Veritabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri

Yılmaz VURAL, Şeref SAĞIROĞLU

ÖZET

Veritabanı yönetim sistemleri (VTYS) kurumların veya bireylerin kritik bilgilerinin tutulduğu hassas ve korunması gereken yazılımlardır. İnternet üzerinden erişilebilen ve veritabanlarını kullanan web uygulamalarının sayısı her geçen gün artmaktadır. Ağ destekli ortamlarda veritabanları için alınan güvenlik önlemleri çoğunlukla yetersiz kalmakta ve güvenlik ihlalleri yaşanmaktadır. Yüksek seviyede VTYS güvenliğinin sağlanabilmesi için teknolojik önlemlere ek olarak insan faktörü de dikkate alınmalı ve teknik seviyeden idari seviyeye kadar tüm kullanıcılarda bilgi güvenliği farkındalığı yeterli seviyede oluşturulmalıdır. VTYS güvenliğinin yüksek seviyede sağlanması için bu çalışmada VTYS ile doğrudan veya dolaylı olarak etkileşen tüm bileşenler açıklanmış ve bu bileşenlere tek bir çatıdan farklı bir bakış açısıyla bakılmasını sağlayan katmanlı bir yaklaşım sunulmuştur. Sunulan katmanlı yaklaşım sayesinde yüksek seviyede VTYS güvenliğinin sağlanmasıyla ilgili olarak güvenlik önlemlerinin alınmasına katkıda bulunulacağına ve VTYS güvenliği açısından bir farkındalık oluşturacağı değerlendirilmektedir.

Anahtar Kelimeler: Bilgi Güvenliği,Veritabanı Güvenliği, Güncel Tehditler, Korunma Yöntemleri

Database Management Systems Security: Recent Threats and Prevention Methods

ABSTRACT

The core functionality of a Database Management System (DBMS) is to store and secure critical personal and corporate data. Number of web based applications using databases accessed through internet are increasing day by day. Preventing this environment and applications most of the time is not enough and possible, the counter measures, security threats and breaches are increasingly faced in general. In addition to the technical prevention methods, human factors and user awareness from beginners to experts must be taken into account. Extra effort should be spent to raise user awareness to a desired minimum level. This article explains the system components interacting with any DBMS directly and indirectly and presents a solution framework handling all components from a multi layered point of view. It is concluded that DBMS security can be achieved through to the presented solution framework to protect any particular DBMS from security threats and to provide DBMS security awareness.

Key words: Database Security, Information Security, Protection Methods of Database Security, Recent Threats

1. GİRİŞ

Değişik sektörlerde (finans, taşımacılık, sağlık, eğitim, vb.) hizmet veren kurumların sahip oldukları sayısal bilgileri depolamak, işlemek ve hizmete sunmak üzere kullandıkları veritabanı yönetim sistemleri bilgi sistemlerinin güvenlik açısından en kritik halkasını oluşturmaktadır. Veritabanı yönetim sistemlerinde yer alan bilgilerin mahremiyetlerinin korunması ve herhangi bir kaybın oluşmaması için bu ortamlarda bulunan bilgilerin güvenliğinin yüksek seviyede sağlanması gerekmektedir (1). Her geçen gün yaygınlaşan web uygulamaları sayesinde kritik ve hasas bir bileşen olan veritabanı yönetim sistemlerine internet üzerinden erişim sağlanabilmesi bu ortamlarda güvenliğin sağlanmasının önemini ve zorluğunu arttırmıştır. İnternet üzerinden veritabanı yönetim sistemlerine erişilebilmesinin etkisiyle tehditler ve meydana gelen güvenlik ihlallerinin sayısının her geçen gün arttığı, veritabanı yönetim sistemlerinin güvenliğiyle ilgili yayımlanan raporlar ve çalışmalarda sunulmaktadır (1-6).

Next Generation Security firması tarafından veritabanı güvenliği ile ilgili 2007 yılında yapılan çalışmada (2) çok sayıda veritabanı yönetim sisteminin hiçbir korumaya sahip olmadığı tespit edilmiştir. Yapılan bu çalışma ile çok basit yöntemlerle korunmasız olan veritabanı sistemlerinde yer alan firmaların, kurum veya kuruluşların bilgilerine internet üzerinden doğrudan erişilebileceği gösterilmiştir. Kullanılan yöntemde rastgele IP numarası oluşturan basit bir yazılım geliştirilmiş ve bu yazılımla 1.160.000 IP numarası içeren bir liste oluşturulmuştur. Bu listedeki bilgisayarlara, bilgi seviyesi çok düşük saldırganların yazabileceği basitlikte saldırı kodları gönderilmiştir. Basit yazılımlarla yapılan çalışma sonucunda hiçbir korumaya sahip olmayan 157 MSSQL ve 53 adet Oracle veritabanı sunucusuna doğrudan erişilmiştir. Çalışmanın sonucunda tüm dünyada

Makale 22.04.2008 tarihinde gelmiş,09.08.2010 tarihinde yayınlanmak üzere kabul edilmiştir.

Y. VURAL, TÜRKSAT A.Ş Gazi Üniversitesi Gölbaşı Yerleşkesi Teknoplaza Binası Gölbaşı 06380 Ankara

e-posta : yvural@turksat.com.tr

Ş. SAĞIROĞLU, Gazi Üniversitesi, Müh.-Mim. Fakültesi, Bilgisayar Mühendisliği Bölümü, Maltepe 06570, Ankara

e-posta : ss@gazi.edu.tr

Digital Object Identifier 10.2339/2010.13.2, 71-81

2.7 milyar IP adresi olduğu dikkate alınmış ve toplamda 368 bin MS SQL ile 124 bin Oracle veritabanı sunucusunun hiç bir korumaya sahip olmadığı yönünde bir açıklama yapılmıştır (2). Çalışma sonucunda korunmasız olan veritabanı sistemlerinin yarısından fazlasında mevcut açıkların sebebinin, ücretsiz olarak dağıtılan yamalarının yüklenmemesinden kaynaklandığı tespit edilmiştir. Sıradan ve basit bir yöntemle yapılan bu çalışmanın ileri seviyede bilgiye sahip saldırganlar tarafından planlı ve belirli hedeflere yönelik yapıldığı düşünüldüğünde veritabanı güvenliğinin yüksek seviyede sağlanmasının önemi ve gerekliliği daha iyi anlaşılacaktır.

ABD'de Ponemon Enstitüsü tarafından 2007 yılında yapılan bir diğer çalışmada, güvenlik açıklarının meydana getirdiği kayıpların giderek arttığı ortaya koyulmuştur (4). Raporda 2006 yılında kurumların gizliliği ihlal edilmiş müşteri başına 182 dolar harcama yaparken 2007 yılında bu rakamın 197 dolara çıktığı hatta bazı finans kurumları için söz konusu maliyetlerin müşteri başına 239 doları bile geçtiği tespit edilmiştir. Bu maliyetlerin büyük çoğunluğunun güvenlik ihlallerine bağlı kayıplardan ve yeni müşteriler bulma zorunluluğundan kaynaklandığı belirtilmiştir. Çalışma sonucunda veri hırsızlığı olaylarında en büyük açıklardan birisi verilerin depolandığı, üçüncü şahıslarla paylaşıldığı web uygulamalarıyla bütünleşik çalışan veritabanı yönetim sistemlerinden kaynaklandığı tespit edilmiştir (4).

Bir diğer önemli çalışma ise 2007 yılında veritabanı güvenliği konusunda Application Security firması tarafından yapılmıştır. Yapılan anket çalışmasına 649 büyük ölçekli firma katılım sağlamıştır (5). Ankete cevap veren katılımcıların çoğunluğunu finans ve kamu sektörü çalışanları oluşturmuştur. Raporda kurumların %30'unda 101-500, %23'ünde 1000'den fazla %21'inde ise 500-1000 arasında veri tabanına sahip oldukları tespit edilmiştir. Katılımcı kurumlar veritabanı içerisinde %53'ü çok kritik, %25'i önemli olan müşteri bilgileri, ticari gizliliği olan bilgiler ve çalışanlara ait bilgileri sakladıklarını belirtmişlerdir. Ayrıca anketi cevaplayan kurumlar, veritabanı güvenlik tehditlerini korsanlar, veri hırsızlıkları, veri kayıpları, içeriden gelen tehditler ve zararlı yazılımlar olarak sıralamışlardır. Katılımcıların çoğunluğu içeriden gelen tehditlere karşı korunmasız olduklarını vurgulayarak iki yıl içerisinde saldırıya maruz kaldıklarını ve gizli müşteri bilgileri ile çalışan personelin özlük bilgilerinin çalındığını söylemişlerdir. Bu araştırma bilgisizlik, ilgisizlik ve bilinçsizlik gibi sebepler yüzünden kurumların veritabanlarını istenilen düzeyde koruyamadıklarını göstermesi açısından önemlidir.

