları kontrol edebilen, gerçekleşen ya da gerçekleşemeyen eylemlerin bilgilerini (kütükler) içinde barındıran ve sayısal ortamın gerekleri nedeniyle de karmaşıklık seviyesinin artmış olduğu bir sistemin güvenliğinin sağlanması için atılması gereken adımları içerir. Şekil 1'ye bakıldığında kimlik yönetim sisteminin organizasyondaki konumu daha rahat görülecektir. Şekil 1 - *KYS'siz kurumsal* 'in aksine, kimlik yönetiminin bütün işlevleriyle iş süreci haline getirilmiştir. Ayrıca *Denetleme* fonksiyonu da KYS'ye entegre olmuş ve KYS içindeki bütün bilgi akışının aynı zamanda çevrimiçi denetlenebilir olması sağlanmıştır.

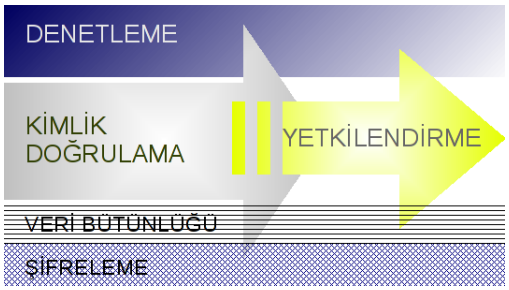


Şekil 2 - KYS destekli kurumsal süreçler

Bir bilgi sisteminin

- Birden fazla uygulamayı barındırdığını
- Uygulamaların birbiri ile sanal kimlikler ile etkileşim içinde olduğunu
- Müşterilerin sisteme dahil olduğunu (B2C)
- Tedarikçilerin sisteme dahil olduğunu (B2B)
- Çalışanların birden fazla uygulamayı kullanabildiğini

varsayarsak, her bir uygulamanın Şekil 3 uyarınca geliştirilmesi (güncellenmesi) ve başlangıç ve bitiş uçlarda güvenliğin sağlanması gerekmektedir. Şekil 3'te görüleceği üzere, kaynaklara erişimi sağlayan kritik iş akışlarının şifrelenmesi, veri özetleri kullanılarak veri bütünlüğünün sağlanması ve kimlik doğrulama, yetkilendirme süreçlerinin çevrimiçi denetlenebiliyor olması gerekmektedir.



Şekil 3- Temel Veri Erişim İş Akışı

Uygulamalar kimlik doğrulama ve yetkilendirme işlevlerini KYS aracılığı ile gerçekleştirmelidirler. Merkezi bir KYS

yapısının hayata geçirilmesi, uygulamaların güvenliğinin temin edilmesini ve buna ek olarak kurumsal değişikliklere daha hızlı adapte olabilen, işletim masraflarını azaltan, daha rahat yönetilebilen bir sistemin ve proaktif, doğruluğundan emin olacağımız rapor sonuçları üreten bir denetleme mekanizmasının oluşturulabilmesini mümkün kılacaktır [2]. Diğer taraftan, bu işlevleri yerine getiren bir yapı, uluslararası standartlara sürekli uyumlu, canlı bir sistemin var olmasını sağlayacaktır [10].

