
GAZİ ÜNİVERSİTESİ
Gazi
1926

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ GEREKSİNİMLERİNİN VERİ TABANI SİSTEMLERİNDE UYGULANMASI

Rabia YILDIZ

YÜKSEK LİSANS TEZİ

BİLİŞİM SİSTEMLERİ ANA BİLİM DALI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

TEMMUZ 2022

Rabia YILDIZ tarafından hazırlanan "ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ GEREKSİNİMLERİNİN VERİ TABANI SİSTEMLERİNDE UYGULANMASI" adlı tez çalışması aşağıdaki jüri tarafından OY BİRLİĞİ ile Gazi Üniversitesi Bilişim Sistemleri Ana Bilim Dalında YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Danışman: Doç. Dr. Çelebi ULUYOL

Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ...……

Başkan: Prof. Dr. Mahir DURSUN

Elektrik-Elektronik Mühendisliği Bölümü, Gazi Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Üye: Dr. Öğr. Üyesi Serkan GÖNEN

Bilgisayar Mühendisliği Bölümü, İstanbul Gelişim Üniversitesi

Bu tezin, kapsam ve kalite olarak Yüksek Lisans Tezi olduğunu onaylıyorum. ……...

Tez Savunma Tarihi: 06/07/2022

Jüri tarafından kabul edilen bu tezin Yüksek Lisans Tezi olması için gerekli şartları yerine getirdiğini onaylıyorum.

……..…….

Prof. Dr. Aslıhan TÜFEKCİ

Bilişim Enstitüsü Müdür

ETİK BEYAN

Gazi Üniversitesi Bilişim Enstitüsü Tez Yazım Kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- Tez içinde sunduğum verileri, bilgileri ve dokümanları akademik ve etik kurallar çerçevesinde elde ettiğimi,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne uygun atıfta bulunarak kaynak gösterdiğimi,
- Kullanılan verilerde herhangi bir değişiklik yapmadığımı,
- Bu tezde sunduğum çalışmanın özgün olduğunu,

bildirir, aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

Rabia YILDIZ

06/07/2022

ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ GEREKSİNİMLERİNİN VERİ TABANI SİSTEMLERİNDE UYGULANMASI

(Yüksek Lisans Tezi)

Rabia YILDIZ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Temmuz 2022

ÖZET

Teknoloji, hızla artması ile birlikte kurumlarda iş süreçlerinin bir parçası haline gelmiştir. Artan teknoloji ile bilgi miktarı artmış ve bilginin güvenliği büyük önem kazanmıştır. Bu sebeple, kurumların mevcut sistemlerinin ve iş süreçlerinin kesintisiz bir şekilde zarara uğramadan çalışabilmesi için Bilgi Güvenliği Yönetim Sistemini kurması ve işletmesi gerekmektedir. Ülkemizde de, eylem planları hazırlanmış bilgi güvenliği yönetim sisteminin dinamik bir yapıya kavuşturulması istenmiştir. Ülkemiz genelinde kurum ve kuruluşlar, veri tabanında bulunan verilerin öneminden dolayı doğabilecek riskleri de makul düzeye indirgemek için Bilgi Güvenliği Yönetim Sistemlerini kurmalı ve gerek kurum personelinin gerekse bilgi işlem sistemi sorumlularının standardı anlaması ve sahiplenmesini sağlamalıdır. Bu çalışma, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri sertifikasyon sürecinde yer alacak birçok sorumlunun, veri tabanı kavramı ve önemini kavrayıp veri tabanı yönetim sisteminde asgari gerçekleştirilmesi gereken gereklilikleri belirlemesine, standardı anlama ve özümseme aşamasında yaşayacağı problemleri ve belirsizlikleri en aza indirgemesine fayda sağlayacaktır. Böylece veri tabanı sorumluları da; standardın dayatması gibi gördükleri BGYS süreçlerinin ek iş yükü getirmediğini aksine standardın gereksinimlerinin veri tabanı yönetim sistemleri üzerinde uygulanabilir olduğunu anlayabileceklerdir. Ayrıca bu alanda yapılacak çalışmalara bir çerçeve oluşturması açısından önem arz etmesi de beklenmektedir.

Bilim Kodu	:	92403
Anahtar Kelimeler	:	Bilgi güvenliği yönetim sistemleri, ISO/IEC 27001, kurumsal bilgi güvenliği, veri tabanı yönetim sistemleri, veri tabanı güvenliği.
Sayfa Adedi	:	150
Danışman	:	Doç. Dr. Çelebi ULUYOL

APPLICATION OF ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEMS REQUIREMENTS IN DATABASE MANAGEMENT SYSTEMS

(M. Sc. Thesis)

Rabia YILDIZ

GAZİ UNIVERSITY

INFORMATICS INSTITUTE

July 2022

ABSTRACT

With the rapid increase on technology, it has become a part of business processes in institutions. With the increasing technology, the amount of information has increased and the security of information has gained great importance. For this reason, institutions need to establish and operate the Information Security Management System so that their existing systems and business processeses can operate uninterruptedly without any damage. Action plans were also prepared in our country, and it was requested that the information security management system be given a dynamic structure. Institutions and organizations throughout our country should establish Information Security Management Systems in order to reduce the risks that may arise due to the importance of the data in the database to a reasonable level and ensure that the database supervisors understand and own the standard. At this point, it is not enough for us to find what we need because the standard says what needs to be done without mentioning how to do it and the number of academic studies prepared is low. This study will help many responsible people who will take part in the ISO/IEC 27001 Information Security Management Systems certification process, to understand the database concept and its importance, to determine the minimum requirements to be fulfilled in the database management system, and to minimize the problems and uncertainties that they will encounter during the process of understanding and assimilation of the standard. Thus, the database administrators will be able to understand that the ISMS processes, which they see as the imposition of the standard, do not impose additional workload, on the contrary, that the requirements of the standard are applicable on database management systems and will be able to see how it is done. It is also expected to be important in terms of forming a framework for the studies to be carried out in this field.

Science Code	:	92403
Key Words	:	Information security, information security management systems, ISO/IEC 27001, database management systems, database security.
Page Number	:	150
Supervisor	:	Doç. Dr. Çelebi ULUYOL

TEŞEKKÜR

Bu tezin belirlenmesi ve yazılması sürecinde katkı ve yönlendirmeleri ile destek veren, önerilerinden faydalandığım danışmanım Doç. Dr. Çelebi ULUYOL'a; konu hakkındaki teknik bilgileri, yorumları ve değerlendirmeleri ile tezime katkıda bulunan kıymetli hocalarıma ve arkadaşlarıma; Yüksek Lisans eğitimim süresince destekleriyle beni yalnız bırakmayan değerli aileme teşekkür ve şükranlarımı sunarım.

İÇİNDEKİLER

Sayfa

Sayfa

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

Şekil **Sayfa**

KISALTMALAR

Bu çalışmada kullanılmış kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Kısaltmalar	Açıklamalar
BDDK	Bankacılık Düzenleme ve Denetleme Kurulu
BGYS	Bilgi Güvenliği Yönetim Sistemi
CMMI	Yetenek Olgunluk Model Entegrasyonu (Capabilitiy Maturity Integratıon)
COBIT	Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (The Control Objectives for Information and related Technology)
CPU	Merkezi İşlem Birimi (Central Process Unit)
DCL	Veri Kontrol Dili (Data Control Language)
DDL	Veri Tanımlama Dili (Data Definition Language)
DML	Veri İşleme Dili (Data Manipulation Language)
IEC	Uluslararası Elektroteknik Komisyonu (International Electrotechnical Commission)
ISACA	Bilgi sistemleri denetim ve kontrol birliği (Information Systems Audit and Control Association)
ISO	Uluslararası Standart Organizasyonu (International Standart Organization)
ITIL	Bilgi Teknolojileri Altyapı Kütüphanesi (Information Technology Infrastructure Library)
KVKK	Kişisel Verilerin Korunması Kanunu
PCI DSS	Ödeme Kartları Endüstrisi Veri Güvenliği (Payment Card Data Security Standard)
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al
SQL	Yapısal Sorgu Dili (Structured Query Language)
TSE	Türk Standartları Enstitüsü
TÜRKAK	Türk Akreditasyon Kurumu
VPN	Sanal Özel Ağ (Vitual Private Network)

1. GİRİŞ

Bilgi; tarih boyunca insanoğlunun en değerli varlığı olmuştur. İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda günümüzde bilgiye ulaşmak kolaylaşmıştır. Elektronik ortamlarda bulunan bilgilerin katlanarak artmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel ve kurumsal olarak en üst seviyelere çıkmıştır. Elektronik sistemlerin artması, ağ sistemleri üzerinden bilgi paylaşımı, bilgiye erişim yöntemlerindeki gelişmeler, sistemsel sıkıntıların tehdit oluşturması ve sonuç olarak veri kayıplarının sürekli artıyor olması bilgi güvenliğinin öneminin artmasındaki en büyük etkenler arasında yer almaktadır. Bilgi sistemlerine yapılan kötü niyetli saldırılardan dolayı bilgi güvenliğine verilen önem artmıştır ve yeni yaklaşımların, standartların kurumlar bünyesinde benimsenmesi ve uygulanması zorunluluğunu ortaya çıkmıştır [1].

Bilgi güvenliğinin sağlanabilmesi için ihtiyaç ve süreçlerine uygun olarak kurumların kendi bilgi güvenliği politikalarını ve prosedürlerini belirlemesi gerekmektedir. Bu politika ve prosedürler, kurum faaliyetlerinin gözden geçirilmesi, sistemlere erişimlerin takip edilmesi, gerçekleşen değişikliklerin kaydının tutularak değerlendirilmesi, kullanıcı yetkilerinin görevler ayrılığı ilkesine göre kısıtlanması gibi işlemleri de takip ederek bilginin güvenliğinin kontrol edilmesini sağlamaktadır.

Kurumlar mevcut sistemlerinin ve iş süreçlerinin kesintisiz bir şekilde zarara uğramadan çalışabilmesi için geniş kitlelerce kabul görmüş, geçerliliği olan standartlara göre Bilgi Güvenliği Yönetim Sistemi (BGYS) kurması ve işletmesi gereklidir. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı tarafından, ülkemiz genelindeki bütün bileşenleri kapsayacak şekilde 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı yayınlanmıştır. Bununla, özellikle kamu kurumları arasında iletişimin sağlandığı, güvenli hat olarak tabir edilen KamuNet ağının kurulması çalışmaları kapsamında tüm kamu kurumlarına ISO27001 kurulması zorunlu hale getirilmiştir [2].

Günümüzde bilişim projelerinin neredeyse hepsinde bir veri tabanı yönetim sistemi kullanılmaktadır. Kurumlarda bu taleplerden dolayı yatırımlarının büyük çoğunu bilişim alt yapısına aktarmaktadır. Bu da bilişim sistemlerinin vazgeçilmez parçası olan veri tabanlarının önemini artırmakta ve her kurum güçlü veri tabanlarına sahip olmak istemektedir. Bu güçlü veri tabanlarında veri sözlüğü, güvelik, yedekleme, felaket durumunda geriye dönüş fonksiyonlarının her biri 27001 standardına da uygun hale

getirilmeli ki bu güçlü veri tabanlarındaki büyük miktardaki hassas veriler hızlı ve güvenli bir şekilde gereksinim duyulan bilgiye dönüştürülebilsin. Bilgiye izni veya yetkisi olmayan erişim, kullanım, değiştirme, açığa çıkarma, yok etme ve hasar vermeyi önlemek olarak ifade edilen bilgi güvenliğinin temel üç bileşeni "gizlilik (confidentiality), bütünlük (integrity) ve erişilebilirlik (availability), veri tabanında hassas verilerin korunumu için de olmazsa olmazdır [3].

Kurum ve kuruluşlara getirilen BGYS kurma ve bunu ISO27001 standardı ile belgelendirme zorunluluğu ile Türkiye'de bulunan kurum ve kuruluşların Bilgi Güvenliği Yönetim Sistemlerini oluşturması sağlanmaktadır. Sertifika sahibi olmak isteyen kurumlar ve personel ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri ve bu standarda tavsiye niteliği taşıyan ISO/IEC 27002 Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri standartlarını incelediklerinde kendilerinin ne yapması gerektiğini anlayabilmektedir. Fakat yapmaları gerekenlerin nasıl yapılacağı konusunda kendilerine rehberlik edecek bir bölümü standartta bulamamaktadırlar. İşte tam da bu esnada kendilerine yardımcı olacak bir kaynak ihtiyacı ortaya çıkmaktadır. Ülkemizde Bilgi Güvenliği Yönetim Sisteminin kurulması ve dinamik bir şekilde sürdürülmesi ile ilgili yeterli kaynak olmamasından doğan ihtiyaç ile danışmanlık kuruluşları devreye girmektedir. Ülkemizdeki ISO/IEC 27001 sertifikalarının birçoğu eğitim firmaları veya danışmanlık firmaları ile yapılan ortak çalışmalar ile alınmaktadır. Danışmanlık firmaları, her kurumun kendi kurum kültürüne göre hassas verilerinin farklılık göstereceği hususunu göz ardı edip pek çok kurumda benzer bir bilgi güvenliği yönetim sistemini oluşturarak sadece kurumların belgelendirme sürecini başarıyla tamamlamasını hedef almaktadır. Fakat bu şekilde sertifika sahibi olan kurumların çoğu bilgi güvenliği konusunda pek fazla bilgi sahibi değildir [4]. Bu şekilde kurulan BGYS ile bilgi güvenliğinin sağlıklı yürütülmesi de mümkün gözükmemektedir.

Her kurumun kendi kurum kültürü olduğu ve hassas noktalarının farklılık gösterdiği düşünüldüğünde bir kurumda işleyen sistem diğerinde aksaklıklara sebebiyet verebilmektedir. Bunun için her kurum ISO27001 Bilgi güvenliği yönetim sistemi standardını iyice anlamalı, zorunlu olan maddeleri uygulamalı ve kuruluşun isteğine bağlı olan maddeleri de inceleyerek kendi yapısına uygun ihtiyaçlarını karşılayanları belirleyip uygulamalıdır. Kurum personeli, BGYS çalışmalarının kurumsal bir ihtiyaç olduğunu, mecburiyetten değil gereklilikten yapılması gerektiğini kabul etmelidir. Sürecin en zorlu aşaması çalışanların motivasyonu ve gereklilerin yapılması ve benimsenmesi konusunda gösterilecek kararlılıktır [5].

Bilgi güveliğini kurumların eksiksiz olarak sağlayabilmesi için gerek kurum personelinin gerekse bilgi işlem sisteminin temel bileşeni olan veri tabanı sorumlularının ISO27001 standardını anlaması ve sahiplenmesi büyük önem arz etmektedir. Bu nedenle de, veri tabanı sorumlularının teknik yeterliliklerine ışık tutmak ve BGYS'yi sahiplenmelerini sağlamak için ihtiyaç duyulan fakat şimdiye kadar herhangi bir otorite tarafından hazırlanmamış kaynak eksikliğinin kapsamlı hazırlanan bu çalışma ile giderilebileceği düşünülmektedir.

Bilgi güvenliği kavramı, bilgi güvenliği yönetim sistemi ve kurumlar açısından öneminin anlaşılması, ISO27001 Bilgi Güvenliği Yönetim Sistemi Standardı ve gereklerinin nasıl uygulanacağının kavranması, veri tabanı kavramının ve öneminin anlaşılması, veri tabanında bulunan verilerin öneminden dolayı doğabilecek riskleri makul düzeye indirgemek için uygulanması gereken kontrollerin belirlenmesi bu çalışmanın amacını oluşturmaktadır. Bölüm bölüm çalışmanın amacını oluşturan yukarıdaki konulara detaylı yer verilmekte olup sık rastlanan veri tabanı güvenlik tehditlerinden bahsedilmekte, çalışmanın esas konusu olan veri tabanı ile ilgili bilinmesi gereken genel konular anlatılmakta ve standardın gereksinimlerinden veri tabanını doğrudan ya da dolaylı olarak ilgilendiren kısımlar sınıflandırılıp set halinde verilmekte ve her birinin nasıl sağlandığı anlatılmaktadır.

Bu çalışma, ISO/IEC 27001 standardına veri tabanı yönetim sistemlerini uyumlu hale getirmek isteyen veri tabanı sorumlularının, neyi, ne için ve nasıl yapacağı sorularına cevap bulmasını sağlayarak standardın dayatması gibi gördükleri ve nasıl yapılacağını bilmedikleri gereksinimlerin veri tabanı yönetim sistemleri üzerindeki uygulanabilirliği adım adım görmeleri bu sayede de veri tabanlarında bilgi güvenliğinin eksiksiz ve dinamik bir şekilde sağlanmasını hedeflemektedir.

2. BİLGİ GÜVENLİĞİ

Bu bölümde bilgi, bilgi güvenliği, bilgi güvenliğinin temel unsurları ve bilgi güvenliği yönetim sistemi ile ilgili bilinmesi gereken temel kavramlara ve ilgili süreçlere değinilecektir.

2.1.Bilgi Nedir?

Bilgi Latince 'deki herhangi bir şeye şekil vermek anlamına 'informare' kelimesinden gelmektedir. Bilgi, gelecekteki kararların şekillenmesinde ve şimdiki kararların alınmasında kullanılan, işlenmiş veri (data) olarak da tanım5lanabilir. Literatürde çok farklı şekillerde tanımlanmıştır. Bilgi doğruluğu ispatlanmış inançlardır.

Bilginin temelini veri ve enformasyon oluşturur. Veriler, belirli bir bağlamda işlendiğinde anlamlı hale gelerek bilgiyi oluşturmaktadır. Bilgi, verinin işlenmiş halidir.

Bilgi birçok biçimde bulunabilir. Bilgi; yazılı şeklide tutulabilir, sözlü olarak ifade edilebilir ya da elektronik ortamda tutulabilir. Hangi formda olursa olsun, bilgi mutlaka uygun bir şekilde korunmalıdır. Bilgi güvenliğinin sağlanabilmesi için bilginin gizliliğinin ve bütünlüğünün korunması gerekmektedir.

2.2.Bilgi Güvenliği Nedir?

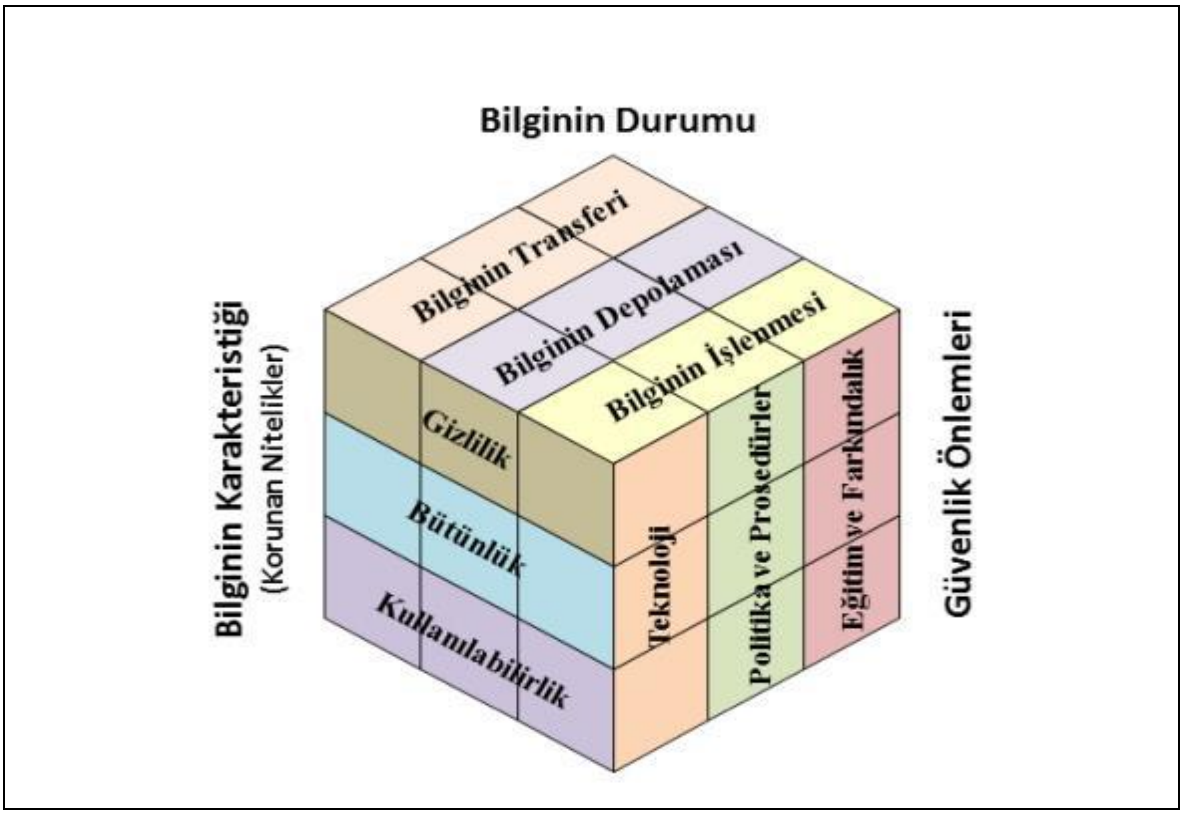
Bilgi güvenliği, farklı ortamlardaki bilgileri izinsiz-yetkisiz erişimlerden, bütünlüğü bozacak işlemlerden ve kötü niyetli saldırılardan korumaktır. "Gizlilik", "Bütünlük" ve "Süreklilik(erişilebilirlik)" olarak isimlendirilen üç temel unsurdan meydana gelir. Bu üç temel güvenlik öğesinden herhangi biri zarar görürse güvenlik açığı oluşur. Bilgi güvenliği başarıyı tamamlayan yönetim sistemi içinde yer alan bir araç ve yöntemler bütünüdür.

Bilgi güvenliği, bilgilerin izinsiz veya yetkisiz erişimlerden, ifşa edilmesinden, değiştirilmesinden, yok edilmesinden kısaca kişisel veya kurumsal mahremiyetin korunması işlemidir [6].

Bilgi güvenliği, kurumların faaliyetlerine en az sorun ile devam edebilmesini ve bilgi varlıklarının korunmasını sağlar. Böylece kurumların güvenilirliğini güvence altına alır.

2.3. Bilgi Güvenliği Temel Unsurları

Literatürde bilgi güvenliği ile ilgili farklı modeller bulunmaktadır. Bu modellerden en kapsamlılarında biri McCumber tarafından geliştirilen bilgi güvenliği modelidir. Model Şekil 2.1' de görüldüğü üzere 3*3*3 hücrelereden oluşan Rubik küpüne benzemektedir [7].



Şekil 2.1. McCumber bilgi güvenliği modeli [7]

Şekil 2.1'de verilen bilgi güvenliği modeli; teknoloji, politikalar, eğitim ve farkındalık güvenlik önlemlerini, bilginin durumuna bağlı olarak korunması gereken gizlilik, bütünlük ve kullanılabilirlik unsurlarını tek bir çatı altında ele almaktadır.

Bilgi güvenliğinin gizlilik, bütünlük, erişilebilirlik temel unsurları üzerine kurulu olduğu düşünülse de aslında bunlarla bütün halinde çalışan bir çok unsur daha vardır. Şekil 2.2'de görülen bu unsurlardan biri dahi eksik olsa güvenlik tam anlamıyla sağlanmış olamaz, bu unsurlar birbirini tamamlayıcıdır.

Şekil 2.2. Bilgi güvenliği unsurları [8]

Şekil 2.2'de kimlik sınaması, yetkilendirme, kayıt tutma, gizlilik, veri bütünlüğü, süreklilik, güvenilirlik, inkar edememe bilgi güvenliği unsurları verilirken detayları bir sonraki kısımda ele alınmıştır.

2.3.1. Gizlilik (Confidentiality)

Gizlilik, bilginin sistemler üzerinde veya bir gönderici ile alıcı arasında taşındığı ya da saklandıkları yerlerde o bilgiye sadece erişebilmesini istediğimiz yetkili kişilerin erişip yetkisiz kişilerin erişememesi, bilgiyi ele geçirememesidir. Gizlilik konusu veri gizliliği ve mahremiyet olarak da düşünülebilir. Bilgi bir veri tabanında tutulduğunda bu bilginin sadece belli kişiler tarafından görülmesi istenir. Bu gizliliği sağlamak için de şifreleme teknolojileri kullanılır.

2.3.2. Bütünlük (Integrity)

Verinin orijinal halinde durmasıdır. Bütünlük, verinin tam ve eksiksiz olması ve doğruluğunun sağlanmasıdır. Bilginin veri tabanında veya gönderim halinde iken yetkisiz bir değiştirme işlemi, tahrip edilme veya silinme gibi işlemler istenmez. Bütünlüğün korunması için elektronik imza, açık anahtar altyapısı gibi teknolojiler kullanılır.

2.3.3. Erişilebilirlik (Availability)

Erişilebilirlik, bilginin yetkililer tarafından ihtiyaç duyulan her zaman ya da problem çıkması durumunda ulaşılabilir ve kullanıma hazır durumda olmasıdır. Herhangi bir sorun halinde bilginin erişilebilir olması süreklilik unsurunun ihtiyaçlarındandır. Erişilebilirlik unsurunun sağlanması için bilgiye erişim sağlayan kanalların doğru ve güvenli çalışması gerekir.

2.3.4. Güvenilirlik (Reliability-Consistency)

Güvenirlik, bir bilgisayar ya da bilgi iletişim sisteminin tasarıma uygun olarak sürekli çalışması, işlemleri eksiksiz yapması, beklenen sonucun üretilmesi ve elde edilen sonuçların beklenenle uyumlu olması durumudur [9].

2.3.5. İnkâr edememe (Non-Repudiation)

Bilgi aktarımının olduğu sistemlerde hem alıcı hem de gönderen veriyi aldığını inkâr edememelidir. Bu prensip log kayıtlarının tutulması ile birlikte değerlendirilebilir. Özellikle gerçek zamanlı işlem yapan finans sektöründe kullanılmaktadır. Genel olarak ön şart, “Kimlik Doğrulama” ve “Bütünlük” prensiplerinin sağlanması beklenir.

2.3.6. Kimlik doğrulaması (Authentication)

Kimlik doğrulaması; sisteme girmek isteyen cihaz veya kullanıcının, sisteme yetkili olan kullanıcı bilgilerinin tutulduğu veri tabanında eşleşmesi var mı diye karşılaştırılırsak eğer kullanıcı bilgilerinden biri ile uyuşuyor ise kullanıcıya erişim izni verilmesidir. Eğer veri tabanında depolanan hiçbir kullanıcı bilgisi ile uyuşmuyorsa kimlik doğrulaması başarısız olur ve kullanıcı sisteme erişemez. OTP (tek kullanımlık şifre) , biyometrik kimlik doğrulama, şifre gibi çeşitli kimlik doğrulama yöntemleri bulunmaktadır [10].

2.3.7. Yetkilendirme (Authorization)

Yetkilendirme, genel olarak kullanıcının kimliğinin doğrulandığını varsayarak, herhangi bir bilgiye erişmek için gerekli izne sahip olup olmadığının kontrol edilerek düzenlenmesidir. Sistemde tanımlı ve kimlik doğrulaması yapılmış bir kullanıcının, bilgiye erişim ve eylemlerle ilgili izinlerin ve yetkilerin belirtilmesidir [11].

2.3.8. İzlenebilirlik/kayıt tutma (Accountability)

İzlenebilirlik, kullanıcının sistem içerisindeki bütün hareketlerinin işlem saatleri ile birlikte kayıt altında tutulmasıdır. Bir sistem ya da ağ yapısı içerisinde kullanıcının işlemlerinin kayıt altında tutulması problemlerin denetimi, takip edilmesi, analizi ve çözümü için gereklidir.

2.4. Kurumsal Bilgi Güvenliği

Kişisel güvenliği doğrudan etkileyen faktör kurumsal bilgi güvenliğidir. Kurumsal bilgi güvenliği sağlanmadıkça, kişisel güvenlikte sağlanamaz. Kurumsal bilgi güvenliği, kurumların bilgi varlıklarının tehlikelerden korunması amacıyla gerekli güvenlik önlemlerinin alınmasıdır. Kurumsal bilgi güvenliği birçok faktörün etki ettiği yönetilmesi zorunlu olan karmaşık bir süreçtir. Yani, bilgi güvenliği ciddi bir kurum kültürü ve her bir çalışanının katkısını ve katılımını gerektirir.

Bilgi güvenliğini sağlamak için tüm dünyada kurumsal bilgi güvenliğinin standartlaştırılma çalışmaları devam etmektedir. Bu konuda önderlik eden İngiltere tarafından geliştirilen BS–7799 standardı, ISO tarafından kabul edilerek önce ISO–17799 sonrasında ise ISO–27001:2005 adıyla dünya genelinde bilgi güvenliği standardı olarak kabul edilmiştir. Ülkemizde Avrupa Birliği Uyum Kriterlerinde de geçen bu standartların uygulanması konusunda yapılan çalışmalar yetersiz olup bu standardı uygulayan kurum ve kuruluşların sayısı çok azdır. ISO–27001:2005 standardı ülkemizde TS ISO/IEC 27001 “Bilgi Güvenliği Yönetim Sistemi” standardı adı altında yayınlanmış ve belgeleme çalışmaları ilk bu standartla başlatılmıştır. Kurumlar açısından bilgi sistemlerinin korunabilmesi ve sürekliliğinin sağlanması, BGYS’nin kurumlarda hayata geçirilmesiyle mümkündür. BGYS’nin kurulmasıyla; birçok denetim birbirini tamamlayacak şekilde profesyonel olarak gerçekleştirilir. BGYS’nin kapsamı kurumların ihtiyaçları doğrultusunda tespit edilir.

2.5.Bilgi Güvenliği Yönetim Sistemi

Bilgi Güvenliği Yönetim Sistemi kısaltılmış adıyla BGYS, bilgileri yönetmek amacıyla benimsenen planlı bir yaklaşımdır. BGYS'nin temel amacı hassas bilginin korunmasıdır. Bilgi Güvenliği Yönetim Sistemi; bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini yöneten sistemli, sürdürülebilir, dokümante edilmiş, üst yönetimce kabul edilmiş ve desteklenmiş, uluslararası güvenlik standartlarının temel alındığı bir bütündür [12].

Bilgi güvenliğinin sağlanması sadece teknoloji ile mümkün değildir. Bilgi güvenliği üç ayak üzerinde duran bir sandalye gibidir bu üç ayak insan, süreç ve teknolojidir bunlardan birinin eksikliğinde sandalyenin dengesi kaybolacaktır. Bu yüzden bilgi güvenliğinde bu üç faktör birlikte değerlendirilmeli ve bilgi güvenliği yönetimi teknoloji, insan ve süreç faktörlerine göre oluşturulmalıdır.

Bilgi güvenliği, bilgi güvenliği yönetim sistemlerinde başarıyı tamamlayan en önemli araçtır. Bilgi güvenliği yönetim sisteminin kurulumunda personel, tedarikçiler ve üst yönetim hesaba katılmalıdır. BGYS kurulumu sadece bilgi işlem birimlerinin sorumluluğunda olan bir sistem değildir çünkü bilgi işlem personelinin kurumun tüm birimlerinde ki iş ve işleyişlere hâkim olması mümkün değildir. Bu nedenle her birimin bilgi birikimleri, beklentileri ve riskleri üst yönetiminde desteği ile kurulum aşamasında birim personelleri ile birlikte değerlendirilir. Varlık ve riskler ortaya konularak tüm yönetim kademelerini içine alan bir politika hazırlanır ve uygulanmaya başlanır. Böylece yönetim kademesi ileride büyük sorunlar oluşturabilecek riskleri sürekli değerlendirerek sorun oluşmadan önce çözmüş olur. Roller ve sorumluluklar, görevler ayrılığı BGYS kurulurken belirlenmiş olacağından bir sorun anında, acil müdahale gerektiğinde tüm personel kendine düşen işi bilir ve denetim izleri oluştuğundan soruna sebebiyet veren sorumlularda tespit edilir. Kurulan BGYS sistemi sayesinden bir felaket durumunda da yaşanması olası olan veri kayıplarının ve maddi kayıpların önüne önemli ölçüde geçilir ve iş sürekliliği sağlanmış, kurumun itibarı korunmuş olur. BGYS'yi kuran bir kurum güvenlik standartlarına, düzenlemelere, yasa ve yönetmeliklere uyum sağlar, bilgi varlıklarını tehditlere karşı korur.

Bilgi Güvenliği Yönetim Sistemleri (BGYS); üst yönetim tarafından da desteklenen bir yönetim sistemidir. Kurumlar risklerin en aza indirilmesi ve devamlılığın sağlanması, BGYS'nin kurumlarda uygulanmasıyla mümkündür. BGYS'nin kurulmasıyla; birçok denetim birbirini tamamlayacak şekilde gerçekleştirilir. Kurumsal bilgi güvenlik

politikalarının oluşturulması, risk yönetimi ve uygulanabilirlik beyannameleri BGYS kurulabilmesi ve uygulanabilmesi için, yapılması gereken adımlardır.

2.5.1. Bilgi güvenliği yönetim sistemi çeşitleri ve standard kuruluşları

Dünyada ve Türkiye'de bilgi güvenliğinin sağlanması amacıyla çeşitli bilgi güvenliği yönetim sistemleri bulunmaktadır. Bunlardan en çok kabul görüp en yaygın kullanılanları şunlardır:

- PCI-DSS
- COBIT
- ITIL
- HIPAA
- CMMI
- PRINCE2
- BS25999
- ISO27001

PCI-DSS

Kart ile yapılan ödemelerin güvenliğinin sağlanması, sahtecilik ve dolandırıcılık işlemlerine karşı etkin bir koruma geliştirmek amacıyla geliştirilmiştir. Dünya genelinde kabul görmüş standartlar arasında yer almaktadır. Payment Card Data Security Standard yani PCI DSS'in Türkçesi Ödeme Kartları Endüstrisi Veri Güvenliğidir [1]. Kartlı ödeme sistemleri içinde yer alan kuruluşların veri güvenliği riski en az seviyeye inmektedir. Hizmet sağlayıcılar ile ilgili kriterler Visa ve Mastercard 'ın web sitelerinde detaylı bir şeklide yer almaktadır.

COBIT

COBIT, Control Objectives for Information and related Technology kelimelerinin kısaltmasından oluşmaktadır. Information Systems Audit and Control Association yani ISACA ve IT Governance Institute (ITGI) tarafından bilgi teknolojileri yönetiminde ulaşılması gereken hedefleri ortaya koymak amacıyla geliştirilmiş ve ilk sürümü 1996 yılında yayınlanmıştır [13].

COBIT'in son sürümü 5.0 'dır. COBIT 5'te, yönetişim ve yönetim terimleri birbirinden farklı ele alınmıştır. Yönetişim; işletme hedeflerini belirlerken paydaşların ihtiyaçlarını ve durumlarını değerlendirerek karar üretme yoluyla yönlendirirerek yön ve hedeflere uyumu izler. Yönetim ise; işletme hedeflerine ulaşmak için yönetişim tarafından belirlenmiş yön ile uyumlu olarak planlama, inşa etme işlemlerini gerçekleştirir [10].

ITIL

ITIL, BT yönetimi, olay yönetimi, değişiklik, konfigürasyon, problem ve kullanılabilirlik yönetimi gibi BT operasyonlarının net bir görüntüsünü sunmaktadır [14]. 1990'lı yıllarda özellikle Avrupa'da birçok kamu kuruluşunun benimsemesi ve uygulaması ile tüm dünyada kabul edilen bir standart haline gelmiştir.

HIPAA

HIPAA, hastanın tıbbi gizliliğinin korunması için internet uygulamaları veya elektronik sistemler kullanan yerlerin yükümlülüklerini yerine getirmek zorunda olduğu kuralları ve düzenlemeleri sağlayan bir Amerika Birleşik Devletleri mevzuatıdır. Önemli olan nokta sağlık kurumlarının datalarının gizliliği ve bilgilerin izinsiz erişime karşı korunmasını temin etmektir.

CMMI

CMMI (Capabilitiy Maturity Integratıon Yetenek Olgunluk Model Entegrasyonu) bir süreç modelidir. İyileştirme yaklaşımıdır ve ne yapılması gerektiğini açıklar. Projeye rehberlik eder ve ortaya konulan seviyelere göre olgunluk gelişimi sağlanır. Dünya'da ve Türkiye'de özellikle IT sektöründe ve yazılım geliştirme departmanlarında kullanılan bir referans modeldir.

PRINCE2

PRINCE (Projects In Controlled Environments) 1970'li yıllardan beri geliştirilmektedir. En son Haziran 2009'da yenileme yapılmıştır. Proje yönetim metodolojisidir. Sorun çıktıları, kullanım kılavuzları, şablonlar içermektedir.

BS25999

İngiliz Standart Enstitüsü tarafından geliştirilmiştir. İş sürekliliği yönetimidir ve her sektöre uygundur. Dünyanın en iyi uzmanlarından oluşan bir grup tarafından geliştirilmiştir.

ISO27001

Türkiye'de en çok kullanılan ve tezimizinde ilerleyen bölümlerinde üstünde daha çok duracağımız standartır.

Standart kuruluşları, uluslararası platformlarda kurumsal kuruluşlar olarak faaliyetlerini sürdürmektedir. Standard kuruluşları şunlardır:

- ISO
- IEC
- CEN
- TSE
- TÜRKAK

ISO

International Organization For Standardization kelimelerinin baş harflerinin birleşimi olarak kısaltılan ISO yani Uluslararası Standartlar Teşkilatı, Uluslararası Elektronik Komisyonu'nun kapsamındaki konular dışında kalan bütün teknik ve teknik dışı alanlardaki standartların oluşturulması çalışmalarını yürütmek amacıyla 1947 yılında kurulan kuruluşa üye ülkelerin sayısı 162'dir [15]. ISO'nun temel amacı uluslararası standartları tüm ülkelerce kabül ettirebilmektir. Uluslararası bu kuruluşun ülkemizdeki temsilcisi TSE'dir.

IEC

International Electrotechnical Commission, birçok dünya ülkesinin üyesi olduğu elektrik, elektronik ve ilgili teknojilerle ilgili uluslararası standardlar hazırlamayı ve uluslarası standardları geliştirmeyi hedeflemektedir. TSE' de IEC üyesi ülkeler arasında yer almaktadır.

CEN

CEN, European Committee for Standardization yani Avrupa Standartlarının kısaltmasıdır. Standartları Avrupa Birliği düzeyinde uyumlu hale getirmek için oluşturulmuştur [16]. TSE 2012 yılından beri CEN'in tam üyesi olup Avrupa Standartlarını uyumlaştırarak Türk Standadı olarak yayımlamaktadır.