E-ticaret web uygulamaları, B2B senaryoları ve ekstranetler gibi birbirine bağlı sistemlerin çoğalmasıyla, veritabanları artık her zamankinden daha fazla kullanıcıya, isteğe ve olası saldırıya açık duruma gelmiştir (6). Veritabanı yönetim sistemleri pek çok güvenlik korumasına sahip olmasına rağmen kutudan çıktığı gibi kullanılması ya da yetersiz yapılandırma ve benzeri nedenlerden dolayı saldırılara karşı korunmasızdır. Veritabanı yönetim sistemleri diğer tüm yazılımlar gibi keşfedilmiş veya keşfedilmeyi bekleyen açıkları içerisinde barındırmaktadırlar. Bilginin topluca depolandığı ve ulaşılabildiği bu ortamların yeterli düzeyde korunması kurumlar ve bireyler açısından son derece önemlidir.

Ülkemizde bilgi güvenliği alanında çalışan uzman kuruluşlardan birisi olan Intellect firması tarafından uluslararası ve ulusal uygulamalarda meydana gelen gelişmeler ülkemiz açısından değerlendirilmiştir. Değerlendirmede 2008 yılında kurumların güvenlikle ilgili önem vermesi gereken 3 ana konudan birisinin veritabanı güvenliği olduğu açıklanmıştır (3).

Her yıl milyarlarca dolarlık zarara yol açan, donanım ve yazılımları etkisiz hale getirip, veritabanı güvenliğini tehlikeye sokan güvenlik tehditlerine karşı önlemlerin zamanında alınmasıyla meydana gelebilecek kayıplar en aza indirgenecektir. Tehditleri ve riskleri minimuma indirecek kurumsal bilgi güvenlik altyapılarının kurumsal iş süreçlerine entegre edilmesi etkin bir güvenlik yönetim sisteminin oluşturularak tüm veritabanı faaliyetlerinin gerçek zamanlı izlenmesi veritabanı güvenliğinin sağlanması açısından önemlidir. Veritabanı erişimi olan web uygulamalarının giderek artması ve kullanımının yaygınlaşması sonucunda veritabanı güvenliğinin yüksek seviyede sağlanması kurumlar açısından zorunluluk halini almıştır.

Veritabanı yönetim sistemlerinin güvenliğinin sağlanması konusunda bilgi eksikliğinin giderilmesi, kurumların dikkatinin bu konuya bir daha çekilmesi ve istenen düzeyde güvenlik farkındalığı oluşturulması bu çalışmanın yapılmasındaki önemli amaçlardır.

Bu amaçlardan hareket edilerek çalışmanın ikinci bölümünde genel anlamda veritabanlarının tanımları, yapıları ve çalışma sistemleri ile veri modelleri gibi temel bilgiler kısaca özetlenmiş, üçüncü bölümde güncel veritabanı güvenlik tehditleri açıklanmış, dördüncü bölümde ise veritabanı güvenliğinin sağlanmasına yönelik alınması gereken koruma önlemleri açıklanmıştır. Ayrıca çalışmanın sonuçlar kısmında ise elde edilen bulgulara yer verilerek veritabanı güvenliğinin yüksek seviyede sağlanması hususunda değerlendirmeler yapılmış ve önerilerde bulunulmuştur.

2. VERİTABANI YÖNETİM SİSTEMLERİ

1960'lı yılların başında Charles Bachman tarafından Bütünleştirilmiş Veri Depolama (Integrated Data Store) ismiyle ilk genel amaçlı veritabanı yönetim sistemi tasarlanmıştır (7). Bachman veritabanı alanında yaptığı bu öncü çalışmalardan dolayı 1973 yılında Turing ödülünü alan ilk bilgisayar bilimcisi olmuştur (7). İlk veri tabanı modelinden sonra ortaya çıkan üç temel veri tabanı modeli ağ modeli, hiyerarşik model ve 1976 yılında ilk defa Peter Chen tarafından geliştirilen ilişkisel veri tabanı modelidir (8). Günümüzde halen her alanda kullanılan ilişkisel modelin yanında yeni gelişmekte olan nesne yönelimli veritabanı modeli de kullanılmaktadır (9).

Veritabanı en genel tanımıyla, kullanım amacına uygun olarak düzenlenmiş veriler topluluğudur (10). Web üzerinde çalışan basit bir sözlükten, ülkemizde yaşayan tüm vatandaşların bilgilerinin tutulduğu merkezi nüfus idaresi sistemine kadar bir çok uygulama veritabanına ihtiyaç duymaktadır. Veritabanı bir kurum veya kuruluşun (üniversiteler, hastaneler, havayolları, finans kuruluşları, insan kaynakları, askeriye vb.) uygulama veya sistem programlarının kullandığı kritik bilgilerin (müşteri bilgileri, satış bilgileri, ürün bilgileri, ödeme bilgiler, öğrenci bilgileri, açılan dersler, kimlerin kaydolduğu, öğretmen bilgileri, sınav tarihleri, sistem yapılandırma bilgileri, vb.) bütünü olarakta tanımlanabilir.

Yeni bir veritabanı oluşturmak, veritabanını düzenlemek, geliştirmek ve bakımını yapmak gibi çeşitli karmaşık işlemlerin gerçekleştirildiği yazılım sistemleri veritabanı yönetim sistemleri (VTYS) olarak adlandırılmıştır (11). VTYS veritabanlarını uygulamalar adına hazırlayan, denetleyen ve standart bir arayüz sağlayarak dosya yapıları, veri yapısı, fiziksel hafıza gibi ayrıntılarla ilgilenilmeden, veri giriş-çıkışı için uygun arayüzler geliştirilmesini sağlayan yazılımlardır (12). Tek kullanıcılı küçük uygulamaların ihtiyaç duyduğu veriler basit bir yazılım tarafından yönetilebilirken, istemci-sunucu mimarisinde çalışan dağıtık web uygulamalarının kullandığı veritabanları için gelişmiş VTYS'lere ihtiyaç vardır. Her iki çalışma mimarisinde istemciler veri girişi, sorgulama ve raporlama işlemleri yaparken VTYS sunucuları ise verilerin saklanması ve istemci isteklerinin yerine getirilmesinden sorumludur (11).

VTYS'de verileri tutmak üzere bir çok türde nesne ve bu nesnelere erişimleri düzenlemek üzere kullanıcılar, roller ve gruplar yer alır. VTYS üzerinde yer alan kullanıcılar, roller ve grupların erişim haklarının en-az yetki kuralına (least privilege) göre verilmesi VTYS güvenliğinin yüksek seviyede sağlanması açısından önemlidir.

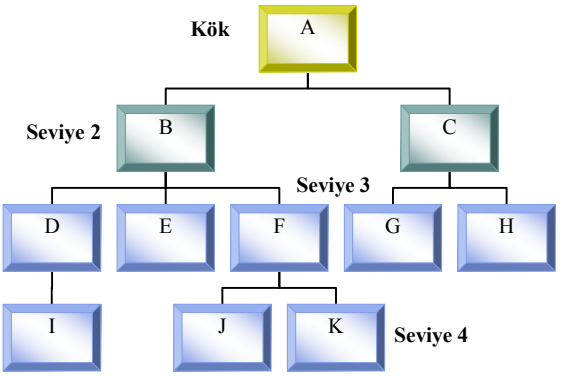
Veri modeli, veritabanı yönetim sisteminde verinin kavramsal olarak ne şekilde temsil edileceğini gösteren modeli ifade etmektedir. Veri yapıları veri nesnelerinden, veri nesneleri arasındaki ilişkilendirmelerden ve nesneler üzerindeki işlemlerin gerçekleştirilmesini sağlayan kurallardan oluşmaktadır (13). Veri modeli, veri üzerinde hangi işlemlerin gerçekleştirildiğine değil hangi verinin gerektiğine ve bunların ne şekilde tasnif edildiğine odaklanmaktadır. Veri modeli bir anlamda binanın ne şekilde inşa edileceğini değil, mimarın hazırladığı mimari planları göstermektedir. Yapısal olarak veritabanları hiyerarşik, ağ, ilişkisel ve nesne yönelimli olmak üzere 4 farklı modelde sınıflandırılmaktadır. Bu modeller takip eden alt bölümlerde özetlenmiştir.

2.1. Hiyerarşik Model

1960'ların sonunda IBM tarafından bilgi yönetim sistemi (Information Management System-IMS) adıyla ilk ticari VTYS geliştirmiş ve bu yapı hiyerarşik veri modeline temel teşkil etmiştir (7). Bu model, o yıllarda çok yaygın olan ana bilgisayar (mainframe) ortamlarında çalışan uygulamalar tarafından kullanılmıştır. Hiyerarşik veri tabanları, bilgileri bir ağaç yapısında depolar. Kök olarak bir kayıt ve bu köke dallarla bağlı alt kayıtlar bu modelde çalışan veritabanlarının yapısını oluşturmaktadır.