2.1. Kaynaklar ve Kimlik Yönetim Sistemi Entegrasyonu

Uygulamalar aksiyon ve eylemler gerçekleştirirler ve bu eylemler sanal ya da gerçek kimlikler üzerinden gerçekleştirilebilir. Dolayısıyla, uygulamanın sunduğu servisler ya da hizmetlerin özneleri kimliklerdir. Bütün boyutlarıyla uygulamaya alınmak istenen bir KYS için, veri akışının uçtan uca değerlendirilmesi ve bütün bileşenlerin güvenli hale getirilmesi esastır. Özneler, nesneler üzerinde eylemleri gerçekleştirirler [11]. Kimliğin eriştiği nesne ise *kaynak* (resource) olarak tanımlanabilir. Bütün kimliklerin kaynak erişimlerini tek tek takip etmek ve yönetmek zor olacağından, kaynak grupları ve kimlik grupları (roller) oluşturulabilir. Kaynaklara erişim için kimlik bazında istisna kurallar oluşturulabilmekle beraber, rollere kaynakları kullanma yetkileri atamak daha yönetilebilir ve izlenebilir bir ortam sunacaktır. Nitekim kimlikler, rollere göre değil de kişi gruplarına göre (Örn. müşteri, tedarikçi, iş ortağı, çalışan, BT pesoneli) sınıflandırıldığında, kurulumu güçleştiren kesişmeler olabilecektir. Bir çalışan aynı şirketin müşterisi hatta tedarikçisi bile olabilir.

Kaynak gruplarında, Şekil 3'ün uygulanabilmesini sağlamak amacıyla,

- Uygulamalar, sunduğu servisler ve servisler üzerinden gerçekleştirilebilen eylemler (Örn. ekle, güncelle, sil)
- Veritabanları
- İşletim sistemleri
- Dizin sistemleri

şeklinde sınıflandırma yapılabilir.
Ağ cihazları kaynak olarak listeye eklenmemiştir. Doğrudan iş verisi içermediklerinden, kapsam dışı bırakılmıştır. Bu cihazların http tabanlı arayüzleri *Uygulamalar* kaynak grubuna, işletim sistemi seviyesinde de *İşletim Sistemleri* kaynak grubuna dahil edilebilir. Depolama sistemleri ve ilintili cihazlar da ayrı bir kaynak grubu olarak ele alınabilir.

2.1.1. İşletim Sistemlerinin KYS'ne Geçirilmesi

Kurum ve kuruluşların birçoğunda heterojen bir yapı oluşmuş ve Unix, Linux, MS Windows ve Mac türevi işletim sistemleri değişken oranlarda hizmete alınmıştır. *Sanallaşma* teknolojisinin ortaya çıkışı ile beraber, işletim sistemlerinin üzerinde, işletim sistemleri kaynak grubuna dahil edilebilecek, yeni bir tabaka ortaya çıkmıştır. İşletim sistemlerinin kimlik yönetim sistemine katılımı hem kimlik doğrulama hem de yetkilendirme seviyesinde yapılabilmektedir [13], [14]. Bu kapsamda kimlik doğrulama sisteme giriş kontrolü ve yetkilendirme de kimliğin ait olduğu işletim sistemi grup bilgisinin, dosya ya da klasöre (kaynak) grup erişim izinleri ile karşılaştırılması anlamına gelmektedir.

İşletim sistemlerinin merkezi bir kimlik yönetimine geçişi için birkaç senaryo mevcuttur.

1. Windows tabanlı işletim sistemleri merkezi kimlik doğrulama ve yetkilendirme işlemlerini sadece Aktif Dizin (Active Directory) üzerinden gerçekleştirebilmektedir. Bu gerçekten yola çıkarak, Unix tabanlı işletim sistemlerinin, Aktif Dizin üzerinden kimlik doğrulama ve yetkilendirme (grup) sorgularını yapması tercih edilebilir. Böyle bir senaryoda da iki seçenek karşımıza çıkmaktadır.
    - LDAP protokolü üzerinden Aktif Dizin entegrasyonu

      Aktif Dizin üzerinde Unix kimlik yönetimi uyumlu LDAP dizin işlevlerinin oluşması için Microsoft's Services for Unix 3.5 kurulmalıdır. LDAP protokolü kullanılır ise, Aktif Dizin ile kendi dilinde konuşulmadığından, şifre politikaları uygulanamayacaktır. Diğer taraftan, Şekil 3'e göre *şifreleme* ve *veri bütünlüğü* özelliklerinin sağlanabilmesi için güvenli bağlantı gerçekleştirilmesi durumunda, istemci tarafında sertifika yönetimi yapılmak zorunda kalınacaktır.
    - *Winbind* üzerinden, *Microsoft RPC* çağrıları ile entegrasyon