Türk Standardları Enstitüsü (TSE)

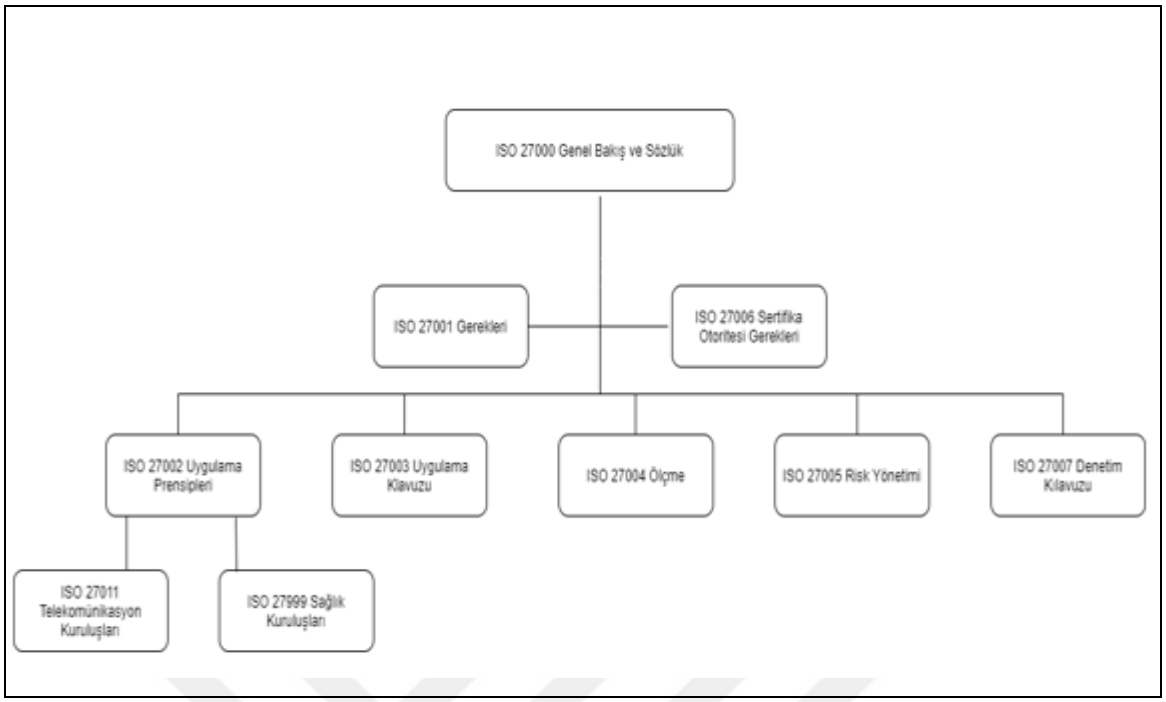
Kuruluşun temeli 1954 yılında Türkiye Odalar ve Borsalar Birliği (TOBB) bünyesinde hazırlanan tüzüğe dayanan Türk Standartları Enstitüsü, her türlü usul ve hizmet standartlarını yapmak için 1960 yılında çıkarılan 132 sayılı kanun ile kuruluşunu tamamlamıştır. Bağlı olduğu bakanlık, Türkiye Cumhuriyeti Sanayi ve Teknoloji Bakanlığıdır. Enstitü, özel hukuka tabi olan bir kamu kurumu olup markası TSE'dir. Her türlü standartları hazırlamak ve hazırlatmak, kabul edilen standartları yayımlamak gibi görevleri yerine getiren TSE'nin kabul ettiği standartlara Türk Standardı denir. Bu standartlar, standardın ilgili olduğu bakanlığın onayı ile zorunlu kabul edilebilir. Bir standardın şart koşulabilmesi için zorunlu kılınması yani Türk Standardı olması şarttır. Zorunlu kılınan standartlar Resmî Gazete 'de yayımlanır ve yürürlüğe girer [17].

Türk Akreditasyon Kurumu (TÜRKAK)

TÜRKAK, 1999 yılında 4457 sayılı kanunla Başbakanlığa bağlı olarak kurulmuş olup günümüzde Dış İşleri Bakanlığına bağlı bir kuruluş olarak faaliyetlerini sürdürmektedir. Uygunluk değerlendirme kuruluşlarını akredite etmek yani yeterliliklerini, ulusal ve uluslararası standartlara uyumluluklarını ve bu kuruluşlarca düzenlenen belgelerin ulusal ve uluslararası alanda kabulünü temin etmek amacıyla dünya genelinde kabul görmekte olan gereklilikleri esas alarak faaliyet gösteren bir kuruluştur [18].

2.5.2. ISO/IEC 27000 bgys standartları ailesi

ISO 27000 ailesi bir kısmı zorunluk içeren bir kısmı ise zorunluluk içermeyen sadece kılavuz niteliği taşıyan pek çok standarttan oluşmaktadır. Bu ailenin en iyi bilinen ve en geniş kullanım alanına sahip olan standardı ISO27001'dir.



Şekil 2.3. BGYS ailesi standardları arasındaki ilişkiler

ISO / IEC 27000 BGYS standart ailesindeki ilişki şekil 2.3'de özetlenmiştir.

ISO27001 ve ISO27006 standardları zorunluluk içeren gereksinimleri açıklar.

- ISO/IEC 27006: Bu Uluslararası Standart, ISO / IEC 17021-1 ve ISO / IEC 27001 içerisinde yer alan gereksinimlere ek olarak, bir bilgi güvenliği yönetim sisteminin (BGYS) denetim ve belgelendirmesini sağlayan kuruluşlar için gereksinimleri belirler ve rehberlik sağlar [19].

Şekil 2.3'te yer alan tek başlarına zorunluluk içermeyen ama tüm standard ailesini etkileyen standartlara da kısaca değineceğiz:

- ISO/IEC 27002: Bilgi güvenliği kontrollerinin uygulanması hususunda bir çok hususu ele alan ve öneriler sunan bir standarddır. Kılavuz olarak kullanılır, kontrol maddelerine uyulma zorunluluğu yoktur.
- ISO/IEC 27003: ISO / IEC 27001'de belirtilen bilgi güvenliği yönetim sistemi gereklilikleri hakkında rehberlik etmekte ve bunlarla ilgili öneriler, olasılıklar ve izinler sunmaktadır. Bilgi güvenliğinin tüm yönleriyle ilgili genel rehberlik sağlamak bu belgenin amacı değildir [20].

- ISO/IEC 27004: İzleme, ölçüm, analiz ve değerlendirme gerekliliklerini yerine getirmek için bilgi güvenliği performansını ve bilgi güvenliği yönetim sisteminin etkinliğini değerlendirmelerine yardımcı olmak amacıyla hazırlanmıştır [21].
- ISO/IEC 27005: Bu belge ISO / IEC 27001'de yer alan genel kavramları destekleyerek risk yönetimi yaklaşımını temel alan bilgi güvenliğinin eksiksiz uygulanmasına yardımcı olmak için hazırlanmıştır [15].
- ISO/IEC 27007: Bu belge, ISO 19011: 2011'deki kılavuza ek olarak, bilgi güvenliği yönetim sistemi (BGYS) denetim programının yönetilmesi, denetimlerin yapılması ve BGYS denetçilerinin yeterliliği hakkında rehberlik sağlar [22].
- ISO/IEC 27011: Telekomünikasyon alanında faaliyet gösteren kuruluşlarda ISO27001'in ek-a kısmındaki kontrol maddelerinin yerine getirilmesi için rehberlik eden bir kılavuzdur.
- ISO/IEC 27799: Sağlık alanında faaliyet gösteren kuruluşlarda 27001 maddelerinin yerine getirilebilmesine rehberlik eden yardımcı bir kaynak, kılavuzdur.

2.5.3. ISO/IEC 27001 bilgi güvenliği yönetim sistemi

Bu bölümde bilgi güvenliğinin sağlanması aşamasında insan, süreç ve teknolojileri içeren yönetim sistemi olan ve günümüzde en çok kullanılan yönetim sistemi olan 27001'e detaylı yer verilmiştir.

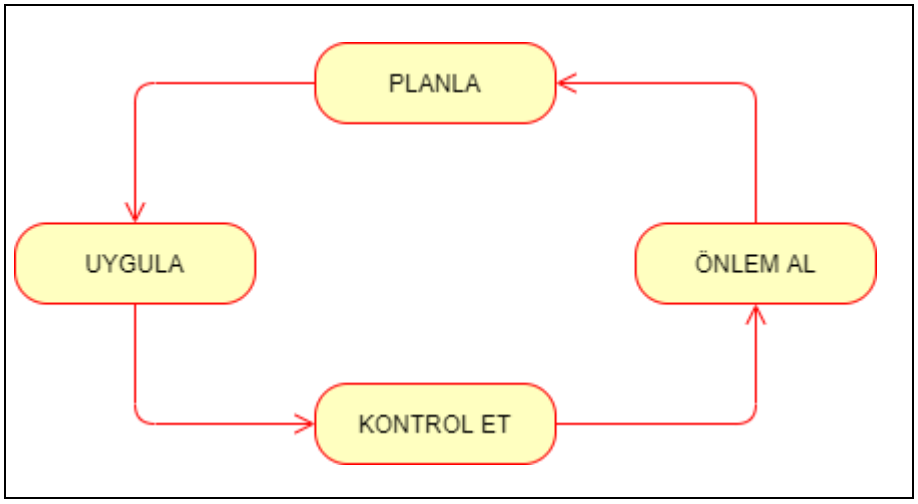
Tarihsel gelişimine baktığımızda ilk kez 1993 yılında BSI(British Standarts Institution) tarafından başlatılmış ve bir İngiliz standardı olarak 1995 yılında kabul edilmiştir. 2000 yılında ISO ve IEC kuruluşları ortak bir çalışma ile ISO/IEC 17799 standardını geliştirmişlerdir bu standard 2005 yılında ISO/IEC 27001:2005 sürümü olarak yayınlanmıştır. TSE tarafından çevirisi yapılarak ülkemizde de TS ISO/IEC 27001:2005 adıyla kabul edilmiştir. Bu standardlar ailesine ihtiyaçlara göre yeni kılavuzlar ve yeni standardlar oluşturulmaya başlanmıştır. Şekil 2.3'te de görüldüğü gibi 27000-27999 arasındaki standardlar bilgi güvenliği konusuna aittir. Hızla gelişen teknoloji dünyasında kabul gören standardların ihtiyaçları karşılayamadığı durumlarda aynı standard revizyona girerek sonuna tarih eki almıştır. ISO/IEC 27001'in son versiyonu 2017 yılında yayınlanmış ve bu standardın da çevirisi yapılarak TS ISO/IEC 27001:2017 bir türk standardı olarak kabul edilmiştir.

ISO27000 ailesindeki tüm standardlar bilgi güvenliği yönetim sisteminin kurulması, ISO27001 standardının başarıyla yerine getirilebilmesi için yardımcı olmaktadır. Bu standardın zorunluluklarını yerine getirdiğine inanan kurumlar yapacakları veya dışarıdan yaptıracakları denetimler ile kendilerini TÜRKAK tarafından akredite edilen belgelendirme kuruluşlarının denetimine hazırlar. Belgelendirme kuruluşu standardın gereksinimlerinin yerine getirildiğini düşünürse kuruma sertifika hazırlayarak kurumun bilgi güvenliği yönetim sisteminin varlığını ve bu sistemin güvenilirliğini tasdiklemiş olur.

Bu standard, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, sürdürmek ve iyileştirmek için bir modeldir. Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, tüm kuruluş türlerini içine alır. BGYS, bilgi varlıklarını korumak için yeterli ve orantılı güvenlik kontrollerini sağlar. Bir kuruluşun ISO 27001 sertifikasına sahip olması, kurumun güvenlik risklerini bildiği, yönettiği ve bu riskleri yok etmek için kaynak ayırdığı anlamına gelir.

ISO/IEC 27001 PUKÖ yaklaşımı

ISO/IEC 27001 standardının gereksinimleri yerine getirilirken en baştan en sona PUKÖ döngüsü durmadan devam eder. Yönetim sistemi kurulmasında Şekil 2.4'te gösterilen Planla-Uygula-Kontrol Et-Önlem Al modeli esas alınmaktadır. Bu model ile özetle; ne yapılacağı planlanır, planlanan kararlar gerçekleştirilir, gerçekleştirilen kararlarda eksikler var mı diye kontrol edilir ve ortaya çıkan eksiklikler için önemler alınır.



Şekil 2.4. PUKÖ döngüsü

Şekil 2.4’ deki döngü adımlarını tek tek inceleyecek olursak;

Planla

BGYS kurulumu da PUKÖ’nun ilk adımını Planlamayı temsil eder. Çünkü Planla aşamasında kurumda, BGYS’nin kurulması, ihtiyaç, hedef ve kapsamın belirlenmesi bunlara göre politika, prosedür ve risklerin belirlenerek oluşturulması aşamaları gerçekleştirilir.

Uygula

BGYS’nin oluşturulması Uygula adımında gerçekleştirilir. BGYS politikası, prosedürü, süreç ve kontrolleri bu adımda gerçekleştirilip işletilir.

Kontrol Et

Bilgi güvenliği sürekli takip edilmesi ve gözden geçirilmesi gereken bir yönetim sistemidir. BGYS politika ve prosedürleri, amaç ve kullanım deneyimlerine göre değerlendirilmeli ve eksiklikler ortaya çıkarılmalıdır.

Önlem Al

BGYS’nin sürekli iyileştirilmesini sağlamak için gözden geçirmeler ve denetimlerde çıkan eksikliklerin giderilmesi çalışmaları bu aşamada yapılmaktadır.

Bilgi güvenliği yönetim sisteminin kurulması, uygulanması ve yönetilmesi

Bilgi güvenliği yönetim sisteminin kurulması, uygulanması ve yönetilmesi aşamalarında ISO27001 standardında yer alan kontrollerden faydalanılmaktadır. Bilgi güvenliği yönetim sistemi sürekli devam eden bir süreçtir ve bu süreç sistemin başından sonuna kadar PUKÖ modelindeki adımlar ile tekrarlanır. Bilgi güvenliği yönetim sisteminin kurulumu da PUKÖ modelinin ilk adımı olan planla ile gerçekleşmektedir.

Bilgi güvenliği yönetim sisteminin sağlıklı işleyebilmesi ve yararlı çıktılar elde edebilmesi için kurulumu üst yönetimin desteklemesi ve Bilgi güvenliği yönetim sisteminin gerekliliğine inanması gerekmektedir. Üst yönetim, kurumun bilgi güvenliği hedeflerini ortaya koyan, kurumda bilgi güvenliğine yön veren bir bilgi güvenliği politikası oluşturmalıdır.

Üst yönetim desteği alınarak bilgi güvenliği ekibi kurulmalıdır. Bu ekip Bilgi güvenliği yönetim sisteminin kurulması, uygulanması ve yönetilmesi çalışmalarını takip etmek ile görevlendirilmelidir. Bu ekibe her birimden temsilciler seçilerek katılım sağlanır ise BGYS'yi kurumun tamamının sahiplenmesi ve BGYS ile kurumun tamamındaki güvenlik ihtiyaçlarının giderilmesi sağlanır.

Bilgi güvenliği yönetim sisteminin kurulum aşamasında ilk yapılması gereken işlerden biri de kapsamın belirlenmesidir. Kapsam ile kurumun Bilgi Güvenliği Yönetim Sisteminin neleri içine alacağı, kurumun hangi birimlerini ve yerleşkelerini kapsayacağı belirlenmektedir. Bu aşamada en önemlisi yönetilebilir bir kapsam belirlenmesidir. Kapsam kurulum aşamasından sonra da ihtiyaca göre değiştirilebilmektedir.

BGYS ekibinin kurulması ve kapsamın belirlenmesi ile birlikte kurumun BGYS yol planı oluşturulmalı ve kurum için değerli olan ve güvenliğinin sağlanması gereken varlıkların envanteri çıkarılmalıdır.

Bilgi güvenliği yönetim sistemi, kurumun belirlenen kapsamına uygun olacak şekilde dokümante ve kayıt altında tutulmalıdır. Politika ve prosedürler hazırlanmalıdır.

Bilgi güvenliği yönetim sisteminin kurulumu ve uygulanması aşamalarında kurum için risk oluşturabilecek veya oluşturan durumlar belirlenmeli ve bu risklerin kontrolünü sağlamak, planlamak, riski işlemek ve riski değerlendirmek için sistematik bir risk değerlendirme yaklaşımı belirlenmelidir.

ISO 27001 standardının ekler kısmında yer alan kontrol maddelerinin hangisinin kapsam içinde veya dışında kalacağı, kapsam dışında kalanların kalma nedenlerinin neler olduğu, seçilen kontrol maddelerinin seçilme nedenleri uygulanabilirlik bildirgesinde yer alır. Bu kontrol maddelerinin yanına kendi uygulamak istediğimiz kontrol maddeleri varsa onlar da eklenebilmektedir.

Üst yönetim, değişen ve gelişen teknoloji etkisi ile de Bilgi Güvenliği Yönetim Sistemi'nin sürekli uygunluğunu, doğruluğunu ve etkinliğini temin etmek amacıyla planlı aralıklarla gözden geçirme toplantıları yapmalıdır.

Akreditasyon sağlayan bir firma, kurumun talebi üzerine kurumun bilgi güvenliği yönetim sisteminin uygunluğunun denetimini yapar. Denetimde eğer eksiklikler belirlenirse sonrasında bu eksiklikler tamamlanarak belgelendirme işlemi yetkili firma tarafından

gerçekleştirilir. Akreditasyon kuruluşu ve belgelendirme kuruluşunun damgası ile onaylanan sertifika ile kurumun BGYS güvenilirliği tasdiklenmektedir.

Kurum personeline, bilgi güvenliği politikalarının ve amaçlarının benimsetilmesi gerekmektedir böylece personelin güvenlik açığı oluşturabilecek çalışma alışkanlıklarından vazgeçmesi sağlanacaktır. Bilgi güvenliği yönetim sisteminin kurumun kültürüne nüfus etmesini sağlamak için personele yönelik 27001 bilinçlendirme eğitimleri düzenlenmeli ve farkındalıklar arttırılmalıdır.

2.5.4. Bilgi güvenliğine yönelik tehditler

Bilişim teknolojilerindeki gelişmeler ve bu teknolojilerin kullanımı ile veriler ve insanlar arasındaki bağlantılar internet çatısı altında birleşmiştir. Bu birleşme doğru bilgiye daha hızlı ulaşma, iş ve zaman verimliliği gibi pek çok kazanımı bizlere sunsa da elektronik ortamlarda saklanan bilgi kaynaklarının güvenliğine ve sunulan hizmetlere yönelik tehditleri de beraberinde getirmekte ve bilginin güvenliğinin sağlanması zorlaşmaktadır.

Bilgi güvenliği alanında meydana gelen güvenlik ihlallerinin büyük bir kısmı sistem ve ağdan uygulamalara ve hatta veri tabanlarına kaymaktadır. Ağ ve sistemlerin güvenliğinin önemi kurumlar tarafından kabul edilmiş ve güvenliği sağlamak için gerekler yerine getirilmektedir bu farkındalığı uygulama ve veri tabanı güvenliği için de sağlamak bilgi güvenliği için kritik bir öneme sahiptir.

Bilgi güvenliği ile ilgili güncel tehditler sınıflandırıldığında [23];

- Doğal afetler veya teknik arızalardan kaynaklanabilir. Örneğin deprem, sel, hortum, yangın gibi çevresel ve sıcaklık, rutubet, gürültü gibi fiziksel tehditler, yedekleme medyalarında bozulma meydana gelmesi, kaza veya arızalardan oluşabilecek hasarlar, kablo hasarları, ekipmanın zarar görmesi, donanım arızası, destek servislerinin kesintisi sayılabilir.
- Prosedürel eksikliklerden kaynaklanabilir. Örneğin disipline edilmemiş eylemler veya tehdidin fark edilememesi, iş sürekliliğinde meydana gelen plan zayıflıkları, prosedürel ve yönetimsel eksiklikler, güvenlik politikası içerisinde meydana gelen hatalar, operasyonel zorluklar, tedarik zincirinde eksiklik, yasal düzenlemelerdeki sorunlar, yetersiz anlaşmalar sayılabilir.

- İnsan faktöründen kaynaklanabilir. Örneğin log dosyalarının yanlışlıkla ya da kasten değiştirilmesi, gizli kanallardan bilgi sızdırılması, çalışanın bilgi güvenliği farkındalığında zayıflık, arıza/kaza bildirimlerinde çalışanlarda farkındalık eksikliği, çalışanın güvenlik ihlalleri, şifreleme anahtarlarının ele geçirilmesi, fiziksel müdahale, inkâr, hatalı bilgi giriş/çıkışı sayılabilir.
- Kötücül ve lisanssız yazılımlarla ilgili tehditler olabilir. Örneğin kötü niyetli yazılımlar (virüs, trojan, worm vb.), yanlış ve yeniden yönlendirilen mesajlar, uygun olmayan kimlik tanıma mekanizması, yetkisiz yazılım kurma, yetkisiz bilgisayar erişimi, bilgiye yetkisiz erişim sayılabilir.

2.5.5. Bilgi sistemlerinde güvenlik

Bilgi güvenliği yönetim sistemi birçok konuyu kapsamaktadır. Bilgi sistemleri teknik olan ve bilgi işlem personelinin alanına giren konulardır. Bu konudaki kontrol tedbirlerinin ve müdahale planlarının önceden belirlenmesi gerekir [4].

Yazılım Güvenliği

Yazılım güvenliği, öncelikle mevzuatlara uyumlu olmalıdır. Kullanılan yazılımların lisanslı olması gerekir. Kurum içinde ihtiyaç olan yazılımların yetkili kişiler tarafından kurulması ve güncellenmesi gerekir. Yazılım geliştirme ve satın alma konuları da teknik personel tarafından yapılmalıdır.

Ağ Güvenliği

Kullanılan ağ sistemlerinin teknik personel tarafından kurulmasını ve bakımlarının yapılmasını gerektirir. Kablosuz iletişimle ilgili şifrelemeler yapılmalıdır. Avrupa ağ ve bilgi güvenliği ajansının (ENISA) raporuna göre cep telefonundan internete bağlanılmasıyla ilgili yaşanan güvenlik olaylarından 300.000 kişinin etkilendiği ve kısa sürede tükenen güç kaynaklarından dolayı uzun kesintilerde haberleşmenin aksadığı durumlarının yaşanabildiği belirtilmiştir [4].

Donanım Güvenliği

Yetkili personelin dışında kimse kuruma bilgi giriş çıkışı yapamamalıdır. Kullanılan yazıcılarda kimlerin ne kadar, hangi seviyede bilgiyi dışa aktarabileceği sınırlandırılmalı ve raporlanabilmelidir. Taşınabilir veri depolama ortamları yetkili personel dışında

kullanılmamalıdır. Kullanılan cihazların bakım ve onarım faaliyetleri yetkili kişiler tarafından yapılmalıdır.

İnternet Güvenliği

Gizlilik ilkesini ön plana çıkartan bir kurumda internet bağlantısı yasaklanabilir fakat zor olan kurum dış dünyaya açıkken güvende kalabilmektir. İnternet kullanımında öncelikle mevzuata uyum çok önemlidir. Yasaklı siteler ve uygulamaların kullanımı, kurumlarda sistem yöneticisi tarafından yasaklanmalıdır. Geriye dönük internet log kayıtlarının tutulması gereklidir. Kurumun sanal ortamda sahip olduğu Web sitesi ve eposta hizmetleri gibi hizmetleri de BGYS kapsamında işletilmeli ve bilgi güvenliği gerekleri yerine getirilmelidir.

Kullanıcı Hesabı Güvenliği

Çalışanların kullandıkları kurum bilgisayarlarını, bir kullanıcı hesabı ile çalıştırmaları gereklidir. Bu sayede birçok hareketin raporlanması sağlanır. Kullanıcı yetkileri politikalarla belirlenmelidir. Hesaplar güçlü şifrelerle korunmalıdır. Görev değişikliklerinde personele kullanıcı hesabı bilgileri imza ile verilmeli ve alınmalıdır.

Şifreleme Güvenliği

Günlük hayattaki en basit bilgilerimizin yer aldığı ortamlarda bile şifreleme sistemi kullanmaktayız. Kurum içinde de şifreleme sistemi ihtiyacı bulunmaktadır. Kurum erişiminde kullanılan şifreleme işlemleri belirli sürelerde sistem tarafından şifre yenilemeyi zorunlu hale getirmelidir. Kurum şifre politikası kullanıcılara duyurulmalı ve kullanıcılarda farkındalık oluşturarak şifre güvenliği sağlanmalıdır. Keylog (klavye tuş takibi) programlarına karşı alınabilecek tedbirler anlatılmalıdır.

2.5.6. Bilgi güvenliği yönetim sisteminin faydaları

Kurumlarda bilgi güvenliği yönetim sisteminin sağladığı çok sayıda ve önemli yarar vardır. Bu faydalardan başlıcaları aşağıda belirtilmektedir:

- Kurum hangi bilgi varlıklarının olduğunu belirler ve değerinin farkına varır. Bilgi güvenliğine yönelik tehditler başlığı altında bahsi geçen her bir madde için

varlıklarını, koruma metotları, kuracağı kontroller ile bir süreç içerisinde koruyarak bilgiyi güvende tutar.

- İş sürekliliğini sağlar, bir tehlike karşısında işe devam etme yeterliliği oluşturulur. Uzun yıllar işini garanti eder.
- Performans sürekli izlendiğinden sistemin gelişimi ve yenilikleri takibi daha hızlı olur, kurum güvenlik açısından da gelişen teknolojinin gerisinde kalmaz.
- Kurum, güvenlik standartlarına, düzenlemelere, yasa ve yönetmeliklere uyum sağladığını bağımsız bir şekilde gösterir. Yüksek prestij getirir. Güven sağlar.
- Personel, tedarikçi ve üst yöneticilerin bilgi güvenliği konusunda farkındalıklarının artırılması sağlanarak kurum genelinde bilgilerin doğru ve güvenilir bir biçimde saklanması sağlanır.
- Bilgi kaynaklarına olan erişimlerin denetim altında olması sağlanır.
- Bilgi güvenliliğinin ana unsurları gizlilik, bütünlük ve erişilebilirliğin temeline dayanan bir bakış açısının geliştirilmesi sağlanır.

3. VERİ TABANI YÖNETİM SİSTEMİ VE GÜVENLİĞİ

Veri tabanı yönetim sistemleri, kurumların veya kişilerin kritik bilgilerinin tutulduğu hassas yazılımlardır. Bu sistemler, çok kullanıcılı ortamlarda aynı veriye aynı anda birçok kullanıcının güvenilir bir şekilde ulaşabilmesi ile görevlidir. Gelişen teknolojiyle birlikte hızla sayısı artan bilişim projelerinin de neredeyse hepsinde bir veri tabanı yönetim sistemi kullanılmaktadır. Bu sistemler için alınan güvenlik önlemleri bazen yetersiz kalmakta ve veri ihlalleri yaşanmaktadır. Bu bölümde, veri tabanı yönetim sistemleri ve güvenliği ile doğrudan veya dolaylı etkileşen tüm bileşenler açıklanmıştır.

3.1. Veri Tabanı

Veri tabanı kelimesi, çözüme erişmek için işlenebilir duruma getirilmiş bilgi ortamı olarak tanımlanmaktadır. Bilişim sistemlerinde ise, belirli bir konu ile ilgili, yönetilebilir, güncellenebilir, taşınabilir veri kümelerinin bir arada bulunduğu ve dijital ortamda saklandığı yapılardır.

Veri tabanı, ilk bilgisayarın buluşu ile hayatımızda yerini almak üzere şekillenmeye başlamıştır. Büyük miktardaki verileri saklayabilmek için klasik dosya sistemleri kullanılsa da veri tekrarı, veri sorgulaması, veri erişilebilirliği, veri güvenliği gibi bir çok işin kontrol altına alınabilmesi için veri tabanı sistemi geliştirilmeye başlanmıştır.

Veri tabanı, hayatın her alanında pek çok kullanıcı tarafından geniş bir kullanım alanına sahiptir. Bir marketteki ürünlerin stok durumu, kar zarar analizi, sözlükler, hastaneler, öğrenci yönetim sistemi, bankacılık sistemi, internet ortamında yer alan bütün bilgiler veri tabanlarında tutulmaktadır. Bu verilerin çeşitli ihtiyaçlar doğrultusunda işlenmesi için gerekli yapıları sağlayan sisteme, veri tabanı yönetim sistemleri denmektedir.

3.2. Veri Tabanı Yönetim Sistemleri

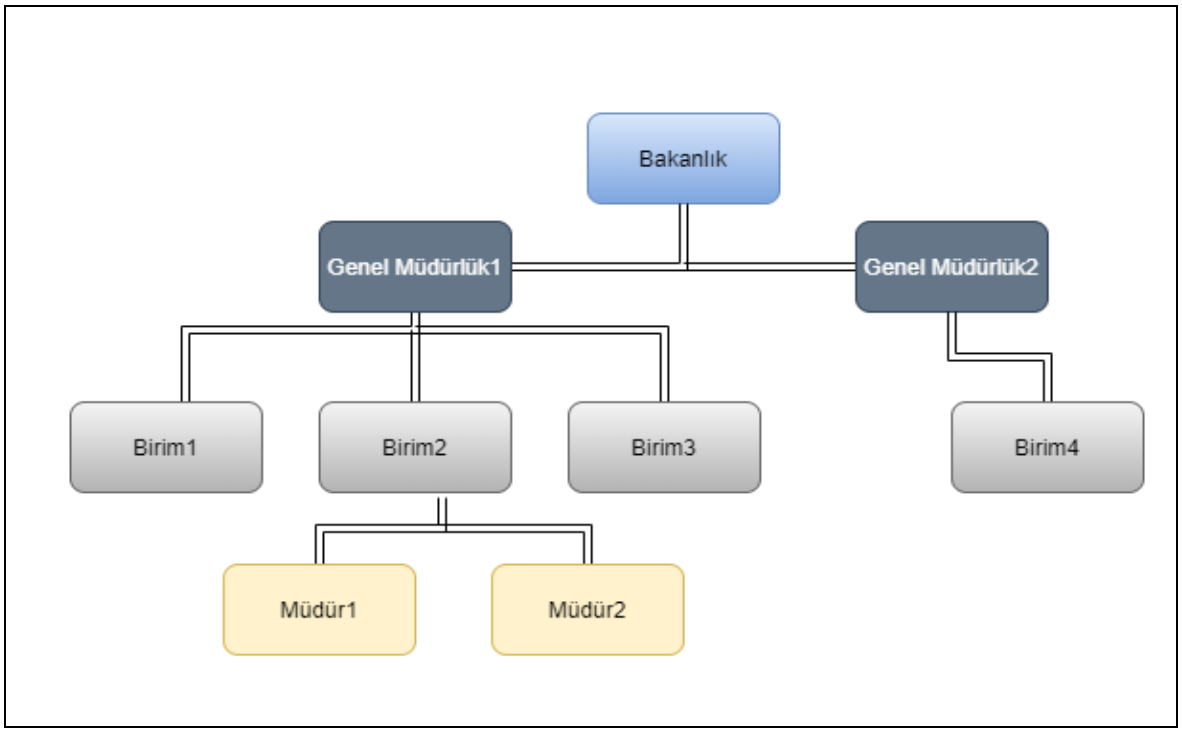
Veri tabanı yönetim sistemleri, kurum ve kişilerin hassas verilerini düzenli bir şekilde saklayan, veri tabanına erişim izni olan kişilerin yetkilerini düzenleyen, verilerin gizliliğini, bütünlüğünü sağlayan yani veri tabanı yönetimini sağlayan sistemlerdir. Oluşturulan bir veri tabanını düzenlemek, bakımını yapmak, geliştirmekle beraber bir veri tabanını oluşturmakta için de veri tabanı yönetim sistemleri kullanılır.

Günümüzde gerek web tabanlı, mobil tabanlı yazılımların sayısındaki hızlı artış gerekse kuruluşların kendi bünyesinde sakladıkları veriler veri tabanı yönetim sistemlerinin popüler olarak kullanılmasını sağlamıştır. Kullanıcıların isteklerine göre geliştirilmiş bir çok veri tabanı yönetim sistemi vardır. Bunlardan en yaygın kullanılanları; Oracle, Microsoft SQL Server, MySql ve PostgreSQL gibi yazılımlardır. Yaygın kullanılan bu sistemlerin ortak noktası ilişkisel veri tabanı yapısına sahip olmasıdır.

Her bir veri tabanı yönetim sistemi veriyi mantıksal düzeyde düzenleyebilmek için bir veri modeli kullanır. En yaygın kullanılan 4 farklı veri modeli vardır bunlar basit ve gelişmiş olarak ikiye ayrılmaktadır. İlişkisel ve nesneye yönelik veri modelleri gelişmiş, hiyerarşik ve ağ tabanlı veri modelleri de basit veri tabanı modelleridir.

3.2.1. Hiyerarşik veri tabanı modeli

Hiyerarşik veri modeli en eski veri modeli olmakla birlikte günümüzde pek kullanım alanı kalmamıştır. Hiyerarşik modelde kökte bir amaç en üstte ana başlık olarak bulunmakta, bu bilgiye bağlı alt bilgilerde alt başlıklar şeklinde yer alarak bire çok ağaç yapısı kullanılmaktadır. En üstte oluşan kayda bağlı olarak bilgiler alt dallara doğru ilerlemektedir, böylece her bir alt kaydın bağlı olduğu bir üst kayıt muhakkak vardır.

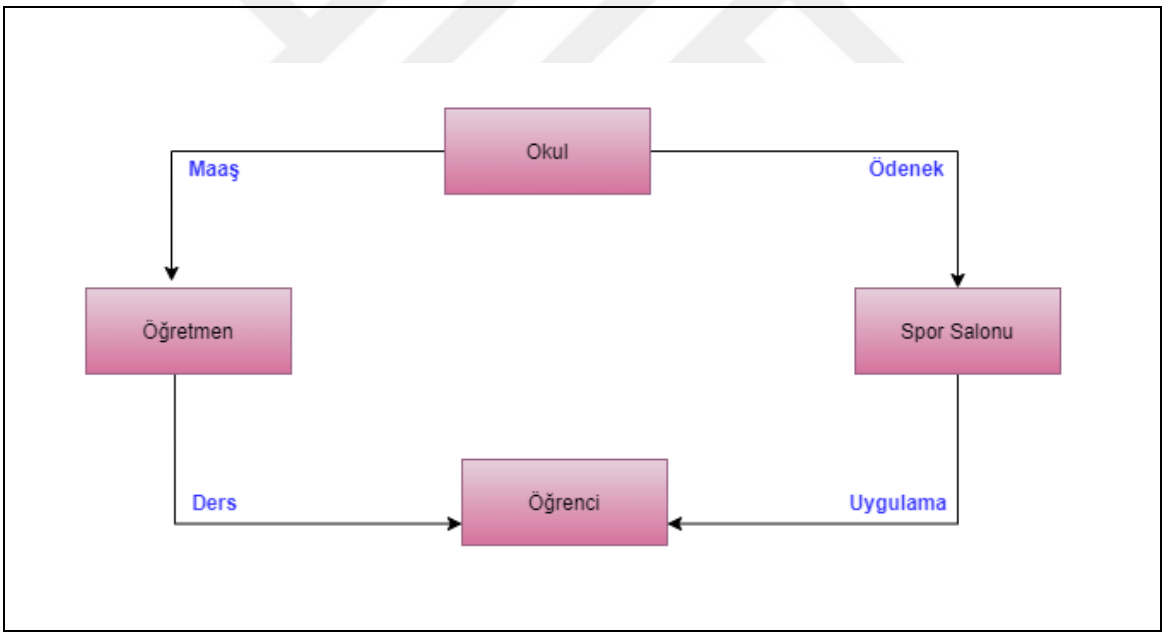


Şekil 3.1. Örnek hiyerarşik veri tabanı modeli

Hiyerarşik veri tabanı modeline Şekil 3.1'de örnek olarak verilen yapıda bakanlık kök, genel müdürlükler ağacın dallarıdır. Bir bakanlığa birden çok genel müdürlük bağlı olabilir bu genel müdürlüklerin her biri o bakanlığa bağlıdır. Her genel müdürlükte birçok birim olabilir bu birimlerin her biri o genel müdürlüğe bağlıdır. Her birimde birçok çalışan olabilir fakat her çalışan bir birime bağlıdır. Hiyerarşik veri modelinde, verilere ulaşmak için kökteki amaçtan başlanarak alt dallara doğru ilerlenmelidir.

3.2.2. Ağ tabanlı veri tabanı modeli

Basit veri modellerinden olan ağ tabanlı veri tabanı modeli hiyerarşik modelin istekleri karşılamaması sonucunda ona alternatif olarak geliştirilmiştir. Grafik ve tablo temeline dayanan bu veri modelinde, veri tipleri tablolar ile kayıtlar arasındaki ilişki ise grafik okları ile gösterilmektedir.



Şekil 3.2. Örnek ağ tabanlı veri tabanı modeli

Şekil 3.2'de gösterilen ağ veri tabanı modeli yapısal olarak hiyerarşik modele benzemektedir. Hiyerarşik modele ek olarak ağ modelinde bir öğe, farklı bir öğe ile ilişkilendirilebilir, bağlantı açısından herhangi bir kısıtlama yoktur.