Hiyerarşik yapıda en üst seviye köktür (root). Kök kendisinin altında bulunan parçaların atasıdır (parent). Şekil 2.1'de örnek olarak verilen hiyerarşik yapıda A kök olup B ve C segmentlerinin atasıdır. Benzer şekilde B segmenti D,E,F segmentlerinin atası; D ise, I segmentinin atasıdır. Aynı zamanda F J ve K'nın C ise H ve G'nin atasıdır. Sırasıyla aşağıdaki segmentler üst seviyedeki segmentlerin çocukları (children) olarak adlandırılır. Böyle ilişkiler bire-çok (one-to-many yani 1:M) olan ilişkilerdir.

1:M ilişkisine örnek verilecek olursa, bir üniversite birçok fakülteye sahip olabilir ancak her fakülte sadece bir üniversiteye aittir. Her fakültede birçok bölüm olabilir ancak bölümler sadece bir fakülteye aittir. Her bölümde çok sayıda akademisyen çalışabilir ancak her akademisyenin kadrosu sadece bir bölüme aittir.



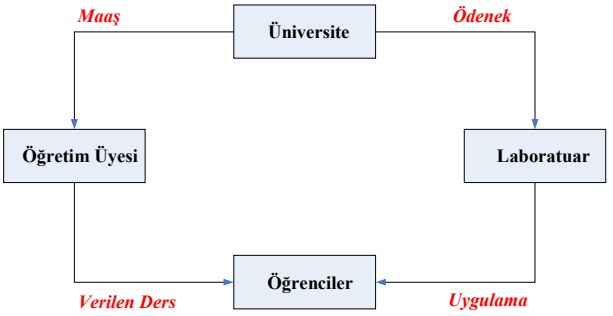
Şekil 2.1. Hiyerarşik model şematik gösterimi

Hiyerarşik veritabanı ağaç yapısında olduğundan veriye erişmek için ağaçta kök segmentten başlanarak yolculuk yapılmaktadır. Bu modelde programcı veritabanındaki gerekli verilere erişmek ve almak için verinin erişim yolunu bilmeye ihtiyaç duymaktadır. Veritabanı yapısındaki herhangi bir değişiklik, yolun değişmesine yol açacağından uygulama programlarında problemler meydana gelecektir. Uygulamalar veritabanı modeline bağımlı olduğundan değişiklikten önce çalışan uygulama programlarında değişiklikten sonra problemler oluşabilecektir.

2.2. Ağ Modeli

1971 de CODASYL (COnference on DAta SYstem Languages) grubu kullanıcı ve bilgisayar üreticileri için COBOL dili standartlarını belirlemiş ve bu standartlar ANSI (American National Standarts Institute) tarafından kabul edilmiştir (14). Bu standartlaştırma başarısından sonra CODASYL grubu veritabanı standartlarını oluşturmak için DBTG'yi (DataBase Task Group) kurarak grubu veritabanı standartlarını oluşturmak üzere görevlendirmiştir. DBTG yaptığı çalışmalar sonucunda ağ şeması, alt şema ve dil olmak üzere üç önemli veritabanı bileşenini tanımlamıştır (15).

Ağ veri modelleri, tablo ve grafik temellidir. Grafikteki düğümler veri tiplerine karşılık gelirken tablolar şeklinde temsil edilir. Grafiğin okları, ilişkileri temsil eder ve tabloda bağlantılar olarak temsil edilir. Spesifikasyonu, iki ayrı veri yapılandırma aracı vardır: Kayıt tipi ve bağlantı. Kayıt tipleri varlık tiplerini belirler. Bağlantılar ise, ilişki tiplerini belirler. Şekil 2.2'de örneği verilen grafiğe ise veri yapısı grafiği adı verilmektedir.



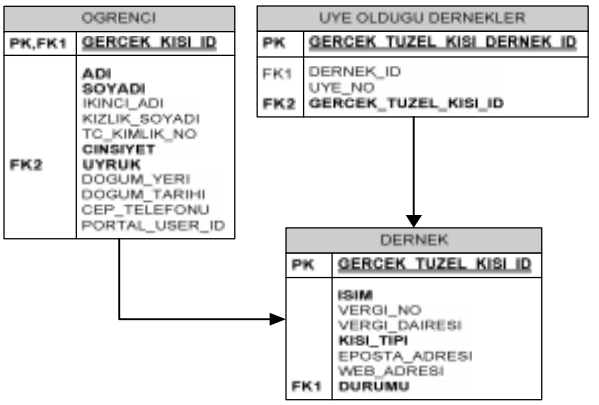
Şekil 2.2. Ağ veri modeli şematik gösterim

Şekil 2.2'de gösterilen ağ veri modeli birçok yönlerden hiyerarşik modele benzemektedir. Ağ içinde bulunan bir öğe, farklı bir öğeyle ilişkilendirilebilmektedir. Hiyerarşik yapılardan farklı olarak, ağ yapılarında bağlantı açısından herhangi bir sınırlama yoktur. Ağ veri modelleri, düğümler arasında çoklu ilişkiler kurulamadığı için, kısıtlı bir veri modeli olarak kabul edilmektedir.

2.3. İlişkisel Model

E.F. Codd tarafından geliştirilen bu model, geliştiricisi tarafından "Bilgisayar kullanıcıları çoğunlukla çizelgelerin yazılmasını ya da gösterilmesini ister. Çizelgeden daha yalın, daha evrensel, daha çok ihtiyaç duyulan ve daha kolay anlaşılan veri yapısı ne olabilir? Niçin kullanıcıların veri tabanındaki tüm veri ve bağıntıları çizelgeler biçiminde görmesine izin verilmesin?" ifadeleriyle tanımlanmıştır (16-17). İlişkisel bir veritabanında varlıklar, öznitelikler ve ilişkilere ait bütün veriler tablolarda tutulmaktadır. Tablolar arasındaki ilişkiler matematikteki ilişki teorisine (the relational theory) dayanır. Tablolarda bulunan satırlar (row) kayıtların kendisini, sütunlar (column) ise bu kayıtları oluşturan verilerin ne türden olduklarını belirtir. IBM tarafından geliştirilen DB2 ilişkisel modele dayalı ilk VTYS ürünüdür. İlişkisel modele dayalı diğer VTYS'ler 1980'lerin sonlarına doğru geliştirilmiştir. Günümüzde DB2, Oracle ve MS SQL ilişkisel modele dayalı en çok bilinen ticari VTYS ürünleridir (18)

Şekil 2.3' de öğrencilerin üye olduğu derneklere ait veritabanı ilişkisel modele örnek olarak gösterilmiştir. Veritabanı öğrenci, üye olduğu dernekler ve dernek olmak üzere 3 tane tablodan oluşmaktadır. Bir tablo içindeki verileri birbirinden ayırt etmek için kullanılan anahtarlar tablolar arasında geçiş imkânı sağlamaktadır. Bir tabloda birden fazla anahtar değer tanımlanabilir. İlişkisel modelde anahtarların aynı olduğu bir tablodaki ikinci bir satır veri olarak girilemez.



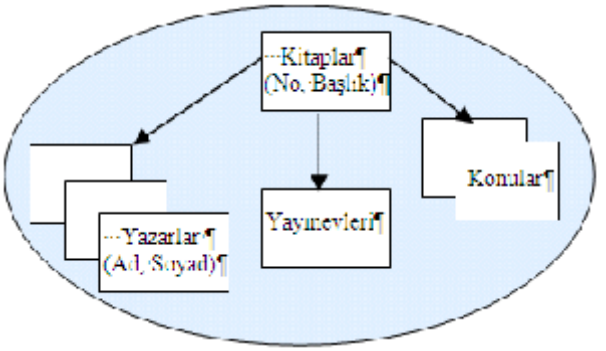
Şekil 2.3. İlişkisel veritabanı şematik gösterim

2.4. Nesne Yönelimli Model

Nesne yönelimli programlama 1980'lerin ortasında başlamıştır. Bu programlama mimarisini örnek alan modelin amacı verileri nesne formatında tutarak ilişkisel formata dönüştürmeden bir veri tabanında depolamaktır. İlk üç model veriyi kayıt yapısını kullanarak temsil ettikleri için kayıt-temelli modeller olarak adlandırılmaktadır. Bu modelde bilgi nesneye yönelik programlamada kullanılan nesne formunda gösterildiği için nesne modelli olarak tanımlanmaktadır. Veritabanı yetenekleri nesneye yönelik programlama yetenekleriyle birleştirildiğinde ortaya nesneye yönelimli veritabanı modeli (NVTYS) çıkmaktadır (19).

Nesneler, tablo içerisinde yer alan bir kayıttan çok daha karmaşık yapıya sahiplerdir. Nesne yönelimli veri tabanında, yapısı gereği arama işlemleri çok daha hızlıdır. Özellikle büyük tablolarla çalışırken ilişkisel veri tabanlarına göre daha hızlı sonuca ulaşmaktadırlar (20). Şekil 2.4'te örneği gösterilen nesne yönelimli veritabanı modelinin diğer avantajı ise, çok karmaşık bir yapıya sahip olan büyük veritabanı tasarımlarını kolaylaştırmasıdır.