      Winbind servisi üzerinden Microsoft RPC çağrıları ile Aktif Dizin ile konuşulması, daha entegre bir yapı sunmakla birlikte, uygulamaların ve işletim sistemlerinin bağımsız güncellemeler yapabilmesi nedeniyle beklenmeyen sonuçlar doğurma riskini barındırmaktadır.
2. Unix işletim sistemlerinin açık kaynak kodlu dizinler üzerinden kimlik doğrulama ve yetkilendirme yapmaları sağlanabilir. Böyle bir durumda, Windows işletim sistemleri ile aynı kimlik verilerini kullanabilmek amacıyla, dizin verisinin düzenli aralıklarla Aktif Dizin ile tek taraflı senkronizasyonu gerçekleştirilmelidir. Özellikle uygulamaların tümleşik oturum yönetiminde kullanılan dizin sunucunun bu amaç için kullanılması, daha az dizin sunucusu barındırmak ve yönetmek anlamına gelecektir.

İşletim sistemlerine giriş yapmış kullanıcıların, aynı zamanda uygulamaları da şifre girmeden kullanabilmesi kurumsal bir istek olarak karşımıza çıkabilir. Hem ticari hem de açık kaynak kodlu KYS ürünleri, örneğin *Kerberos* protokolünü kullanarak, bu servisi sunmaktadır.

2.1.2. Uygulamaların KYS ile Entegrasyonu

İş verilerinin sayısal ortamda yönetilmeye başlanması ile beraber, iş akışlarının ve verilerin uygulamalar aracılığı ile kontrolü ve verilerin sayısal olarak saklanması mümkün olmuştur. Kurumsal seviyede bilgi güvenliği söz konusu olduğunda, Şekil 3'de verilen fonksiyonların bütün kaynak erişim süreçleri için gerçeklenebilmesi ve kimlik yönetiminin de merkezi bir yapıya kavuşturulması gerekmektedir. Şirket bünyesinde farklı amaca hizmet eden uygulamalar çok farklı yazılım altyapısı ve farklı iş mantığı yapıları üzerine bina edilmiş olabilir.

KYS'lerin hayata geçirilmesi sırasında, en çekinilen konu da uygulamaların ne şekilde ve hangi seviyelerde değişiklik yapılarak KYS'ye entegre edilebileceğidir. Uygulamaların KYS ile entegrasyonunun kuşbakışı olarak zihinde canlandırılabilmesi için birkaç konunun göz önünde bulundurulması gerekmektedir.

- HTTP tabanlı uygulamalar için asıl olan tümleşik oturum yönetimine geçişin sağlanmasıdır. KYS tümleşik oturum yönetim sunucusu bütün HTTP tabanlı uygulamalara erişim öncesi araya girer ve kullanıcı için oluşturulmuş bir çerezin varlığını kontrol eder.
- HTTP tabanlı uygulamaların KYS ile entegrasyonu, uygulama sunucusu üzerine bir ajan (agent) uygulamanın kurulması ile sağlanabilir. Ajan uygulamalar, asıl kaynağa erişim için kullanıcı tarafından gönderilen talepleri keser ve KYS tümleşik oturum sunumcusu tarafından oluşturulan ve internet tarayıcısı tarafından gönderilen çerezin varlığını kontrol ederler. Çerezin geçerliliği sağlanır ise, yetkilendirme sorgusu (talep edilen kaynaklara erişim yetkisinin olup olmadığı) yapılır ve sonuç uygulamaya döndürülür.
- HTTP tabanlı uygulamaların ters vekil sunumcu (Reverse Proxy) arkasında çalışması durumunda, ajan uygulamanın sadece ters vekil sunumcu üzerinde yürütülüyor olması yeterli olacaktır ve bu durumda politika ajanlarının yönetimi de kolaylaşacaktır zira her uygulama sunucusu üzerinde ayrı bir ajan kurulması ihtiyacı ortadan kalkacaktır.
- KYS uygulamaları, kimlik doğrulama ve yetkilendirme sorgularının herhangi bir ajan uygulama kurulumuna ihtiyaç olmadan yazılımsal olarak gerçekleştirilebilmesi için yazılım arayüzleri (API) sunarlar. Bu servislerin kullanımı için, uygulamaların uygun şekilde güncellenmesi gerekmektedir.