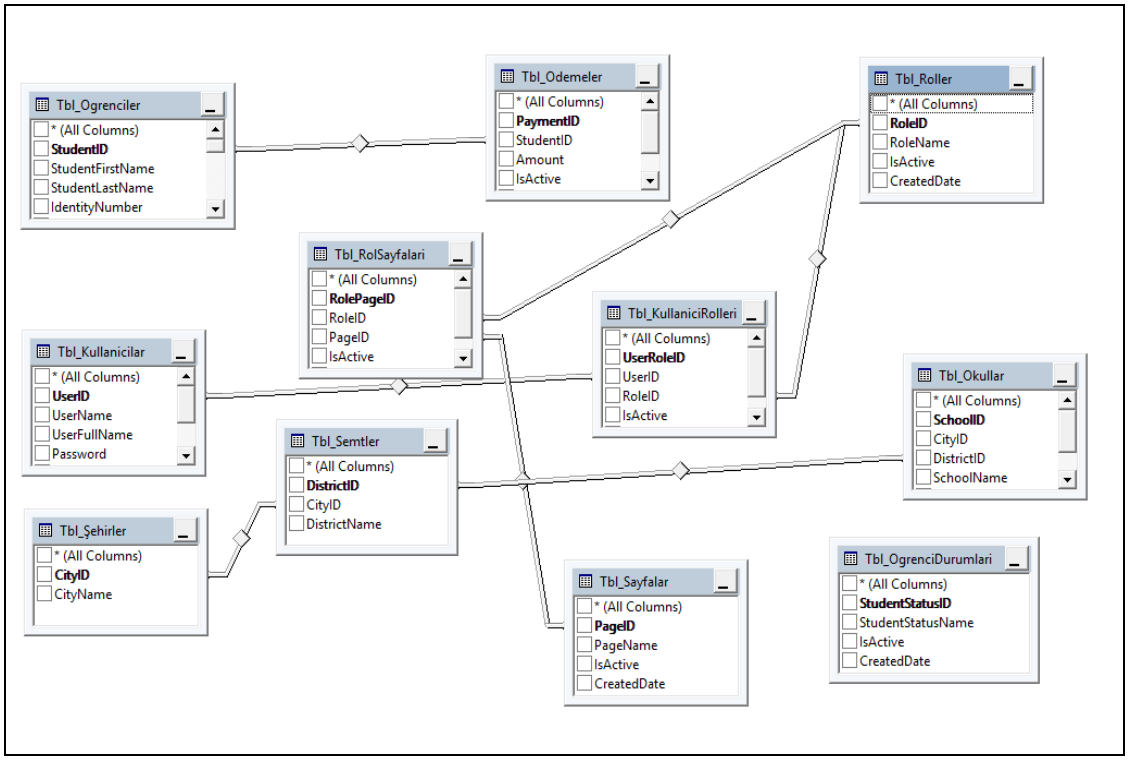
3.2.3. Nesne yönelimli veri tabanı modeli

Nesne tabanlı veri modellerinde veriler nesne olarak modellenir ve alt özellikleri yapılandırılır böylece nesneye yönelik bir programlama dilinde oluşturulan nesneler veri tabanında da nesne olarak karşılığını bulur. Arama işlemlerinde nesne yönelimli veri tabanı modeli diğer veri tabanı modellerine oranla çok daha hızlıdır. Bir diğer avantajı da karmaşık yapıdaki büyük veri tabanlarının tasarımını kolaylaştırmasıdır.

3.2.4. İlişkisel veri tabanı modeli

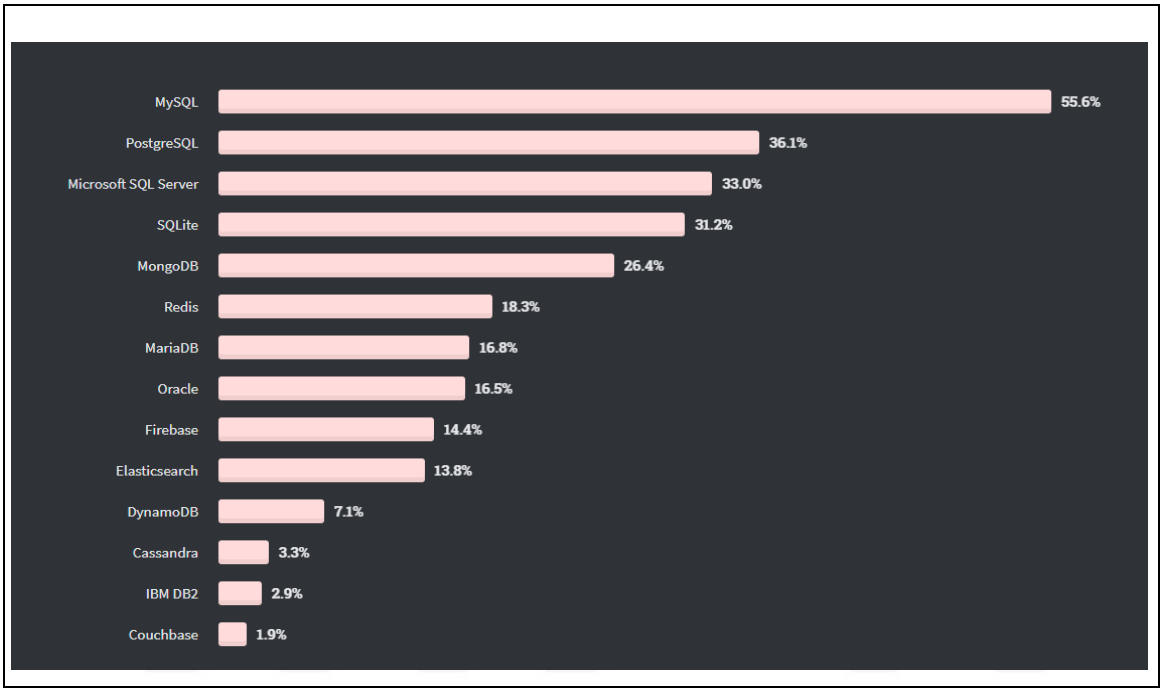
İlişkisel veri tabanı modeli, belirli bir kapsamda oluşturulmuş tabloların saklanması ve bu tablolar arasında ilişki kurulmasını, birden fazla kullanıcının aynı anda veriye ulaşabilmesini, verinin tutarlılığının korunmasını, verinin bütünlük içerisinde tutulmasını sağlayan yapılardır. Veri tabanı yönetim sistemlerinin önemli bir bölümünün temelini ilişkisel veri modeli oluşturmaktadır.

İlişkisel veri modelinde veriler tablolarda tutulmaktadır, tabloların sütunları tutulan verinin niteliğini göstermekte, satırları da verilerin kendisini tutmaktadır. Tablodaki belirli bir satırı diğer tüm satırlardan ayırt etmek için kullanılan anahtarlar ile birden çok tablo verileri birbiri ile bağlantı kurabilir ve sorgulama işlemler daha hızlı sonuçlanır.



Şekil 3.3. Örnek ilişkisel veri tabanı modeli [24]

Şekil 3.3'te gösterilen veri tabanı modelleri, tabloları birbiriyle ilişkilendirip aynı verilerin tekrarını önlemesi, veri tutarlılığı ve veri bütünlüğü sağlama konularında sunduğu avantajlardan dolayı günümüzde en çok kullanılan Oracle, MySql gibi veri tabanı sistemlerinin çoğunun mimarisini oluşturmaktadır.



Şekil 3.4. 2020 yılında veri tabanı kullanım oranları [25]

Şekil 3.4 'te StackOverFlow'un büyük katılım ile gerçekleştirdiği anket sonucuna göre oluşturduğu 2020 yılının en popüler veri tabanlarında ilk 3 sırada ilişkisel veri tabanları yer almaktadır.

Oracle veri tabanı

Oracle şirketi tarafından geliştirilmiş ilişkisel bir veri tabanı yönetim sistemidir. Büyük miktardaki veriyi birden fazla kullanıcının erişimine sunar bu sırada verinin bütünlüğü bozulmadan hizmetini vererek verinin güvenliğini de sağlar. Bütünlüğü veri tabanı düzeyinde sağladığı için daha az kod yazılarak da bütünlük sağlanmış olur. Veri depolama alanlarını ayarlama fırsatı verir. Birçok işlemci üzerinde çalışabilmekte, istemci sunucu mimarisinin tüm avantajlarını sisteminde kullanabilmektedir.

Oracle veri tabanı yönetim sistemleri yine Oracle tarafından geliştirilmiş PL/SQL açılımı ile Procedural Language/Structured Query Language dilini kullanmaktadır. PL/SQL

oracle veri tabanı sistemleri üzerinde kullanılmak için geliştirilmiş özel bir dildir. PL/SQL prosedürel bir dildir blok yapısına, if else, for, while gibi kontrol mekanizmalarına izin vermektedir bu özellik SQL dillerinde bulunmamaktadır. PL/SQL yapısal dillere ait, tetikleyici, prosedür gibi fonksiyonları ayrıca programlama üzerindeki akış kontrolleri ve değişkenleri oluşturma özelliklerinin SQL'e eklenmesiyle ortaya çıkmış bir dildir.

Oracle 12c sürümü ile dünyanın bulut ortamı için tasarlanmış ilk veri tabanını geliştirmiştir. Oracle sonraki sürümleriyle de kullanıcıların depolanabilir bulut teknolojisinde; veri tabanı servislerini birleştirme, standartlaştırma işlemlerini kolaylaştırmaya devam etmektedir.

Microsoft SQL server veri tabanı

İlişkisel yönetim veri tabanı sistemlerinden biri olan Microsoft SQL Server, Microsoft firması tarafından geliştirilmiştir. Microsoft SQL Server ile veri işleme, depolama, indeksleme, analiz etme gibi çeşitli işlemlerin hepsi yapılabilir. Microsoft SQL Server veri tabanı yönetim sistemi sunucu olarak çalışabilir diğer uygulamalar ya da kullanıcıların sisteme bağlanarak veri manipülasyonlarını yapmasını sağlar. Microsoft, Microsoft SQL Server'da, pek çok senaryoyu konu alan farklı yetenek setlerine sahip bir çok farklı sürüm geliştirmiştir.

SQL Server'ın veri sorgulama dili veri tabanı mantığının ana dili olarak da nitelendirilebilecek Transact Structured Query Language kısaltılmış hali ile TSQL 'dir. Microsoft kendi platformu için SQL dilinin üzerine çeşitli iyileştirmeler ve eklemeler yaparak TSQL dilini geliştirmiştir. Yapısal sorgu dillerinden olan TSQL veri işleme, değişken kullanma, döngü, fonksiyon, prosedür oluşturma, hata ayıklama gibi bir çok işlemi gerçekleştirmeye izin vermektedir.

SQL server Windows tabanlı sunucular ve programlama dillerinde en yaygın kullanılan veri tabanı yönetim sistemlerindendir, windows'un yanı sıra Linux işletim sistemini de desteklemektedir.

MySQL veri tabanı

Güçlü bir veri tabanı yönetim sistemi olan MySQL de ilişkisel veri tabanı yönetim sistemidir. Asp, php gibi web tabanlı uygulamalarda çok yaygın kullanılan MySQL veri

tabanı, birçok işletim sistemine de uyumlu olmakla beraber Linux işletim sisteminde daha hızlı performans göstermektedir.

MySQL çifte lisansa sahip bir veri tabanıdır yani hem ücretsiz kullanım imkanı sunarken hem de ticari lisans kullanmak isteyenler için ücretli versiyonu mevcuttur. Açık kaynak kodlu bir yazılım olduğu için MySql veri tabanı geliştirilmeye ve değişikliğe açıktır. MySql veri tabanı, tabloların kontrolü ve optimizasyonunu hızlı ve sağlam bir şekilde yapan çoklu iş parçacıklı, çok kullanıcılı bir veri tabanıdır.

PostgreSQL veri tabanı

PostgreSql, California Üniversitesinde temelleri atılan, açık kaynak kodlu olup aktif bir şekilde gelişimi devam eden nesne tabanlı ilişkisel bir veri tabanıdır. Verileri hızlı ve güvenli bir şekilde tutup, yüksek erişilebilirlik ve yüksek güvenilirliğe sahip olduğu dünyada kabul görmüş bir sistemdir.

PostgreSQL, SQL dilini geliştirerek kullanmakta ve çok gelişmiş bir sorgu planlayıcısına da sahip durumdadır. Linux, Unix ve NT çekirdeğine sahip tüm Windows sistemlerinde çalışabilmekte, tüm modern programlama dillerini de desteklemekte olup dünyada yaygın bir kullanım alanına ulaşmıştır.

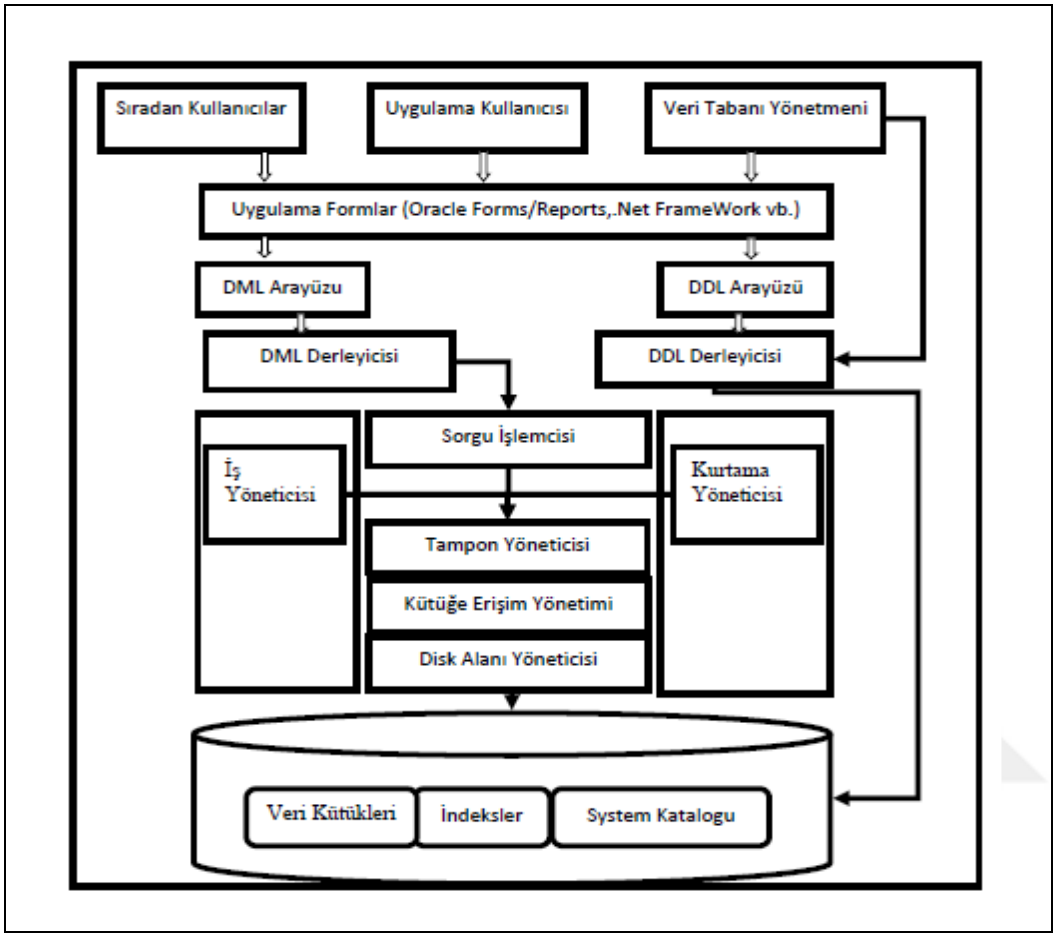
Tüm PostgreSQL işlemleri ACID yani atomicity(Atomiklik), consisency(Tutarlılık), Isolation(İzolasyon), Durability(Dayanıklılık) uyumludur. PostgreSql nesne yönelimli bir veri tabanı olduğundan, veri tabanlarında farklı ve yeni olasılıkların ortaya çıkmasını sağlayan kalıtım özelliğini kullanmaktadır.

3.3.Veri Tabanı Yönetim Sistemi Bileşenleri

Her bir veri tabanı yönetim sisteminin sahip olduğu veri tabanı bileşenleri vardır. Uygulamada yönetim sistemlerine göre bileşenler farklılık gösterse de teoride ve temelde ortak noktaları hayli fazladır.

Birbiriyle ilişkisi olan veriler veri tabanında mantıksal ve fiziksel katmanlarda tutulur. Fiziksel katman işletim sistemi üzerinden görüntülenmektedir. Mantıksal katman ise tutulacak verinin yapısını ve ilişkilerini tanımlayan, tablo, görüntü, indeks, prosedür, fonksiyon gibi tüm nesnelerdir. Mantıksal katmana veri tabanına bağlanıp SQL komutları

çalıştırılarak erişilebilmektedir. Şekil 3.5’ te veri tabanı yönetim sistemi yapısı özet olarak gösterilmiştir.



Şekil 3.5. Veri tabanı yönetim bileşenleri [26]

3.3.1. Veri tabanı yöneticisi

Veri tabanı yönetim sisteminin en önemli parçalarından biri kullanıcılardır. Kullanıcılar, şekil 3.5’ te de görüldüğü gibi 3 grupta ele alınır. Uygulama kullanıcıları bir programlama dili kullanarak daha az teknik bilgiye sahip olan sıradan yani son kullanıcının kullanacağı programı yazar.

Veri tabanı yöneticisi, veri tabanı yönetim sisteminde ki tüm verilere ulaşabilen, veri tabanının bütünlüğünü ve güvenliğini sağlayan, veri tabanının performansını artıran, güncelleme, yedekleme, kurtarma gibi veri tabanının devamlılığını sağlayacak işlemleri yapan teknik bilgiye sahip kullanıcılardır. Ayrıca veri tabanı yöneticileri, veri tabanına

bağlanacak kullanıcıları oluşturarak kullanıcılara veri tabanı üzerinde yetkiler ve roller tanımlayabilir.

3.3.2. Yapılandırma dosyaları

Yapılandırma dosyalarında veri tabanının fiziksel yapısı, adı, oluşturulma tarihi gibi bilgiler yer almaktadır. Veri tabanı sistemlerinin nasıl çalıştığını belirleyen bu dosyalar parola güvenlik ayarları, kimlik doğrulama ayarları, veri tabanı yönetici grup ayarları, veri tabanındaki şifreleme mekanizması gibi birçok kritik noktada kullanılmaktadır. Bu nedenle yapılandırma dosyalarının güvenliğini sağlamak için kontroller yapılmalı ve güvenlik ihlali oluşması önlenmelidir.

Bu dosyaların olduğu dizine erişim kontrolleri çok sıkı takip edilmeli veri tabanı yöneticisi dışındaki kullanıcıların bu dizine müdahale etme yetkisi olmamalıdır çünkü bu dizinde yapılacak kötü niyetli müdahaleler veri tabanı bütünlüğünü etkileyebilecek seviyededir.

3.3.3. Veri dosyaları

Tüm veri tabanı verilerini içeren, işletim sistemi üzerinde disklerde bulunan dosyalardır. Mantıksal katmandaki tablo, indeks verileri fiziksel katmanda veri dosyalarındadır. Veri dosyalarının biçimi üzerindeki veri tabanı sistemlerine göre özeldir örneğin oracle veri dosyası içerisindeki verileri oracle programı dışındaki hiçbir programla anlaşılamayacak formatta tutulur.

Genellikle veri dosyaları içinde bulunan veri sözlüklerinin ele geçirilmemesi için veri dosyalarının güvenliğinin sağlanması gerekir eğer veri sözlüğü ele geçirilirse veri tabanı kontrollerinin bir işlevi kalmaz.

3.3.4. İstemci, ağ kütüphanesi

Veri tabanı yönetim sistemi önemli bileşenlerinden olan istemci, genellikle veri tabanından farklı bir yerden, üzerinde bulunan kütüphaneler veya sürücüler sayesinde veri tabanı bağlantısını gerçekleştirir.

İstemci ile ağ üzerinden veri tabanı bağlantısının sağlanması için de veri tabanında ağ sürücüsü bulunması gerekir. Ağ servisleri de kullanılarak istemci ve veri tabanı arasında bağlantı kurulup veri alışverişi gerçekleşir.

İstemci ve ağ sürücüleri kötü niyetli kişiler tarafından veri tabanlarına zarar vermek için hedef görülmektedir. Genellikle istemci, veri tabanından farklı bir bilgisayar üzerinde çalıştığından denetimi ve erişim kontrolleri daha zor yönetilmektedir bunu bilen saldırganlar tarafından istemci sürücülerinin değiştirilmesi veya zararlı programlar bulaştırılması ile veri tabanının güvenliğini bozulur.

3.3.5. Yedekleme ve geri dönüş

Veri tabanı yönetim sistemleri her ne kadar veri güvenliğini sağlamayı hedeflese de sistem veya donanım ile ilgili yaşanılacak olaylar veya kullanıcı hataları sonucunda veriler zarar görebilir. Bu tarz durumlarda bozulan bilgilerin veya ulaşılamayan veri tabanlarının düzeltilebilmesi için veri tabanı yedeklerine ihtiyaç duyulmaktadır.

Veri tabanı yönetim sistemlerinde yedek alma ile ilgili değişik yöntemler mevcuttur veri tabanının durumuna göre bu yöntemlerden hangisinin kullanılacağı, yedeği kimin alacağı, ne sıklıkla yedek alınacağı, alınan yedeğin büyüklüğü, veri tabanında ne kadarlık kaybın tolere edilebileceği konularını değerlendirerek uygun bir yedekleme stratejisine veri tabanı yöneticisi karar vermelidir.

Yedekleme türüne karar vermek için veri tabanı yöneticisi ihtiyaçlarını doğru belirlemelidir. Yaygın olarak veri tabanlarında tam, fark ve artırımlı yedekleme türleri kullanılmaktadır bunlar arasında en güvenilir olanı tam yedeklemedir. Tam yedeklemede bütün veri olduğu gibi yedeklenir buda yedekleme süresinin uzun ve yedekleme alan kapasitesinin büyük olmasına sebep olduğundan hep tam yedek alınması yerine belirli periyotta tam yedek alınıp fark ve artırımlı yedekler ile tam yedek desteklenmektedir. Fark yedekleme, tam alınan son yedekten veya artırımlı yedekten sonra oluşan farkların yedeğini alır. Artırımlı yedeklemede en son yedekleme işleminden sonra verilere yapılan değişiklikleri içerir [27]. Fark ve artırımlı yedekleme sadece farkın yedeğini aldığı için tam yedeklemeye göre işlem süresi daha kısa, yedeğin kapladığı alanda daha küçüktür.

Kurumlarda iş sürekliliğinin sağlanabilmesi için veriye her daim erişim olması ve veri kaybına karşı önlem alabilmek için başarılı yedekleme işleminin yapılması ve yedeklenen verinin ihtiyaç anında geri yüklemesinin yapılması gerekmektedir. Tam yedek almak, yedek alınırken uzun sürse de yedekten geri dönüşte tam yedekten geri dönmek daha kısa sürede gerçekleşir bu nedenle sürekli fark yedekleri almak yerine belirli periyotlarla tam yedek

alınmalıdır. Ayrıca eğer en son alınan tam yedek bozulursa sonrasında alınan fark yedeklerin hiçbir önemi kalmaz çünkü veri tabanını en güncel haline getirebilmek için tam yedeğin üzerine tüm fark yedeklerinin yüklenmesi gerekir. Yedekler başarılı bir şekilde geri yüklenebilirse servislerin kalıcı olarak kesintiye uğraması veya verilerin geri dönülmez biçimde kaybolması engellenebilir.

3.3.6. Veri sözlüğü

Veri tabanlarının en önemli bileşenlerinden olan veri sözlüğü (data dictionary), veri tabanı hakkında genel bilgileri içeren salt okunur tablolar ve görünümlerin oluşturduğu bir sistem kataloğudur. Veri sözlüğü, veri tabanı oluşturulurken oluşur sonrasında veri tabanı yönetim sistemleri, veri tabanı üzerindeki değişikliklerden ilgisi olanları veri sözlüğüne otomatik kaydeder veya günceller. Veri sözlüğünde tutulan başlıca veriler şunlardır [28]:

- Veri tabanı üzerindeki tüm şema isim ve tanım bilgileri
- Veri tabanı şema nesnelerinin tanımları, nesnelere ayrılan alan ve nesnelerin bu alanın ne kadarını kullandığı
- Veri tabanı kullanıcı bilgileri ve kullanıcılara tanımlanan roller
- Veri tabloları üzerindeki bütünlük sınırlamaları
- Genel veri tabanı yapısı hakkındaki bilgiler

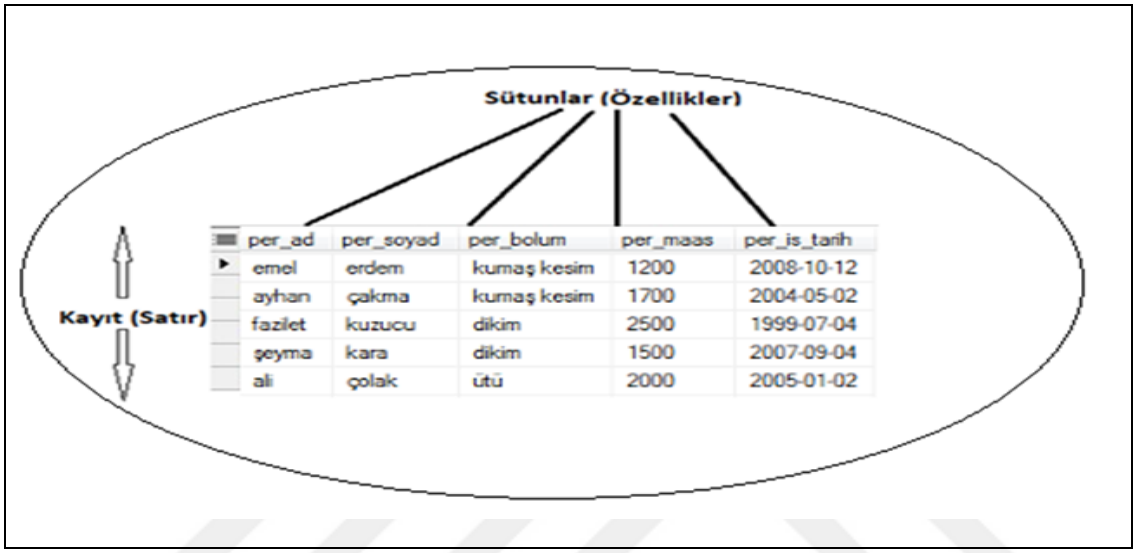
Veri tabanında bir tablo yaratıldığında bu tablonun kolon bilgileri, bu tabloya erişim yetkisi olan kullanıcı bilgileri, tablo üzerindeki kullanıcıların hakları ve daha fazlası veri sözlüğüne otomatik kaydolur. Bu bilgileri, veri tabanı kullanıcıları hangi tabloya erişim yetkisi olup olmadığını kontrol etmek için de kullanabileceği için veri sözlüğündeki kullanıcılara referans olabilecek bu bilgileri yetkili tüm veri tabanı kullanıcıları görüntüleyebilmektedir. Veri tabanı hakkındaki genel bilgilerin tutulduğu veri sözlüğü tablolarında yapılacak bir işlem veri tabanında geri alınamaz hasara neden olabilmektedir bu nedenle veri sözlüğünün bu tablolarını her kullanıcı görüntüleyememektedir.

3.3.7. Veri tabanı nesneleri

Veri tabanları tablo, görünüm, indeks, tetikleyici, fonksiyon gibi birçok öğeden oluşmaktadır. En sık kullanılan veri tabanı nesneleri özetlenmiştir:

Tablo

İlişkisel veri tabanı yönetim sistemlerinde depolamanın temel birimi tablolardır. Tablolar, verilerin satır ve sütunlar şeklinde gruplanmasıyla oluşur. Her bir sütun bir özelliği ifade etmektedir. Satır ise özelliklerin alabileceği değerler ile oluşan, tablodaki verilerin eksiksiz kaydını temsil eden kayıtlardır. Şekil 3.6'da bir veri tabanı tablo örneği gösterilmiştir.



Şekil 3.6. Veri tabanlarında tablo örneği

Şekil 3.6'da satır ve sütunlardan oluşan klasik bir tablo örneği gösterilmektedir. Bir tablodaki her sütun farklı isimlendirilir ve farklı veriler içerir. Her sütun için bir veri türü belirlenir. Tutulacak veriye göre veri türü farklılık gösterir örneğin ad sütunu metin veri türü ile maaş sütunu sayısal veri türü ile ilişkilendirilir. Her satıra, sütun için tanımlanmış olan veri türünde kayıtlar girilir.

Anahtarlar

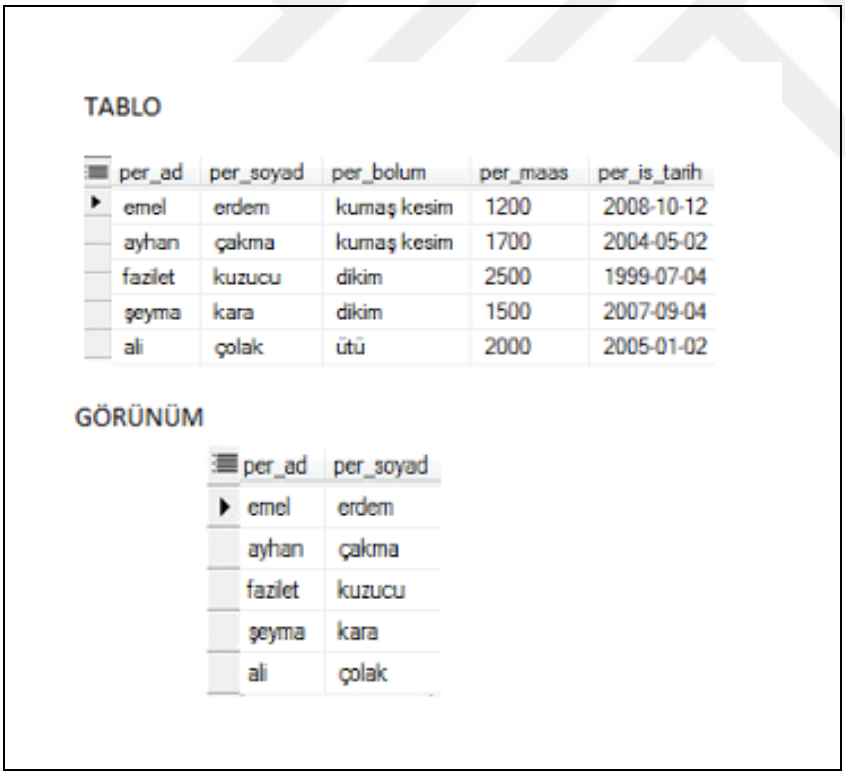
İlişkisel veri tabanı yönetim sistemlerinde anahtar olarak bir sütun veya birkaç tane sütun belirlenebilir. Bir tabloda aynı satırın birden fazla olmamasını, tabloda veri tekrarı yaşanmasının önüne geçilmesini birincil anahtar (primary key) sağlar. Birincil anahtar olan sütunda hiçbir satır boş geçilemez ve satırda tekrar eden değerler yer alamaz, benzersiz olmalıdır. İlişkisel veri tabanlarında mutlaka birincil anahtar olmalıdır. Birincil anahtar, veri tabanında kayıt silme, düzeltme, birleştirme gibi işlemlerde veri tabanı yöneticisine büyük kolaylık sağlamaktadır.

Yabancı anahtarlar (foreign key), birbiri arasında ilişki bulunan tablolar arasında referans görevi gören sütunlardır. Yabancı anahtarlar, referans edilen tabloların birincil anahtarlarıdır. Yabancı anahtarlarda birincil anahtarlar gibi boş değer içeremezler ama birbirleriyle aynı değeri içerebilir.

Tekil(benzersiz) anahtarlarsa (unique key) birincil anahtar ile aynı özellikleri taşır tek bir fark ile tekil anahtarlarda sütun boş değeri alabilir. Her birincil anahtar aynı zamanda benzersiz anahtardır fakat her benzersiz anahtar birincil anahtar değildir.

Görünüm

Görünüm (view), bir ya da birden fazla tablodan istenilen alanların hazırlanan sorgu ile alınması ile oluşan sanal tablolardır. Görünümler, tablolar gibi veri tabanında veri tutmadığından yer kaplamaz sadece bu görünümün tanımı yani SQL sorgusu veri sözlüğünde saklanmaktadır.



Şekil 3.7. Tablo ve görünüm ilişkisi

Şekil 3.7’ de görünüm ve tablo arasındaki ilişkisi örnek ile gösterilmiştir.

Görünümler kullanılarak:

- Bir tablonun güvenliğini sağlayarak, sadece ihtiyaç duyulan satır ve sütuna erişim imkanı sunulabilir yani verinin istenmeyen tarafına erişim görünüm kullanılarak sınırlanmış olur.
- Birden çok tablodan verilerin karmaşık sql sorguları ile join yapılmasının önüne geçilebilir.
- İstenilen veriye ulaşmada performans artırılabilir. Ama eğer bu avantaj dikkatli kullanılmaz, tek bir tablodan karşılanabilecek bir veri için ihtiyaçtan fazla tablonun birleşimi ile oluşan görünümden veri karşılanmaya çalışırsa bu sisteme gereksiz bir yük bindirebilir.

İndeks

İndeksler (indexs), tablolarda işaretçi gibi kullanılarak bir tablo üzerindeki bir kaydı aramada kullanılan nesnelerdir. Tablolarda çok sorgulanan alanlara indeks tanımlanması, bir sorgu çalıştığında tüm tablonun aranmasının önüne geçerek veriye daha az işlemle ulaşılmasını sağlar. Bir telefon rehberi örneğini düşünecek olursak bir isim arandığında, ikili arama algoritması kullanılarak aradığımız kayıt rehberin hangi bölümündeyse o kısımdan aramaya devam edilip kaydın bulunamayacağı yerler atlanarak veriye, tam tablonun aranarak bulunmasından çok daha hızlı ulaşılması sağlanır.

Belirli bir boyutun üzerinde olan tablolarda indeks çeşitlerinden en uygun olanı belirleyerek kullanmak arama performansını çok iyileştirmektedir. Ama tablo belirli bir boyutun altındaysa indeks kullanımı yerine tam tablo taraması daha hızlı sonuç verebilir. İndeks kullanılıp kullanılmamasının gerekliliğine, veri tabanında toplanan istatistik bilgilerine bakılarak karar verilebilir.

İndeksler, order by, group by gibi sıralama içeren select cümleleri kullanılırken de performans artışı sağlayacaktır. Eğer indeks oluşturulmamışsa select deyimi sıralamayı en baştan oluşturacak buda performans kaybına sebep olacaktır.

Tetikleyici

Tetikleyiciler (trigger), bir ilişkisel veri tabanında bir işlem yapıldıktan önce veya sonra ya da süreç içerisinde bir olaya bağlı olarak çalışan SQL kodlarıdır. Bir tabloda güncelleme,

silme, ekleme işlemlerinden biri gerçekleştiğinde işlemin gerçekleştiği tabloda veya başka tabloda otomatik çalışarak kodlanan işlemi gerçekleştiren prosedürel program parçacıkları olarak da kullanılır tetikleyiciler.

Tablo kısıtlamaları veya diğer nesnelerle yapılacak işlemleri tetikleyiciler ile yapmaya çalışırsak bu veri tabanında performans kaybına neden olur. Bu nedenle tetikleyicileri, herkes oluşturmamalıdır özellikle bir veri tabanının açılması, kapanması veya sunucu hata mesajlarıyla tetiklenen sistem tetikleyicileri uzman kişilerce oluşturulmalı ve büyük yapılarda veri tabanı yöneticilerinin kontrolünde oluşturulmalıdır.

Prosedürler ve fonksiyonlar

Prosedür ve fonksiyonlar, belirli işlemleri gerçekleştirmek için oluşturulmuş özel SQL cümle kümeleridir. Fonksiyon ve saklı yordamların yani prosedürlerin pek çok avantajı bulunmaktadır. Bunlar:

- Aynı veri tabanını kullanan farklı uygulamalar için ya da uygulamanın farklı modülleri için tekrar tekrar aynı kodları yazmak yerine prosedür ve fonksiyonlar ile bir kez yazılarak tek bir noktadan ulaşılması sağlanır.
- Fonksiyon veya prosedürlerde tanımlanan iş kurallarında bir değişiklik gerektiğinde her uygulamada değişiklik yapmak yerine sadece tek bir noktada değişiklik yapılır. Buda daha hızlı müdahale imkanı sağlar.
- Fonksiyon ve prosedürler veri tabanı yönetim sistemleri içinde hazırlandığı ve derlenmiş bir şekilde saklandığı için uygulamalara veya veri tabanı kullanıcılarına daha hızlı erişim imkanı vererek daha fazla performans elde edilmesini sağlar.

Sıra

Sıra, tablolardaki kayıtlara otomatik, azalan veya artan numara vermek için kullanılır. Hemen hemen tüm veri tabanı yönetim sistemlerinde tekil numara üretme mantığı olmakla birlikte farklı kullanım biçimlerine sahiptirler. SQL Server, MySQL gibi veri tabanı yönetim sistemlerinde otomatik artış özelliğine sahip kolonlar bu işi, tablo oluşturulurken ilgili kolonda identity, auto ıncrement ifadeleri ile otomatik yapmaktadır fakat oracle, postgresql gibi veri tabanı yönetim sistemlerinde tablolar oluşturulduktan sonra adı, artan veya azalan olacağı, artış veya azalış miktarı belirtilerek sequence yani sıralar oluşturulur.

Sıra numaraları tablolardan bağımsız oluşturulmaktadır yani bir sıra numarası farklı farklı tablolarda kullanılabilmektedir. Tüm tablolar oluşturulan tek sıraya bağlanarak veri tabanındaki tüm kayıtlar eşsizleştirilebilir fakat bu veri tabanında performans kaybına yol açmaktadır bu nedenle sıra oluşturulan veri tabanı yönetim sistemlerinde her tablo için yeni sıra oluşturulması önerilmektedir.

3.3.8. Yapısal sorgu dili (SQL)

SQL (Structured Query Language) yani yapısal sorgu dili, veri tabanı yönetim sistemlerinin çoğu, ilişkisel veri tabanı yönetim sistemlerinin tamamı tarafından desteklenen, veri tabanları ile bağlantı kurup onlar üzerinde işlem yapmak için kullanılan standartlaşmış bir dildir. Veri tabanı kullanıcıları ile veri tabanları arasındaki iletişim aracı olarak veri tabanına yeni veri eklemek, istenilen kriterlerdeki verileri sorgulamak, var olan verileri güncellemek veya silmek, veri tabanı nesnelerini oluşturmak, veri tabanı erişiminin denetlenmesini sağlamak gibi pek çok işlemi gerçekleştirmek için kullanılmaktadır.

SQL, prosedürel yani yordamsal bir dil değildir bu yüzden blok yapısına, if else, for, while gibi kontrol mekanizmalarına sahip değildir. Çoğu veri tabanı yönetim sistemleri yapısal dillere ait, tetikleyici, prosedür gibi fonksiyonları ayrıca programlama üzerindeki akış kontrolleri ve değişkenleri oluşturma özelliklerini gerçekleştirebilmek için SQL dilinde çeşitli iyileştirmeler ve eklemeler yaparak PL/SQL, TSQL gibi kendi veri tabanı sistemlerinde kullanılacak dilleri geliştirmişlerdir.