İlişkisel veri tabanı verileri iki boyutlu tablolar halinde getirirken, nesne modelinde veriler tek parça halinde gelmektedirler. Dolayısıyla birden fazla veri dönmesi gereken durumlarda nesne yönelimli model performans olarak iyi sonuçlar vermemektedir.



Şekil 2.4. Nesneye yönelik veritabanı örneği

İlişkisel modelden nesne yönelimliye dönüştürümün yüksek maliyetinden dolayı model günümüzde ticari anlamda başarı kazanamamıştır. Yukarıda anlatılan modellerden farklı olarak 1990'lı yıllarda Nesne-

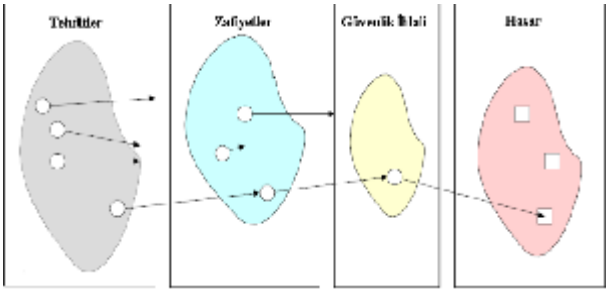
İlişkisel veritabanı modeli ortaya çıkmıştır. Bu model ilişkisel modelin iyi bilinen özelliklerini nesne yönelimli özelliklerle birleştirmiştir. Kullanıcı tanımlı veri türleri, kullanıcı tanımlı fonksiyonlar, kalıtım ve alt sınıflar bu modelde göze çarpan önemli özelliklerdir.

Veritabanı yönetim sistemlerinin güvenliğini tehdit eden güncel gelişmeler ise takip eden bölümde açıklanmıştır.

3. TEHDİTLER

Tehdit, bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini olumsuz yönde etkileme olasılığı olan tanımlı risklerdir (21-22). Tehditlerin etkili olabilmesi için veritabanı yönetim sistemleri üzerindeki zafiyet ve zayıflıkları kullanmaları gereklidir. Tehditlerin veritabanlarına etkisi, tehlikenin oluşma olasılığı, bilgi varlığı üzerindeki açık ve bilginin değeri ile doğru orantılıdır. Tehditler uygun ortam şartlarının oluşmasıyla veritabanlarına zarar verecek kusurları içeren zafiyetlere, zafiyetler saldırganlar tarafından kullanıldığında güvenlik ihlallerine yol açarak veritabanlarına zarar vermektedir. Tehditlerin veritabanı yönetim sistemleri üzerinde hasar oluşturmasına kadar izlediği süreç Şekil 3.1'de şematik olarak gösterilmiştir.

Veritabanı yönetim sistemlerinin kullanılmaya başlandığı ilk yıllarda günümüzdeki gibi ağ ortamları yaygınlaşmadığından en büyük güvenlik tehdidini erişim ihlali yaparak gizli bilgilere ulaşmaya çalışan şirket içi kullanıcılar oluşturmuştur. Veritabanı yönetim sistemlerine ilk yıllarda uygulamalar aracılığıyla sadece kurum içinden erişim sağlanabildiğinden geliş yönü açısından tehditleri kontrol etmek günümüze oranla daha kolay olmuştur. E-devlet uygulamaları, e-ticaret web siteleri ve intranetler gibi birbirine bağlı ağ ortamlarındaki uygulamaların kullanımının yaygınlaşmasıyla, veritabanı yönetim sistemleri her zamankinden daha fazla saldırıya açık duruma gelmiştir. Günümüzde kurumlar kötü niyetli, bilinçsiz, bilgisiz ve ilgisiz çalışanların oluşturduğu iç tehditlerin yanında dışarıdan gelebilecek tehditlere karşıda koruma önlemleri almak zorundadırlar.



Şekil 3.1. Tehdit-Hasar süreci

Veritabanı yönetim sistemlerinin güvenliğini tehdit eden unsurları doğal afetler, prosedürsel eksikler, insan faktöründen kaynaklanan tehditler ve zararlı yazılımlarla ilgili tehditler olmak üzere 4 grupta incelemek mümkündür. Veritabanı yönetim sistemlerinin güvenliğini dolaylı veya doğrudan etkileyen bu tehditler takip eden alt başlıklarda kısaca açıklanmıştır.

3.1. Doğal Afetler

Veritabanlarının yanında tüm bilgi sistemlerini hatta insan hayatını doğrudan etkileyen doğal afetler önceden tespit edilemedikleri için engellenmeleri genellikle çok zordur. Bu tehditlere karşı tüm tedbirler önceden planlanmalı ve uygulanmalıdır. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, kasırgalar, fırtınalar ve çığ düşmesi gibi afetler meydana gelebilecek tehditlere örnek olarak verilebilir. Doğal afetlerle ilgili tehditlerden herhangi birinin meydana gelmesi genellikle veritabanlarının yanında tüm bilgi sistemlerinin zarar görmesine veya çalışmamasına sebebiyet vermektedir. Bu tür tehditleri en az indirgemek için kurumsal yapıya uygun felaket senaryoları üretilmeli ve felaketten en kısa zamanda nasıl geriye dönülebileceğiyle ilgili (disaster recovery) iş devamlılığı konusundaki çalışmalar önceden yapılmalıdır.

3.2. Prosedürsel Eksiklikler

Veritabanlarını dolaylı yönden ancak üst düzeyde tehdit eden prosedürsel eksiklikler kurumsallaşma süreçlerini tamamlayamayan kurum ve kuruluşlarda sıklıkla görülür. Veritabanı yedekleme prosedürlerinin olmaması, veritabanı kurulum ve bakımı ile ilgili prosedürlerin eksikliği, acil durumlarda veya felaket anlarında devreye alınacak bilgi süreklilik planlarının olmaması, güvenlik bilinçlendirme eğitimlerinin planlanması ve uygulanmasına ait eksiklikler, güvenlik politikası ve prosedürlerinin olmaması, bilgi güvenliğiyle ilgili görev ve sorumlulukların verilmesindeki eksiklikler bu prosedürsel eksikliklerden kaynaklanan tehditlere örnek olarak verilebilir.

3.3. İnsan Faktörü

Veritabanı güvenliğinin sağlanmasında en zayıf halka olan insan faktöründen kaynaklanan tehditleri istem dışı veya kasıtlı olarak yapılan kullanıcı davranışları olarak iki grupta incelemekte fayda vardır. Veritabanı ile ilişkilendirilmiş uygulama üzerinde belirli bir düzeyde yetkiye sahip olan bir kullanıcının, uygulamayı bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu bilginin gizlilik, bütünlük ve erişilebilirlik ilkelerinin biri veya birkaçı ihlal edilebilir.

Son kullanıcılar, yazılım geliştiricileri, veritabanı yöneticileri, sistem yöneticileri gibi değişik düzeyde bilgi sahibi olan çalışanlar tarafından istem dışı veya ihmalkârlık sonucu yapılan davranışlardan kaynaklanan bazı önemli tehditler maddeler halinde aşağıda sıralanmıştır.

• Çalışanların bilinç eksikliği veya kasıtlı olarak güvenlik politikalarına uymaması veya ihlal etmesi,

- Güvenlik önlem ve kontrolleri almadan veritabanı etkileşimli uygulama yazılımlarının geliştirilmesi,
- Veritabanı sunucularının fiziksel güvenliğinin sağlanamaması,

- Eğitimsiz veya bilgisiz çalışanların veritabanı yönetim sistemlerini güvensiz, eksik veya hatalı yapılandırması,
- Veritabanı erişim haklarının en az yetki kuralına göre yapılandırılmaması,
- Veritabanı kayıtlarının (log) analiz edilmeden silinmesi veya hiç tutulmaması,
- Veritabanının hatalı yedeklenmesi, hiç yedek alınması veya alınan yedeklerin test edilmemesi,
- Veritabanı sunucusu üzerinde gereksiz servislerin hizmete açılması,
- VTYS'lerin kutudan çıktığı gibi varsayılan (default) ayarlarında bulunması

olarak verilebilir.

Verilen örneklerden anlaşılacağı gibi bilgisizlik, bilinçsizlik, isteksizlik, çıkar elde etme, ihmalkârlık ve görevini kötüye kullanma gibi insan hatalarından kaynaklanan tehditler önemli bir yer tutmaktadır.

3.4. Web Üzerinden Gelen Tehditler

Web üzerinden gelen tehditler her ne kadar insan faktöründen (güvensiz altyapılar, güvensiz kodlama, hatalı yapılandırma, vb) kaynaklanan tehditler olsa da veritabanı güvenliği ihlallerinin oluşmasındaki en önemli tehditlerin başında geldiğinden ayrı bir alt başlıkta incelenmiştir. Web uygulamaları kullanıcı dostu arayüzüne sahip olması, herhangi bir yerden herhangi bir zamanda herhangi bir bilgisayardan platform bağımsız olarak kullanılabilmesi, kurulumunun ve bakımının maliyet efektif olması gibi nedenlerden dolayı veritabanında depolanan bilgileri insanlara ulaştırmak için en kolay ve en etkin yöntem olarak karşımıza çıkmaktadır.