HTTP politika ajanının kullanıldığı uygulamalar için son kullanıcı ve kaynak erişimi (Örn. HTTP tabanlı sayfanın çağrılması) şu akış gerçekleşir.

1. HTTP sunucuya entegre modül olarak çalışan, HTTP ajanı isteği keser ve istekte erişilmek istenilen kaynak korunmuyor ise (listeden kontrol edilir) şifresiz geçiş izni verilir.
2. Erişilmek istenen kaynak kimlik doğrulama gerektiriyor ise, kullanıcı *tümleşik oturum sunucusu* [2] giriş sayfasına yönlendirilir. (*HTTP Location* başlığı kullanılır)
3. Giriş kimlik bilgileri ve/veya biometrik/akıllı kart yöntemleri ile giriş yapılır. Kimlik yönetim sistemi tarafından, ilgili uygulama için öngörülen kimlik doğrulama prosedürleri uygulanır. (Örn. Hem şifre, hem de akıllı kart PIN girişi istenebilir)
4. Başarılı giriş sonrası KYS tarafından çerez oluşturulur ve kullanıcı internet tarayıcısı tarafından saklanır. Bundan sonraki iletişimlerde bu çerez kullanılarak HTTP ajanı tarafından kaynak erişim yetkisi kontrol edilir.
5. Bütün erişim kuralları yorumlandıktan sonran kullanıcının istenilen kaynağa erişebiliyor olması durumunda ilgili kaynağa yönlendirme yapılır.

2.1.3. Veritabanlarının KYS ile Entegrasyonu

Açık kaynak kodlu veritabanları da dahil olmak üzere (örn. PostgreSQL) profesyonel kullanım için hizmete alınan veritabanlarının büyük bir bölümü LDAP, Kerberos v.s. gibi protokoller üzerinden kimlik doğrulamayı desteklemektedir. Yaygın kullanılan ticari veritabanları ek olarak yetkilendirmeyi (rol yönetimi) de LDAP dizin üzerinden yapabilmektedir. Bu bağlamda karşımıza çıkan sorun, ticari veritabanlarının sadece kendi ürünü olan dizin sistemleri ile entegrasyonu desteklemeleri ve diğer dizinler ile entegrasyon için de sadece senkronizasyon hizmeti sunmalarıdır. Veritabanlarının LDAP dizin üzerinden kimlik doğrulama ve yetkilendirme (rol atamaları) yapıyor olmaları KYS entegrasyonu kapsamında bir gerek olmakla beraber, veritabanlarının böyle bir yapıya geçirilmesi durumunda sadece aynı firmaya ait dizin sunucularını destekliyor olmaları, KYS merkezi dizin sunucusu ile senkronizasyon gerçekleştirilse bile, verinin birden fazla yerde tutulması (redundancy criteria) anlamına gelebileceğinden bir dezavantaj olarak görülebilir. Sistem ve kaynak erişim denetiminin merkezi olarak raporlanabilmesi için, veritabanı LDAP dizin sunucusu üzerinde tutulan erişim kütüklerinin, KYS merkezi sunucusuna taşınması gerekmektedir.