IBM şirketi System R projesinde ilk veri tabanı yönetim sistemini kurmuş ve matematiksel bir söz dizimine sahip olan SQUARE adlı bir dil geliştirilmiştir. Daha sonra Yapılandırılmış İngilizce Sorgu Dili (Structured English Query Language) kısaca SEQUEL olarak adlandırılan İngilizceye benzer söz dizilimine sahip olan sorgu dili geliştirilmiştir. Bu yapısal sorgu dilinin ismi de değiştirilerek günümüzdeki SQL adını almıştır.

SQL sorgulama dili 3 ana bölümde incelenebilir. Bunlar “Veri tanımlama Dili / DDL” (Data Definition Language), “Veri İşleme Dili / DML” (Data Manipulation Language), “Veri Kontrol Dili / DCL” (Data Control Language) dilleridir.

Veri tanımlama dili (DDL)

Verinin tutulacağı nesneleri veya veri tabanını oluşturmak için kullanılan veri tabanı yapısını etkileyen SQL ifadeleridir. Kullanılan en temel komutlar:

- Create: Veri tabanını veya veri tabanında tablo, view, görünüm gibi nesneleri oluşturur.
- Alter:Veri tabanı nesnelerinin yapısını değiştirir.
- Drop: Veri tabanı nesnelerini siler.

Veri işleme dili (DML)

Veri işleme dili yani DML veri tabanındaki kayıtlar üzerinde yapılan değişiklikler için kullanılan komutlardır. Kullanılan en temel komutlar:

- Select: Veri tabanındaki kayıtları sorgular ve getirir.
- Insert: Nesneye yeni kayıt ekler.
- Update: Nesnedeki kaydı günceller.
- Delete: Nesnedeki kaydı siler.

Veri kontrol dili (DCL)

Bir veri tabanı kullanıcısı ve rolü için ifade ve nesne kullanımına izin tanımlar. Temel iki komutu vardır. Bunlar:

- Grant: Veri tabanı kullanıcısı veya rolüne izin tanımlar.
- Revoke: Veri tabanı kullanıcısı veya rolüne daha önce tanımladığı tüm izinleri iptal eder.

Temel sorgular

SQL komutları kullanılarak aşağıdaki işlemler yapılmaktadır:

- Veri tabanı nesneleri yaratılmakta ve bu nesneler üzerinden işlemler yapılmaktadır.
- Veri tabanı nesneleri üzerindeki kayıtların istenilen filtrelerde görüntülenmesi sağlanmaktadır.
- Veri tabanı nesnelerindeki kayıtlar güncelleştirilmektedir.
- Veri tabanı nesneleri veya bu nesnelerdeki kayıtlar silinebilmektedir.
- Veri tabanı nesnelerine yeni kayıtlar girilebilmektedir.

Bunlarla ilgili bazı örnekler aşağıda verilmektedir:

CREATE TABLE komutu ile tablolar oluşturulur. CREATE TABLE tablo_adı(...); Komutun kullanımında tablo adı belirtilir ve parantez içerisinde kolon tanımlamaları ‘,’ ile birbirinden ayrılarak yapılır.

Aşağıdaki örnekte Personel isimli tablonun nasıl oluşturulduğu gösterilmiştir.

```
CREATE TABLE Personel
(isim CHAR(15) NOT NULL,
soyisim CHAR(15) NOT NULL,
sicil INT NOT NULL,
adres CHAR(75));
```

İsim, soyisim, sicil ve adres kolonlarına sahip olan personel tablosunda her bir kolonun veri tipi ve fiziksel depolama alanında ne kadar yer ayrılacağı, not null ifadesi ile de ilgili kolona mutlaka veri girilmesi gerektiği, alanın boş bırakılamayacağı belirtilmiştir.

DROP TABLE komutu ile veri tabanını veya veri tabanı içerisinde istediğimiz nesneyi kaldırabiliriz. Veri tabanından tablo silmek için genel format şu şekildedir:

```
DROP TABLE tablo_adı;
```

ALTER TABLE komutu genel olarak veri tabanı içerisinde oluşturulmuş bir tablonun yapısında değişiklik yapmak için kullanılır. Tabloya yeni bir kolon eklemek, var olan kolonu silmek ya da veri tipini değiştirmek için kullanılır.

Kolon ekleme işlemi için genel format şu şekildedir:

```
ALTER TABLE tablo_adı ADD alan_adı veri_türü;
```

Kolon kaldırma işlemi için genel format şu şekildedir:

```
ALTER TABLE tablo_adı DROP alan_adı;
```

Kolonun veri tipinde değişiklik yapmak için genel format şu şekildedir:

```
ALTER TABLE tablo_adı MODIFY alan_adı veri_tipi;
```

INSERT INTO komutu ile veri tabanına veri eklenmektedir. Tabloya yeni veri eklemek için kullanılan genel format şu şekildedir:

INSERT INTO tablo_adı(alanadı_1,alanadı_2) VALUES (değer1, değer2),

UPDATE komutu ile kayıt güncellenmektedir. Tabloda belirli bir şarta uyan kaydı güncelleştirmek için kullanılan genel format şu şekildedir:

UPDATE tablo_adı SET alan_adı = ‘değer1’
WHERE şart;

DELETE komutu ile kayıtlar silinmektedir. Tabloda belirli bir şarta uyan kaydı silmek için kullanılan genel format şu şekildedir:

DELETE tablo_adı
WHERE şart;

SELECT komutu ile tablo veya tablolardaki veriler alınıp gösterilmektedir. Çok sık kullanılan bir komuttur. Genel kullanım formatı şu şekildedir:

SELECT * / alan_adı
FROM tablo_adı
WHERE şart
ORDER BY alan_listesi ASC/DESC
GROUP BY alan_listesi
HAVING şart

Select komutunun yanında * sembolünün olması ilgili tablodaki tüm kolon bilgilerinin görüntülenmesini sağlamaktadır. Select komutunun yanına * sembolü yerine işlem yapılacak alanların adı yazılarak select sorgusu sonucunda o kolonların görüntülenmesi sağlanır.

From cümleciği select sorgusundan dönecek kolon bilgilerinin hangi tablo ya da görünümden alınacağının belirtildiği alandır. Her select komutunda from cümleciği olmak zorundadır.

Where cümleciği ile tablo üzerindeki tüm kayıtlar yerine, verilen şartı sağlayan kayıtlar filtrelenerek getirilir. Eğer where cümleciği kullanılmamış ise select sorgu sonucunda tüm kayıtlar görüntülenir. Where cümleciğinde şart belirtlirken iki veri birbiri ile karşılaştırılacağından bu iki verinin türü aynı olmalıdır yani karakter bir veri karakter ile nümerik bir veri nümerik bir veri türü ile karşılaştırılmalıdır.

SQL komutları ile dönen kayıtlar sonuç tabloları olarak da kullanılmaktadır. Where cümleciği ile de istenilen sonuç tablosunu oluşturmak için Çizelge 3.1' deki karşılaştırma operatörleri kullanılır.

Çizelge 3.1. Matematiksel operatörler [29]

OPERATÖRLER VE ANLAMLARI

Operatör	Anlamı	Örnek	Sonuç
=	Eşittir	**="Sales"**	Sadece alanın değeri **"Sales"** olan kayıtları bulur.
<	Küçüktür	**<100**	Alanın değeri 100'den küçük olan tüm kayıtları bulur.
<=	Küçüktür veya eşittir	**<=100**	Alanın değeri 100'den küçük veya 100'e eşit olan tüm kayıtları bulur.
>	Büyüktür	**>100**	Alanın değeri 100'den büyük olan tüm kayıtları bulur.
>=	Büyüktür veya eşittir.	**>=100**	Alanın değeri 100'den büyük veya 100'e eşit olan tüm kayıtları bulur.
<>	Eşit değildir.	**<>"Sales"**	Alanın değeri **"Sales"** olmayan tüm kayıtları bulur.

Between operatörü ile de karşılaştırma operatörlerinde yapılan işlemler daha kısa ve daha etkin yapılabilmektedir. Bu operatör ile belirtilen aralıktan büyük olanlar ve belirtilen diğer aralıktan küçük olanlar getirilir. Aşağıdaki örneklerde aynı işlem between ve karşılaştırma operatörü ile yapılmıştır:

```
SELECT ad
FROM personel
WHERE dogum_yılı >'1955' AND dogum_yılı< '2000'
```

```
SELECT ad
FROM personel
WHERE dogum_yılı  BETWEEN '1955' AND '2000'
```

Daha komplike ve birleşik şartlar için AND, OR, NOT gibi mantıksal operatörler de kullanılır. AND operatörü şartta yazan tüm koşulların aynı anda sağlanması durumunda select işlemi yapılmasıdır. OR operatörü ile select işlemi, şartlardan en az birinin sağlanması durumunda gerçekleşmektedir. NOT operatörü şartın gerçekleşmemesi durumunda yapılacak select işlemidir.

IN operatörü or operatörünün yaptığı işi daha kısa ve anlaşılır yapmak için kullanılır. Or ile yazılan şartların hepsini IN() parantez içinde yazarak şartlardan en az biri sağlanıyorsa sonucu listeler.

Operatör kullanımı fazla ise bunlar parantezler kullanılarak birbirinden ayrılır ve işlem öncelik sırasına göre parantez içleri sorguda çalışır böylece karmaşıklık azaltılmak istenir.

Select komutunda belirli kriterleri sağlayan kayıtlar üzerinde değerleri toplama, minimumunu alma, satırları sayma gibi işlemler Çizelge 3.2' deki gruplama fonksiyonları kullanılarak yapılmaktadır.

Çizelge 3.2. SQL işlemler [30]

İşlem	**Açıklama**
AVG	Kayıtların ortalamasını hesaplar. (Veri tipi numerik olmalıdır)
COUNT	Kriterle belirlenen kayıtları sayar.
COUNT*	Seçili satırları sayar
MAX	Kriterle belirlenen değerlerden maksimumunu verir
MIN	Kriterle belirlenen değerlerden minimumunu verir.
SUM	Toplam verir.
STDEV	Değerlerin standart sapmasını verir.
STDEVP	Populasyondaki (tüm) değerlerin standart sapmasını verir.
VAR	Değerlerin varyansını verir.
VARP	Populasyondaki (tüm) değerlerin varyansını verir.

GROUP BY komutu select ifadesinde kullanılarak kayıtların gruplanmasını sağlar. Gruplandırdığımız veri üzerinde Çizelge 3.2 'deki gruplama fonksiyonlarını uygularken HAVING sözcüğü ile şart da verilebilir. Select komutu içerisinde having sözcüğünün kullanılabilmesi için Group By komutunun yer alması gerekmektedir. Group By komutunun olmadığı yerde having sözcüğü kullanılamaz.

Where sözcüğü ve Group By aynı select komutu içerisinde bulunuyorsa öncelikle where sözcüğü çalışır. Having sözcüğü ve where sözcüğü ikisi de istenilen şartın sağlanma durumunu kontrol ettiğinden birbirine benzetilse de where sözcüğü bir tablonun tüm satırları üzerinde işlem yapan şartlar için having ise sadece gruplanmış kayıtlar üzerinde işlem yapan

şartlar için geçerlidir. Ayrıca having sözcüğü içerisinde en az bir tane gruplama fonksiyonu olması gerekmektedir.

```
SELECT dept_no, AVG(Maas)
FROM Personel
WHERE cinsiyet_kod = 'K'
GROUP BY dept_no
HAVING AVG(Maas) >8000
```

Yukarıdaki select komutu her depertmandaki kadın personele ait maaş ortalamasını hesaplayacak ve kadın personel maaş ortalaması 8000'i geçen departman numaralarını sonuç tablosunda gösterecektir. Having veya where şartı içerisinde yazılan kolonun select komutu sonuç tablosunda yer alma zorunluluğu bulunmamaktadır.

ORDER BY komutu select ifadesi içerisinde kullanılarak gösterilecek bilgiyi düzenlemektedir. Order by komutu yanında belirtilen kolonların veya kolonlara bağlı olarak verilerin artan veya azalan biçimde sıralanmasını sağlar. Order by komutu select ifadesinin son komutu olmalıdır ve bu komut alt sorgularda kullanılamamaktadır.

```
SELECT sicil, isim, soyisim
FROM Personel
ORDER BY isim,soyisim DESC;
```

Yukarıdaki örnekte çok sayıda alana göre sıralama yapılmaktadır bu sorguda isme göre artan, aynı isim olan kayıtlarda da kendi aralarında soyisime göre azalan sıralama yapılacaktır.

ASC ascending yani artan anlamındadır order by komutunda kolon isminin yanında bir şey yazılmadıysa bu da ASC sıralama kabul edilir. DESC descending yani azalan sıralamadır burada veriler z'den a'ya ya da büyükten küçüğe doğru sıralanmaktadır.

3.4.Veri Tabanı Yönetim Sistemlerinin Sağladığı Faydalar

Veri tabanı yönetim sistemleri, veri tabanını hazır hale getirerek veri tabanı üzerinde yapılan işlemlerin güvenli ve başarılı sonuçlanmasını sağlar. Veri tabanı yönetim sisteminin getirdiği avantajlar şu şekilde sıralanabilir:

- Veri tekrarını azaltır veya yok eder, böylece tekrarlanan veriler sistemi hantallaştıramaz ve veri bütünlüğünü bozamaz.
- Veri tutarlılığını sağlar, böylece bir veri tabanında birden fazla örneğin her zaman aynı veriyi gerçek zamanlı tutarlılık seviyesinde yakalayabilmesini sağlar.
- Veri paylaşımı yaparken gelen yeni istekte önceki kullanıcının işleminin bitmesini bekletmez, aynı anda birden çok kullanıcının veri tabanı yönetim sistemlerine erişmesine imkan sunar.
- Tüm tabloların birbiriyle uyum içerisinde çalışmasını sağlar böylece bir tabloda ki veride gerçekleştirilen silme, güncelleme gibi işlemler o verinin olduğu tüm tablolar üzerinde gerçekleşir.
- Verilerin kasıtlı ya da yanlışlıkla bozulmasına sebebiyet verecek olayları önlemek için veri tabanı yönetim sistemlerinde çok sıkı erişim ve yetki kontrolleri vardır böylece veri güvenliği sağlanır.
- Veri bağımsızlığı, merkezi veri tabanı yönetim sistemini ilgilendiren bir yapıdır. Veri bağımsızlığı sayesinde uygulamalar, verilerin ve veri tabanının yapı ve organizasyonundan bağımsızlaştırılır.

3.5. Veri Tabanı Saldırı Örnekleri

Veri tabanı sistemlerinde kişisel verilerin de fazlaca bulunuyor olması veri tabanlarını saldırganların hedefi haline getirmektedir. Teknolojideki gelişimle birlikte yapılan siber saldırı sayıları da artış göstermektedir. Güvenlik riskleri hakkında çalışan OWASP'ın yayınladığı en yaygın 10 uygulama güvenliği açığında SQL Enjeksiyon (Injection) da yer almaktadır.

Aşağıda, gerçekleşen en büyük veri ihlallerine örnekler verilmiştir [24,31,32,33].

Amerika Birleşik Devletleri İstihbarat Merkezi'ne (CIA) Rusya tarafından gerçekleştirildiği iddia edilen saldırıda, bilgisayar korsanları e-ticaret şirketlerinin bilgisayar ve uygulamalarındaki banka hesap bilgilerini, kişisel verilerini ele geçirmiştir.

İnternet servisi Yahoo, maruz kaldığı siber saldırılar ile en büyük veri ihlalinin yaşandığı platformlardan biri olmuş buda şirket imajında büyük değer kaybettirmiştir. İnternet tarihinin en büyük veri ihlallerinden olan bu saldırıda Yahoo, neredeyse tüm veri tabanını

kaptırmış 3 milyardan fazla hesabın adları, soyadları, doğum tarihleri, telefon numaraları gibi hassas verilerinin etkilendiği açıklamıştır.

İş arayan ve iş veren kişilerin kullandığı sosyal medya mecralarından olan linkedIn' de düzenlenen saldırıda saldırgan, saldırıları düzenlemek için şirket çalışanlarına ait bilgileri kullandığını belirtmiştir. Bu saldırılarda yaklaşık 165 milyon kullanıcının bilgileri ele geçirilmiş ve hesapları internet ortamında satışa sunulmuştur.

Singapur'da kamu sağlık sistemine sızan saldırganlar 1.5 milyon kişinin kişisel bilgilerini ele geçirmiştir. Dünyanın bu boyutta sağlık sistemlerini hedef alan ilk saldırısı niteliğinde olan bu saldırıda hastaların adları, sosyal güvenlik numaraları, doğum tarihleri gibi verileri ele geçirilmiştir.

Uluslararası otel zincirlerinden en büyüğü olarak bilinen Marriott uğradığı saldırı sonucunda otelde geçmiş yıllarda da kalmış olan toplam 500 milyon kişinin, kişisel verileri ele geçirilmiştir. Yüz milyonlarca kişinin doğum tarihi, pasaport numaraları, telefon numaraları gibi kişisel bilgilerinin yanında bazılarının kredi kartı bilgileri de çalınmıştır.

Ülkemizde bir dönem faaliyet sürdüren İmar bankasında, tek hesap üzerinden çift kayıtlar tutulmuştur. Bu kayıtların tutulduğu veri tabanlarından biri yasal kayıtlı iken diğeri kayıtdışı olduğundan Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) tarafından İmar Bankası'nın faaliyetleri durdurulmuştur.

Şirketlerin veri tabanlarından edinilen bilgilerin ele geçirilmesi ile yaşanan bu skandallar bilgi güvenliğinin, veri tabanlarındaki verilerinin güvenliği sağlamanın önemine gözler önüne sermiştir. Veri tabanında, 27001 BGYS gereksinimleri uygulandığında yaşanacak veri kayıpları az seviyeye indirilecektir fakat gelişen teknoloji ile yeni güvenlik açıkları doğacak bilgisayar korsanları da yeni yollar ile saldırılarına devam edecektir.

3.6. Veri Tabanı Güvenlik Tehditleri

Tehditler, veri tabanlarındaki zayıflıkları ve zafiyetleri kullanarak veri tabanına zarar verebilirler. Tehditler uygun koşullar oluşursa açıklıkları bulunan zafiyetlere dönüşebilir, zafiyetlerde saldırganlar tarafından kullanılarak veri tabanlarına zarar verebilecek güvenlik ihlallerini doğurabilir.

Veri tabanı yönetim sistemlerinin yeni kullanılmaya başlandığı dönemde veri tabanlarına uygulamalar aracılığı ile sadece kurum içinden erişilebildiğinden en büyük tehdit kurum içi kullanıcıların oluşturduğu güvenlik ihlalleridir. Günümüzde e-devlet, e-ticaret gibi birbirine bağlı ağ ortamlarındaki uygulamaların kullanımının yaygınlaşması veri tabanlarının karşılaşacağı saldırı çeşitliliğini de artırmaktadır. Günümüzde kurumlar iyi niyetli fakat bilinçsiz veya kötü niyetli kullanıcıların oluşturabileceği iç tehditlere ve kurum dışından gelebilecek dış tehditlere karşı önlemler almak zorundadırlar [34].

Kurumlar veri tabanlarında bulunan verilerin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak için en önemli veri tabanı tehdidi listesini değerlendirerek bu tehditlere karşı uyumluluk ve riski aza indirme gereksinimlerini karşılayabilirler.

En önemli veri tabanı tehditleri 10 başlık altında listelenmiştir:

3.6.1. Aşırı ve kullanılmayan yetki tehdidi

Veri tabanı üzerinde bir kullanıcının iş akışı için gerekli olan alanlara erişebilmesi için yetki verilmeli, yetkisi dışındaki alanlara erişememesi sağlanmalıdır. Kullanıcılara gereğinden fazla yetki verilirse ya da çalışanın iş rolü değiştiğinde yetkiler düzenlenmezse kötü niyetli çalışanlar verileri açığa çıkarabilir. Örneğin, bir banka çalışanın görevi, müşterilerin hesap bilgilerindeki iletişim adreslerini değiştirmek ise ama tüm hesap işlemlerine müdahale edebileceği şekilde aşırı yetki verildiyse çalışan bu yetki ile ailesinin hesap bakiyesini artırabilir. Bir başka örnek, sağlık kuruluşuna ait uygulama üzerinden hasta kayıtlarını giren personel işten ayrıldığında veri tabanı üzerindeki yetkileri kaldırılmadığında personel işten kötü şartlar altında ayrıldıysa verileri değiştirebilir, silebilir, ifşa edebilir.

Veri tabanı kullanıcıların aşırı yetkilendirilmiş olma sebebi iş rollerine uygun yetki kontrollerinin iyi tanımlanmaması veya yönetilmemesidir. Erişim yetkisi denetim mekanizmaları oluşturulur, yetkiler erişim politikasına göre verilir, uygulama tarafından gelen bir sorgunun kullanıcının yetkisi dahilinde olup olmadığı kontrol edilir ve iyi bir denetim izi sağlayarak ayrıcalıkların kötüye kullanılması durdurulursa gereksiz risk oluşumlarının önüne geçilebilir.

3.6.2. Yetki suistimali tehdidi

Veri tabanı kullanıcıları yetkilerini suistimal ederek tehdit oluşturabilirler. Örneğin bir öğrenci otomasyon sisteminde, öğrenici kimlik bilgilerini düzenleyen kötü niyetli bir

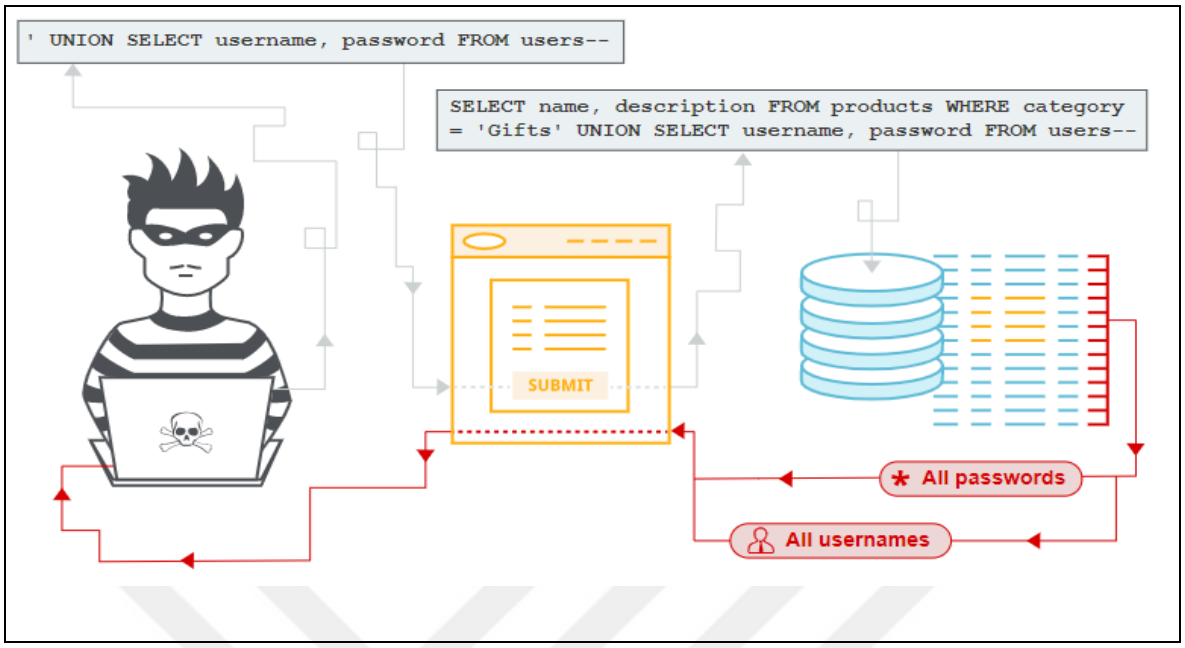
çalışan, kullandığı uygulamaların koyduğu verilerin kopyalanması, birden fazla kayda tek seferde bakılmaması gibi veri tabanı denetimini de sağlamaya yararı olacak kısıtları aşıp veri tabanına bağlanmak için excell gibi alternatif istemcileri ve kendine tanımlanan hakları kullanarak tüm öğrencilerin bilgilerinin bir kopyasını çıkarabilir.

Veri tabanında kısıtlı yetkisi bulunan bir kullanıcının yazılım ya da veri tabanındaki bir açıklıktan faydalanarak kendi yetkisini artırması, kendine veri tabanı yöneticisi yetkisi tanımlaması da bu tehdit grubuna girmektedir.

Bu tehditlere, veri tabanı erişimi bilgilerine denetim uygulanması, sunucu seviyesinde atak önleme sistemleri (IPS) ve sorgu seviyesinde yapılacak erişim kontrolleri ile önlem alınabilir. Sorgu seviyesinde denetim yapılmaz ise kullanıcı çalıştıracağı sorgu ile kendi yetkisini veri tabanı yöneticisine hiçbir engele takılmadan yükseltebilir.

3.6.3. SQL enjeksiyon tehdidi

Çalıştırılan sorgu içerisindeki müdahaleler neticesinde ortaya çıkan tehditlerdir. Veri tabanı ve uygulama üzerindeki önlemlerin yetersiz olması ya da uygulama yazılımcılarının bilgi eksiklikleri gibi sebeplerden yararlanarak SQL veri kanalına yetkilendirilmemiş veri tabanı yordamları eklenebilir. Bu eklenen yordamlar veri tabanında çalıştırılarak veri tabanına veri kaydedilebilir, silinebilir, değiştirilebilir, tüm veriler ifşa edilebilir. Başarılı bir SQL enjeksiyon saldırısı ile saldırgan veri tabanına ulaşıp onu yönetebilir hatta veri tabanı sunucusunda sistem yönetici olmasına olanak sağlayabilir. Şekil 3.8’te bir saldırganın normalde görüntüleyemeyeceği kullanıcı şifrelerini SQL Enjeksiyon kullanarak ele geçirme işlemi gösterilmektedir.



Şekil 3.8. SQL enjeksiyon örneği [35]

Şekil 3.8'deki veri tabanı sunucuları üzerinde SQL enjeksiyonu kullanarak işletim sistemi seviyesinde komutlar çalıştıran saldırganın bundan sonraki hedefi bu veri tabanı kullanıcı hesabı ile diğer sunucu ve bilgisayarlara erişebilmek, bundan sonraki erişimlerinde doğrudan sistemlere bağlanabilmek için gerekli olan servisleri kendi kullanımını açmak olacaktır [34].

SQL enjeksiyon tehditlerini en aza indirgemek için, direk sorguların yazılması yerine saklı yordamlar kullanılmalı ve Model-View-Controller (MVC) mimarileri uygulanarak program mantığı birbirine bağlı üç öğeye bölünmelidir. Ayrıca IPS atak önleme sistemleri, sorgu seviyesinde erişim denetimi ve olağan olaylar ile gerçekleşen olayı eşleştirme sistemlerinin olması da tehditleri önleyebilmek için gereklidir. Böylece güvenlik açığı olan saklı yordamlar veya sql enjeksiyon karakter dizginleri ile sorgu erişim denetimi arasında eşleştirme yapılır ve olağan iş operasyonu dışında bir durum varsa ihlal tespit edilmiş olur.

3.6.4. Kötü amaçlı yazılım tehdidi

Virüs, Truva atları, solucanlar, fidye yazılımları gibi birçok zararlı yazılım vardır ve bunlar sisteme zarar vermek, hassas bilgileri elde etmek için kullanılarak veri tabanı güvenliğini tehdit etmektedir. Son zamanlarda zararlı yazılımların hedefi haline gelen veri tabanları için saldırganlar, veri tabanı yönetim sistemlerine tanımlanmış tcp portlarına özel solucanlar tasarlayarak veri kayıplarına sebep olabilmektedir.

Kötü amaçlı yazılımlar ile kurumsal ve kişisel veriler risk altındadır. Ransomware de dosya erişimlerine engel olan verileri ciddi anlamda tehdit eden bir fidye yazılımıdır. Ransomware ile saldırganlar kilitleme yazılımlarını kullanarak cihazı kilitleyebilir ve sisteme erişimi kısıtlar veya şifreleme yazılımları ile dosya ve belgelerin açılmasını önleyebilir ve tekrar yapıyı eski haline getirmek için de fidye talebinde bulunabilirler.

Kötü amaçlı yazılım tehdidinden korunmak için veri tabanı sunucusunun güvenlik duvarı aktif, antivirüs programı yüklü, işletim sistemleri güncel ve erişim denetimi aktif yapılmalıdır.

3.6.5. Zayıf denetim takibi tehdidi

Hassas verilerin tutulduğu veri tabanları, yapılan her işlemin kayıt altında tutulması ve gerektiğinde analiz edilmek üzere izleme faaliyetlerinin yürütülmesi temeli üzerine yerleştirilmelidir. Zayıf veri tabanı denetim mekanizmaları birçok düzeyde ciddi risklere sebep olmaktadır.

Zayıf veya hiç olmayan veri tabanı denetimine sahip kurumlar 27001 Bilgi Güvenliği Yönetim Sistemleri, Sağlık Bilgi Taşınabilirliği ve Hesap Verilebilirlik Yasası gibi veri tabanı denetim gerekliliklerini ifade eden standartlar ile uyum sağlayamayacaklardır. Veri tabanı denetim izlerini takip etmeye yarayan entegrelerin CPU'yu ve disk kaynaklarını harcaması üzerine kurumlar, entegreleri devre dışı bırakmaya ya da kapasitesini düşürmeye yönelmektedirler bu benzeri durumlarda da veri tabanı denetimi, saldırı tespiti ya da adli bir durum karşısında ayrıntılı log kayıtları bulunamamaktadır.

Veri tabanı yöneticisi olan bir kişinin bilgisizliği veya kötü niyeti sonucunda denetim takibi kapatılabilir böylece kontroller devre dışı kalır ve veri tabanı her türlü saldırıya karşı savunmasız hale gelebilir. Bunu önlemek için sadece veri tabanında değil veri tabanı sunucusunda da görevler ayrılığı esasında denetim yapılması gerekmektedir.

3.6.6. Yedek verinin ifşa olma tehdidi

Yedek veri tabanı depolama ortamları sadece hassas verileri koruma amaçlı olmayıp güvenlik politikaları ile de güvenliği sağlanması hedeflenen yapılar haline gelmiştir. Çünkü veri tabanlarının yedeklendiği ortamlar, dijital ortamlar üzerinden yapılabilecek saldırılara, veri tabanı yedekleme disklerinin ve kasetlerinin fiziki olarak hasara uğramasına, çalınmasına veya kaybolmasına karşı korunmasız yapılardır. Ayrıca veri tabanı üzerinde

düşük seviyede yetkisi bulunan kullanıcıların hassas veriler üzerinde ki işlemlerinin denetlenmesi ve izlenmesi konusunda yetersiz kalınırsa yedekleme faaliyetlerinde de tehditler meydana gelebilir.

Yedekleme işlemleri kurumlarda belirli periyotlarda otomatik yapılmaktadır, bu yedekleme işlemlerine sadece belirli yetki seviyesindeki personelin erişimi olmalıdır. Alınmış bir yedek uygulama sunucusu üzerinde bulundurulursa yaşanabilecek olumsuz bir durumda hem yedek hem uygulama zarar görmüş olur.

Yedekler sadece yetkili personelin girebileceği fiziksel güvenlik önlemleri alınan bir ortamda tutulmalıdır. Yedeklerin bir kopyası kurum merkez yerleşkesinde diğeri ise uzak bir kurum yerleşkesi niteliğinde olan Felaket Kurtarma Merkezlerinde tutulmalıdır. Ayrıca veri tabanı yedekleri şifrelenmiş bir şekilde saklanarak yedek kopyalarının güvenliği sağlanmalıdır.

3.6.7. Yanlış yapılandırma ve güvenlik açığı tehdidi

Veri tabanı üzerinde bulunan güvenlik açıklıklarını kullanan kötü niyetli kullanıcılar, yetkilendirilmemiş erişim, veri kaybı veya servis kesintilerine sebep olabilir. Bu tehditleri önlemek için veri tabanının üzerinde çalıştığı sunucuda, işletim sisteminde, uygulamada güvenlik açıklıklarını tespit etme çalışmaları yapılmalıdır. Tespit edilen her bir açığın ortadan kalkması için uzmanları tarafından yürütülen çalışmalar ile bütünleşik bir koruma sağlanmış olur. Veri tabanı üretici firmasının hazırladığı güncellemelerin takip edilerek uygulanması tespiti yapılmış olan veri tabanı güvenlik açıklarını kapatabilir.

Veri tabanın dikkatsizlik veya bilgisizlikten dolayı yanlış yapılandırılması da veri tabanlarının en büyük tehditlerinden biridir. Birçok kullanıcıda bilgileri bulunan fazla yetkili ortak kullanıcıların kullanılması, güvenlik korumasının devre dışı bırakılması, istemci sunucu arasındaki trafiğin şifrelenmeden sağlanması, sistem üzerinden bilgi toplanabilecek hata mesajlarının açık bırakılması gibi yanlış yapılandırmalar veri tabanını saldırılara maruz bırakabilir. Bu tehdidi en aza indirebilmek için işletim sistemi ve veri tabanında güncellemelerin düzenli uygulanması gerekmektedir.

3.6.8. Yönetilmeyen hassas veri tehdidi

Veri tabanındaki hassas veriler kurumdan kuruma değişiklik göstermektedir. Veri tabanında kişilerin özel nitelikli kişisel verilerini, finansal bilgilerini tutan kurumların hassas veri miktarı daha fazladır ve veri tabanı risk seviyesi de buna bağlı olarak artış göstermektedir. Kurumsal veri tabanlarında verilerin önem derecesine göre sınıflandırılması ve bu sınıflandırmaya bağlı olarak erişim denetimleri yapılmalıdır. Erişim denetimlerinde olağan işleyiş dışında bir verilere bir işlem gerçekleştirilmeye çalışıldığında uyarı üretilmeli ve bu tehdide müdahale edilmelidir. Ayrıca kontrol denetimleri veri alanına da yapılmalı böylece hassas verileri ele geçirmek isteyen kötü niyetli bir kullanıcı, veri tabanında şifrelerin şifreleme algoritması ile tutuluyor olmasından dolayı şifreleri kullanamamalıdır.

3.6.9. Hizmet dışı bırakma tehdidi

Hizmet çalışmasını engelleme saldırısı olarak ifade edilen dos ve ddos atakları; çevrimiçi bir uygulama veya hizmeti, verilere erişimi bant genişliğinin tamamını kullanarak engellemek amacıyla sistemi isteklere cevap veremez hale getirmektir. Genellikle kurum dışından yapılan bu ataklarda, veri tabanının sunucu kaynaklarını çok sayıda sorgu ile boğarak veya aşırı sistem kaynağı tüketecek sorgular çalıştırarak yeterli kaynağı kalmayan sunucuların yanıt verememesi ve hatta sunucuların çökmesi hedeflenir.

Dos ve DDos saldırıları kurumlara, kullanıcılara, internet altyapısına ciddi bir tehdit oluşturmakta ve gerçekleştiği takdirde de önemli itibar kayıpları yaşatmaktadır. Dos ve DDos saldırılarına karşı ağ, uygulama, veri tabanı katmanlarının çoğunda korunma sağlanmasını gerekir. Uygulama ya da sunucuya port üzerinden ve bağlantı noktalarından erişimlerin yapılmasını sağlamak, saldırı tespit sistemleri kullanmak, veri tabanını kullanan uygulamaların erişim kaynaklarını kontrol etmek hizmet dışı bırakma saldırılarını büyük oranda engelleyebilir.

3.6.10. Sınırlı güvenlik uzmanlığı ve eğitim

İnsan faktörü göz ardı edilerek sadece teknik anlamda ele alınan güvenlik önlemleri asla yeterli olmamaktadır. Teknik anlamda yetersiz bilgiye sahip personel veri tabanı için büyük bir tehdit oluşturacaktır. Bu nedenle yeni bir ürün veya hizmet devreye alınacağı zaman alanında uzman kişilerden destek alınmalı kullanıcıların yeni ürüne adaptasyonunu ve ürün hakkındaki bilgisini en üst düzeye çıkarabilmesi esas alınmalıdır.

Bilgi güvenliği politikaları, kurumların kabul edilebilir güvenlik seviyesini belirleyerek üst düzey personel de dahil olmak üzere tüm personelin ve tüm tedarikçi kuruluşların uyması gereken kurallar bütünüdür [36]. Veri tabanı güvenliğinin sağlanmasında önerilen katmanlı yapının oluşturulması ve dinamik bir şekilde uygulanabilmesi için bilgi güvenliği politikaları önemli bir yapıdır. Ayrıca bilgi güvenliği kapsamında eğitim politikaları oluşturularak, nitelikli personel yetiştirmek amaçlanmakta ve kullanıcı eğitimleri düzenlenerek farkındalık oluşturulmaktadır.

4. İLGİLİ ARAŞTIRMALAR

Yüksek Öğretim Kurulu (YÖK) sitesi, Scholar Google ve Gazi Üniversitesi Kütüphane veri tabanları kullanılarak anahtar kelimeler ile alan yazın taraması yapılmıştır ve bu tarama sonucunda bilgi güvenliği, siber güvenlik, dijital veri güvenliği, bilişim güvenliği gibi anahtar kelimler barındıran çalışmaların benzer sonuç ve önerileri olduğu gözlemlenmiştir. Bunlar üzerine yapılmış çalışmalara aşağıda kısaca yer verilmiştir.

Eloff ve Delamini (2009) tarafından yayınlanan çalışmada bilgi güvenliğinin doğuşu ve zaman içerisinde geldiği hal konu alınmıştır. Bu makalede, bilgi güvenliğinin aslında yazının ilk bulunduğu zamandan itibaren var olduğuna ama bilgisayarın icadı ve teknolojinin gelişimi ile bilgi güvenliği kavramının dijital ortamlar için daha çok kullanıldığına, ilk bilgisayar virüsünün tarihte nasıl ortaya çıktığı ve bunun bilgi güvenliği ile ilişkisine değinilmiştir. Ayrıca anket sonuçlarının da değerlendirildiği bu çalışmada, bilgi güvenliğinde yaşanan problemlerin çoğunun temelinin insan faktörü olduğu ve genelde örgütsel yapılar ile bilgi güvenliğinin tehdit edildiği tespit edilmiştir [37].