Dinamik içerikli web sitelerinde, web tarayıcıları taleplerini web uygulamalarına ilettikten sonra bu istekler doğrultusunda veritabanı sorgulaması yapılır ve talep edilen isteklere ait sonuçların yer aldığı sayfalar üretilerek, tarayıcılar üzerinde gösterilir. Dinamik içerikli web sayfalarının bu esnek çalışma yapısı birçok güvenlik tehdidini ve ihlâllerini beraberinde getirmektedir. Özellikle kullanıcıdan girdi alınarak dinamik içerik sağlamak amacıyla veritabanı desteği sağlayan uygulama kodlarıyla (asp, jsp, php, cgi, vb.) geliştirilen web uygulamaları, veritabanı güvenliğini üst düzeyde tehdit etmektedir (23).

3.4.1 SQL enjeksiyonu

SQL veri tabanlarına erişmek ve onları kullanmak için 1975 yılında IBM tarafından geliştirilen ANSI (American National Standards Institute) standartlarına uygun bir alt dildir (21). SQL ifadeleri bir veri tabanı üzerinde veri oluşturma, okuma, değiştirme ve bulma gibi temel işlemlerin istemciler tarafından yapılmasını sağlar. Günümüzde VTYS'lere göre farklılaşan SQL dilinin pek çok çeşidi (Oracle, DB2, Informix, Sybase, Interbase, Progress, MSSQL Access, Ingres, PostgreSQL, MySQL, vb) olmasına rağmen hepsi en alt düzeyde ANSI standartlarını desteklediğinden temel komutlar (Select, Update, Delete, Insert, Drop, Union, vb.) hepsinde aynıdır.

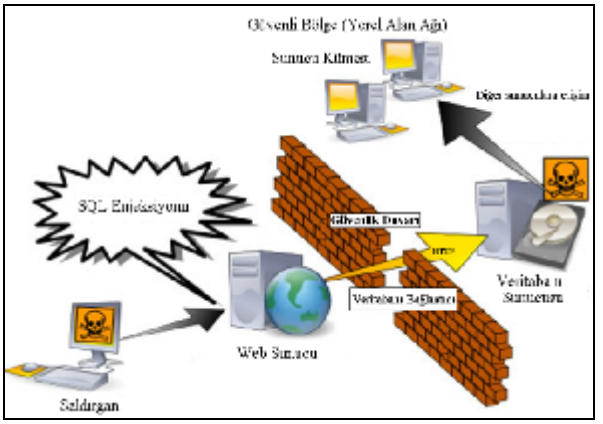
Web uygulamaları kullanıcı kaynaklı girdileri, dinamik web sayfası talepleri için, değişik SQL cümleleri oluşturmada kullanabilir. SQL enjeksiyonu yöntemi, kullanıcı girdilerine göre SQL cümleleri oluşturan web sitelerinde, kullanıcı kaynaklı girdilerin doğrulanmaması veya yetersiz doğrulanmasından kaynaklanan zafiyetlerin kullanılarak, SQL cümlelerinin manipüle edilmesini sağlayan saldırı yöntemleridir (24-25). SQL enjeksiyonu yöntemiyle veritabanları üzerinde yapılabilecek saldırılardan bazıları aşağıda sıralanmıştır.

- Veritabanları üzerinde istenmeyen işlemlerin (sorgulama, ekleme, silme, değiştirme, vb.) yapılabilmesi,
- Kimlik doğrulama mekanizmaları atlatılabilmesi,
- İşletim sistemi seviyesinde komutların çalıştırılabilmesi,
- Yeni kullanıcılar veya gruplar oluşturulabilmesi

gibi bir çok saldırı bu yöntemle yapılabilmektedir.

Eğer bir web uygulaması, istemci kaynaklı girdileri etkin bir biçimde denetleyemezse, SQL enjeksiyon yöntemiyle uygulama tarafından çalıştırılan SQL cümlesi oluşumu değiştirilerek güvenlik ihlalleri oluşturulabilir. SQL enjeksiyon yöntemiyle SQL cümlesi değiştirilerek bilgisayar sistemlerine sızılması durumunda, SQL servisini çalıştıran kullanıcı haklarına sahip olunacaktır. Veritabanı üzerinde bu haklara sahip olan kişi ileri derece saldırı tekniklerini kullanarak veritabanı dışındaki diğer sunucu bilgisayarları üzerinde de Şekil 3.2'de gösterildiği gibi erişim hakkı kazanabilir.

Şekil 3.2'de şematik olarak gösterildiği gibi saldırgan hedef web sitesi üzerinde SQL enjeksiyonu yapabileceği dinamik içerikli web sayfalarını tespit ettikten sonra, SQL enjeksiyonu aracılığıyla veritabanı sunucu bilgisayarına veritabanını çalıştıran servisin (muhtemelen üst seviyede erişim hakları bulunan yönetici hesapları) kullanıcı hesabıyla ulaşabilir.



Şekil 3.2. SQL enjeksiyonu şematik gösterimi

Veritabanı sunucu bilgisayarı üzerinde, SQL enjeksiyonu yardımıyla işletim sistemi seviyesinde komutlar çalıştıran saldırganın bir sonraki hedefi diğer bilgisayarlar ve özellikle sunucular olacaktır. Saldırgan, diğer sunucu bilgisayarlarına veritabanı kullanıcı hesabıyla bağlantı yaptıktan sonra tüm sunucu bilgisayarlara daha sonra doğrudan bağlanabilmesi (remote desktop, telnet, http, ftp, vb.) için gerekli olan servisleri kendi kullanımına açabilecek ve saldırıdan beklediği sonuçları elde edebilecektir.

3.4.2 Veritabanı Solucanları

Solucanlar, herhangi bir yardım almaksızın ağ üzerindeki bilgisayarların korunmasızlıklarından faydalanarak kendiliğinden diğer bilgisayarlara bulaşan ve bilgisayar ağları üzerinde hızla yayılan saldırı yapma amaçlı kullanılan zararlı yazılımlardır (26). Son zamanlarda işletim sistemleri veya web sunucularını hedef alan solucanlar yerine daha korunmasız olan veritabanlarını hedef alan solucanların sayısında hızlı bir artış görülmüştür. Günümüzde modern VTYS'lere özgü olarak tanımlanmış portlar (Microsoft SQL, TCP-1433,UDP-1434; Oracle TCP-1521, IBM DB2 523-50000; IBM Informix, TCP-9088, TCP-9099, Sybase, TCP-4100, TCP-2025, MySQL, TCP-3306, PostgreSQL, TCP-5432) kullanılarak erişilebilmesinden dolayı saldırganlar veritabanlarına özgü solucanlar geliştirmiş ve bu solucanların verdiği kayıplar dünyada büyük yankılar uyandırmıştır.

Solucanların uygulama kodlarında bulduğu açıklar aracılığıyla yayılabilmesi güvenlik duvarlarının çoğunlukla etkisiz hale getirilmesini sağlamaktadır. Örneğin bir solucanın SQL enjeksiyonu açığını bulması ve bulduğu bu açıkla kendisini veritabanına bulaştırarak diğer uygulamalara kolayca bulaşması mümkündür. Bu ve benzeri yöntemlerle uygulama seviyesinde etkili olan bu solucanlar sadece internet üzerinde çalışan bilgisayarlar için değil aynı zamanda güvenlik duvarlarını atlatarak güvenli bölgede yer alan yerel alan ağını da üst seviyede tehdit etmektedir.

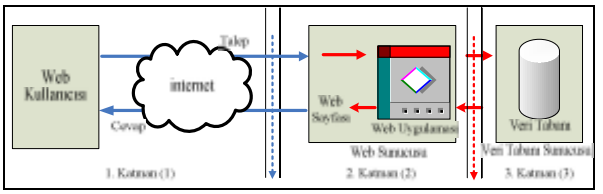
İlk veritabanı solucanı olan Spida 2002 yılında çok sayıda MSSQL sistemini etkilemiştir (27). Solucan MSSQL kurulumu sırasında veritabanı yöneticileri tarafından sistem yöneticisi haklarına sahip olan "sa" isimli hesaba ait parolanın boş geçildiği veritabanlarında etkili olmuştur. Solucan "sa" yetkisiyle veritabanı üzerinde oturum açmış ve MSSQL'in işletim sistemi seviyesindeki "xp_cmdshell" komutundan faydalanarak veritabanı sunucusunun kontrolünü ele geçirmiştir. Ayrıca solucan kendisini diğer MSSQL sunucularına yaymak üzere ağ üzerinde tarama işlemleri yaptığından, ağ üzerinde çok yoğun bir trafik oluşmasına neden olmuş ve kurumların işlerini aksatmıştır. Solucan sunucunun ağ yapılandırmasını ve sunucu üzerindeki tüm parolaların özetlerini bir dosyaya kayıt ederek virüs yazarının oluşturduğu tahmin edilen ixltd@postone.com adresine göndermiştir (28). Bu tarihten itibaren veritabanlarını hedef alan çok sayıda daha tehlikeli solucanlar (SQL Slammer, Code Red, Nimda, vb.) yazılmış ve kurumlar yüksek tutarda zararlara uğratılmıştır.