Veritabanı kaynaklarına erişimleri de Şekil 3'e uygun olarak gerçekleştirmek, *KYS Merkezli Bütünsel Bilgi Güvenliği Modeli* 'ne geçiş için önemlidir. Şekil uyarınca, kimlik doğrulama ve yetkilendirme (rol atama) işlemlerinin LDAP dizinler üzerinden yapılması atılacak ilk adımdır. Bu geçiş sonrası denetleme işlevi kolaylıkla gerçekleştirilebilecektir. Veritabanına erişimin güvenli hale getirilmesi (şifreleme ve veri bütünlüğü) diğer önemli bir adım olmakla birlikte, güvenlik sıkılaştırmaları da korunan veriye erişim sağlayan önemli bir kanalın da kontrol altına alınmasını sağlayacaktır.

2.2. Tamamlayıcı Güvenlik Önlemleri

Organizasyon için değerli olan verinin korunması gerekir. Korunan verinin güvenliğinin sağlanması için veri erişim kanallarının Şekil 3'e göre yönetilmesi ve güvenli hale getirilmesi yeterli olmayacaktır. Bahsi geçen bölüm altında belirtilen güvenlik önlemleri veriye erişimin güvenli, denetlenebilir ve yönetilebilir hale getirilmesini sağlamakla beraber, uç kullanıcının kimlik denetimi, sürekli erişilebilirlik ve felaket kurtarma senaryoları gibi güvenlik önlemlerini içermediğinden, kurumsal seviyede bir güvenlik ancak güçlü kimlik doğrulama (biometrik , akıllı kart vb.), fiziksel güvenlik, süper yetkili kullanıcıların rolü, son kullanıcı uygulamalarının rolü gibi ek önlemler ile sağlanabilecektir. Diğer taraftan, güçlü kimlik doğrulama yöntemlerinin kullanılması son kullanıcı kaynaklı muhtemel açıklıkların minimize edilmesini temin edecektir. Daha yönetilebilir bir son kullanıcının kontrolü için ağ erişim kontrol (Network Access Control) ürünleri devreye alınarak, anti-virüs, saldırı önleme ve açıklık denetleme işlemleri gerçekleştirilebilir.

2.3. Kurumsal Bilgi Güvenliği Yönetimi ve ISO/IEC 27001

KYS uygulamaları ile, kimin, neye, ne zaman ulaşacağının kontrol altına alınıp raporlanabildiği bir bilgi güvenliği yapısına ulaşılabileceği gösterilmiştir. Fakat erişim güvenliğinin sağlanmış ve kontrol edilebiliyor olması, yönetilebilir bir bilgi güvenlik sistemine ulaşıldığı anlamına gelmemektedir. Kimlik yönetimi iş süreçleri (yeni kullanıcı ekleme, güncelleme, yetki atama, vs.); uygulamalar, veritabanları, dizinler ve işletim sistemleri için yönetilebiliyor olmakla beraber, verinin sürekli erişilebilmesini sağlayacak, felaket (disaster) durumlarında veriyi geri döndürecek (recovery) önlemler alınmadan, iş sürekliliğinin sağlanması mümkün değildir. Bunun da ötesinde, BT yapısı iş süreçlerine ve iş ihtiyaçlarına paralel olarak değişebileceğinden, kurumsal bilgi güvenliğinin temini süregiden, yönetimsel bir süreçtir. BT altyapısının hem donanımsal hem de süreçsel olarak tam bir haritasını çıkaran, varlık envanterini oluşturup, varlıkların sahiplerini atayan ve korunan bütün kaynakların sürekli erişilebilir olması için gerekli önlemleri içeren prosedürlerlerin hizmete alınması gerekmektedir. Bu amaçla oluşturulmuş standartlar mevcuttur. Özellikle ISO 27001 bu ihtiyaca yönelik hazırlanmış olmakla beraber, COBIT, ITIL gibi devreye alınabilecek başka standart ve çerçeveler bulunmaktadır.