Luo ve diğerleri (2012), phishing saldırıları üzerine yapılan çalışmalardan faydalanarak phishing saldırılarındaki başarıların altında yatan psikolojik nedenleri tespit etmeye çalışmışlardır. İndiana Üniversitesinde, yüksek lisans öğrencilerine verilen bilgi güvenliği dersi kapsamında 105 öğrenciye üniversite e-posta adresinden 2010 senesinde phishing maili gönderilmiş 22 dakika içerisinde 38 öğrencinin e-posta linkini tıkladığı ve bunlardan 16'sının kullanıcı adı ve şifre bilgilerini girdiği belirlenmiştir. Çalışmanın sonucunda, insanların bilişsel ön yargılarından yararlanarak saldırılarda başarı sağlamanın teknolojik zafiyetleri kullanarak başarı sağlamaktan daha etkili olduğu anlaşılmış ve bu tür saldırıların önüne geçerek bilgi güvenliğini sağlamak için insanlara bu konularda eğitimler verilerek bilinçlendirilmesi gerektiği vurgulanmıştır [38].

Akyıldız ve Yiğit (2013), sızma testlerinin önemini vurgulamak için bir model ağ prototipi hazırlamış ve gerçek hayatta karşılaşılan saldırıların uygulamaları yapılmıştır. Bu çalışmada yapılan testler sonucunda, ağlara erişimde alınan fiziksel önlemlerin yeterli olmadığı, kablosuz ağlarda bilinen güvenlik açıklıklarına karşı yeterli önlemler alınmadığı ve bu açıklıklar ile çok ciddi bilgilerin elde edilebildiği, ağlara erişim gerçekleştikten sonra şifrelerin kolayca devre dışı bırakıldığı, kolay tespit edilebilen şifreler ile ağ zafiyetlerine sebep verildiği tespit edilmiştir. 27001 Bilgi Güvenliği standartları göz önüne alınarak

fiziksel güvenlik, ağ güvenliği, uygulama güvenliği önlemlerinin hayata geçirilmesi, gerekli politikaların hazırlanması ve hem teknik ekibe hem kullanıcılara bilgi güvenliği farkındalık eğitimlerinin uzman kişilerce verilmesi gerekliliği tespit edilmiştir [39].

Hekim ve Başıbüyük (2013), Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları makalesinde ülke olarak doğru strateji ve planlar gerçekleştirmezsek karşılaşacağımız risklerin artacağına değinmiştir. Siber güvenlik kavramının bilgi güvenliği ve bilgisayar güvenliği kavramları ile benzer manalarda kullanıldığı, siber güvenlik denilince de akla geniş bir kapsamda tüm iletişim altyapısı güvenliğinin gelmesi gerektiği açıklanmıştır. Siber suçları tek tek ele aldıkları ve istatistiklere yer verdikleri bu çalışmada, en az maliyet ile en etkili yöntem olan sosyal mühendislik konusunda daha detaylı ele alınmıştır. İnsan temelli bir saldırı olan sosyal mühendislik saldırılarından korunabilmek için insanların bilinçlendirilmesinin şart olduğu ve kamu kurumlarının birbiri ile, kamu kurumlarının özel sektör ile koordineli bir çalışma yürütmesi ve bilgi paylaşımı yapması gerektiğine değinilmiş ayrıca yürütülen bilişim projelerine muhakkak güvenlik ayağının eklenmesi ve denetlenmesi gerekliliği vurgulanmıştır [40].

Bostan ve Şengül (2018), son 20-30 yıl içerisinde kurum ve kuruluşların bilgi güvenliği farkındalığı konusunu; güvenlik gereklerinin neler olduğu, kullanılabilecek araç ve gereçlerin tanıtımı ve kullanımını şeklinde ele aldığı, bu yaklaşımın da bireylerde arzu edilen davranış geliştirme için yetersiz kaldığı belirtilmiştir. Siber sistemlerde gerekli güvenlik seviyesine ulaşmak için güvenlik farkındalığı oluşturulması ve güvenli davranış biçimi alışkanlığı kazandırılması ile sistemlerin daha güvenli tasarlanacağı ve kullanılacağı konularına değinilmiş ve siber sistemlerdeki her bireyin sorumlulukları ve rolleri çerçevesinde gerekli bilgi prensibine uygun olarak özelleştirilmiş içerikleri ile çevrimiçi öğrenme ortamlarında eğitimlerin gerçekleştirilmesinin faydası vurgulanmıştır [41].

Çetin (2014), literatür taramaları ve yüz yüze sorulardan geliştirdiği kişisel veri güvenliği farkındalığı anketini 526 kişiye uygulamış değerlendirmeye uygun görülen 501 kişinin pek çoğunun bilgi güvenliğine önem verdiği görülürken yarısının güncel tehditlerden haberdar olmadığı ve yarısından azının da olası bir tehdit durumunda nereye haber vermesi gerektiğini bilmediği ortaya çıkmıştır. Cihaz güvenilirliğinin artması için katılımcıların neredeyse hepsinin bilgisayarlarında anti virüs programının yüklü olduğu ancak cep telefonu ve tabletler gibi mobil cihazlarında bu önlemi yeterli ölçüde almadıkları görülmüştür. Kişisel verileri yedekleme ve şifreleme, kişisel verileri paylaşımı risk farkındalığı konularında

kadınların erkeklere göre farkındalıklarının daha gelişmiş olduğu ve kullanıcıların eğitime ihtiyaç duyduğu ve istekli olduğu tespit edilmiştir [42].

Eminağaoğlu ve Gökşen (2009), gerek Türkiye ve gerekse diğer ülkelerden aldığı istatiksel verilerden yararlanarak bilgi güvenliğinde yapılan en yaygın hatalara dikkat çekmiş ve alınabilecek çözüm önerileri ile önlemler üzerinde durmuştur. Bilgi güvenliği denilince akla belli başlı sektörlerin, bilgisayar ve teknolojinin geldiği fakat insanların bilgi güvenliği konusunda bilinçlendirilmesiyle bilgi güvenliğinin genele yayılması gerektiği vurgulanmıştır. Ayrıca alınan teknolojik, yönetimsel, hukuksal önlemlerin tek başına alınmasının yetersiz kaldığı bunun için teknik personelden başlanarak en zayıf halka olarak tabir edilen son kullanıcının bilgilendirilmesi, üst yönetimin sürece katılması ve yasal zeminlerin hazırlanması önerileri sunulmuştur [43].

McCormac ve diğerleri (2017); yaş, cinsiyet, risk alma eğilimi, korumacı davranışları, kişilik özellikleri, organizasyon faktörleri gibi bireysel farklılıklar olan bağımsız değişkenler ile bilgi güvenliği kapsamında bilgi, tutum ve hareketler arasındaki değişimin boyutu ve farklılıklarını çalışmalarında incelemiştir. İleri yaştaki bireyler genç bireylere oranla daha yüksek bilgi güvenliği farkındalığı puanı alırken, kişilik özelliklerine göre yumuşak başlı, sosyal, kendisi ile dünya arasında daha iyi ve ideal bir uyuma sahip olan yani öz-denetimi yüksek bireylerin bilgi güvenliği farkındalıklarının daha yüksek olduğu tespit edilmiştir [44].

King(2017), Amerika Birleşik Devletleri'nin Hawaii ve Alaska şehirlerinde bulunan küçük ve orta ölçekli çalışma merkezlerinden 210 personele anket yapılmış ve kurumsal bilgi güvenliği yönetişimi ile bilgi güvenliği standartları arasında birbiriyle direk ilişkili bir bağlantı olup olmadığı incelenmiştir. Elde edilen anket çalışması sonuçları ile kurumsal bilgi güvenliği yönetişimi ile bilgi güvenliği standartları arasında doğrusal bir ilişki olduğu sonucuna varılmıştır [45].

Akay(2014), tarafından yayınlanan yüksek lisans tezinde, dünyada en kapsamlı BGYS standardı olarak kabul görmüş 27001 standardının tarihsel gelişimi ve sürümleri arasındaki farklılıkları açıklamış, iki kuruluş ile mülakatlar gerçekleştirmiş ve elde edilen bulgular ele alınmıştır. BGYS'nin sadece teknik bir konu olarak algılanmaması gerektiği bu algı ile kurulan BGYS'nin etkinliğinin düşük olduğu, ISO 27001 gerekliliklerinin uygulanması esnasından teoride ve pratikte paralellik sağlanması gerektiği, her kurumun kendi

ihtiyaçlarına cevap verecek standardı ve kontrol hedeflerini seçmesinin gerekliliği vurgulanmıştır [4].

Gencer (2015), kurumsal ve uluslararası saygınlık görmek için ISO27001 sertifikasının öneminden, kamu kurumlarında da giderek yaygınlaşmasından bahsetmiştir. Bu çalışmasında, ISO27001 standardı gerekliliklerini kurum iş ve işleyişlerinde günlük yürütülen çalışmalar haline gelmesi için dinamik bir yapı haline getirmeyi amaçlamıştır. Bilgi güvenliği çalışmalarına ilk olarak varlık envanteri ile başlanması gerektiği, varlıkların güvenlik açısından değerlendirilmesinin önemi belirtilmiştir. Kurumlarda bilgi güvenliği sürecinin, sertifikasyon süreci sonrasında da dinamik yürütülebilmesi için sistemin yönetiminin bir uygulama aracılığıyla yapılması gerekliliği vurgulanmış ve insan faktörünün etkisi ne kadar azaltılır uygulama ne kadar ön planda kullanılırsa sistemin o kadar başarılı olacağı üzerinde vurgu yapılmıştır [46].

Shoraka (2011), yaptığı çalışmada ISO 27001 Bilgi Güvenliği Yönetim Sistemi sertifikasyonuna sahip olan kuruluşlarda sertifikasyon sahibi olmanın bu kuruluşlara ekonomik bir katma değer sağlayıp sağlamadığı araştırılmıştır. Araştırma kapsamında, çoğunlukla sermaye piyasalarında, bilgi güvenliğinin kurularak sertifikasyonun sürecinin tamamlanması ve bunun duyurulması sonucunda herhangi bir ekonomik değer kazandırmadığı ve hatta sertifika sahibi olan kuruluşlar ile sertifika sürecinin tamamlamamış kuruluşlar arasında bilgi güvenliği ihlal olaylarına verilen tepkiler arasında da farklılıklar görülmediği tespit edilmiştir [47].

Aktaş (2020), BGYS standartlarından ulusal geçerliliğe sahip olan ISO27001 standardının erişim kontrol prosedürünün şirketler için önemi ve uygulanmasının bilgi güvenliğine katkısı incelenmiştir. Çalışma kapsamında hazırlanan ankete, ISO 27001 Bilgi Güvenliği Yönetim Sistemine sahip olan ve olmayan farklı sektörlerden, farklı eğitim seviyelerinden ve farklı yönetim kademelerinden 343 çalışan katılmış ve elde edilen veriler sonucunda BGYS sertifikasına sahip şirketlerin bilgi güvenliğine dair riskleri erişim kontrol politikaları ile en aza indirdiği, sertifika sahibi olmayan şirketlerin erişim kontrol seviyelerinin kritik seviyede olduğu tespit edilmiş, erişim kontrolünün önemli bir güvenlik hizmeti olduğu ve BGYS'nin erişim güvenliği ve kontrolüne önemli faydalar sağladığı vurgulanmıştır [48].

Yapılan alan yazın ve gerçek hayat uygulama araştırmalarında, bilgi güvenliğinin daha etkin bir şekilde yönetilebilmesi için teknik cihazlar, yeni uygulama ve modeller, güvenlik testleri

üzerine çalışıldığı; fiziksel güvenlik, ağ güvenliği, uygulama güvenliği, erişim güvenliği politikalarının gereklilikleri üzerinde durulduğu ancak bütün bu çabalara rağmen tehditlerin tam olarak aşılamadığı ve sistemlere yönelik saldırıların tam olarak önlenemediği görülmektedir. Pek çok konuda olduğu gibi bilgi güvenliğinde de istekli, bilinçli ve bilgili insanlar başarının anahtarıdır. Kötü niyetli uzman bir kişi tarafından, kurum dışından yapılacak olan bir saldırıdan daha zararlı ve riskli olanı, iyi niyetli fakat bilinçsiz veya kötü niyetli kullanıcıların oluşturabileceği iç tehditlerdir. Bu konuda, bilgi güvenliğine yönelik yapılan çalışmalar olmasına rağmen hedef kitle göz önüne alınarak, belirli bir teknik alan özelinde yapılan bilgi güvenliği çalışmaları sayıca çok azdır. Çalışmaların çoğunda, bilgi güvenliği farkındalığının oluşmasında insan faktörü üzerinde durulduğu, bilgi güvenliğine yönelik farkındalık eğitimlerinin gerekliliğinin ve kurulan BGYS'nin olgunluk seviyesinin değerlendirildiği görülmektedir. Diğer taraftan çalışmalardaki; fazla bilgi yüklemesi, yönlendirme problemleri, aranılan bilgiye ulaşılamaması sebeplerinin de personelin BGYS'yi sahiplenmesi konusunda problemler oluşturduğu görülmüştür. Gerçekleştirilen bu çalışmanın; veri tabanı sorumlularının teknik yeterliliklerine ışık tutmak ve BGYS'yi sahiplenmelerini sağlamak için ihtiyaç duyulan fakat şimdiye kadar herhangi bir otorite tarafından hazırlanmamış kaynak eksikliğini gidermesi ve veri tabanı sorumluların bilgi güvenliğini kanıksaması, öğrenmesi ve rutin haline getirmesi konusunda katkı sağlaması planlanmıştır.

5. ISO/IEC 27001 BGYS KONTROL MADDELERİ

Buraya kadar, kontrol amaçları ve kontrolleri iyi anlayabilmek için bilgi güvenliği ile ilgili temel bilgilere 2. bölümde değinilerek bir alt yapı oluşturulmuştur.

ISO/IEC 27001 standardını yapısal olarak ele aldığımızda 2 bölümden oluşmaktadır. Birinci bölüm, uygulanması zorunlu olan ana bölümdür. 2.bölüm ise kontrol amaçları ve kontrollerinin verildiği ekler kısmıdır. ISO 27001 Standardı ekler bölümü ile 19 sayfada, BGYS sürecinin tamamını kapsamakta ve neler yapılması gerektiğini söylemektedir. Fakat nasıl yapılacağı ve nelere dikkat etmemiz gerektiği konularına yer vermemektedir. Bu noktada hazırlanmış akademik çalışmaların sayıca az olması, hazır kullanılan otomasyon sistemlerinin her kurumun kendi kurum kültürü olduğu ve hassas noktalarının farklılık göstereceği hususunu tam karşılayamaması bizim için yeterli olmamaktadır.

ISO/IEC 27001:2017 BGYS Standardı ekler bölümü, kurum veya kuruluşların genel gereksinimlere uygunluğunu sağlayan, insan kaynakları politikalarından iş sürekliliği planlarına kadar çok detaylı kontrol amaçları ve kontrollerini kapsamaktadır. ISO 27001 standardı, Çizelge 5.1'de de gösterildiği üzere 14 ana güvenlik kontrol maddesi altında toplam 114 kontrolü içermektedir [49]. Ana maddeler neye ulaşılması gerektiğini belirten kontrol hedefini, 114 kontrol ise bu hedefe ulaşmak için uygulanabilecek kontrolleri belirtmektedir.

Çizelge 5.1. ISO 27001:2017 BGYS Gereksinimleri Standardı'nın Ek-A kontrol amaçları [49]

KONTROL AMAÇLARI	KONTROL SAYISI
A.5 Bilgi Güvenliği Politikaları	2
A.6 Bilgi Güvenliği Organizasyonu	7
A.7 İnsan Kaynakları Güvenliği	6
A.8 Varlık yönetimi	10
A.9 Erişim Kontrolü	14
A.10 Kriptografi	2
A.11 Fiziksel ve Çevresel Güvenlik	15
A.12 İşletim Güvenliği	14
A.13 Haberleşme Güvenliği	7
A.14 Sistem temini, Geliştirme ve Bakımı	13
A.15 Tedarikçi ilişkileri	5
A.16 Bilgi Güvenliği İhlal Olayı Yönetimi	7
A.17 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları	4
A.18 Uyum	8

Bilgi güvenliği sadece güvenlik cihazları veya politikalar hazırlanarak oluşturulacak bir sistem değil de kontrol hedef gerekliliklerin gerektirdiği gibi üst yönetim desteği alınmış, insan faktörü ön planda tutularak farkındalıkları artırılmış, teknik yeterlilikleri için eğitimler sağlanmış, risk değerlendirmeleri yapılmış, denetimler gerçekleştirilmiş yani her açıdan detaylı değerlendirilerek sürekli gelişen ve kontrol edilen bir sistem olarak uygulanmalıdır. Kontrol hedefleri bize temel oluşturacak şekilde hazırlanmıştır ve bu maddelerinin uygulanma zorunluluğu yoktur fakat isteğe göre de devre dışı bırakılamaz ancak uygulanabilirlik bölümünde yer almayan konular için ilgili maddeler kapsam dışı bırakılabilir. Kontrol maddeleri eğer kurumun tüm ihtiyaçlarını karşılayamıyorsa yeni maddeler ile BGYS farklı konularda da gözden geçirilebilir.

Kontrol hedeflerinin açıklanmasında, bu kontrollerin uygulanması esnasında kılavuz olarak hazırlanmış ISO/IEC 27002 uygulama prensipleri temel alınarak bilgi güvenliğinin sağlanmasında rolü olabilecek her konu için gereklilikler aşağıda açıklanmıştır.

5.1. Bilgi Güvenliği Politikaları (A.5)

Kurumda, önemli bilgilerin yönetimi, dağıtımı ve korunması için ilgili yasa ve düzenlemelere uygun politikalar hazırlanması ve yönetim desteği sağlanması amaçlanmaktadır.

Bilgi güvenliği politikaları ana maddesinin tek alt maddesi ve 2 kontrol maddesi vardır. Bunlarla A.5 maddesi için, bilgi güvenliğinin tanımı, genel kapsamı ve hedefinin belirlenmesi, oluşturulan politikaların üst yönetim tarafından onaylanması, desteklenmesi, tüm çalışanlara ve 3. taraflara duyurulması ve farkındalık sağlanması, kurumun politikaları belirli aralıklarla veya gerekli oldukça etkinliğini sağlamak için gözden geçirmesi gerekliliklerine değinilmektedir.

Kurumun her kademesinde, iş sürekliliğinde gerekli olup bilgi güvenliğini zorunlu tutan her konuda politika hazırlanabilir. Bu politikalar kurumun bilgi güvenliğine yön veren temel Bilgi Güvenliği Politikası'nın içerisinde olabileceği gibi, kurumun seçimine göre farklı konularda farklı dokümanlar şeklinde de oluşturulabilir. Temiz masa temiz ekran, kişisel veri saklama ve imha, internet kullanımı, iş sürekliliği, erişim ve benzerleri gibi daha da çeşitlendirilebilecek konular için hazırlanan politikalar çalışanlara ve ilgili taraflara duyurulmalıdır bu nedenle de politikaları yazarken, ilgili okuyucu tarafından erişilebilir ve anlaşılabilir olmasına dikkat edilmelidir.

5.2. Bilgi Güvenliği Organizasyonu (A.6)

Bilgi güvenliği organizasyonu iki alt ana madde ile karşımıza çıkmaktadır. İlk bölüm 5 kontrol maddesiyle bilgi güvenliğinde görev ve sorumluluklara yönelik bir yönetim oluşturulmasını, ikinci bölüm de uzaktan çalışma ve mobil cihazların kullanımındaki güvenliği sağlamayı amaçlamaktadır. Mobil cihaz kullanımındaki güvenlik riskini en aza indirgemek için ve çalışanların kurum ağına uzaktan erişimlerinde bilgiyi korumak, güvenli erişim sağlamak için politikalar oluşturulmalı ve güvenlik önlemleri uygulanmalıdır.

Kurumda BGYS sürecini kurmak ve yönetmek için bilgi güvenliği sorumlulukları oluşturulup yetki prosesleri tanımlanmalı varlıklar ve bilgi güvenliği süreçleri tanımlanmalı ve sorumluluklar belirlenmelidir. Bilgi güvenliğinin geliştirilebilmesi ve uygulanabilmesi için sorumlulukların büyük çoğunluğu bilgi güvenliği yöneticisine atanmalı ama her bir varlık için varlığın korunmasından sorumlu bir varlık sahibi belirlenmelidir.

Yetkisiz personel erişimlerini, bilgi eksikliğinden kaynaklı veya kasıtlı değişiklikleri, varlıkların yanlış kullanımını azaltmak için çelişen görev ve sorumluluklar olmamalı görevler ayrımı yapılma, tek kişi yetkilendirme ihtiyacı duymadan varlıklara erişememeli, değişiklik yapamamalıdır.

Kurumlar ihlal olaylarında, internet üzerinden maruz kaldıkları saldırılar karşısında harekete geçmek, ne zaman ve hangi otoritelere olayları nasıl raporlayacaklarını belirlemek için prosedürler hazırlamalıdır.

İç ve dış paydaşlarla iletişim sistemleri geliştirme gereklilikleri kontrol edilerek güvenlik konularında iş birliği ve koordinasyonu sağlamak, gizli bilgiyi korumak için gizlilik antlaşmaları hazırlanmalıdır.

Proje yönetimlerinde, projenin konusu ne olursa olsun her zaman bilgi güvenliği konusu dikkate alınmalıdır. Tüm projelerde bilgi güvenliğine uygun sorumluluklar tanımlanmalı ve bilgi güvenliği politikaları hayata geçirilmelidir.

Kurumsal cihazların kullanımı esas olmakla beraber kurumsal olmayan mobil cihazların da kullanımında bilgi güvenliği konuları dikkate alınmalıdır. Kurumsal mobil cihazlar , istisnai durumlar dışında kişisel amacalar için kullanılmamalı, mobil cihazların barındırdığı bilgilerin güvenliği için; cihaza erişim pin kodu, parola gibi güvenlik katmanı ile olmalı, kaybolmaya veya çalınmaya karşı cihazın fiziksel güvenliği sağlanmalı, zararlı yazılımlara karşı cihaz korunmalı, kurum politikasına uygun olmayan programlar cihaza yüklenmemelidir. Personele mobil cihaz kullanımı, ağ bağlantıları konularında riskler ve uygulanması gereken politikalar ile ilgili eğitimler verilmelidir.

Bilişim alt yapısına uzaktan erişim, uzaktan çalışma ihtiyaçları karşısında erişilen, işlenen veya depolanan bilgiyi korumak için güvenlik önlemleri alınmalı ve bunları kapsayan bir politika hazırlanmalıdır. Uzaktan erişim ve çalışma faaliyetleri kurumun belirlediği güvenli uygulamalar aracılığı ile gerçekleştirilmeli, kurum tarafından kabul edilmiş fiziksel ortamdan kurumun erişim yetkisi verdiği personel bilgiye erişebilmelidir.

5.3. İnsan Kaynakları Güvenliği (A.7)

Bilgi güvenliği yönetim sistemleri sadece bilgi işlem birimlerince teknoloji ve süreçlerin yürütülmesi ile canlı tutulabilecek bir sistem değildir, sistem ancak tüm kurumun katılımı ile gerçekleştirilirse dinamik ve sürdürülebilir olmaktadır. Çünkü bilgi güvenliği insan,

teknoloji ve süreç faktörlerinin kümesi olarak ele alınmakta ve teknolojik çözümler tek başına asla yeterli olmamaktadır. Bu madde de bilgi güvenliğinin vazgeçilmez parçası olan insan kaynakları güvenliğinin sağlanmasına yönelik oluşturulmuştur.

İnsan kaynakları güvenliği 3 alt ana madde içermektedir. Kontrol maddeleri ile istihdam öncesi, iş yaşantısı sürecinde ve son olarakta işe son verilmesi veya değişiklik olması durumunda yapılması gerekenler açıklanmaktadır.

İşe alım öncesinde adaylar veya yüklenicilerin bilgi güvenliği açısından işe uygun olup olmadıklarının tespit edilmesi için kanunlar ve etik değerler ışığında iş gereksinimleri ve erişebilecekleri bilgilerle orantılı olarak tarama yani geçmiş doğrulama kontrolleri gerçekleştirilmelidir. Çalışanlar ve diğer paydaşlar kendilerinin ve kurumun rol ve sorumluluklarını belirten hükümleri, erişecekleri bilgileri gizlilik ve ifşa etmeme sözleşmelerini imzalamalıdırlar.

Çalışma esnasında yönetimin, çalışan ve paydaşlardan bilgi güvenliği politikalarına uygun hareket etmelerini istemeli ve kendi de sorumluluklarını da yerine getirmelidir. Kurum çalışanları ve dış kaynakların bilgi güvenliği sorumluluklarının bilincinde olmaları, bilgi güvenliği farkındalıkları ve eğitimleri almaları gerekmektedir. Bilgi güvenliği ihlaline sebep olan çalışanlar için disiplin süreci oluşturulmalı ve bu süreçten tüm çalışanlar haberdar olmalıdır.

İşe son verme veya değiştirilmesi durumunda kurumun çıkarlarını korumak amacıyla sona eren, devam eden veya yeni eklenen sorumluluklar tanımlanmalı, tanımlı yetkiler düzenlenmeli ve istihdam öncesi imzalanan sözleşmelerdeki işe son verme durumunda da devam eden sorumluluklar yürürlüğe konmalıdır.

5.4. Varlık Yönetimi (A.8)

Kurumların varlık envanterinin çıkarılması ve bu envanterin yönetilmesi bilgi güvenliği için en önemli maddelerden biridir. Varlık yönetimi 3 alt ana madde ve 10 kontrol maddesi ile karşımıza çıkmaktadır. İlk ana maddede kuruluşların varlıklarını tespit etmek ve sorumlulukları tanımlamak, ikinci ana maddede bilginin korunmasını önem derecesine göre sağlamak ve üçüncü ana maddede bilginin yetkisiz erişim, değiştirilme, ifşa ve yok edilmesini engellemek detaylı anlatılmaktadır.

Sunucular, veri tabanları, uygulamalar, akıllı cihazlar, kurumsal bilgisayarlar ve telefonlar gibi bilgi ve bilgi işleme araçları ile ilişkili tüm varlıklar belirlenmeli ve varlıkların hepsi bir yaşam döngüsünde yazılı hale getirilmelidir.

Varlık yaşam döngüsünde yani envanterde tutulan tüm varlıklar oluşturulduğunda ya da kuruma transferi yapıldığında sahip atamaları yapılmalıdır. Varlık sahipleri; varlık envanterinin kaydedildiğinden, varlıkların uygun sınıflandırıldığından, erişim kontrol politikası dikkate alınarak varlıkların erişim kısıtlamalarını ve sınıflandırılmasını tanımlamalı ve varlıkların silinme veya imha edilmesi durumunda uygun işlemlerin yapıldığını kontrol etmelidir.

Bilgi ve varlıkların kabul edilebilir kullanımları tanımlanmalı, kullanıma dair kurallar belirlenip yazılı hale getirilmelidir.

İşe son verme durumunda çalışanlar ve diğer paydaşlar kuruma ait olan varlıkların iadesini yapmalı ve bu süreçler dokümante edilmelidir.

Bilginin, kurumdaki önemini belirleyerek o öneme göre koruma seviyesi oluşturmak için bilgilerin sınıflandırılması gerekmektedir. Bilgi ifşa edildiğinde veya yok edildiğinde kurumun bu durumdan ne kadar etkileneceğini ya da bilgilinin bütünlüğü bozulduğunda ne kadar etkileneceğini belirleyebilmek için gizlilik, bütünlük ve erişilebilirlik temel unsurları göz önüne alınarak prosedürler hazırlanmalı o prosedürler doğrultusunda bilgi sınıflandırmaları yapılmalı ve varlıkların değerlerinde olabilecek değişiklikler takip edilerek sınıflandırmalar gözden geçirilmelidir.

Bilgi sınıflandırma düzeni ile bağlantılı olarak bilgilerin fiziksel, elektronik ortam, kayıt ortamları, basılı raporlar gibi etiketlendirmelerini ve varlıkların işlenmesini tanımlayan prosedürler oluşturulmalı ve uygulamalıdır.

Belirlenen ve benimsenen sınıflandırma düzenine göre varlıkların kullanım prosedürü geliştirilmeli ve uygulanmalıdır. Sınıflandırma ile tutarlı kullanım, işleme, depolama ve iletişim bilgisi için varlık kullanım prosedürü güncellenmelidir.

Depolanan bilginin açığa çıkarılmasını, değiştirilmesini, yok edilmesini önlemek; taşınabilir cihazların, teçhizatın kullanımı, bilgi varlıklarının, fiziksel varlıkların gerekmeyenlerinin geri kazanılamaz hale getirilmesi, taşınabilinir ortamın kaldırılması gerekiyorsa bunun için yetkilendirmeler dikkate alınmalı ve kayıt izleme logları saklanmalıdır.

İhtiyaç kalmayan ortamın yok edilmesi hususlarında bilgi güvenliğini sağlamak için yürütülmesi gereken gereklilikler prosedür ile tanımlanmalı ve yapılacak işlemler tutanak kayıtları oluşturularak tutulmalıdır.

Bilgi içeren ortam aktarım sırasında yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır. Bunun için de; güvenilir taşımacılık veya kuryeler kullanılmalı, paketleme oluşabilecek fiziksel hasarlardan korumak için üreticinin belirlediği tekniklere uygun yapılmalıdır.

5.5. Erişim Kontrolü (A.9)

Bilgi sistemlerine yapılan erişimlerin tanımlanan rol ve sorumluluklar çerçevesinde kullanıcının bilgiye erişiminin engellenmesi veya bilgi erişim yetkisi olan kullanıcının kayıt altına alınarak kontrollü yapılması ile ilgili maddedir. Sistemlere erişim kontrolünün nasıl gerçekleşeceğini belirlemek için üst yönetimden alt düzeyde çalışan kullanıcıya kadar hepsini kapsayan ve gerektiği kadar bilgi prensibini ilke edinen prosedür hazırlanmalı ve uygulamalıdır.

Bilgi güvenliğini sağlamanın en temel taşı erişim kontrolüdür. Erişim kontrollerinin iş gereklilikleri ilk ana maddesinde bilgiye erişimin kontrollü bir şekilde yapılmasını sağlamak için bir politikanın temel alınması, ağ ve ağ sistemlerine erişimlerin sınırlandırılması gerekliliği açıklanmaktadır. İkinci ana maddesi olan kullanıcı erişim yönetiminde, sistemlere kullanıcı erişimi açıklanmakta yani kullanıcı hesaplarının açılması kapatılması, yetkilerin düzenli aralıklarla gözden geçirilmesi, erişim haklarının kaldırılması veya düzenlenmesi konuları, kullanıcı sorumlulukları ana maddesinde de kullanıcıların kimlik doğrulama bilgilerinin muhafazasından kendilerinin sorumlu olduğu açıklanmaktadır. Dördüncü ana madde olan sistem ve uygulama erişim kontrolünde, kullanıcıların ve yöneticilerin sistemlere erişimlerinin kontrol edilmesi, erişim izni olmayanların sistemlere erişimlerinin kısıtlanması için ilkeler açıklanmaktadır. Aşağıda bu kontrol amaçları için gerekli olan kontrol maddeleri detaylı ele alınmaktadır.

Bilgi ve iş güvenliği ihtiyaçlarını kapsayan bir erişim kontrol politikası yazılmalı, düzenli olarak gözden geçirilerek takip edilebilirliği sağlamalıdır. Erişim mantıksal ve fiziksel olabilir. Fiziksel güvenlik erişim kontrolünde, bina girişine, sistem/sunucu gibi oda girişlerine sadece yetkili olan kullanıcıların girişleri sağlanmalıdır. Güvenlik görevlileri, kilitler ile bu kontrol bir miktar sağlanabilse de teknolojik kontroller, kimlik doğrulama,

izlenebilirlik ve yetkilendirme işlemleri ile bilgi sistemlerinin erişim kontrolü belirlenen erişim yetkilerine uygun olarak sağlanmaktadır. Erişim yetkileri belirli periyotlarla gözden geçirilmeli ve erişim talepleri, erişim haklarının yönetimi kayıt altında tutulmalıdır.

Kurum çalışanlarının hangi ağa ve ağ servislerine erişeceği belirlenmeli bu süreç için bir yetkilendirme ve kimlik doğrulama prosedürleri hazırlanmalı yönetim ve kullanıcılar bu prosedürleri bilmelidir böylece yetkisi olmayan kişilerin ağa erişmesi engellenerek güvenli bir ağ ve ağ sistemleri oluşturulmalıdır. Ağ erişimleri kayıt altın alınarak ağ hizmetlerinin kullanımı izlenmelidir.

Çalışanların rol ve sorumluluklarına uygun olarak resmi bir kullanıcı kaydetme ve silme süreci oluşturulmalı, kullanıcının erişim haklarında meydana gelebilecek değişiklikler düşünülerek takip sistemi oluşturulmalıdır.

Tüm kullanıcı türleri için sistemlere ve hizmetlere erişimin sağlanması ve geri alınmasını sağlamak için resmi bir erişim izni verme süreci olmalıdır. Bu süreçte kullanıcı rolleri ile tanımlanan erişim hakları tutarlı olmalı ve erişim politikasına uygun olmalıdır. Erişim haklarının kaydı merkezi olarak tutulmalı ve periyodik olarak gözden geçirilmelidir.

Ayrıcalıklı erişim hakları yönetimi ile ayrıcalıklı erişim tanımlaması gerçekten gerekli olan kullanıcılar belirlenmeli, hakların verilmesi ve kullanılması sınırlandırılmalı, tüm yetkilendirmeler ve ayrıcalıklı hakları kayıt altına alınmalı ve işleri ile ayrıcalıklı hakların doğrudan ilişkili olup olmadığı kontrol edilmelidir.

Gizli kimlik doğrulama bilgilerinin tanımlanması süreci oluşturmalı ve yönetimin oluşturup kullanıcıya verdiği gizli kimlik bilgilerini kullanıcılar kendi muhafaza etmeli, bir gruba ait olan gizli kimlik doğrulama bilgileri sadece o grup üyeleri tarafından bilinmeli ve korunması için bir taahhüt olmalıdır.

Kullanıcı erişim hakları gözden geçirilerek çalışanların pozisyonlarında değişiklik olursa veya rollerinde erişim hakları da bu pozisyona ve iş gerekliliklerine göre düzenlenmelidir. Kullanıcıların erişim hakları belirli periyotlarla varlık sahipleri tarafından gözden geçirilmelidir.

3. taraf ve kurum kullanıcılarından iş sözleşmesi veya anlaşması biten kullanıcıların bilgi sistemlerine erişim hakları kaldırılmalı veya askıya alınmalıdır. Sözleşmede bir değişiklik yapıldıysa da haklar yeni sözleşmeye göre düzenlenmelidir.

Kullanıcılar, kendi gizli kimlik doğrulama bilgilerinin kullanımından, emniyetinden kendi sorumludur. Parolaların gizli kimlik doğrulama bilgisi olarak kullanımında, parolalar güçlü belirlenmeli, ilk oturum açıldığında değiştirilmeli, güvenilir bir koruma ile kayıt altına alınmalıdır.

Bilgiye erişim kısıtlamasında, erişim kontrol politikasına göre sistem ve uygulamalara kullanıcıların erişim ve erişim haklarının kontrolleri sağlanmalı ve gerektiğinde kısıtlanmalıdır.

Erişim kontrol politikasına uygun olarak uygulamalara, sistemlere ve veri tabanlarına güvenli oturum açma prosedürü oluşturulmalı bu süreç güvenli oturum açılması işlemini kontrol etmeli, oturum açmada başarılı veya başarısız olan girişleri kayıt altına almalı, yetkisiz kişilerin oturum açmak için ihtiyaç duyacakları sistem ve uygulama hakkındaki bilgileri açığa çıkarmalıdır.

Parola yönetim sistemi ile yeterli nitelik seviyesinde güçlü parolalar belirlenmesi, kullanıcıların kendi parolalarını kendilerinin belirlemesi, değiştirebilmesi ve değişikliği belirli periyotlarla yapmaları sağlanmalıdır. Parola bilgilerinin tutulduğu dosyalar korunmalı, parolalar korumalı formatta saklanmalıdır.

Sistemin üzerinde değişiklik yapabilecek, ayrıcalıklı destek programlarının kullanımı sadece güvenilir kullanıcılara yetki verilerek kısa süreliğine tanımlanmalıdır. Uygulama yazılımları ile destek programları bir kategoride düşünülmemelidir.

Program kaynak koduna sınırlı erişimin sağlanması için bir kontrol prosedürü belirlenmeli, sistemin zarara uğratılarak kullanılmaz hale gelmesini önlemek için sıkı şekilde kontrol edilmelidir.

5.6. Kriptografi (A.10)

Kriptografi, okunabilir bir bilgiyi şifreleyerek anlaşılamaz hale getirerek güvenli ortamda bilginin deşifre edilmesi yöntemidir. Kriptografi kontrollerinde, bilginin gizliliğinin ve bütünlüğünün korunması için gerekli politika belirlenmeli ve anahtar yönetimi süreci oluşturulup uygulanmalıdır.

Kriptografik kontrollerin kullanımına ilişkin politika gizlilik, bütünlük, inkar edilemezlik ve kimlik doğrulama gibi bilgi güvenliği politika amaçlarını da karşılayacak kriptoloji

tekniklerinden minimum risk ve maxsimum verim almak ve hatalı kullanımı önlemek için uygulanmalıdır.

Kriptografik anahtarların üretimi, kullanımı, korunması, imha edilmesi, şifrelenmiş bir bilginin ele geçirilmesi veya hasar görmesi durumunda nasıl geri alınacağı yani bir anahtar yaşam döngüsü ile ilgili anahtar yönetim süreci oluşturulmalı ve uygulanmalıdır.

5.7. Fiziksel ve Çevresel Güvenlik (A.11)

Fiziksel ve çevresel güvenlik iki alt ana madde ve 15 kontrol maddesi ile karşımıza çıkmaktadır. İlk ana maddede bilgi varlıklarına yönelik olarak binaya, bilgi işleme alanları gibi fiziki çevreye nasıl bir sistem ile erişim sağlanarak güvence altına alınacağı, ikinci ana madde de teçhizat güvenliğinin nasıl sağlanacağı konularına detaylı yer verilerek bilgi işleme varlıklarımızın kasıtlı veya kasıtsız karşılaşacağı tehditlere karşı almamız gereken önlemler anlatılmaktadır.

Kurum veya kuruluş kritik bilgi sistemleri ortamlarının nasıl korunacağı ile ilgili sınırlarını tanımlamalı ve bu sınırlar dahilinde güvenlik kontrolleri uygulanmalıdır. Bu fiziksel sınırda uygulanması gereken alt yapı ve çevresel önlemler risk değerlendirme sonuçlarına göre belirlenmeli, sınırların içindeki varlıkların önemine göre kart kontrollü girişler, güvenlik görevlisi, iç ve dış tüm duvarlar yetkisiz fiziksel erişime karşı dayanıklı olmalı ve bu sınıra ulusal ve uluslararası standartlara uyumlu olarak kamera, saldırı algılama ve yangın sistemleri takılarak izlenmelidir.