Veritabanı solucanlarının yanında burada açıklanmayan bir çok zararlı yazılım (virüs, truva atları, vb.) veritabanı güvenliğini tehdit eden diğer unsurlardır. Günümüzdeki zararlı yazılımlar yapılandırma hatası yerine yazılımların açığını kullandığı için çok daha etkilidir. Veritabanı güvenliği tehditleri konusunda farkıdanlık oluşturması amacıyla bu bölümde özetlenen tehditler, tehlikeler ve zafiyetlerden korunma yöntemleri takip eden bölümde açıklanmıştır.

4. KORUNMA YÖNTEMLERİ

Veritabanı yönetim sistemleri tehditlerinden korunmak ve yüksek seviyede veritabanı güvenliğinin sağlanması için modern veritabanlarının bilgi sistemleri içerisindeki yeri öğrenilmeli ve korunma yöntemleri için katmanlı bir güvenlik yaklaşımı uygulanmalıdır. Sadece VTYS'lerin güvenliğini sağlamak veritabanı güvenliğinin sağlanması için yeterli değildir. Güvenlik seviyemizin en zayıf halkamıza eşit olduğu dikkate alınırsa veritabanlarına her yerden erişilmesini sağlayan web uygulamalarının çalışma mimarisinde yer alan her bir bileşeni için ayrı ayrı korunma yöntemlerinin belirlenmesine ve uygulanmasına ihtiyaç vardır.

Veritabanlarıyla bütünleşik olarak çalışan dinamik içerikli web siteleri veya portalleri kullanıcı yönlendirmeleri doğrultusunda çalışan web uygulamaları içermektedir. Dinamik web siteleri Şekil 4.1'de şematik olarak gösterildiği gibi üç katmanlı bir yapı içerisinde çalışmaktadır (29).



Şekil 4.1. Üç katmanlı dinamik web mimarisi

Şekil 4.1'de gösterilen katmanlar aşağıda maddeler halinde kısaca açıklanmıştır.

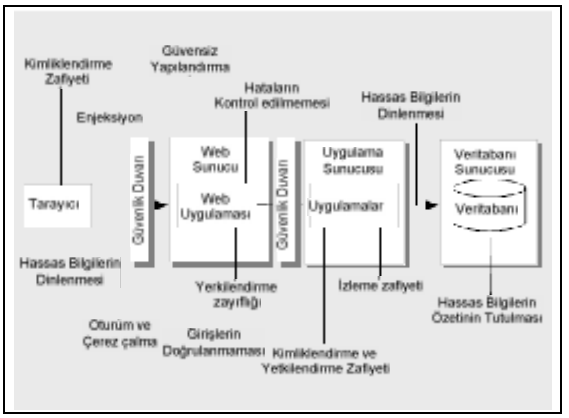
1. Katman: Web siteleri için taleplerin başladığı Web tarayıcılarıdır (Internet Explorer, Mozilla, Firefox, Netscape, vb.). Web tarayıcıları üzerinden kullanıcılar, web sunucusuna içerikle ilgili taleplerini iletirler.

2. Katman: Dinamik sayfaların üretildiği uygulama katmanıdır (Hypertext Processor-PHP, Active Server Pages-ASP, Java Server Pages-JSP, WebSphere, ColdFusion, SunONE, vb.).

3. Katman: Web uygulamaları tarafından kullanılan verilerin depolandığı veritabanı yönetim sistemleridir (MS SQL, My SQL, Informix, Oracle, vb.).

Katmanlı yapıda geliştirilerek istemci sunucu mimarisinde çalışan bir web uygulamasının alınan ekstra güvenlik önlemlerine rağmen (ağ seviyesinde çift güvenlik duvarı) yeterli olmadığı ve koruma ön-

lemlerine rağmen karşılaşabileceği olası önemli tehditlerden bazıları Şekil 4.2'de gösterilmiştir.



Şekil 4.2. Ekstra korunma yöntemlerine rağmen güvenlik tehditleri

Alınan korunma yöntemlerine rağmen güvenlik ihlallerinin yaşanması veritabanı güvenliğinin sağlanması için gerekli olan yöntemlerin tek bir çatı altında toparlanmasını zorunlu kılmaktadır. Bu gereksinim üzerine çalışma kapsamında yapılan araştırmalar ile daha önceki tecrübeler ve edinilen bilgilere dayanılarak bu çalışmada veritabanı güvenliğinin sağlanması için yatayda dört dikeyde tek katmanlı bir veritabanı güvenlik bakış açısı sunulmuştur.

Şekil 4.3'de gösterilen katmanlı yaklaşımın çalışma yapısı uçtan uca ele alındığında, birinci katmanda insan ve fiziksel güvenliğin sağlanması ikinci katmanda ağ ve haberleşme güvenliğinin sağlanması, üçüncü katmanda sunucu güvenliğinin sağlanması, dördüncü katmanda uygulama güvenliğinin sağlanması gereklidir. Dikeyde tüm katmanlarda uygulanması gereken bilgi güvenliği politikaları yatay katmanlarda yapılan çalışmaların aksamaması açısından önemlidir.

Şekil 4.3. Katmanlı veritabanı güvenlik çerçeve yaklaşımı

Bu çalışmada sunulan ve tek bir çatı altında veritabanı korunma yöntemlerini bir arada toplayan 4 katmanlı güvenlik çerçeve yapısı, takip eden alt başlıklarda sırasıyla açıklanmıştır.

4.1 İnsan Güvenliği (Farkındalık)

Bu makalede ve daha önce literatürde bilgi güvenliğiyle ilgili yapılan diğer çalışmalarda (raporlar, anketler, kitaplar, makaleler, vb.) vurgulandığı gibi bilgi güvenliğinin ve veritabanı güvenliğinin sağlanmasındaki en zayıf halka insan faktörüdür (30). İnsan faktöründen kaynaklanan zafiyetlere kodlama hataları, sistem yapılandırma hataları, telefon veya diğer iletişim araçlarıyla hassas bilgilere ulaşılması gibi örnekler verilebilir. Bu ve benzeri insan odaklı zafiyetlerin saldırganlar tarafından kullanılması durumunda veritabanı güvenliği ihlalleri yaşanacak ve kayıplar meydana gelecektir.

Çalışmada sunulan katmanlı veritabanı güvenlik yaklaşımında birinci katmanda yer alan insan güvenliğinin sağlanmasından teknik sorumlular kadar yöneticiler ve son kullanıcılar olmak üzere veritabanı uygulamasıyla doğrudan ve dolaylı ilişkisi olan tüm insanlar sorumludur. Yüksek seviyede veritabanı güvenliğinin sağlanması ancak ve ancak tüm tarafların sorumluluklarını yerine getirmesiyle sağlanabilecektir. Veritabanı güvenliğinin dolayısıyla bilgi güvenliğinin sağlanmasında en zayıf halka olan insan faktöründen kaynaklanan zafiyetlerin giderilmesinde en etkili sonuç eğitim ve bilinçlendirme çalışmaları yardımıyla insanlarda bilgi güvenliği kültürü oluşturulmasıyla sağlanacaktır.

İnsan güvenliğinin sağlanması açısından çözüm olan bilgi güvenliği eğitimleri ve bilinçlendirme farklı yöntemlerle veritabanlarıyla doğrudan veya dolaylı etkileşimde olan insanlara periyodik olarak verilmelidir. Bu yöntemlere bilinçlendirme toplantıları, web üzerinden verilecek eğitimler ve bilgi notları, e-posta yoluyla uygulama kullanıcılarının bilinçlendirilmesi, yazılar ve duyurular, seminerler, kurum içi bültenler ve güvenlik posterleri şeklinde örnekler vermek mümkündür. İnsana bağlı güvenlik riski hiçbir zaman tamamen yok edilemese de iyi planlanmış bilgi güvenliği eğitimleri riskin kabul edilebilir bir seviyeye indirilmesine yardımcı olacaktır. İnsanların bilgiyi ve bilgi kaynaklarını koruma konusunda üzerlerine düşen sorumlulukları anlaması bilgi güvenliğinin sağlanması açısından kritik bir öneme sahiptir

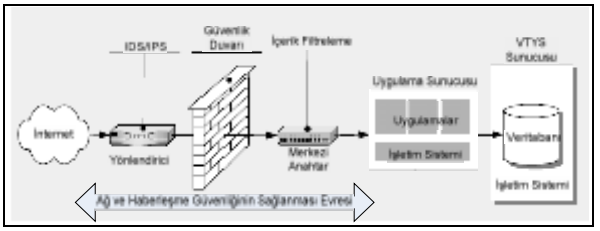
Birinci katmanda yer alan ve sağlanması gereken diğer önemli unsur ise kullanıcı veya sunucu uygulamalarının çalıştığı ortamlarda fiziksel güvenliğin sağlanmasıdır. Fiziksel güvenlik, hassas bilgi ve bilgi sistemlerinin yer aldığı fiziksel mekânlara erişilmesini engelleyen veya belirlenen yetkiler dâhilinde erişilmesini sağlayan yöntemlerin kullanıldığı çözümlerdir. Fiziksel güvenliğin sağlanmasına binaların çevrelerine çitler çekilmesi, kapıların önlerine nöbetçiler veya bariyerler konulması, kapı giriş çıkış sistemleriyle kimliklendirme ve yetkilendirme yapılması, kameralarla tüm olayların kayıt altına alınması örnek olarak verilebilir.