3. Sonuç

İş süreçlerinin sayısal ortama kayması ile beraber BT süreçleri daha büyük önem kazanmış ve iş sürekliliğinin sağlanmasında anahtar bir faktör olmuştur. Kimlik yönetiminin organizasyon bazında bütüncül ve BT sistemlerinde bulunan fiziksel ya da sayısal kaynakları kapsayıcı bir şekilde ele alınmaması, en temel bilgi güvenliği esası olan veriye erişimin kontrolünü yönetilemez hale getirmiş, hızlı ve doğru denetlemeyi neredeyse imkansız kılmıştır. *KYS Merkezli Bütünsel Bilgi Güvenliği Modeli*'nin uygulanması durumunda, veriye erişen bütün iş ve bilgi teknolojileri süreçlerinin kontrol altına alınabiliyor olduğu ve kaynak erişim kontrolünün BT süreçleri olmaktan çıkıp, organizasyon hiyerarşisi içinde kontrol edilebilen iş süreçleri haline geldiği görülmüştür. Ayrıca, kurumsal bilgi sisteminde önemli rollere sahip süper yetkili kullanıcıların da denetlenebiliyor hale gelmesi, kimlik yönetimi iş akışlarının ilgili yönetici pozisyonlar tarafından yönetilebilmesi sayesinde mümkün olmuştur. Kimlik yönetim sisteminin başarılı bir şekilde bütün kaynak erişimlerini kontrol edebiliyor olması, yönetilebilir bir kurumsal bilgi güvenliği sağlanmış olduğu anlamına gelmeyeceğinden, ISO/IEC 27001 yönetim standartlarının da kurum ve kuruluşta uygulanması ile beraber, denetlenebilen ve güvenliğini yönetebildiğiniz bir sistem oluşmasını sağlayacaktır.

4. KAYNAKLAR

[1] The Role of Identity Management in Sarbanes-Oxley Compliance, White Paper, Sun Microsystems http://www.sun.com/software/products/identity/wp_identity_mgmt_sarbanes_oxley.pdf

[2] Kimlik Yönetimi, Kavramlar ve Gereksinimler, Yılmaz Çankaya, Haziran 2009, www.bilgiguvenligi.gov.tr

[3] Unified Logons between Windows NT and UNIX using Winbind, Tim Potter, Andrew Tridgell, Ekim 2000 http://wireless.ictp.it/school_2001/labo/linux/linux_guides/winbind.pdf

[4] Wave 10 IT Security Roadmap Report,TheInfoPro http://www.brainshark.com/theinfopro/infosec-pr1

[5] The History of Information Security: A Comprehensive Handbook, Karl de Leeuw and Jan Bergstra, 2007 Elsevier B.V

[6] Eine kurze Einführung in die Global Scaling Theorie, André Waser http://www.info.global-scaling-verein.de/EssaysD.htm

[7] Akıllı Kartlar ve Uygulamaları; Akıllı Kart Nedir?, Mustafa Başak, Tubitak UEKAE Dergisi, Cilt 1, Sayı 1, Eylül-Aralık 2009

[8] Application Research of using design pattern to improve layered architecture, Chen Liyan, 2009 IITA International Conference on Control, Automation and Systems Engineering (case 2009), ISBN: 978-0-7695-3728-3

[9] Oracle Database Vault, White Paper, Oracle Corp. June 2007 http://www.oracle.com/technology/deploy/security/database-security/pdf/database-vault-11g-whitepaper.pdf

[10] Using Identity Management to Achieve Security and Compliance, White Paper, Ocak 2005, Sun Microsystems http://www.sun.com/software/products/identity/wp_security_compliance.pdf

[11] Nesne Kavramı Üzerine http://yayim.meb.gov.tr/dergiler/148/5.htm

[12] Kholmatov, Alisher Anatolyevich and Yanıkoğlu, Berrin, "Identity authentication using improved online signature verification method", Pattern recognition letters, Vol.26, No.15, November 2005, 2400-2408 (SCI)

[13] Active Directory Users, Groups, Computers http://technet.microsoft.com

[14] Unix Tabanlı İşletim Sistemlerinin Merkezi Kimlik Yönetimi, Yılmaz Çankaya, Ekim 2009, www.bilgiguvenligi.gov.tr