Güvenli ve kritik alanlara sadece yetkili personelin erişimine izin verilecek fiziksel giriş kontrolleri uygulanmalıdır. Ziyaretçilerin giriş ve çıkışları kayıt altına alınmalı, güvenli alanlara erişimler kontroller gerçekleştirilerek sadece yetkili olan personel ile sınırlanmalı ve hakları düzenli olarak gözden geçirilmeli, kurum dışı personelin kritik alanlara erişimleri sadece gerektiğinde ve kısıtlı olmalıdır.

Ofis, oda ve tesislerin güvenliğinin sağlanması için kritik verilerin olduğu alanlara erişimde kontroller alınmalı, kritik tesisler kolayca ulaşılamayacak şekilde konumlandırılmalı ve tabela, işaret gibi yerini belli edecek şeyler kullanılmamalıdır.

Yangın, deprem, sel gibi doğal afetler ve insan kaynaklı tehditlere karşı fiziksel koruma tedbirleri alınmalı ve uygulanmalıdır.

Güvenli alanlar hakkında personel yeterli olacak kadar bilgi bilmeli, kamera, telefon gibi kayıt cihazları ile alanlara girmemeli ve 3. taraf çalışanların alanlara refakatçi eşliğinde girmesi sağlanmalı ve kayıt altına alınmalıdır.

Dağıtım ve yükleme alanları ile yetkisiz kişilerin kuruma gireceği alanlar mümkünse bilgi işleme tesislerinden ayrı tutulmalı, girişler yetkilendirilmiş personeller ile sınırlandırılmalı, teslim alınan ürünlerin doğruluğu ve sağlamlığı kontrol edilerek kayıt altına alınmalıdır.

Teçhizatlar yerleştirilirken oluşabilecek tehditlere karşı önlemler alınmalı, gereksiz ve yetkisiz erişimler asgari düzeyde tutulabilecek şekilde yerleştirilmelidir. Sistem odası veya kritik veri içeren araçlar yetkisiz kişilerce erişilemeyecek ve hatta gözlemlenemeyecek şekilde kontrol altına alınmalı, bu alanlarda nem, ısı kontrolü, su sensörü, kabinetlerin ayaklarının sabitlenmesi gibi gerekli kontroller yapılarak teçhizatlar korunmalıdır.

Elektrik, su, gaz, kanalizasyon, havalandırma gibi destekleyici alt yapı hizmetlerinden kaynaklanan bozulma veya kesintilerden teçhizatların korunması için iş sürekliliği testleri yapılmalı, ekipmanların bakım ve kontrolleri düzenli gerçekleştirilmelidir.

Sistem odası gibi bilgi barındıran yerlerdeki güç ve iletişim kabloları dinleme ve fiziksel etkilere karşı tedbirler alınarak korunmalı, güç ve iletişim kabloları birbirinden ayrılmalı, kablolar yer altında olmalı ve hassas bilgiler için ekstra güvenlik önlemleri alınmalıdır.

Kurum içerisinde bakımı olan teçhizatlar yasal yükümlülüklere ve üretici firmasının önerdiği periyot ve şartlarda, yetkili ve yetkin personel tarafından yapılmalıdır. Teçhizat bakım için kurum dışına çıkarılacaksa veya kurum dışı personel yapacaksa gerekli kontroller yapılmalı, gerekirse içindeki hassas bilgiler temizlenmelidir.

Ekipman, bilgi veya yazılımın kurum dışına çıkarılması gerektiğinde uyulması gereken bir kontrol mekanizması oluşturulmalı ve işlemler kayıt altına alınmalıdır.

Kurum dışındaki teçhizat ve varlığın kurum dışında olmasının getirdiği riskler göz önüne alınarak gözetim altında tutulmalı ve gerekli güvenlik uygulanmalıdır. Ev veya farklı bir lokasyondan yani uzaktan çalışma için detaylı risk değerlendirme yapılmalı ve ilgili tedbirler alınmalıdır.

Teçhizatın depolama ortamı içeren tüm parçaları elden çıkarılmadan veya tekrar kullanılmadan önce kontrol edilmeli, hassas bilgi içeren depolama ortamları fiziksel imha

edilmeli veya format veya standart silme işlemleri yerine bilgiyi tamamen yok eden teknikler kullanılarak depolama cihazındaki bilgiler yok edilmeli, lisanslı yazılım varsa kaldırılmalı veya güvenli şekilde üzerine yazılması sağlanacak kontroller yapılmalıdır.

Gözetim altında olmayan teçhizatın korunmasını kullanıcı sağlamaya çalışmalı bunun için kullanıcılar sorumluluklarının ve güvenlik gereklerinin farkında olmalıdır.

Kağıtlar, depolama aygıtı gibi ortamları kapsayarak bilgi veya veri kaybını azaltmak için temiz masa temiz ekran politikası oluşturulmalıdır. Bu politikaya göre kullanıcılar bilgisayarının başından ayrılırken mutlaka kapatmalı veya ekranı kilitleyerek yetkisiz erişimleri önlemeli, hassas bilgiler masa üzerlerinde veya çoğaltma cihazlarının üzerinde bırakılmamalıdır. Çok kritik bilgiler doğal afetlere karşı korumalı yanmaz kasalarda muhafaza edilmelidir.

5.8. İşletim Güvenliği (A.12)

ISO 27001:2013 sürümü öncesinde haberleşme ve işletim yönetimi ana maddesi altında incelenmekteydi 2013 sürümü ile İşletim Güvenliği ana maddesi başlığını alarak 7 alt madde ve 14 kontrol maddesi içermektedir. Bu ana maddelerle bilgi işleme sistemlerinin güvenli ve doğru işletilmesini, sistemlerin ve bilginin zararlı yazılımlardan korunmasını, veri kaybının yaşanmamasını, olay kayıtlarının tutulmasını, işletim sistemlerinin bütünlüğünü, teknik zafiyetlerin kötüye kullanılmamasını, denetim faaliyetlerinin işletim sistemleri üzerindeki etkisinin azaltılmasını, sağlamayı amaçlanmaktadır.

İşletim prosedürleri dokümante edilmeli, sadece yetkili kişiler tarafından onaylanmalı ve gerektiğinde güncellenmelidir. İhtiyacı olan tüm kullanıcılar gerektiğinde oluşturulan bu prosedürlere ulaşabilmeli ve bu prosedürlerin içinde sistem kurulumu, destek elemanlarının iletişim bilgileri, kurtarma prosedürleri, sistem denetim takibi yönetimi gibi talimatlar yer almalıdır.

Kurum iş faaliyetlerinin kesintiye uğramaması için iş süreçleri, bilgi işleme tesisleri ve sistemlerinde ki bilgi güvenliğini etkileyen değişiklikler kontrol edilmeli, değişiklik yapıldığında da değişikliklerin planlanması test edilmesi, resmi onay prosedürleri, gereksinimlerin karşılandığının doğrulanması, başarısızlık durumunda geri dönüş prosedürleri gibi tüm adımları içeren bir denetim kaydı tutulmalıdır.

Kapasite yönetimi ile kurumun yürüttüğü iş ve işlemlerin sürekliliğini ve sistem performansını sağlamak için kaynaklar izlenmeli, sorun yaşanmaması için gerekli önlem ve tedbirler alınmalı, gelecekteki kapasite gereksinimi için tespitler ve planlamalar yapılmalıdır. Sistemlerin verimliliğini artırmak için kaynak yönetimi uygulanmalıdır. Uzun tedarik süresi ve yüksek maliyet varsa özel ilgi gerekmektedir. Kapasite yönetiminde, kullanılmayan verinin silinmesi, veri tabanlarının hizmetten çıkarılması, sorguların optimize edilmesi, toplu proseslerin optimizasyonu, bant genişliğinin ayarlanması gibi kritik hususlar yer almaktadır.

İşletim ortamlarındaki yetkisiz erişim ve değiştirmeye ilişkin olarak doğan riskleri en aza indirmek için geliştirme, test ve işletim ortamları birbirinden ayrılmalıdır. Böylece kazara veya bilgi eksikliği ile yapılıp operasyonel bilgilere zarar verecek, ciddi sorunlara neden olabilecek tehditler önlenmiş olabilir. Bunun için farklı sistem ve bilgisayar işlemcilerinin kullanılması, testlerin işletimdeki sistemler üzerinde yapılmaması, yazılım işletim durumuna transferi için kural tanımlanması, farklı kullanıcı profillerinin oluşturulması, hassas verilerin eşdeğer kontrolleri sağlamadan test ortamına atılmaması hususlarına dikkat edilmelidir.

Kötücül yazılımlardan korunmak için, tespit ve kurtarma kontrolleri yanında kullanıcı farkındalığı da oluşturulmalıdır. Kötücül yazılımlara karşı korumada; yetkisiz yazılım kullanımını yasaklayan bir politika kurulması, özel koruma gerektiren kısımların belirlenmesi, kritik iş proseslerinin resmi olarak araştırılması, önceden belirlenen bir bütüne bağlı olarak bilgisayarların taranması, yedekleme prosedürlerinin hazırlanması, çevresel tehditlerin ve fiziksel risklerin en aza indirgenmesi ve bu konularda gerekli eğitimlerin verilmesi gerekmektedir.

Yedekleme, veri kaybını engellemek için yapılır. Bilgi varlıkları için yedekleme politikası hazırlanmalı bu politikada, saklama ve koruma koşulları tanımlanmalıdır. Yedekleme tesisleri, bir hata olduğunda tüm yazılımın telafi edilebilir olmasını sağlamalıdır. Yedekleme planı yapılırken yedekler, merkezden uzak bir yerde muhafaza edilmeli, uygun fiziksel ve çevresel korunma sağlanmalı, yedekleme ortamı düzenli aralıklarla test edilmeli, gizli veri durumunda da yedekleme şifre ile korunmalıdır.

Kullanıcı işlemleri, kural dışı olaylar, hatalar ve bilgi güvenliği olaylarına ait olayın gerçekleştiği tarih, süre, kullanıcı kimliği, olay açıklaması gibi bilgileri içeren kayıtlar üretilmeli, saklanmalı ve düzenli gözden geçirilmelidir.

Kaydı gerçekleştiren cihazlar ve olay kayıtları yetkisiz erişimlere, verinin değiştirilmesi veya silinmesine karşı korunmalıdır. Bunun için kayıt dosyalarının düzenlenmesi, kayıt dosyası depolama kapasitesinin kontrolü takip edilmelidir.

Hesap verilebilirliği sağlamak için ayrıcalıklı haklara sahip olan sistem yöneticileri ve operatörlerinin faaliyetleri de kayıt altına alınmalı ve düzenli olarak gözden geçirilmelidir.

Kurumdaki tüm bilgi sistemlerinin saatleri doğru ve tek bir referans zaman kaynağı ile senkron çalışmalıdır. Zaman gösterimi için; sözleşme gereksinimleri, yasal, düzenleyici, iç ve dış gereksinimler yazılı hale getirilmelidir.

İşletimsel sistemlerin bütünlüğünü sağlamak amacıyla sistemlere yazılım kurma kontrolü prosedürlerle uygulanmalıdır. Kurumda, desteklenmeyen yazılımlara dayanan risklere dikkat edilmeli, yeni bir sürüme yükseltme işlemleri dokümante edilmeli ve yeni sürüm kararlı bir şekilde çalışana kadar eski sürümler saklanmalıdır.

5.9. Haberleşme Güvenliği (A.13)

Haberleşme güvenliğinde amaç kurum içindeki bilginin ve kurumla dış çevre arasındaki iletişim mekanizmalarının güvenliğini sağlamaktır. Haberleşme güvenliği 7 kontrol maddesinden oluşmaktadır. Bu maddeler şu şekilde açıklanabilir:

Ağ kontrollerinde yöneticiler tarafından yetkisiz erişimlerin engellenmesi için gerekli sorumluluklar, prosedürler ve roller belirlenmelidir. Buna uygun bilgisayar sistemleri kurulmalıdır. Kablosuz ağlardan geçen veriler için özel kontrol mekanizmaları kullanılmalıdır. Bilgi güvenliği faaliyetlerini denetlemek için gerekli loglama mekanizmaları kurulmalı ve sistemlerin ağa bağlantıları denetim altında olmalıdır.

Kurum içerisinden ya da kurum dışından sağlanan tüm ağ hizmetlerinin güvenlik mekanizmaları ve hizmet yönetimleri tespit edilmelidir. Kurum bu hizmetlerin güvenli bir şekilde yönetiminin sağlanmasından da emin olmalıdır. Bunun için kimlik doğrulama, şifreleme, güvenli bağlantı için teknik parametreler gibi ağ hizmeti güvenlik önlemleri uygulanmalıdır.

Ağlar gereksinimlerine ve etki alanlarına göre ayrılmalıdır. Bu etki alanlarında sınırlar iyi belirlenmelidir ağlar arasında gerekli geçiş izinleri olmalıdır ama bu geçişler güvenlik

duvarı, filtreleme gibi teknolojilerle kontrol edilmelidir. Ağları ayırırken performans ve maliyet gibi seçeneklerde değerlendirilmelidir.

Bilgi transferinin güvenli sağlanması için gerekli prosedürler ve kontroller belirlenmelidir. Bunların içerisinde dinleme, kopyalama, ele geçirme olaylarını önlemek için gerekli prosedürler, kötücül yazılımlara karşı belirlenen prosedürler, elektronik cihazlarının kullanımını açıklayan kılavuzlar, tüm iş yazışmalarının saklanma ve imha prosedürleri yer alır. Ayrıca bütün personel bu prosedürler hakkında bilgilendirilmeli ve kamuya açık, güvenli olmayan alanlarda gizli bilgileri paylaşmamaları konusunda uyarılmalıdır.

Bilginin güvenli transferinin yapılabilmesi için kuruluşlar ve 3. Taraflar arasında antlaşmalar yapılmalıdır. Bu antlaşmalarda; iletim, izlenebilirlik, paketleme için gerekli teknik prosedürler belirlenmeli, bilgi kaybı durumundaki sorumluluklar tespit edilmelidir. Fiziksel transfer ortamı içinde gerekli standartlar oluşturulmalı ve sürdürülebilmelidir.

Elektronik mesajlarda gerekli kontrol mekanizmalarının içinde; mesajın yetkisiz erişime ve değiştirilmeye karşı korunması, mesajın doğru bir şekilde taşınması, dış hizmet kullanım öncesi onay mekanizmasının olması, halka açık ağlarla ilgili güçlü bir kimlik doğrulama mekanizmasının belirlenmesi gibi kontroller mevcuttur.

Gizlilik ve ifşa etmeme antlaşmaları kurum çalışanlarına ya da dış taraflara uygulanır. Bu kapsamda; korunacak bilginin tanımı, bilginin nasıl korunması gerektiği, antlaşmanın süresi, ifşa durumundaki gerekli sorumluluklar ve prosedürler, antlaşma bitiminde yapılması gerekenler, antlaşma ihlali durumunda yapılması gerekenler gibi mekanizmalar yer almaktadır. Bu antlaşmalar belirli periyotlarla değişen gereksinimlere göre güncellenmelidir.

5.10. Sistem Temini, Geliştirme ve Bakımı (A.14)

Bu maddenin amacı, bilgi güvenliği sistemi altyapısının ve bu sistem dahilindeki uygulamaların güvenliğini sağlamak ve yeni güvenlik gereksinimlerini belirlemektir. Bu çerçevede gerekli güvenlik mekanizmaları belirlenir. Üç alt maddede toplam 13 kontrol maddesinden oluşmaktadır.

Bilgi güvenliği ile ilgili prosesler tasarım aşaması gibi erken süreçlerde oluşturulduğunda daha etkili ve az maliyetli çözümler sağlanabilir. Bunun için yetkilendirme ve erişim prosesleri, kullanıcı görev ve sorumlulukları belirlenmelidir. Kayıt ve izleme ara yüzleri

tasarlanmalıdır, halka açık ağlara hizmet verilmesi durumunda özel kontroller eklenmeli eğer ürün satın alınma durumu varsa da test ve satın alınma süreci de eklenmelidir.

Halka açık ağlar üzerindeki uygulama hizmetlerinde kimlikler için gerekli güven seviyesi oluşturulmalı, yetkilendirme prosesleri ve gizli bilgiyi koruma adımları tanımlanmalıdır. Sipariş bilgilerinin gizliliği ve sigorta gereksinimleri belirlenmeli, gerekli kriptografi kontrol adımları eklenmeli ve hizmetler bir antlaşma ile desteklenmelidir.

Uygulama hizmet işlemlerinde mesajın korunması sağlanmalıdır. Bunun için elektronik imza kullanımı, haberleşme yolunun şifrelenmesi, iletişimin protokollerle güvence altına alınması mesajların doğrudan erişilebilir bir ortamda tutulmaması ve tüm sürecin bir sertifika yönetim süreci ile desteklenmesi sağlanmalıdır.

Güvenli geliştirme politikası hizmet içinde yer alan yazılım ve sistem kurulumu için gerekli bir adımdır. Bunun içerisinde, Geliştirme ortamının güvenliği, yazılım metodolojisinin güvenliği, güvenli veri depoları, güvenli kod kılavuzları, geliştiricilerin güvenlik açıklarını onarma yetenekleri, uygulama versiyonlarının güvenliği gibi hususlar yer almalıdır.

Sistem değişiklik prosedürleri tasarımdan bakıma kadar bütün sistemleri ve ürünleri kapsayacak şekilde yazılı hale getirilmeli ve zorunlu tutulmalıdır. Yapılacak bütün değişikliklerde resmi prosesler takip edilmelidir. Bu kontrol prosedürlerinin içerisinde, yetkili kullanıcıların belirlenmesi, kritik kod kontrollerinin yapılması, iş başlangıcında önce onay alınması, versiyon kontrolü yürütülmesi, bir denetim zincirinin kurgulanması, değişiklik yapılırken işleyen proseslerin olumsuz etkilenmemesinin temin edilmesi gibi maddeler yer almalıdır.

İşletme platformları değiştirildiğinde sistemleri olumsuz etkilememesi için gerekli prosedürler uygulanmalıdır, değişikliklerden birimlerin zamanında haberdar edilmesi, iş planına göre hareket edilmesi, kontrol prosedürlerinin uygulanması bunun için gerekli adımlardandır.

Yazılım paketleri mümkün olduğunca değiştirilmeden kullanılmalıdır. Değişiklik yapılacaksa da sıkı bir şekilde kontrol edilmelidir. Değişiklik yapılırken üretici onayının olup olmadığı, diğer yazılımlarla uyumluluk süreci, ele geçirilme riski, güncelleme kontrolleri gibi adımlara dikkat edilmelidir. Tüm değişiklikler gelecekteki güncellemeler için test edilmeli ve yazılı hale getirilmelidir, orijinal yazılımda saklanmalıdır.

Güvenliği sistem mühendisliği yazılı ve sürdürülebilir olmalıdır yeni teknolojilere ve güvenlik risklerine karşı gözden geçirilmelidir. Kurum içindeki bilgi sistemine uygulanabilmelidir. Güvenlik mühendisliği esasları dış kaynaklı bilgi sistemlerine de uygulanmalıdır.

Güvenli geliştirme ortamı, sistemi oluşturan insanları, kullanılan teknolojileri ve ilgili prosesleri kapsar. Güvenli geliştirme ortamı oluşturulurken çalışan personelin güvenliği, erişim kontrolü, ortamdaki kod değişiklilerinin izlenmesi, yedeklerin güvenli yerde saklanması, veri hareketlerinin izlenmesi gibi hususlara dikkat edilmelidir.

Sistem geliştirme dış kaynaklı satın alındığında, ilgili lisans antlaşmalarına, mülkiyet haklarına, kabul testlerine, güvenlik değerlerinin tam olmasına, yeterli derecede test edilip edilmediğine, dokümantasyonun eksiksiz olmasına ve yasalar çerçevesinde kontrollerinin yapılıp yapılmadığına dikkat edilmelidir.

Sistemler, kapsamlı bir doğrulama ve test süreci gerektirir. Kurum içi geliştirmelerde bu testler başlangıçta geliştirme ekibi tarafından yapılmalı, bağımsız kabul testleri ise sistemin çalışmasını sağladıktan sonra yapılmalıdır.

Sistem kabul testi, sistemin geliştirildiği uygulamalarla uyumlu olmalıdır. Testler bileşenler ve bütünleşik sistemler üzerinde gerçekçi bir test ortamında yapılmalıdır. İlgili hataların giderildiği mutlaka doğrulanmalıdır.

Sistem testlerinde mümkün olan en yüksek hacimli test verisi kullanılabilir. Test verisi, dikkatli bir şekilde seçilmelidir. Test amacı ile gizli verilerin kullanımından kaçınılmalıdır. Test işlemi tamamlandığında test ortamındaki bilgiler silinmelidir. Bütün prosedürler test verilerine de uygulanmalıdır böylece test verilerin korunması sağlanmalıdır.

5.11. Tedarikçi İlişkileri (A.15)

Kurum varlıklarına erişen tedarikçilerle bilgi paylaşımlarında güvenliği sağlayabilmek için kurum tarafından belirlenen gerekliliklerin tedarikçiler tarafından kabul edildiğini belgeye dayalı gösterilmesi hedeflenmektedir. Bunun için 2 alt madde ve 5 adet kontrol maddesi vardır.

Tedarikçinin kurum varlıklarına erişimlerinde doğabilecek riski azaltabilmek için tedarikçi türleri belirlenmeli, türlere göre erişim izinleri tanımlanmalı ve erişimler kontrol altında

tutulmalıdır. Bilgi güvenliği yönetiminin yeterli ölçüde sağlanabilmesi için tedarikçilerle bilgi güvenliği şartları karşılıklı belirlenmeli ve dokümante edilmelidir.

Kurumun bilgisine erişebilen, depolayan ya da bilgi işleme altyapısını sağlayan tedarikçiler ile bilgi güvenliği riskleri ve gereksinimleri, her iki tarafın yükümlülüklerini açıkça belirleyen anlaşmalar ile hazırlanmalıdır. Bu antlaşmalarda, tedarikçinin erişeceği bilginin tanımı, veri sızdırılması, telif hakları gibi konular, çalışma süresi boyunca kurumun güvenlik gereksinimlerinin uygulanması ve tedarikçinin yükümlülükleri, sözleşmenin bitmesinden itibaren gizliliğin korunmasına yönelik hususlar yer almalıdır.

Tedarikçi ilişkileri için belirlenen genel bilgi güvenliği şartlarının dışında bilgi ve iletişim teknolojileri servisleri ve ürün tedarik zincirleri ile ilgili bilgi güvenliğini sağlamak için gerekli olan şartlar da açıkça belirlenmelidir. Kurumun güvenlik gereksinimleri tedarikçi ve alt tedarikçiler tarafından bilinmeli ve bilgi iletişim, teknoloji ürün ve hizmetlerinin dağıtımında bu gereksinimler uygulanmalıdır.

Kurum, tedarikçi hizmetlerinin bilgi güvenliği gereksinimlerine ve belirlenen şartlara uygun yapılıp yapılmadığını tespit etmek için tedarikçi hizmetlerini izlemeli ve gözden geçirmelidir. Bu kapsamda, tedarikçilerin yapılan antlaşmalara uyumluluğu, bilgi güvenliği ihlal olayları hakkındaki bilgileri, sorunları tespiti ve çözümdeki etkisi hususları kontrol edilmelidir.

Tedarikçi servislerinde yapılan değişiklikler, süreçlerin kritikliği ve iş bilgisi dikkate alınarak yürütülmeli ve bilgi güvenliği politika, prosedür ve kontrollerin sürdürülebilmesini de içermelidir.

5.12. Bilgi Güvenliği İhlal Olayı Yönetimi (A.16)

Bilgi güvenliği ihlal olaylarının yönetiminde sürekli ve etkili bir yaklaşım izlemek için yönetim sorumlulukları belirlenmeli, bilgi güvenliği olayları ve zayıflıkları raporlanmalı, güvenlik olaylarına müdahale edilip kanıtlar toplanmalıdır. Bilgi güvenliği ihlal yönetiminin gerçekleştirilmesi için 7 kontrol maddesi vardır.

Bilgi güvenliği ihlal olaylarına hızlı ve sorunsuz müdahale edilebilmesi için sorumluluklar ve prosedürler belirlenmelidir. Böylece yönetim ile uzlaşarak bir bilgi güvenliği sorumluluk ve prosedürleri belirlenerek ihlal olaylarının tespiti, müdahalesi, raporlanması daha hızlı ve etkili hale getirilebilir ve kurum içinde yeterince duyurulabilir.

Bilgi güvenliği olayları ile karşılaşan kurum çalışanları veya yükleniciler karşılaştıkları, bilginin gizlilik, bütünlük, erişilebilirlik ihlalleri, insan hataları, fiziksel güvenlik ihlalleri gibi olayları olabildiğince hızlı bir şekilde belirlenen iletişim noktalarına bildirmelidir.

Kurumun bilgi işleme altyapısını ve hizmetlerini kullanan kullanıcılar ve yükleniciler, sistemlerde veya aldıkları hizmetlerde bir güvenlik açığı olduğunu düşünürlerse bunu kanıtlamaya çalışmadan belirlenen iletişim kanallarına bu açıklığa dair gözlemlerini veya şüphelerini raporlamalıdır.

Bilgi güvenliği olayları değerlendirilmeli ve bu olayların bilgi güvenliği ihlal olayı sayılıp sayılmayacağı ihlalleri sınıflandırma ölçeğine göre belirlenmelidir. İhlal olayı değerlendirme sonuçları kayıt altına alınmalıdır.

Bilgi güvenliği ihlal olaylarına prosedürlere uygun olarak deliller toplanmalı, yetkili kurum personeli veya dış taraflarca iletişime geçilmeli, ihlal olayına sebebiyet veren zafiyet varsa oda belirlenmeli ve ihlal olayına müdahale edilmelidir.

Bilgi güvenliği ihlal olaylarının giderilmesi sırasında kazanılan deneyimler gözden geçirilip kayıt altına alınmalıdır. Böylece herhangi bir ihlal olayının tekrarlanmaması veya tekrarlanması durumunda soruna daha kısa sürede çözüm bulunması sağlanır.

Kanıt niteliği taşıyabilecek her türlü bilginin tanımlanması, toplanması, korunması için prosedür tanımlanmalı ve uygulanmalıdır. Kurum bilgi güvenliği ihlal olayları ile ilgili kanıt olabilecek tüm kayıtların bütünlüğü korunmalı çünkü sadece bütünlüğü korunmuş kayıtlar kanıt olarak kullanılabilir.

5.13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları (A.17)

Kurumun iş sürekliliği yönetim sistemlerine bilgi güvenliği hususlarının da dahil edilip, iş devamlılığı planları oluşturulmalı, yedekleme sistemleri devreye alınmalıdır. İş sürekliliği yönetiminin bilgi güvenliği hususları iki alt ana madde ve dört kontrol maddesinden oluşmaktadır.

Kurum bilgi güvenliği sürekliliğinin sağlanmasını iş sürekliliği sürecinde veya olumsuz durumlarda yangın, sel gibi felaket kurtarma sürecince ele alacağını belirlemeli ve bilgi güvenliği gereksinimlerini planlamalıdır.

Kurum bir olumsuz durum karşısında bilgi güvenliği için istenen düzeyde iş sürekliliğini sağlayabilmek için gereken kontrolleri belirlemeli ve yazılı hale getirmelidir. Belirlenen bu prosedürleri, yetkinliğe sahip personel ile hayata geçirmeli ve sürdürmelidir.

Kurum bilgi güvenliği sürekliliği için oluşturduğu iş süreci veya felaket durumu iş sürekliliği proseslerinin olası durumlarda geçerli ve uygulanabilir olduğunu belirli aralıklarla test etmelidir.

Bilgi işleme araçlarına erişim söz konusu olmama durumu yaşanmaması için yeterli fazlalık yani yedekli bileşenler hazırlanmalı ve gerektiğinde erişimin bu yedekli bileşenden sağlanmalıdır.

5.14. Uyum (A.18)

Bilgi sistemlerinin kurulumunda, kullanımında yasal ve sözleşmeye tabi gereksinimlere, bilgi güvenliği kurumsal politika ve prosedürlerine uyum gerekmektedir. Bununla ilgili standartta 2 alt madde ve 8 kontrol maddesi vardır.

Kurum ve yöneticiler, bilgi sistemleri ile ilgili tüm yasal, meşru, düzenleyici, sözleşmeden doğan gereksinimleri belirlemeli, yazılı hale getirmeli ve güncel tutmalıdır.

Her bilgi sistemi ve kurum için fikri mülkiyet hakları ve tescilli yazılım ürünlerinin kullanımında tüm yasal ve sözleşmeden doğan gereksinimler açıkça tanımlanmalıdır. Telif haklarının ihlal edilmemesi, sadece yetkili yazılım ve lisanslı ürünlerin kullanılması, lisans çerçevesinde belirlenen kullanıcı sayısının aşılmaması, fikri mülkiyet hakları öneminin ve farkındalığının personele duyurulmasına dikkat edilmelidir.

Kayıtlar; kaybolması, silinmesi, değiştirilmesi, yetkisiz erişimlerden korunması için sınıflandırılmalı ve yasal, düzenleyici ve iş şartlarına uygun olarak korunmalıdır. Kayıtların saklanmasında, gerekli veriyi belirlenen zaman diliminde geri getirilebilmesine, gelecek teknolojilere taşınabilir olmasına, ulusal ya da bölgesel yasalara göre belirlenen saklama sürelerine uyulmasına dikkat edilmelidir.

Kişi tespit bilgilerinin mahremiyeti ve korunması için ilgili yasalara ve düzenlemelere uygun bir politika geliştirilmeli ve uygulanmalıdır. Bu politika bu alanda çalışan her personele duyurulmalı ve bilgilerin korunması için önlemler alınmalıdır.

Yasa, düzenleyici ve iş şartlarına uygun olarak kriptografik fonksiyonlar için kullanılan bilgi sistemleri, şifre kullanımıyla ilgili kısıtlamalar dikkate alınmalıdır.

Kurumun bilgi güvenliği ve uygulamasının bağımsız gözden geçirilmesi kurum üst yönetimi tarafından başlatılmalı, inceleme o alandan bağımsız bireyler tarafından yapılmalı, politika, prosedür ve kontrollerde değişiklik yapmak ve geliştirmek için gözden geçirmeler fırsat sunmalıdır. Bağımsız gözden geçirme sonuçları kayıt altına alınmalı, sonuçta eğer kurumun bilgi güvenliği yönetiminde eksiklikler bulunursa bu eksiklikleri gidermek için düzeltici faaliyetler oluşturulmalıdır.

Yöneticiler, güvenlik politikalarına, standartlarına ve diğer güvenlik gereksinimlerine kendi sorumluluk alanlarında bulunan bilgi işleme ve prosedürlerinin uyumlu olması için gözden geçirmeler yapmalı, uygunsuzluk bulunursa de giderilmesi için çalışmaları yürütmeli, bu çalışmaları kayıt altına almalıdır.

Bilgi sistemlerinin, kurumun bilgi güvenliği politika ve standartları ile uyumu, teknik uyum ise teknik uzman ve otomatik araçlar ile sızma testleri ve açıklık değerlendirmeleri varsa da planlanarak uyumluluk testleri yapılmalı ve sistemler düzenli olarak gözden geçirilmelidir.

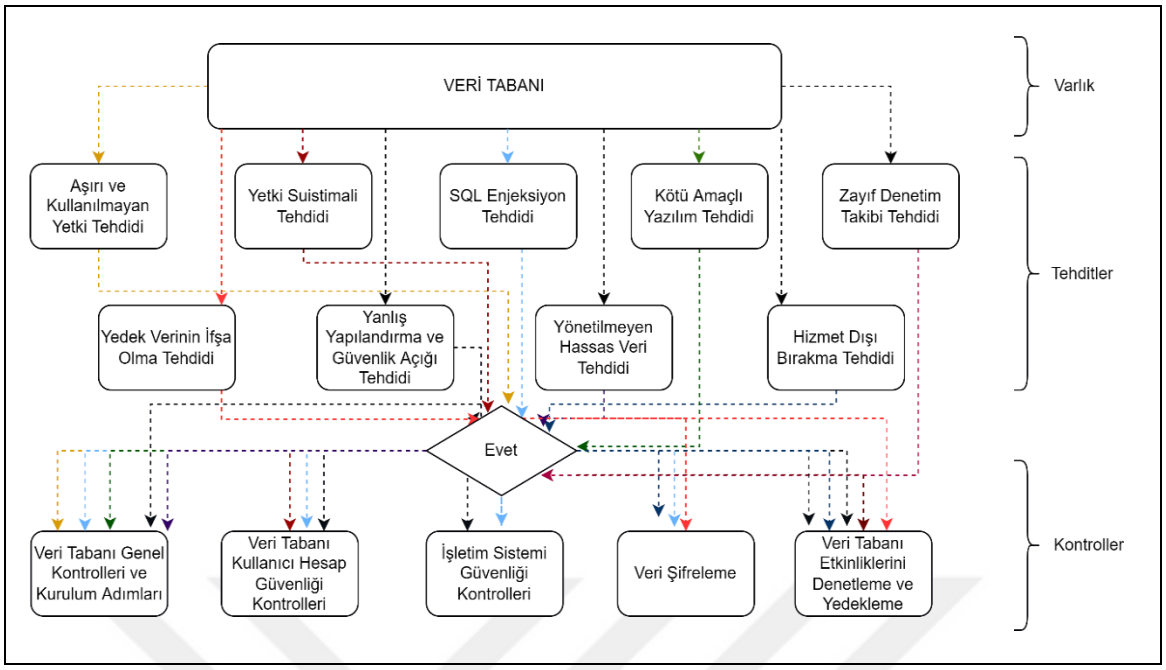
6. YÖNTEM

Veri tabanları, bilgi sistemlerinin merkezinde bulunan kurumların veya bireylerin hassas verilerinin tutulduğu en önemli araçlardan biridir. Veri tabanlarını kullanan uygulamaların sayısı her geçen gün artmakta ve çoğalan verilerin kritikliği nedeniyle de veri tabanları yüksek risk seviyesinde bulunmaktadır. Veri tabanı yönetim sistemlerini ISO/IEC 27001 standardına uyumlu hale getirerek veri tabanı güvenliği üst seviyede sağlanabilmektedir.

Veri tabanı yönetim sistemleri pek çok katmanla birlikte çalıştığından ISO/IEC 27001 Standardı gereksinimlerinde de veri tabanını ilgilendiren maddeleri tek başlık halinde bulmak mümkün değildir. Veri tabanı yönetim sistemleri fiziksel ve çevresel güvenlikten iş sürekliliğine kadar pek çok kontrol maddesiyle ilişkilidir. Bu nedenle beşinci başlık altında tek tek açıklanan kontrol maddelerinden veri tabanı yönetim sistemini doğrudan veya dolaylı ilgilendirenler sınıflandırılarak veri tabanı üzerinde nasıl uygulanacağı 6 ana başlıkta ele alınacaktır. Bu başlıklar şu şekildedir:

1. Veri tabanı genel kontrolleri ve kurulum adımları
2. Veri tabanı kullanıcı hesap güvenliği kontrolleri
3. İşletim sistemi güvenliği kontrolleri
4. Veri şifreleme
5. Veri tabanı etkinliklerini denetleme ve yedekleme
6. Veri tabanı özelinde hazırlanabilecek bilgi güvenliği dokümanları

ISO27001 gereksinimlerinin veri tabanı yönetim sistemlerinde uygulanabilirliğini yüksek seviyede sağlamak için; standartta tanımlanan kontrol maddelerinin tamamına tek bir çerçeve bakış açısı ile bakılarak veri tabanı sorumlularının yapmaları gerekenler tespit edilmeye çalışılmıştır. Bu başlıklar da, veri tabanı sorumlularının hem sürece hakimiyetini en üst seviyeye çıkarabilmeyi hem de uygulanabilirliği ve takibi kolaylaştırarak onlara BGYS'nin ek iş yükü getirmediğini göstermeyi hedefleyerek belirlenmiştir.



Şekil 6.1. Veri tabanı tehditleri ve kontrolleri

Şekil 6.1 akış diyagramında veri tabanı tehditleri ve bu tehditleri önlemek için gerçekleştirilecek kontroller yer almaktadır. Böylece veri tabanında var olduğu saptanan bir tehdidin akış diyagramı kullanılarak modellenmiş olan kontrolleri yapması gerektiği sağlanmış olacaktır. İş sürecinin her aşamasında veri tabanını etkileyen tehditleri ve açıklıkları kontroller ile engellemek veri tabanı güvenliği için gereklidir.

Büyük miktardaki verilerin güvenli tutulduğu, bilgilere bütünlük bozulmadan hızlı erişim imkanı sunan ve birden fazla kullanıcıya aynı anda bilgiye erişim imkanı sağlanan programlara İlişkisel Veri tabanı Yönetim Sistemleri (Relational Database Management Systems - RDBMS) denir. Başlıca ilişkisel veri tabanı sistemleri sıralarsak; Oracle, MSSQL, Sybase, DB2, MySQL gibi örnek programlar mevcuttur. Oracle veritabanı da bunlar içinde en gelişmişlerden, Dünyada ve Türkiye'de büyük kurumsal uygulamalarda en çok tercih edilen veri tabanlarından biridir.

Çalışmamızda tercih ettiğimiz Oracle veri tabanı yönetim sisteminin özelliklerine değinirsek; Oracle aynı anda on binlerce kullanıcıya veri bütünlüğünü bozmadan hizmet verebilmekte, büyük miktarda tutabildiği verilerin depolama alanlarında ayarlama yapabilme imkanı da sunmaktadır. 7/24 haftalarca hiç kapatılmadan çalışabilmekte, istemci sunucu mimarisinin bütün avantajlarını kullanabilmektedir. İşletim sistemi, veri erişim dilleri ve ağ iletişim protokol standartları ile uyumlu çalışmaktadır. Bunların yanında; bilgi

güvenliği ve kişisel verilerin korunması veri tabanında da en çok ihtiyaç duyulan konulardan biridir. Veri tabanlarında kişisel verilerin anonim hale getirilmesi önemli bir konudur özellikle test ortamlarında yazılım geliştiricilerin yetkilerinin canlı ortama göre daha geniş olması bu ortamdaki verileri daha korunaklı hale getirmemiz için önemli bir sebeptir. Veri tabanındaki verilerin anonimleştirilmesi yani verilerin uygun teknikler kullanılsa dahi bir kişi ile ilişkilendirilemez hale getirilmesi işlemini gerçekleştirmek için kullanılacak en yaygın yöntem veri maskeleme özelliğidir. Oracle 12c sürümü ile birlikte Maskeleme (redaction) özelliği getirilmiş böylece hassas bilgilerin tutulduğu tablolarda maskeleme yapılarak ilgili verinin tamamının görünmesi engellenmiştir.