4.2 Haberleşme ve Ağ Güvenliği

Sistemler veya insanlar arasında karşılıklı olarak bilgi alışverişi amacıyla yapılan tüm faaliyetlerin ortak adı haberleşme olarak adlandırılmaktadır. Bilgi sistemleri arasındaki haberleşme güvenliğinin sağlanmasında kriptografik ve steganografik yöntemler kullanılmaktadır (31). Haberleşme güvenliği dışında bu katmanda yer alan ağ güvenliği ise; milyonlarca

bilgisayarın birbirine bağlı olduğu ortamlarda meydana gelebilecek güvenlik açıklarını önleme girişimi olarak adlandırılmaktadır. Ağ veya haberleşme katmanında yer alan zafiyetler kötü niyetli veya meraklı kişiler tarafından kullanıldığında bilgilere yetkisiz erişim, sistemler ve servislerin kullanılamaz olması, bilgilerin değiştirilmesi veya ifşa edilmesi gibi önemli güvenlik ihlâlleri oluşmaktadır. Ağ ortamlarında çalışan veritabanı bütünleşik uygulamaların yaygınlaşmasıyla ağ üzerinde veritabanlarını doğrudan hedef alan zararlı yazılımların (virüsler, solucanlar, enjeksiyonlar, vb.) neden olduğu güvenlik ihlâlleri artmış ve veritabanı güvenliğinin yüksek seviyede sağlanması için alınması gereken önlemler fazlalaşmıştır.

Ağ güvenliği sağlanamadığında saldırganlar iyi yapılandırılamamış ağ cihaz ve yazılımları üzerindeki zafiyetleri kullanarak hasas bilgiler yer aldığı veritabanlarına erişmek isteyeceklerdir. Ağ üzerindeki ortak zafiyetlere VTYS'leri kutudan çıktığı gibi kullanıma almak, ağ üzerinde çalışan uygulamalara ait yamaların zamanında veya hiç yüklenmemesi ve VTYS'lere ağ üzerinden gerekenden fazla erişim hakkının verilmesi örnek olarak verilebilir. Bu zafiyetleri kullanabilecek orta seviyede bilgiye ve saldırı araçlarına sahip olan bir saldırgan bilgi toplama, bilgi dinleme, aldatmaca, oturum çalma, hizmet aksattırma gibi üst düzey saldırıları rahatlıkla gerçekleştirebilecektir.



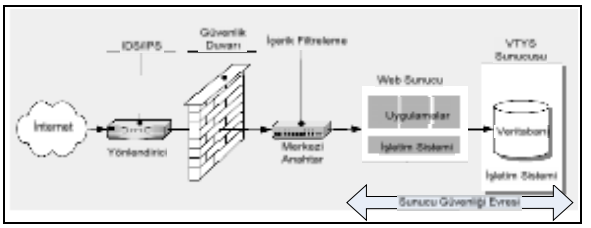
Şekil 4.4. Veritabanı güvenliğinde ağ ve haberleşme güvenliğinin sağlanması evresi

Ağ ortamlarında temel bileşenler olan yönlendirici ve anahtarlar gibi ağ ekipmanlarının güvenli yapılandırılması ve bu bileşenlerin güvenliğinin sağlanması ağ güvenliği açısından önemlidir (32). Ağ güvenliğinin sağlanmasında kullanılan bileşenler güvenlik duvarları (firewall), saldırı tespit sistemleri (IDS)ve içerik filtreleme gibi temel çözümler Şekil 4.4'de gösterilmiştir

4.3 Sunucu Güvenliğinin Sağlanması

Veritabanı güvenliğinin sağlanması için bu çalışmada sunulan katmanlı yaklaşımda üçüncü katmanda yer alan sunucuların güvenliğinin sağlanmasında Şekil 4.5'de gösterildiği gibi işletim sistemlerinin güvenliği ön plana çıkmaktadır.

Sunucu güvenliğinin sağlanması için bu katmanda yapılması gerekenler yama yönetimi, kayıt yönetimi, yedekleme ve geri yükleme senaryolarının oluşturulması, kullanılmayan gereksiz hizmetlerin kapatılması, sunucu tabanlı saldırı engelleme ve saldırı önleme yazılımların kurulması ile sunucular üzerinde en az yetki prensibine uygun şekilde erişim haklarının düzenlenmesi olarak sıralanabilir.



Şekil 4.5. Veritabanı güvenliğinde sunucu güvenliğinin sağlanması evresi

4.4 Uygulama Güvenliğinin Sağlanması

Uygulama güvenliği, bilgi güvenliği kültürüne sahip olan yazılım geliştiricilerin güvenli kodlama esaslarına bağlı kalarak standartlara uygun yazılımlar geliştirmesiyle sağlanmaktadır. Günümüzde veritabanı yönetim sistemlerinin güvenliğinin sağlanmasında en önemli ve kritik görevlerden bir tanesi yazılımcılara düşmektedir. Yazılımlardan kaynaklanan güvenlik açıklarının en aza indirgenebilmesi için yazılımcılar tarafından güvenli kodlamada dikkat edilmesi gereken dört önemli husus vardır.

Yazılımcılar tarafından dikkat edilmesi gereken birincil husus uygulama veri girişlerinin doğruluğunun kontrol edilmesidir. Veri girişlerinin doğruluğunun kontrol edilebilmesi amacıyla girdi veya çıktı alanlarına özgü kabul edilebilecek karakterlerin yer aldığı beyaz liste oluşturulmalıdır. Oluşturulan beyaz liste dışında kalan ve saldırganlar tarafından kötü amaçlı kullanılabilecek diğer karakterlerin girdileri yazılımcılar tarafından engellenmelidir. Veritabanlarını doğrudan etkileyen web uygulamalarını etkileyen saldırıların temelinde uygulama veri girişlerinin tam olarak doğrulanamamasından kaynaklandığı bilinmektedir.

Güvenli kodlamada uygulanması gereken ikinci önemli husus kod gözden geçirmelerinin ve uygulama testlerinin iyi yapılmasıdır. Kodlar test aşamasında test mühendisleri tarafından güvenlik kriterleri göz önüne alınarak yeniden gözden geçirilmeli ve uygulama güvenliği sınanmalıdır. Güvenli kodlamada uygulanması gereken üçüncü önemli husus yetki mekanizmalarının tasarımında yetkilerin ayrıştırılarak güvenliğin sağlanmasındaki önemli ilkelerden biri olan "en az yetki" ilkesine uyulmasıdır. Güvenli kodlamada uygulanması gereken dördüncü önemli husus uygulamalar hakkında önemli bilgiler içeren hataların kontrol edilmesidir. Hata kontrol yönetimi yapılarak oluşan hatalar uygulamalar tarafından güvenli formatta dış dünyaya iletilmelidir.

4.5 Bilgi Güvenliği Politikaları

Bilgi güvenliği politikaları, kurum veya kuruluşlarda kabul edilebilir güvenlik seviyesinin tanımlanmasına yardım eden, tüm çalışanların ve ortak çalışma içerisinde bulunan diğer kurum ve kuruluşların uyması gereken kurallar bütünüdür (33). Güvenlik politikaları bu çalışmada veritabanı güvenliğinin sağlanmasında önerilen katmanlı yaklaşımın etkin bir şekilde uygulanmasında en hassas bileşendir. Bilgi güvenliği politikaları, kurum ve kuruluşlarda bilgi güvenliğinin sağlanması için tüm bilgi güvenlik faaliyetlerini kapsa-

yan ve yönlendiren talimatlar olup bilgi kaynaklarına doğrudan veya dolaylı yönde erişim yetkisi olan tün insanların uymaları gereken kuralları içeren bir belge niteliğinde olmalıdır.

Güvenlik politikaları yöneticiler tarafından desteklenmeli, tabii olanlar tarafından benimsenmeli ve uygulanabilir düzeyde olmalıdır. Bu çalışmada sunulan katmanlı yaklaşım her katmanda yapılması ve uyulması gereken kurallara bilgi güvenliği politikalarında yer verilmelidir. Tarayıcıdan veritabanına kadar olan süreci bir yolculuğa benzetirsek bilgi güvenliği politikaları yolculuk esnasında kullanılan emniyet kemerinin görevini üstlenmektedir.