Kullanıcıların isteklerine göre geliştirilmiş pek çok veri tabanı yönetim sisteminin var olduğu konusu, veri tabanı modelleri ve veri tabanı yönetim sistemleri üçüncü başlıkta daha detaylı ele alınmaktadır. ISO27001 gereksinimlerinin uygulanması için belirlenen başlıklar her bir veri tabanı yönetim sistemi için aynı olsa da sistemden sisteme yöntemsel ve yönetimsel farklılıklar bulunmaktadır. Bu farklılıklar üzerinde durarak her bir uygulanması gerekeni ayrı ayrı incelemek yerine kurumsal manada yaygın kullanıma sahip olan Oracle veri tabanı yönetim sistemi seçilmiş ve yapılması gereken bütün işlemler bu sistem üzerinde uygulamalı olarak işlenmiştir.

7. BULGULAR ve YORUMLAR

Bu bölümde başlıklar altında veri tabanı yönetim sistemlerinin standarda uygun hale getirilmesi için veri tabanında gerçekleştirilecek kontrol ve işlemlerin açıklaması ve nasıl yapılacağı detaylı anlatılmaktadır. ISO27001 kontrol amaçlarının veri tabanına uygulanması aşamasında yapılması gereken bütün işlemler Oracle veri tabanı yönetim sistemi üzerinde incelenecek, örnek sorgular ve sonuçları da verilecektir.

7.1.Veri Tabanı Genel Kontrolleri ve Kurulum Adımları

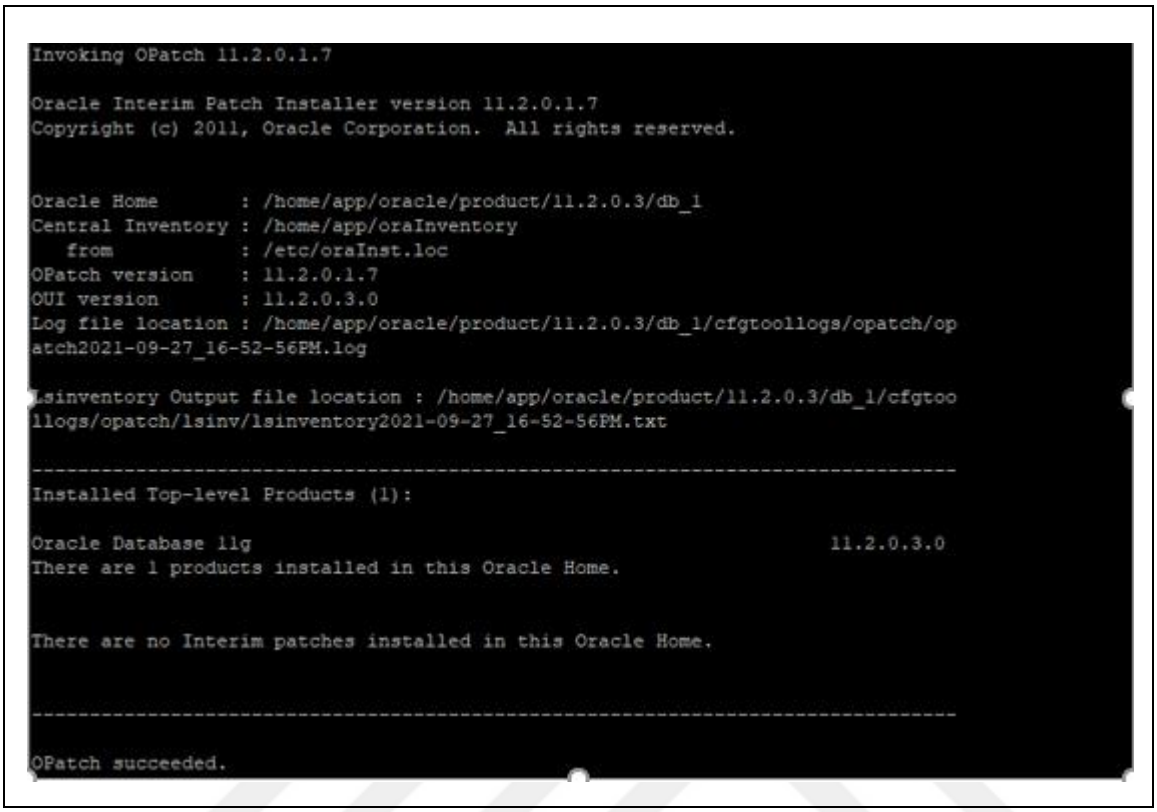
Veri tabanı yazılım sürümü öğrenilir ve bu sürümün güncel olup olmadığı kontrol edilir. Veri tabanı kurumun bilgi güvenliği politikalarına uygun olarak yapılandırılmalıdır. Güncel olmayan ve güvenlik yaması desteği sağlanmayan eski veri tabanları sistem yönetimini zorlaştırmaktadır ve güvenlik açığına sebep olmaktadır. Bunun içinde kurumdaki veri tabanı yöneticileri envanter çıkarmalıdır. Buna göre eski sürümler belirlenir ve veri tabanının en güncel sürümde kullanılması sağlanır. Sürüm bilgisi 'v$version' tablosunda yer alır. Veri tabanında kullanılan sürümü öğrenmek için aşağıdaki sorgu kullanılır ve çıktı alınır:

```
SELECT * FROM v$version;
```

```
Oracle Database 11g Enterprise Edition Release 11.2.0.3.0 - 64bit Production
PL/SQL Release 11.2.0.3.0 - Production
CORE 11.2.0.3.0        Production
TNS for Linux: Version 11.2.0.3.0 - Production
NLSRTL Version 11.2.0.3.0 - Production
```

Veri tabanı yamalarının kurumun bilgi güvenliği yönetim politikalarına uygun olduğundan emin olunmalıdır. Yamaların hangi açığı kapattığı öğrenilmelidir. Bu yamalar canlı veri tabanına alınmadan önce yeteri kadar test edilmelidir. Bu test süresi 3-6 ay arasında değişmektedir. Özellikle güvenlik yamalarının yayınlandıktan kısa süre sonra veri tabanlarında uygulanması gerekmektedir. Yamaların uygulanması genelde kurumlarda kararsızlığa sebep olmaktadır çünkü veri tabanları 7/24 çalışan çok kritik yazılımlardır ve kesintiye uğramaması gerekmektedir. Buna engel olabilme için kümeleme sistemi kullanılmaktadır. Yani bir sunucu çevrim dışı yapılır, yama uygulanır, bu süreçte de diğer sunucu hizmete devam eder. Yama uygulaması biten sunucu tekrar aktif moda alınır böylece kesinti yaşanmadan yama güncellemesi uygulanmış olur. Veri tabanında hangi yamaların uygulandığı bilgisi aşağıda verilen komutla işletim sisteminde bulunabilir.

$ORACLE_HOME/OPatch/opatch lsinventory

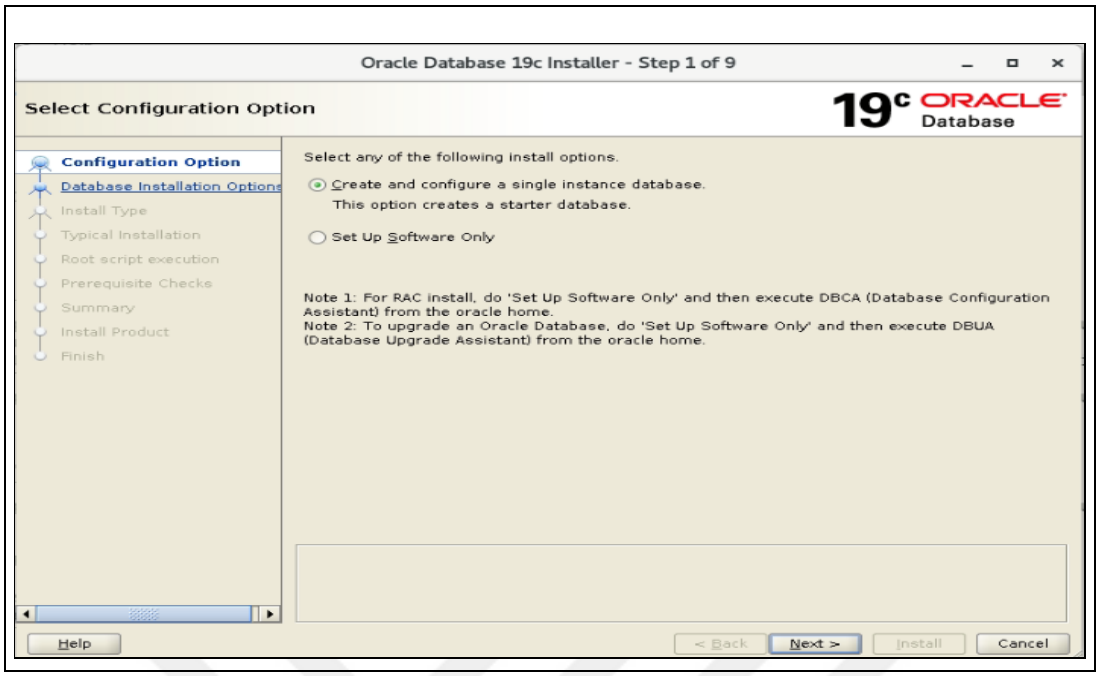


Şekil 7.1. Yama listesi örneği

Yama bilgisini öğrenmek için gerekli komut çalıştırıldığında Şekil 7.1'deki gibi çıktı alınır.

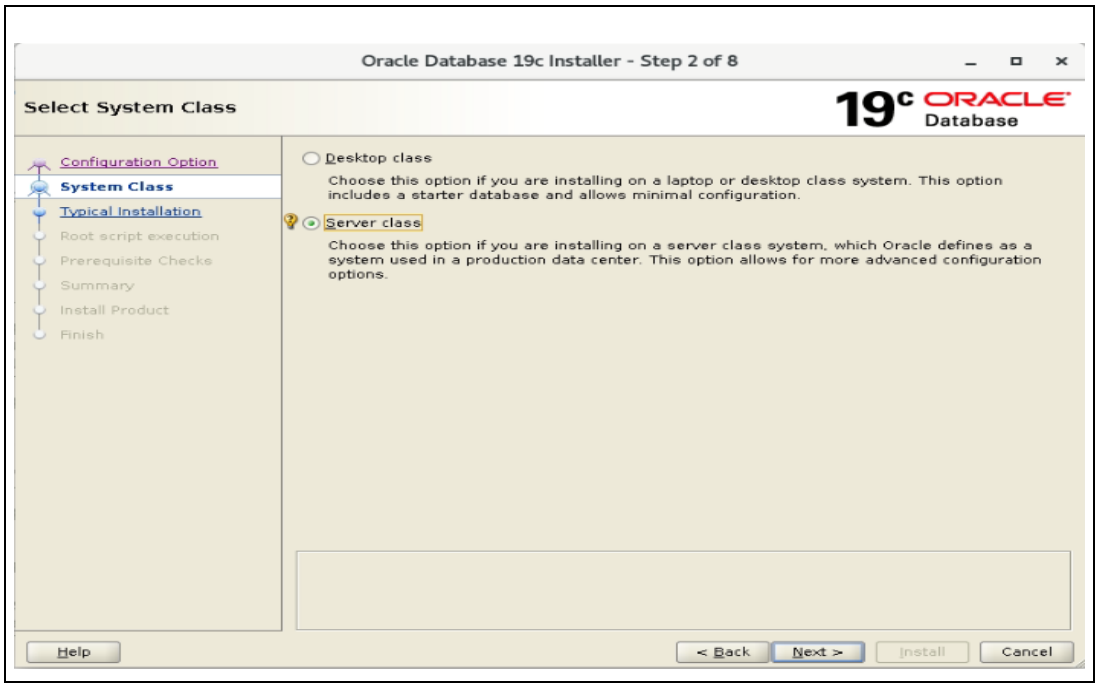
Veri tabanı güvenliğinin en önemli adımlarından biri de veri tabanının standart bir kuruluma sahip olması ve yeterli güvenlik ayarlarını içermesidir. Yeni sistemler canlıya alınmadan önce kontroller tamamlanmalıdır. Yeni bir sunucu kurulumu yapılacaksa işletim sistemi en güncel versiyona sahip olmalıdır. Yeni sunucu üzerine kurulumda bir koşul yoksa veri tabanı da en güncel versiyonda kurulmalıdır. Kurulumdan sonra sisteme ait kullanılmayan yüksek yetkili kullanıcılar varsa bu kullanıcılar kilitlenir. Veri sahibinin isteklerine göre gerekli yedekleme prosedürleri oluşturulur ve veri tabanı ile ilgili envanter dosyası güncellenir.

Güncel sürümlerden olan Oracle 19c standart kurulumunun nasıl yapıldığı özetle Şekil 7.2, Şekil 7.3, Şekil 7.4, Şekil 7.5, Şekil 7.6, Şekil 7.7, Şekil 7.8 görsellerinde yer almaktadır.



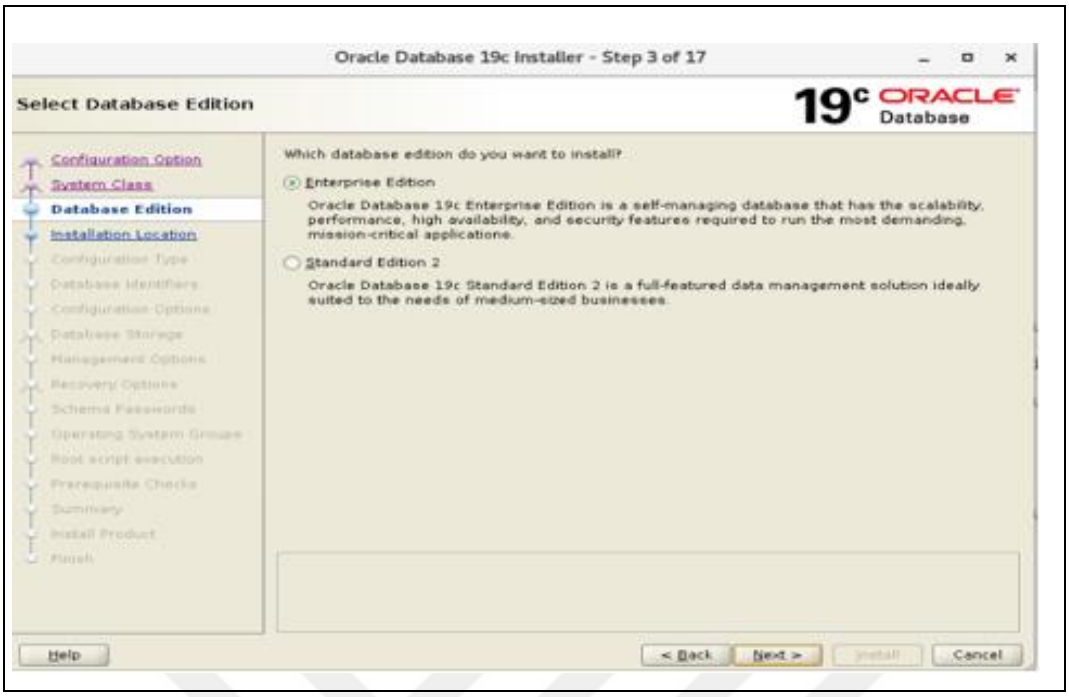
Şekil 7.2 Kurulum seçenekleri

Şekil 7.2' de iki yapılandırma seçeneği sunulmaktadır. Create and configure a single instance database seçeneği seçilerek oracle yazılımını yükler ve aynı zamanda veri tabanı oluşturmamızı da sağlar.



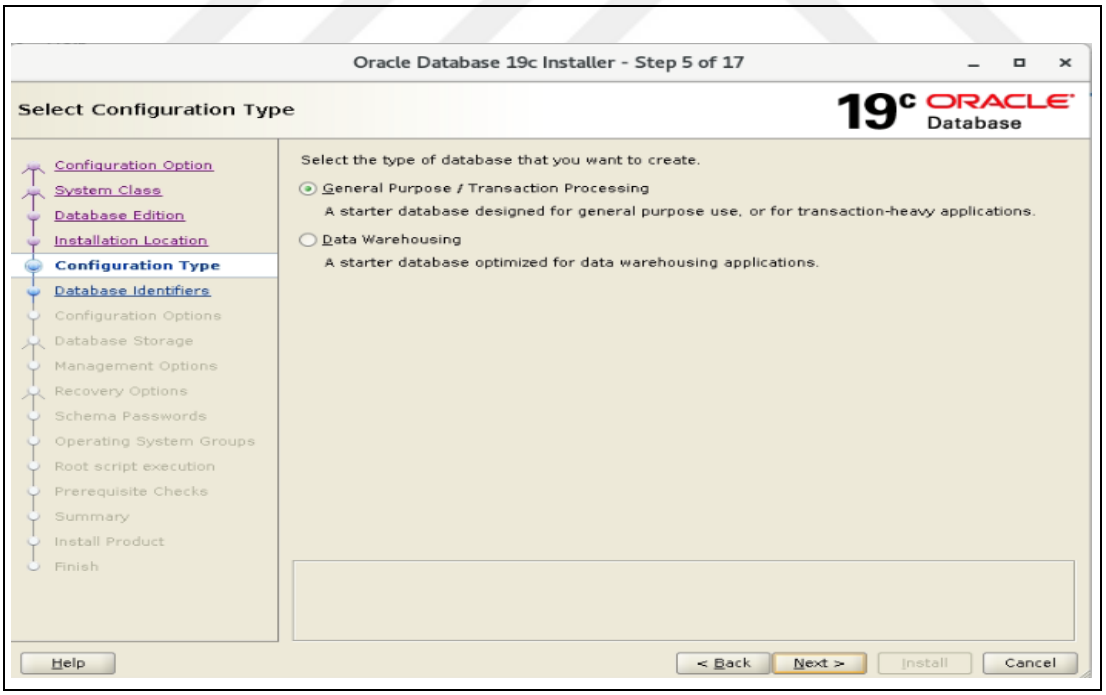
Şekil 7.3. Üzerine kurulacak sistemin türü

Şekil 7.3'te ne tür bir sistem üzerine kurulum yapılacağı bilgisi sorulmaktadır.



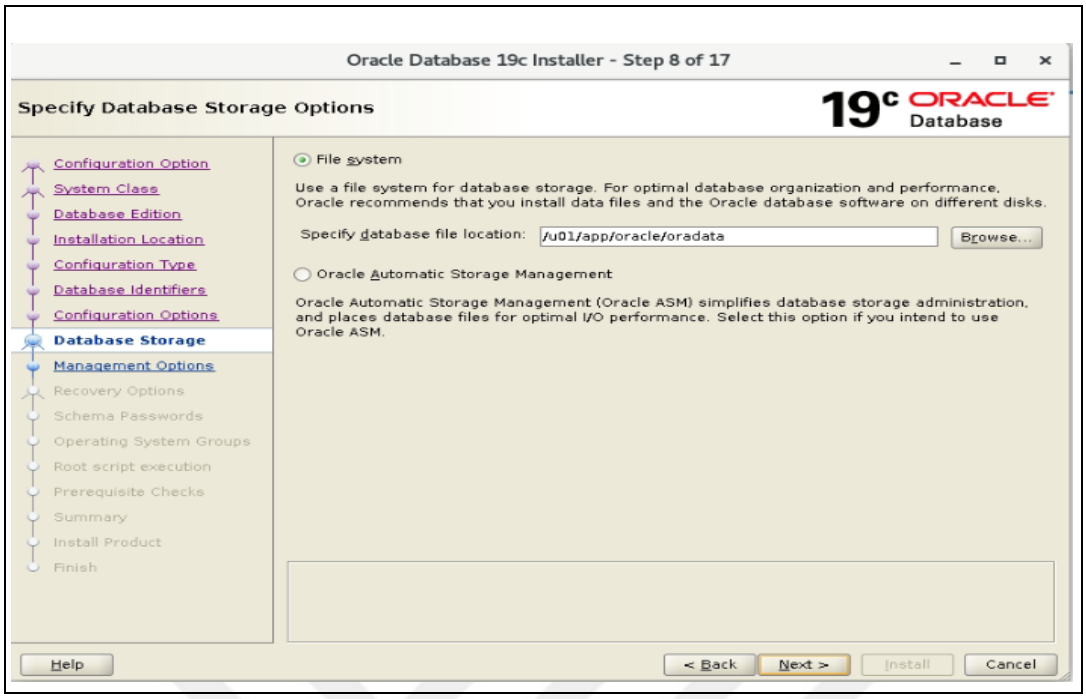
Şekil 7.4. Veri tabanı sürümü

Şekil 7.4'de görüldüğü üzere iki tür sürüm sunulmaktadır.



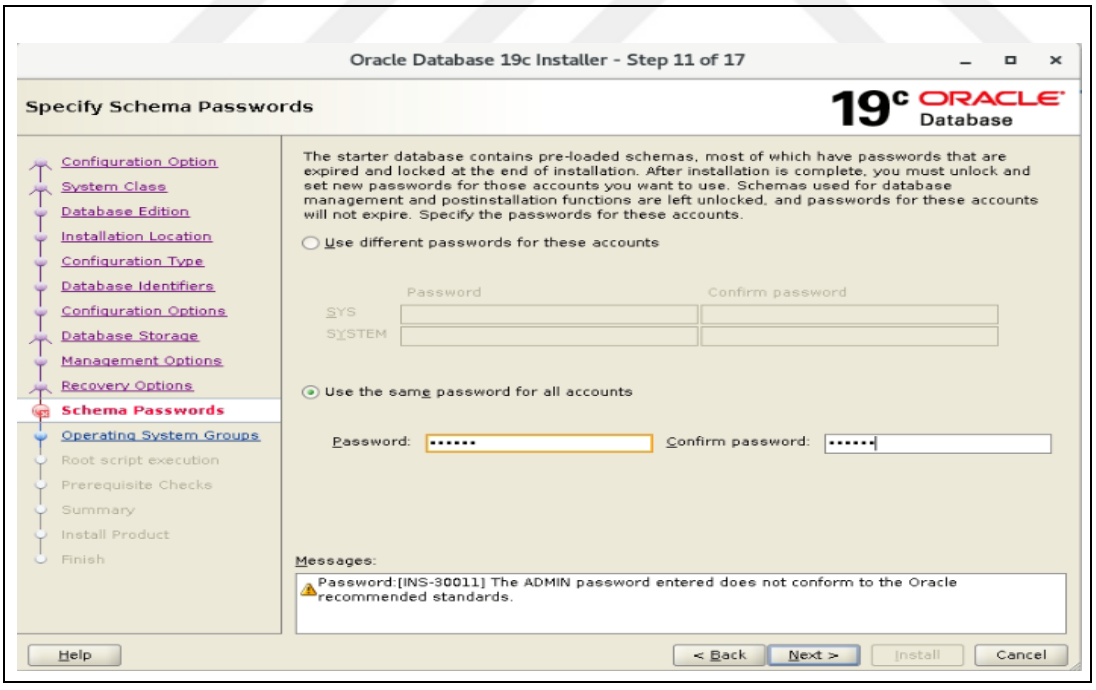
Şekil 7.5. Konfigürasyon seçimi

Şekil 7.5'te OLTP sistemleri için general Purpose/Transaction procesing seçeneğini eğer bir veri ambarı için kurulum yapılıyor ise Data Warehousing seçeneği seçilmelidir.



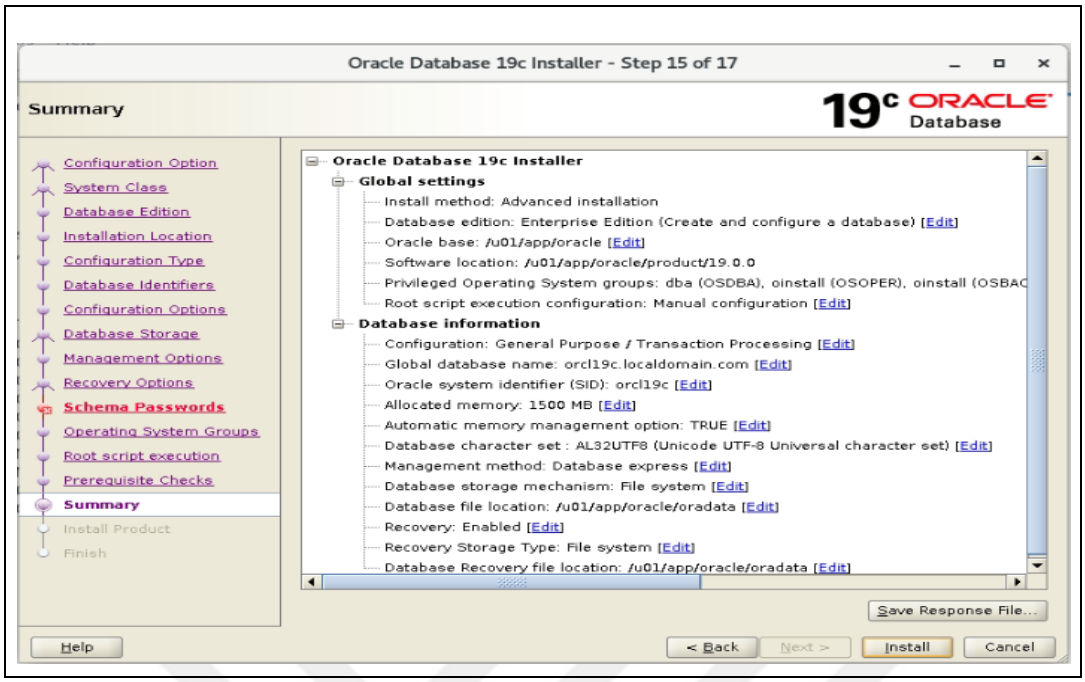
Şekil 7.6. Dosya konumu seçimi

Şekil 7.6'da dosyaların hangi klasörde saklanması istenildiği sorulmaktadır.



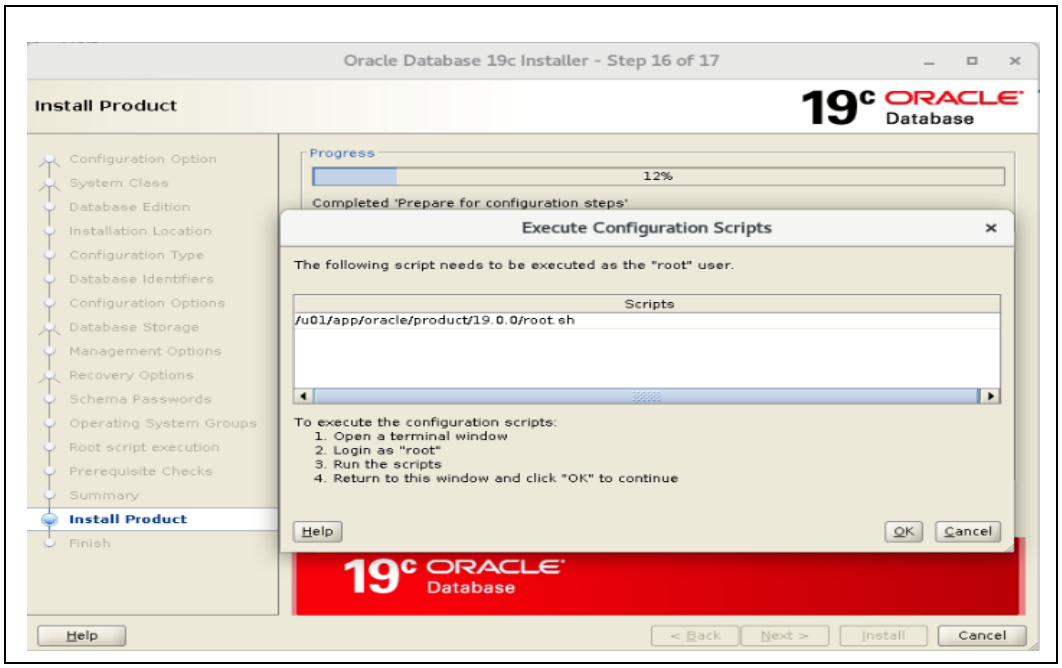
Şekil 7.7. SYS ve SYSTEM kullanıcı şifrelerinin belirlenmesi

Şekil 7.7'de yönetici kullanıcılarınızın şifresini belirlenmektedir.



Şekil 7.8. Kurulum özeti

Şekil 7.8 summary, kurulum özet ekranıdır. Herhangi bir adımda değişiklik yapmak istenildiğinde edit ile o adım ile ilgili kısım düzenlenebilir.



Şekil 7.9. Kurulum işlemleri

Şekil 7.9'a kadar yapılandırmanın önemli adamları gösterilmiştir burada install diyerek kurulum başlatılmaktadır.

7.2. Veri Tabanı Kullanıcı Hesap Güvenliği Kontrolleri

Veri tabanı güvenliğinde en önemli aşamalardan biri de, 27001 gereksinimlerinin pek çok maddesinde de geçen erişim kontrollerinin sağlanmasıdır. Veri tabanında saklanan hassas verilere kimin, nasıl ve ne şekilde ulaşabileceği belirlenmeli, yetkilendirme, kimlik doğrulama ve denetleme gibi işlemlerin takibi yapılmalıdır.

5.5' te bahsedilen, gerektiği kadar bilgi prensibini ilke edinerek hazırlanan erişim politikasına göre kullanıcı hesapları oluşturulmalı, görev değişikliği veya işten ayrılma hallerinde veri tabanı erişimleri kontrol edilmelidir. Bunun için öncelikle, hesapların üst yönetimin onayından geçerek oluşturulduğu incelenir, hiçbir hesap şifahen talepler üzerine oluşturulmuş olmamalıdır. Veri tabanında misafir veya grup hesabı yer almamalı her kullanıcı kendi kullanıcı hesabına sahip olmalıdır. Veri tabanında çok sayıda hesap yer almamalı, uygulama geliştiriciler uygulama aracılığıyla veri tabanına erişmeli birden çok veri tabanı kullanıcıları olmamalıdır. Uzun süre kullanılmayan hesaplar kontrol edilerek kaldırılmalı, iş değişikliği veya görev değişikliklerinde hesaplar düzenlenmeli veya duruma göre ihtiyaç kalmamış ise bu hesaplarda kaldırılmalıdır.

Oracle veri tabanında tüm kullanıcılar ve bu kullanıcıların oluşturulma tarihi, tablo alan, profil, hesap durumu gibi pek çok bilgide dba_users tablosunda tutulur. Kullanıcı listesini ve istenilen alanları almak için aşağıdaki sorgu yazılır:

```
SELECT username, account_status,profile FROM dba_users;
```

USERNAME	ACCOUNT_STATUS	PROFILE
OWBSYS	EXPIRED & LOCKED	DEFAULT
ORDPLUGINS	EXPIRED & LOCKED	DEFAULT
XDB	EXPIRED & LOCKED	DEFAULT
OWBSYS_AUDIT	EXPIRED & LOCKED	DEFAULT
APEX_030200	EXPIRED & LOCKED	DEFAULT
APPQOSSYS	EXPIRED & LOCKED	DEFAULT
EXFSYS	EXPIRED & LOCKED	DEFAULT
ORDSYS	EXPIRED & LOCKED	DEFAULT
SI_INFORMTN_SCHEMA	EXPIRED & LOCKED	DEFAULT
ANONYMOUS	EXPIRED & LOCKED	DEFAULT
CTXSYS	EXPIRED & LOCKED	DEFAULT
ORDDATA	EXPIRED & LOCKED	DEFAULT
WMSYS	EXPIRED & LOCKED	DEFAULT
MDSYS	EXPIRED & LOCKED	DEFAULT
FLOWS_FILES	EXPIRED & LOCKED	DEFAULT
SYSTEM	OPEN	DEFAULT
SYS	OPEN	DEFAULT
MGMT_VIEW	OPEN	DEFAULT
OUTLN	EXPIRED & LOCKED	DEFAULT

Şekil 7.10. Veri tabanı kullanıcıları

Personellerin yer değişikliklerinin bildirilmediği durumlarda takibini yapabilmek için belli süre veri tabanına erişim yapmayan kullanıcılar listelenmesi için de birden fazla yöntem vardır. Bunlardan biri giriş tetikleyicisi oluşturmak böylece tetikleyici kullanılarak hangi makineden, hangi kullanıcı ne zaman bağlanmış bilgileri edinilebilir. Diğer yöntem denetim parametreleri kullanarak bir oracle auditing hazırlamaktır. Böylece aşağıdaki sorgu çalıştırılarak auditing' den 60 gün sisteme erişim yapmamış kullanıcılar Şekil 7.11'deki gibi listenebilir.

SELECT username FROM dba_audit_trail WHERE action_name = 'LOGIN' GROUP BY username HAVING MAX(timestamp) < sysdate – 60;

USERNAME
DBA_OLD
UTLU

Şekil 7.11. Veri tabanına erişmeyen kullanıcı

Şekil 7.11'de sisteme erişim yapmamış kullanıcı listesi elde edilmiştir.

Buradaki gün değeri parametrik olup (SYSDATE – 60) istenirse bugün süresi artırılıp azaltılabilinerek o gün süresince erişmeyen personel tespit edilebilir.

Veri tabanının oluşturulması ile veya yeni bir özellik yüklenmesi ile birlikte gelen varsayılan hesaplar vardır ve bu hesapların internet ortamında da kolaylıkla bulunabilen varsayılan şifreleri vardır. Eğer veri tabanında bir açıklık varsa saldırganlar bunu tespit ederek varsayılan hesap bilgileri ile sisteme sızabilirler. Varsayılan hesapların bazıları yönetimseldir sys,system, dbsnmp, sysman bunların en önemlileridir. Bu kullanıcılar veri tabanı üzerinde önemli ayrıcalıklara sahiptir bu nedenle bu kullanıcılar kilitlenemez fakat varsayılan parolaları güçlü parolalar ile değiştirilerek sadece belirli durumlarda kullanılmalıdır. Bu durumlar:

SYS kullanıcısı, veri tabanı yaratma,veri tabanını kapatıp açma, veri tabanı kurtarma, parametre kütüğü ve sistem tetikleyicisi oluşturma, Oracle'ın hata düzeltici kodlarını çalıştırma, Standby veri tabanını kontrol etme, Oracle'ın güncel paketlerini yükleme, veri tabanı güncelleme işlemlerini gerçekleştirmek için kullanılmalıdır.

SYSTEM kullanıcısı, Veri tabanının canlı yedeğini,kontrol kütüğü yedeğini almak için, tüm veri tabanı verilerini export etmek için, hata izlemek için, veri tabanı uygulama tablo ve indekslerin istatistiklerini toplamak için kullanılmalıdır.

DBSNMP kullancıcısı, enterpise manager yönetim aracını izlemek ve yönetmek için kullanılmalıdır.

Yönetimsel olmayan varsayılan hesaplar ise belirli işler için oluşturulmuş az ayrıcalığa sahip hesaplardır. Bu hesaplar yukarıda bahsedilen hesaplar kadar kritik olmasa da bu hesapları saldırganlar için güvenlik açığı oluşturmasını önlemek için varsayılan parolaları güçlü parolalar ile değiştirilmeli ve hatta bu hesaplar kilitlenmelidir.

Oracle veri tabanının versiyonuna göre varsayılan hesaplar değişkenlik gösterebilmektedir. Aşağıdaki sorgu yazılarak veri tabanındaki varsayılan hesaplar Şekil 7.12 'deki gibi listelenir. Bilgi güvenliği için her veri tabanı kurulumunda, yama geçişinde, versiyon yükseltmesinde aşağıdaki sorgu çalıştırılmalı kilitli olmayan hesaplar tespit edilerek kilitlenmeli ve parolaları güçlü parola ile değiştirilmelidir.

SELECT username, account_status from dba_users WHERE username in (SELECT * FROM DBA_USERS_WITH_DEFPWD) order by username;

USERNAME	ACCOUNT_STATUS
APPQOSSYS	EXPIRED & LOCKED
CTXSYS	EXPIRED & LOCKED
DIP	EXPIRED & LOCKED
EXFSYS	EXPIRED & LOCKED
MDDATA	EXPIRED & LOCKED
MDSYS	EXPIRED & LOCKED
OLAPSYS	EXPIRED & LOCKED
ORACLE_OCM	EXPIRED & LOCKED
ORDDATA	EXPIRED & LOCKED
ORDPLUGINS	EXPIRED & LOCKED
ORDSYS	EXPIRED & LOCKED
OUTLN	EXPIRED & LOCKED
SCOTT	EXPIRED & LOCKED
SI_INFORMTN_SCHEMA	EXPIRED & LOCKED
SPATIAL_CSW_ADMIN_USR	EXPIRED & LOCKED
SPATIAL_WFS_ADMIN_USR	EXPIRED & LOCKED
WMSYS	EXPIRED & LOCKED
XDB	EXPIRED & LOCKED

Şekil 7.12. Varsayılan hesaplar ve durumları

Şekil 7.12'de hesaplar ve bu hesapların durumları listelenmektedir.

Kullanıcılarla ilgili bir diğer güvenlik açığı da verilen parolaların kolay tahmin edilebilir veya bir sözlükte bulunabiliyor olmasıdır. Parolalar hırsızlığa ve kötüye kullanıma açık olduğundan 27001 gereksinimlerinde de belirtildiği gibi güçlü parolalar oluşturularak bilgi güvenliği sağlanmalıdır. Pek çok veri tabanı platformunda zengin parola özellikleri desteğe bulunmaktadır. Oracle'da parola yönetim politikasını kullanıcı profilleri aracılığıyla kontrol ederek parametrelerin aktif hale getirilmesi ile kullanıcının belirlediği parolanın gereksinimleri karşılayıp karşılamadığı kontrol edilir. Fonksiyonun parametreleri şunlardır:

FAILED_LOGIN_ATTEMPT: Bir kullanıcı oturum açmaya çalışırken üst üste kaç kez yanlış deneme yaptığında hesabın kilitleneceğini belirleyen max girilen hatalı parola sayısıdır. Default değeri 10'dur.

PASSWORD_GRACE_TIME: Hesabın kullanım süresinin dolmasına kaç gün kala kullanıcıya bildirileceğini belirleyen gün sayılır. Default değeri 7'dir.