5. SONUÇLAR

Veritabanları bilgi sistemlerinin merkezinde yer alan, yüksek seviyede güvenliğin sağlanması gerektiği kurumların veya bireylerin kritik bilgilerinin tutulduğu hassas ve korunması gereken ortamlardır. Veritabanlarını kullanan uygulamalar yaygınlaştıkça ve çatı bir güvenlik bakış açısı sağlanmadıkça güvenlik sorunları her geçen gün daha fazla artacak ve kurumlar zarara uğrayacaktır. Kurumlar ve bireyler açısından kritik bir öneme sahip olan veritabanlarının güvenliğinin sağlanabilmesi için her seviyeden bu uygulamalarla etkileşimde olan yöneticilere, çalışanlara, bilgi teknolojisi personeline ve kullanıcılara önemli görevler düşmektedir. Bu çalışmada özetlenen güvenlik açıkları ve korunma yöntemlerinin özetlenmesinin yanında elde edilen önemli bulgulardan birisi veritabanı güvenliğinin yüksek seviyede sağlanması için veritabanı ile doğrudan veya dolaylı olarak etkileşen tüm bileşenlere tek bir çerçeve bakış açısıyla bakılmasını zorunlu kılmaktadır. Çalışma kapsamında sunulan katmanlı veritabanı güvenlik yaklaşımı veritabanı sistemlerinin güvenliğinin yüksek seviyede sağlanabilmesi için gerekli olan bileşenler ve aralarındaki ilişkilerin tek bir çatı altında çerçeve bakış açısıyla takip edilmesini sağlamaktadır.

Güvenlik mimarisi ve ölçeklendirme açısından doğru teknoloji ve platformların seçilmesi, seçilen teknolojilerin hatasız ve güvenli yapılandırılması, bakımlarının periyodik olarak yapılması ile katmanlı mimaride inşa edilmeleri veritabanı güvenliğinin üst seviyede sağlanması açısından bu çalışmada elde edilen bir diğer önemli bulgudur. Katmanlı güvenlik mimarileri bilgi güvenliğinin üst düzeyde sağlanmasında önemli bir katkı sağlamaktadır ancak burada dikkat edilmesi gereken en önemli husus, katmanlı mimarilerin kurulum, bakım ve işletilmesinde üst düzeyde teknik bilgiye gereksinim duyulmasıdır. Eğer bu teknik işçilik, kurumun kendi bünyesinde mevcut değilse dış kaynak kullanımına gidilmelidir. Aksi takdirde teknoloji ve mimari seçiminin doğru yapılmasına rağmen eğitim ve yatırımlara gerekli hassasiyetin gösterilmemesi teknolojik yatırımları boşa çıkartacağı gibi daha çok güvenlik ihlallerinin meydana gelmesine neden olacaktır.

Sonuç olarak veritabanı yönetim sistemlerinin güvenliğinin yüksek seviyede sağlanabilmesi için insan, ağ, haberleşme, sunucu ve uygulama güvenliği ile bilgi güvenliği politikalarının katmanlı bir veritabanı güvenlik yaklaşımıyla tek bir çatı altında çerçeve bakış açısıyla ele alınması ve periyodik olarak güvenlik testleriyle test edilmesi sonucunda yüksek seviyede VTYS güvenliğinin sağlanabileceği değerlendirilmektedir.

6. KAYNAKLAR

1. Vural, Y., Sağıroğlu, Ş., Kurumsal Bilgi Güvenliği: Güncel Gelişmeler, ***ISC Turkey Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı***, Ankara, 191-199, Aralık 2007.
2. İnternet: David Litchfield, "The Database Exposure Survey 2007", http://regmedia.co.uk/2007/11/15/thedatabaseexposuresurvey2007.pdf (13.02.2008).
3. İnternet: Intellect, "2008 Güvenlik Trendleri", http://turk.internet.com/haber/yazigoster.php3?yaziid=20106 (14.02.2008).
4. İnternet:Ponemon Enstitüsü, "2007 Annual Study: U.S. Cost of a Data Breach" http://www.ponemon.org (15.02.2008)
5. Ponemon, L., "Database Security 2007:Threats and Priorities within IT Database Infrastructure", ***Ponemon Institute***, Michigan 2-13, (2007).
6. İnternet:Microsoft, "SQL Server ve Güvenlik", http://www.microsoft.com/turkiye/sql/prodinfo/spotlight/security.mspx (14.02.2008).
7. Ramakrishman, R., Gehrke, J., "Database Management Systems", ***McGraw-Hill Professional***, Dubuque, 3-4 (2003).
8. Chen, P., "The Entity-Relationship Model-Toward a Unified View of Data", ***ACM Transactions on Database Systems*** 1(1):9-36 (1976).
9. Çelik, İ., Ünüvar, A., "Nesne Yönelimli Yaklaşımla Özellik Tabanlı Modelleme", ***Mühendis ve Makina Dergisi***, 45(537):39-50(2004)
10. İnternet: Wikipedia "Veritabanı" http://tr.wikipedia.org/wiki/Veri_tabani (13.02.2008).
11. Oppel, J., A., "Databases Demystified", ***McGraw-Hill Professional***, Dubuque, 18 (2004).
12. Burma, A., Z., "Veri Tabanı Yönetim Sistemleri ve SQL/PL-SQL/T-SQL", ***Seçkin Yayınevi***, Ankara, 7-8 (2005).
13. Mazıbaş, M., "Operasyonel Risk Veri Tabanı Modellemesi", ***Bankacılık Düzenleme ve Denetleme Kurumu***, Ankara, 11-16 (2006).
14. İnternet: Wikipedia "CODASYL" http://en.wikipedia.org/wiki/CODASYL (16.02.2008).
15. İnternet: Wikipedia "Network Model" http://en.wikipedia.org/wiki/Network_model (16.02.2008).
16. Codd, E., F., "A Relational Model of Data for Large Shared Data Banks", ***Communications of the ACM***, 13(6):377-387(1970).

17. Codd, E., F., "A Relational Completeness of Database Sublanguages", ***Prentice Hall***, New Jersey, 65-98 (1972).
18. Eyüboğlu, F., "Veri Tabanı Yönetim Sistemleri ve SQL", ***Yıldız Teknik Üniversitesi***, İstanbul, 2 (2005).
19. Teorey, J., T., "Database Modeling and Design", ***Morgan Kaufmann***, San Fransisco, 32-33 (1999).
20. İnternet: Wikipedia "Object Database" http://en.wikipedia.org/wiki/Object_database (17.02.2008).
21. İnternet: Wikipedia "SQL" http://tr.wikipedia.org/wiki/SQL (17.02.2008).
22. Blanding, F. S., "An Introduction to LAN/WAN Security", Information Security Management Handbook Fifth Edition, Tipton, F. H., Krause, M., ***Auerbach Publications***, New York, 394, (2004).
23. Foster, C. J., Osipov, V., Bhalla, N., Heinen, N., "Buffer Overflow Attacks: Detect, Exploit, Prevent", ***Syngress Publishing Inc***., Rockland, 4 (2006).
24. İnternet:Chapela, V., "Advanced SQL Injection"http://www.owasp.org/images/7/74/Advanced_SQL_Injection.ppt (18.02.2008).
25. Anley, C., "Advanced SQL Injection In SQL Server Applications", Next Generation Security Software Publication, Surrey, 18- 21 (2002).
26. Szor, P., "The Art of Computer Virus Research and Defense", ***Addison Wesley Professional***, Hagerstown, 12, (2005).
27. Symantec Corp., "Symantec Internet Security Threat Report Trends for Attack Trends for Q3 and Q4 2002" ***Symantec Volume III***, Cupertino, 22 (2003).
28. İnternet: IWS - The Information Warfare Site, "Microsoft SQL Worm Spida", http://www.iwar.org.uk/infocon/advisories/2002/02-003.htm (18.02.2008).
29. Jia, X., "Design, Implementation and Evaluation of an Automated Testing Tool for Cross-Site Scripting Vulnerabilities", Yüksek Lisans Tezi, ***Darmstadt University of Technology (TUD) - Computer Science Department***, 2-6 (2006).
30. Barrett, N., "Penetration testing and social engineering: Hacking the weakest link", ***Information Security Technical Report***, 8(4):56-58 (2003).
31. Sağıroğlu, Ş., Tunçkanat, M., Altuner, M., "Kriptolojide Yeni Bir Yaklaşım Resimli Mesaj", ***Telekomünikasyon Ekseni Dergisi***, Telekomünikasyon Kurumu, 2(2):22-24, (2002).
32. Groth, D., Toby, S., "Network+ Study Guide, Fourth Edition", ***Neil Edde & Sybex, Inc***., Alameda, 4, (2005).
33. Kalman, S., "Web Security Field Guide", ***Cisco Press***, Indianapolis, 36, 37 (2003).