PASSWORD_LIFE_TIME: Hesabın parolasını kullanabileceği toplam gün sayısıdır. Bu değer sınırsız ayarlanmamalıdır Defaultu 180 gündür.

PASSWORDK_LOCK_TIME: Belirtilen sayıda üst üste yanlış parola denemesi yapıldığında hesabın kilitli kalacağı gün sayısıdır. Bu özellik brüte force saldırılarını önlemeye yardımcı olmaktadır. Default'u 1 gündür.

PASSWORD_REUSE_MAX:Aynı şifrenin tekrar kullanılabilmesi için kaç şifre değişikliği yapılmış olması gerektiğini belirler. Defaultu sınırsızdır.

PASSWORD_REUSE_TIME: Parolanın tekrardan kullanılması için geçmesi gereken gün sayısını belirler.

PASSWORD_VERIFY_FUNCTION: Bu parametre, kullanıcı parolalarını kontrol etmek için parola karmaşıklığı belirten bir fonksiyon alır. Bu fonksiyon kurumun bilgi güvenliği politikasına göre büyük, küçük harf, noktalama işareti, en az kaç karakterden oluşacağı gibi özellikleri içerecek şekilde SYS şemasında oluşturulmalıdır. Sonrasında tüm profillere bu fonksiyon atanarak kontroller sağlanır.

Oracle'ın yazılım yüklemesi ile gelen ve kullanıcıların kullanımı için default hazırladığı Password verify fonsiyonu da aşağıdaki yolda text formatında bulunur. Bu çalıştırılarakta tüm kontroller gerçekleştirilebilir.

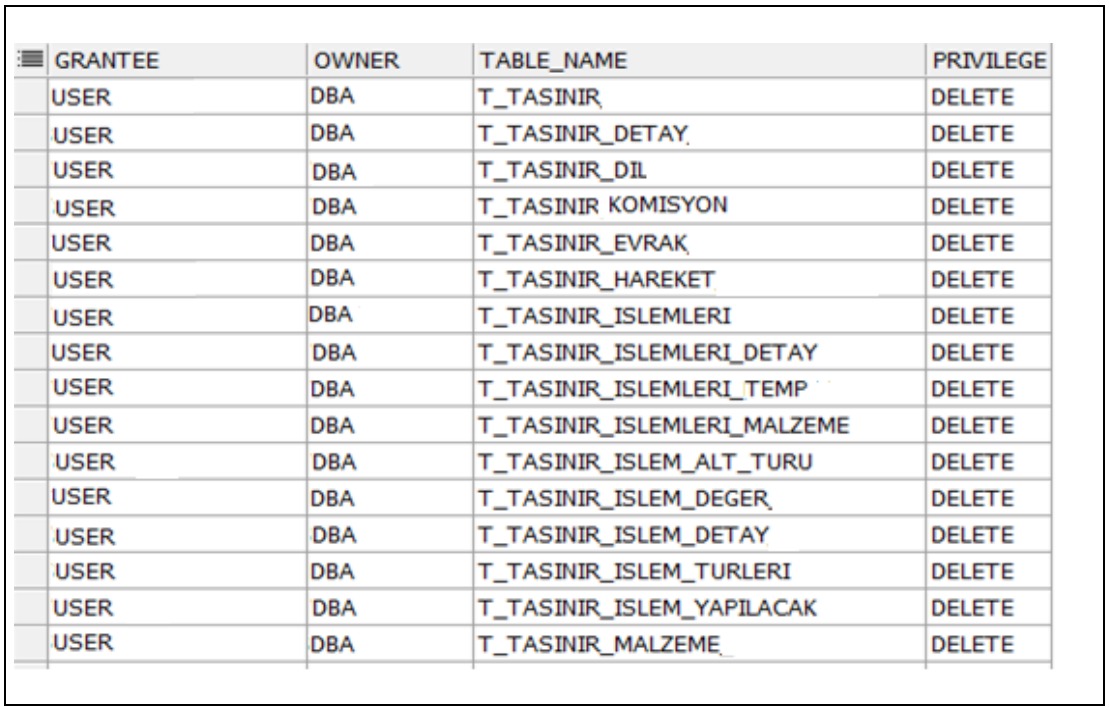
$ORACLE_HOME/rdbms/admin/utlpwdmg.sql

Bilgi güvenliğinin sağlanması için veri tabanına erişen kullanıcının hangi nesnelere, ayrıcalıklara sahip olacağı kurum bilgi güvenliği politikasına göre belirlenmeli ve kontrolleri iyi yapılmalıdır.

Bunun için öncelikle tablolara select yetkisi dışında yetkisi olan kullanıcılar tespit edilmelidir. Select işlemi dışındaki DML işlemlerinin sadece veri tabanı yöneticilerine tanımlı olması en doğru yöntemdir. Aşağıdaki sorgu ile kullanıcıların, select yetkisi dışında hangi şemaya ait hangi nesne üzerinde hangi yetkiye sahip olduğu bilgisi Şekil 7.13'teki gibi

listelenir. Bu liste incelenerek önceden kalmış olan veya yanlışlıkla verilmiş olan örneğin USER kullanıcısına tanımlanmış delete yetkisi gibi yetkiler kullanıcıdan alınır.

SELECT grantee, owner, table_name, privilege FROM dba_tab_privs WHERE privilege NOT IN('SELECT') order by privilege;



GRANTEE	OWNER	TABLE_NAME	PRIVILEGE
USER	DBA	T_TASINIR	DELETE
USER	DBA	T_TASINIR_DETAY	DELETE
USER	DBA	T_TASINIR_DIL	DELETE
USER	DBA	T_TASINIR KOMISYON	DELETE
USER	DBA	T_TASINIR_EVRAK	DELETE
USER	DBA	T_TASINIR_HAREKET	DELETE
USER	DBA	T_TASINIR_ISLEMLERI	DELETE
USER	DBA	T_TASINIR_ISLEMLERI_DETAY	DELETE
USER	DBA	T_TASINIR_ISLEMLERI_TEMP	DELETE
USER	DBA	T_TASINIR_ISLEMLERI_MALZEME	DELETE
USER	DBA	T_TASINIR_ISLEM_ALT_TURU	DELETE
USER	DBA	T_TASINIR_ISLEM_DEGER	DELETE
USER	DBA	T_TASINIR_ISLEM_DETAY	DELETE
USER	DBA	T_TASINIR_ISLEM_TURLERI	DELETE
USER	DBA	T_TASINIR_ISLEM_YAPILACAK	DELETE
USER	DBA	T_TASINIR_MALZEME	DELETE

Şekil 7.13. kullanıcıların yetki listesi

Şekil 7.13'te kullanıcının hangi şema ve nesnede select dışında yetkilesinin var olduğu listelenmektedir.

Kurum içerisinde kullanıcılara yetki verilirken, kullanıcının belirli bir eylemi gerçekleştirmesi, başka şemaya ait nesnelere erişmesi, bir PL/SQL paketi çalıştırması gibi haklar tanımlanmasına ayrıcalık denilmektedir. Ayrıcalıklar veya diğer roller birlikte gruplandırılarak veri tabanı yöneticileri tarafından roller oluşturulabilmektedir. Roller, ayrıcalıklardan daha kolay ve daha iyi yönetilebildiğinden kullanıcılara ayrıcalıkları doğrudan vermek yerine, ayrıcalıkları role vermek sonra kullanıcıları role dahil etmek daha tercih edilmesi gereken yöntemdir.

Kullanıcılar için en kritik sayılabilecek rollerden bazıları 'DROP ANY TABLE', 'ALTER SYSTEM', 'CREATE ANY TABLE', 'DBA', 'SELECT CATALOG ROLE', 'DELETE CATALOG ROLE', 'EXECUTE CATALOG ROLE' gibi yetkilerdir. 'ANY' yetkilerini

içeren ayrıcalıklar da oldukça kritiktir any yetkisi tanımlanan bir kullanıcı veri tabanı veri sözlüğü tablolarına bile erişip değiştirebilir, sadece kendi şemasına ait nesnelerin değil veri tabanındaki tüm nesnelerin davranışına müdahale edebilir. Bu rollere sahip kötü niyetli kullanıcılar veri tabanının bütünlüğüne zarar verebilir. Bu nedenle kullanıcılara yapması gereken işleri yapabilmesi için minimum gerekli ayrıcalıklar verilmeli kritik seviyedeki ayrıcalıkların kimlerde olduğu sorgulanmalı, gereksiz verilen ayrıcalıklar tespit edilerek kaldırılmalıdır. Bir kullanıcıya verilen sistem ayrıcalıkları DBA_SYS_PRIVS veri sözlüğü görünümünde tutulur ve kullanıcıların yetkileri buradan aşağıdaki şekilde sorgulanır :

SELECT * FROM dba_role_privs where GRANTEE IN ('DROP_ANY_TABLE', 'ALTER_SYSTEM', 'CREATE_ANY_TABLE', 'DBA', 'SELECT_CATALOG_ROLE', 'DELETE_CATALOG_ROLE','EXECUTE_CATALOG_ROLE');

Sorgu sonucunda şekil 7.14'deki çıktı alınır. Bu çıktı incelenerek, sorguda belirlediğimiz kritik yetkilere sahip kullanıcıların bu yetkiye ihtiyacı olmadığı tespit edilirse kaldırılır.

GRANTEE	GRANTED_ROLE	ADMIN_OPTION	DEFAULT_ROLE
OEM_MONITOR	SELECT_CATALOG_ROLE	NO	YES
SYS	DELETE_CATALOG_ROLE	YES	YES
DBA	DELETE_CATALOG_ROLE	YES	YES
DBA	EXECUTE_CATALOG_ROLE	YES	YES
SYS	DBA	YES	YES
IMP_FULL_DATABASE	EXECUTE_CATALOG_ROLE	NO	YES
SYSMAN	SELECT_CATALOG_ROLE	YES	YES
UTLU	SELECT_CATALOG_ROLE	NO	YES
DBA	SELECT_CATALOG_ROLE	YES	YES
EXP_FULL_DATABASE	EXECUTE_CATALOG_ROLE	NO	YES
IMP_FULL_DATABASE	SELECT_CATALOG_ROLE	NO	YES
EXP_FULL_DATABASE	SELECT_CATALOG_ROLE	NO	YES

Şekil 7.14. Kritik yetkilere sahip kullanıcılar

Şekil 7.14'te UTLU kullanıcısı SYS kullanıcısında bulunan tabloları listeleyebilecek ve sorgulayabilecek hakkı veren SELECT_CATALOG_ROLE yetkisine sahiptir. Bu kritik role ihtiyacı olmadığı düşünüldüğünde aşağıdaki sorgu ile bu yetki kullanıcıdan alınır.

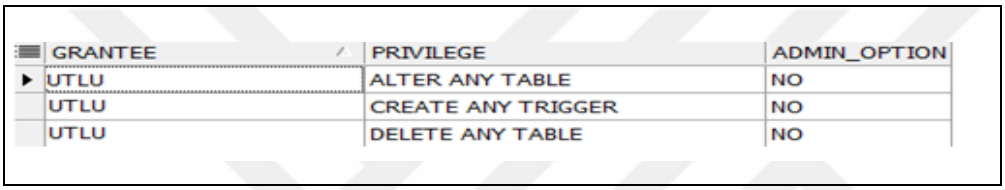
REVOKE SELECT_CATALOG_ROLE FROM UTLU;

Grup veya roller yerine kullanıcılara doğrudan verilen yetkiler, aşağıdaki sorgu ile veri sözlüğünden elde edilerek tüm yetkiler listelenir.

SELECT * FROM DBA_ROLE_PRIVS

Veri tabanında, yönetici yetkisi olmayıp ANY anahtarı kullanan sistem ayrıcalığına sahip kullanıcıları tespit etmek için aşağıdaki sorgu çalıştırılır.

SELECT * FROM dba_sys_privs WHERE PRIVILEGE like '%ANY%' AND GRANTEE in (SELECT username FROM DBA_USERS WHERE PROFILE= 'APPLICATION');



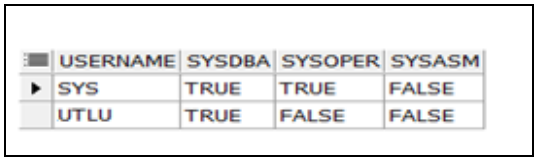
GRANTEE	PRIVILEGE	ADMIN_OPTION
UTLU	ALTER ANY TABLE	NO
UTLU	CREATE ANY TRIGGER	NO
UTLU	DELETE ANY TABLE	NO

Şekil 7.15. ANY anahtarı kullanan kullanıcılar

Çalıştırılan sorgu sonucunda Şekil 7.15 çıktısı elde edilir.

SYSDBA, SYSOPER, SYSASM Oracle veri tabanlarında çok kritik öneme sahip olan yönetici ayrıcalıklarıdır. SYSDBA, Veri tabanını kapama, açma ve veri tabanı üzerinde tüm kritik işlemleri yapabilen roldür. SYSOPER, Veri tabanını kapamak, açmak gibi işlemleri operatörler tarafında yapabilen roldür. SYSASM, ASM sistemlerine bağlanabilmek ve sistem üzerinde işlem yapabilmek için gerekli roldür. Bu roller önemlerinden dolayı sadece veri tabanı yöneticilerine verilmelidir. Veri tabanı yöneticisi dışında başka kullanıcılara verilmiş mi aşağıdaki sorgu ile sık sık kontrol edilerek Şekil 7.16 daki gibi elde edilen çıktılar incelenmelidir. Eğer yönetici rollerinin şema(uygulama) kullanıcılarında da var olduğu tespit edilirse UTLU gibi revoke komutu ile hemen kaldırılmalıdır.

SELECT * FROM v$pwfile_users;



USERNAME	SYSDBA	SYSOPER	SYSASM
SYS	TRUE	TRUE	FALSE
UTLU	TRUE	FALSE	FALSE

Şekil 7.16. Yönetici rollerine sahip kullanıcılar

Şekil 7.16'da yönetici rolüne sahip kullanıcılar ve sahip olduğu ayrıcalıklar listelenmektedir.

Oracle veri tabanlarında tablo, indeks, tetikleyici gibi birbiriyle ilişkili nesneler mantıksal veri dosyalarında yani tablo alan (tablespace)'larda depolanır. Kullanıcının bir tablo oluşturması için create table yetkisi ile birlikte bu tabloyu oluşturacağı tablo alanını belirtmesi gerekir. Bir kullanıcıya sınırsız veya yüksek miktarda tablo alanı verilirse kötü niyetli kullanıcılar veya saldırganlar veri tabanı disk kapasitesini işlem yapamayacak kadar doldurabilir ve dos saldırılarına sebep olabilir. Bu nedenle unlimited tablo aralığına sahip olan kullanıcılar aşağıdaki sorgu ile tespit edilmelidir.

SELECT grantee, privilege FROM dba_sys_privs WHERE privilege = 'UNLIMITED TABLESPACE';

GRANTEE	PRIVILEGE
UTLU	UNLIMITED TABLESPACE
SYSTEM	UNLIMITED TABLESPACE
SYSMAN	UNLIMITED TABLESPACE
SYS	UNLIMITED TABLESPACE

Şekil 7.17. Sınırsız tablo alan olan kullanıcılar

Sorgu sonucunda elde edilen Şekil 7.17'de istenmeyen kullanıcılarda var olan bu yetki tespit edilirse aşağıdaki komut kullanılmalıdır.

REVOKE UNLIMITED TABLESPACE FROM "UTLU";

Veri tabanında nesneler üzerinde yetki verilirken with admin seçeneğinin kullanılırsa yetki verilen kullanıcı başka kullanıcılara bu yetkiyi verebilir. Böylece denetimi zor bir dolaylı yetkilendirme ortaya çıkar. Bu nedenle with admin seçeneği ile verilen yetkilere dikkat edilmeli, aşağıdaki sorgu ile de bu şekilde verilen yetkilere sahip olan SYS, SYSTEM ve DBA dışındaki kullanıcılar tespit edilmelidir.

SELECT grantee,GRANTED_ROLE privilege, admin_option FROM dba_role_privs WHERE admin_option = 'YES' and grantee NOT IN('SYS','SYSTEM', 'DBA')

UNION SELECT grantee, PRIVILEGE, admin_option FROM dba_sys_privs WHERE admin_option = 'YES' and grantee NOT IN('SYS','SYSTEM', 'DBA');

GRANTEE	PRIVILEGE	ADMIN_OPTION
APEX_030200	CREATE OPERATOR	YES
APEX_030200	CREATE PROCEDURE	YES
APEX_030200	CREATE SEQUENCE	YES
APEX_030200	CREATE SYNONYM	YES
APEX_030200	CREATE TABLE	YES
APEX_030200	CREATE TRIGGER	YES
APEX_030200	CREATE TYPE	YES
APEX_030200	CREATE VIEW	YES
APEX_030200	RESOURCE	YES
APEX_030200	UNLIMITED TABLESPACE	YES
AQ_ADMINISTRATOR_ROLE	CREATE EVALUATION CONTEXT	YES
AQ_ADMINISTRATOR_ROLE	CREATE RULE	YES
AQ_ADMINISTRATOR_ROLE	CREATE RULE SET	YES
AQ_ADMINISTRATOR_ROLE	DEQUEUE ANY QUEUE	YES
AQ_ADMINISTRATOR_ROLE	ENQUEUE ANY QUEUE	YES
AQ_ADMINISTRATOR_ROLE	MANAGE ANY QUEUE	YES
CTXSYS	CTXAPP	YES

Şekil 7.18. With admin opsiyonu verilen kullanıcılar

Şekil 7.18'de with admin opsiyonuna sahip olan kullanıcılar listelenmemektedir.

Veri tabanı erişiminde select yetkisi verildiğinde satır bazında bir erişim filtresi uygulanamamakta kullanıcı tüm satırları okuyabilmektedir. Bu sorunu çözmek için oracle'da VPD(Sanal gizli veri tabanı) vardır. Böylece erişimde satır sütun bazlı kontrol etmek için policy'ler yazılabilir. VPD güvenlik ilkesinin uygulandığı bir tablo veya görünüme kullanıcı sorgu yapmak istediğinde VPD politikaları otomatik uygulanır ve kullanıcının istenen ayrıntıda sonuç alması sağlanır [50]. VPD ilkesi ile korunan bir tablo veya görüntüye sorgu yapıldığında politikalar devreye girer ve sql komutunu dinamik olarak değiştirerek where koşulunu devreye alır çalıştıran kişi bu koşuldan etkilenmesine rağmen görmez.

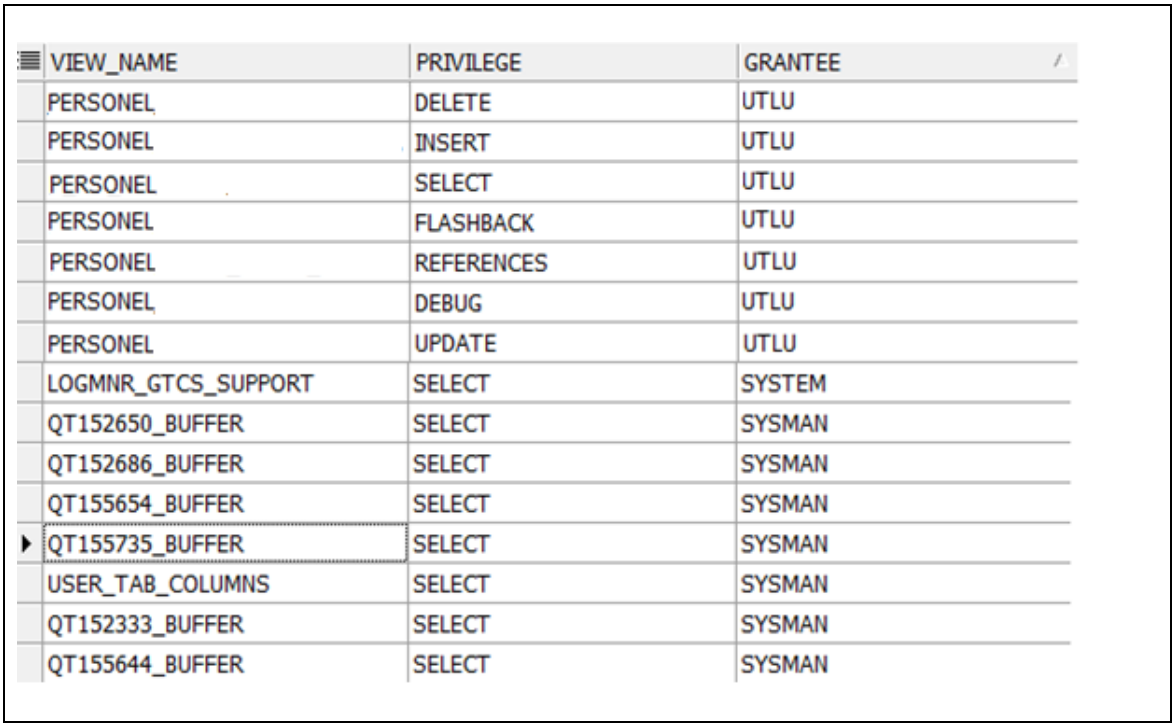
Veri tabanlarında VPD kullanımını incelemek için GV$VPD_POLICY görünümü sorgulanır. GV$_SESSION görünümü ile her bir bağlı kullanıcının oturum bilgilerinin detayı öğrenilir. Ancak bu görünüme ulaşım yetkisi her kullanıcıya verilmez güvenlik açığı oluşturmaması için bu noktada da VPD kullanımı ile bütün kullanıcıların sadece kendi oturum bilgilerine erişim yetkisi verilebilir.

Veri tabanında tanımlanan görünümleri listelemek için aşağıdaki sorgu çalıştırılır:

SELECT view_name, owner FROM all_views;

Veri tabanındaki görünümler üzerinde hangi kullanıcıların ne yetkisi olduğunu öğrenebilmek için de aşağıdaki sorgu çalıştırılır ve Şekil 7.19 çıktısı alınır:

SELECT v.view_name, p.privilege, p.grantee FROM dba_views v JOIN dba_tab_privs p ON p.table_name = v.view_name;



VIEW_NAME	PRIVILEGE	GRANTEE
PERSONEL	DELETE	UTLU
PERSONEL	INSERT	UTLU
PERSONEL	SELECT	UTLU
PERSONEL	FLASHBACK	UTLU
PERSONEL	REFERENCES	UTLU
PERSONEL	DEBUG	UTLU
PERSONEL	UPDATE	UTLU
LOGMNR_GTCS_SUPPORT	SELECT	SYSTEM
QT152650_BUFFER	SELECT	SYSMAN
QT152686_BUFFER	SELECT	SYSMAN
QT155654_BUFFER	SELECT	SYSMAN
QT155735_BUFFER	SELECT	SYSMAN
USER_TAB_COLUMNS	SELECT	SYSMAN
QT152333_BUFFER	SELECT	SYSMAN
QT155644_BUFFER	SELECT	SYSMAN

Şekil 7.19. Görünümler üzerindeki yetkiler

Şekil 7.19'da görünüm üzerinde yetkisi olan kullanıcı ve ne yetkisi olduğu görülmektedir.

Veri tabanlarında public rolü vardır bu rol veri tabanından kaldırılamaz. Veri tabanında herkese verilecek izinlerde ayrı ayrı her kullanıcıya izin tanımlamak veya rol tanımlamak yerine public' e verilen izinler veri tabanında herkese tanımlanmış olur. Bilgi güvenliğinde önemli olan gerekmediği sürece yetki vermemektir. Bu nedenle de hassas fonksiyonlarda veya etkili sistem izinlerinde public'e tanımlamak güvenlik açığına sebebiyet vereceğinden kaçınılmalıdır. Yeterli bilgiye sahip değilken tüm public yetkilerinin iptal edilmesi sistemde ve uygulamalarda problemler yaratabilir. Bu nedenle public rolünden alınması veya kısıtlanması gereken ayrıcalıklar aşağıdadır:

DBMS_RANDOM: Genellikle verileri şifrelemek ve şifreleri çözmek için rastgele sayılar üreterek anahtar oluşturmaya yarayan SYS şemasındaki bir pakettir. Şifreleme anahtarlarının oluşturulması için kullanıldığı ortamlarda DBMS_RANDOM paketine public erişim yetkisi verilir ise kötü niyetli saldırganlar hassas verileri koruyan şifreleme anahtarlarını yeniden yapılanıdabilir ve şifreli verilerin çökmesine sebep olabilir.

UTL_FILE: Veri tabanı sunucusunda işletim sistemi dosyalarını okumak ve yazmak için doğrudan erişim sunan çok güçlü bir yardımcı fonksiyon paketidir. Bu paketi kullanarak bir saldırgan veri tabanı sunucusunu kontrol altına alarak içerisindeki verilere erişebilir, verileri bocabilir veya silebilir. Bu nedenle varsayılan olarak public'e verilen bu ayrıcalık değiştirilmeli ihtiyacı olan kullanıcılar için bir dizin oluşturulmalı ve kullanıcının yetkisi bu dizinle kısıtlanmalıdır [51].

UTL_HTTP: Bu paket veri tabanına veya veri tabanının üzerinde çalıştığı işletim sistemine doğrudan tehdit oluşturmak yerine veri tabanı üzerinden dış dünyaya veri sızdırılmasına neden olur. Bu paket ile veri tabanındaki hassas veriler, kredikartı bilgileri,özlük bilgileri gibi bir sorgu ile çekilerek paylaşılabilir. Varsayılanı public olan bu paket üzerindeki tüm yetkiler kaldırılmalıdır.

UTP_TCP: Veri tabanından ağ üzerinden mesaj gönderimine yarayan bu paketin saldırganlar tarafından kullanılması ile ağ trafiği parçalanabilir, TCP paketleri ele geçirilebilir. Bu nedenle bu paket üzerindeki public'e ait tüm yetkiler alınmalıdır.

Public rolünün etkisi ile tüm kullanıcıların erişim izni olduğundan güvenlik açığına sebep olabilecek DBMS_RANDOM, UTL_FILE,UTL_HTTP, UTL_TCP paketlerinin veri tabanındaki durumu incelenmelidir. Bunun için aşağıdaki sorgu çalıştırılır ve Şekil 7.20 çıktısı alınır.

SELECT grantee, owner, table_name, grantor,prıvılege FROM dba_tab_prıvs WHERE owner= 'SYS' AND TABLE_NAME IN ('DBMS_RANDOM', 'UTL_TCP', 'UTL_FILE', 'UTL_HTTP') AND grantee='PUBLIC'

GRANTEE	OWNER	TABLE_NAME	GRANTOR	PRIVILEGE
PUBLIC	SYS	DBMS_RANDOM	SYS	EXECUTE
PUBLIC	SYS	UTL_FILE	SYS	EXECUTE
PUBLIC	SYS	UTL_HTTP	SYS	EXECUTE
PUBLIC	SYS	UTL_TCP	SYS	EXECUTE

Şekil 7.20. Public rolünde bulunan kritik yetkiler

Aşağıdaki komutlar çalıştırılarak Şekil 7.20'de listelenen bu yetkilerin public'ten alınması sağlanır.

REVOKE EXECUTE ON SYS. DBMS_RANDOM;
REVOKE EXECUTE ON SYS.UTL_FILE;
REVOKE EXECUTE ON SYS.UTL_HTTP;
REVOKE EXECUTE ON SYS.UTL_TCP;

7.3. İşletim Sistemi Güvenliği Kontrolleri

İşletim sistemi güvenliği kontrolleri kapsamlı bir konu olup işletim sistemleri ana temalı çalışmalarda daha detaylı incelenmektedir. Bu başlıkta 27001 Bilgi güvenliği kapsamında veri tabanı tarafını ilgilendiren işletim sistemleri kontrollerine kısaca yer vereceğiz.

Programlar ile donanımlar arasındaki ilişki işletim sistemi tarafından sağladığından hafıza yönetimi ve girdi/çıktı işlemleri de işletim sistemi kontrolündedir. Veri tabanı yönetim sistemleri de birer program olduğundan, fiziksel katmanda veri tabanında bulunan veriler işletim sistemi bloklarından oluşan disk dosyalarında tutulmaktadır. Bu dosyalar, veri, kontrol ve log dosyalarından oluşmaktadır. Oracle Linux, Microsoft Windows gibi uygulamaların üzerinde koşacağı işletim sistemleri ile veri tabanı dosyaları ve işlemleri listelenebilir. Bu nedenle de veri tabanı işletim sistemine erişim, güvenlik açısından son derece önemlidir.

İşletim sistemi sadece veri tabanına ayrılmalı ve veri tabanı yöneticileri dışında hiç kimse ssh, ftp veya uygulama dışından başka bir yöntemle işletim sistemine erişim sağlayamamalıdır. İşletim sistemine sadece veri tabanı yöneticilerin güvenli protokoller üzerinden erişim sağladığı kontrol edilmeli ve işletim sisteminde kaldırılması gereken hesaplar tespit edilirse bunlar kaldırılmalıdır. Oracle veri tabanında "oracle" kullanıcısı dışında hiçbir kullanıcı **$TNS_ADMIN ($ORACLE_HOME/network/admin)** yapılandırma dosyası içinde bulunan bilgilere işletim sistemi üzerinden erişememelidir.

Bunun için de tnsname.ora dosyası 640, listener.ora, sqlnet.ora gibi TNS_ADMIN dizininde bulunan diğer dosyalar 600 erişim hakkına sahip olmalıdır [52].

Veri Tabanı Yönetim Sistemi Bileşenleri başlığı altında da değinilen yapılandırma dosyaları ve veri dosyaları işletim sistemi üzerinden doğrudan güncellenmeye kalkılırsa veri tabanı bütünlüğü zarar görebilir. Her veri tabanı yönetim sisteminin kendine özgü tüm veri tabanı verilerini içeren veri dosyaları, veri tabanının fiziksel yapısı ile ilgili bilgileri barındıran ve veri tabanın yedeğinin alınmasını ve yedekten dönülmesini sağlayan Recovery Manager (RMAN) aracının kalıcı ayarları ve yedekleme bilgilerini içeren kontrol dosyaları, veri tabanında yedekten geri dönme işleminde yüklenen verilerin eksik olan işlenmemiş verilerini tutan redolog dosyaları vardır [53]. Veri tabanının devamlılığının ve bütünlüğünün sağlanabilmesi bozulan bilgilerin veya ulaşılamayan veri tabanlarının düzeltilebilmesi için bu işletim sistemi dosyalarının korunması çok kritiktir. Bu korumayı sağlayabilmek için işletim sistemi dosyalarına sadece gerçekten erişme gerekliliği olan kullanıcılar erişmelidir. Bu nedenle sadece; veri tabanı dosyaları, yedekleme ve yama işlemleri gibi işlemleri gerçekleştiren veri tabanı yöneticilerine erişim hakkı tanımlanmalıdır. İşletim sistemine bağlanarak veri tabanı dosyalarının dizinleri ve bu dizinlerin erişim hakları tespit edilmeli Windows işletim sistemi için everyone hakkına sahip olan dizinlerdeki kullanıcı haklarının gerçekten gerekliliği var olanlar belgelendirilmeli diğer kullanıcılardan bu hak planlı bir çalışma ile geri alınmalıdır. Unix işletim sisteminde de dosya erişim hakkı 770'den fazla olmamalıdır.

Oracle veri tabanında işletim sisteminde yer alan, haklarının kontrol edilmesi gereken önemli dosyaların dizin bilgileri şöyledir:

$ORACLE_BASE/oradata/<sid>

Oracle_base Oracle veri tabanı yöntem sistemi kurulduğunda Oracle yazılımının bulunduğu binary dosyalarının bir önceki klasör adıdır. Veri sözlüğü, sistem geri alma segmenti gibi veri tabanının temel işleyiş bilgileri de bu klasörde bulunan system tablo alanında yer almaktadır. Tablo alanına atanan mantıksal yapılar tablo, prosedür vb. bu tablo alanının fiziksel veri dosyalarında saklanır. Böylece tablo alanına atanan şema nesnelerinin depolama konumları belirlenmiş olur. Tablo alanları yedekleme ve kurtarma işlemleri için de olmazsa olmazdır. ".dbf" uzantılı dosyalar tablo alanı dosyalarıdır.

$ORACLE_HOME/dbs/ INIT.<veri tabanı>.ORA

Oracle veri tabanının başlatılması sırasında arka plan işlemleri parametre dosyalarında başlar. Oracle parametre dosyalarını okuyarak sistemle ilgili bir çok bilgiye ulaşır. Veri tabanının beyni diye de ifade edebileceğimiz controlfile' ın adresi, arşive kaç dakikada çıkılacağı ve arşiv dosyalarının nerede tutulacağı gibi bilgilere parametre denmekte ve bu parametreler birleşerek parametre dosyalarını oluşturmaktadır. Parametre dosyaları oracle yazılım kurulum dosyalarının bulunduğu ORACLE_HOME klasöründedir. Önce bu klasörden parametre dosyaları okunup sonra controlfile'lara erişilip oracle datafile'lar kullanılmaya başlanır. Başlangıç parametre dosyaları init.<veri tabanı>.ora veya init.ora formatında klasörde tutulur. Örneğin veri tabanı ismimiz testdb olsun init.testdb.ora formatındaki dosya parametre dosyasıdır ve $ORACLE_HOME/dbs/ klasöründe bulunur.

Veri tabanı başladığı zaman mutlaka olması gereken önemli parametreler aşağıdaki sorgu çalıştırılarak Şekil 7.21'de görüldüğü gibi listelenebilir:

select name from v$parameter where isbasic='TRUE';

NAME
processes
sessions
nls_language
nls_territory
sga_target
control_files
db_block_size
compatible
log_archive_dest_1
log_archive_dest_2
log_archive_dest_state_1
log_archive_dest_state_2
cluster_database
db_create_file_dest
db_create_online_log_dest_1
db_create_online_log_dest_2
db_recovery_file_dest
db_recovery_file_dest_size
undo_tablespace
instance_number
ldap_directory_sysauth
remote_login_passwordfile
db_domain
shared_servers
remote_listener
db_name
db_unique_name
open_cursors
star_transformation_enabled
pga_aggregate_target

Şekil 7.21.Veri tabanı önemli parametreleri

Şekil 7.21'de de görülen Oracle veri tabanı, parametrelerinin bazıları çevrimiçi olarak değiştirilebilirken bazı parametrelerin değişikliklerinin aktifleşmesi için işletim sisteminin kapatılıp yeniden açılması gerekmektedir.

$ORACLE_HOME/dbs/orapw$ORACLE_SID

Veri tabanlarına bağlanmak istenen kullanıcılar veri sözlüğündeki kullanıcı bilgileri ile kıyas edilerek veri tabanına erişimleri gerçekleştir. Veri tabanı açılmadan önce veri sözlüğünden kıyas yapılamayacağı için veri tabanı oluşturulurken veya hazırlanırken veri tabanına

erişmesi gereken veri tabanı yönetici bilgileri password_file dosyasında tutulur. Orapwd dosyası yüksek yetkiye sahip sys gibi ayrıcalıklı kullanıcıların şifre bilgilerini saklar.

$ORACLE_HOME/network/admin listener.ora

Veri tabanı dinleyicisi (listener), veri tabanına gelen istekleri dinleyip trafiği yöneterek istekleri veri tabanı sunucusuna iletir. $ORACLE_HOME/network/admin klasöründe bulunan listener.ora dosyası; dinlediği veri tabanlarını, dinleyeceği ıp port bilgilerini, listener şifrelerini, listener log ve izleme dosyalarını yani listener'ın nasıl çalışacağına dair gerekli tüm bilgileri içerir. Listener yapılandırmasında değişiklik yapmanın iki yöntemi vardır ilki doğrudan listener.ora dosyasında değişiklik yapmak diğeri terminalden "lsnrctl" komutu ile listener'a bağlanarak değişiklik yapmaktır. Listener.ora dosyasında yapılan değişikliğin aktifleşmesi için listener'ın yeniden başlatılması gerekir.

LSNRCTL SET PASSWORD
LSNRCTL SAVE CONFIG

Listener veri tabanı erişimleri için çok kritik öneme sahiptir. Listener güvenliği, işletim sistemi aracılığı ile yapılmaya çalışılır. Bunun dışında, listener başlatma veya durdurma, listener yapılandırma dosyasında yapılan değişiklikleri loglama gibi işlemlerin güvenliğini sağlamak için listener şifrelenebilir [54]. Şifrelenmiş Listener parolası oluşturmak için yukarıdaki komutlar çalıştırılmalıdır:

ADDRESS= (PROTCOL=TCPS) (HOST=HOST_NAME)(PORT=PORT1)
Kötü niyetli saldırganlar tarafından listener parolasının çalınma ihtimalini azaltmak için listener.ora dosyasında yukarıdaki düzenleme ile SSL protokolü kullanılarak şifreli iletişim ayarı yapılmalıdır.

Veri tabanı erişimlerini kontrol altında tutmak için listener log ve izleme dosyaları aşağıdaki komutlar çalıştırılarak aktifleştirilmeli ve böylece izinsiz giriş denemelerinin takibini yapıp önlemler alınmalıdır.

LSNRCTL SET LOG_DIRECTORY $ORACLE_HOME/Network/Log
LSNRCTL SET LOG_FILE Listener.log
LSNRCTL SET LOG_STATUS=on

Oracle veri tabanı kurulduğunda listener varsayılan 1521 portu üzerinden bağlantı sağlanmasını sağlayacağından varsayılan port bilgisini kullanmak saldırganların veri tabanına kolay erişimine imkan sunacaktır. Bu nedenle veri tabanlarında varsayılan port bilgisi yerine, 1521-1550 ve 1600-1699 aralığından farklı bir port bilgisi vermek saldırganların veri tabanına erişimini zorlaştıracaktır. Aşağıda $ORACLE_HOME/network/admin/listener.ora dosyası içerisinde Listener parametresinin karşılığında yer alan port değişkeninin değeri 15021 ile değiştirilmektedir:

```
LISTENER =
  (DESCRIPTION_LIST =
    (DESCRIPTION =
      (ADDRESS = (PROTOCOL = TCP)(HOST = HOST_NAME)(PORT = 15021))
      (ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC15021))
    )
  )
```

Windows ortamında kayıt defterinde bulunan dosyalar ve içlerindeki anahtarlar veri tabanının güvenli bir şekilde çalışması için yapılandırma değerlerini tutar bu nedenle kayıt defterlerine erişimin güvence altında olması gerekmektedir. Windows kayıt defterinde Oracle veri tabanının parametreleri aşağıda verilmiştir eğer buralara izinsiz erişimler sağlanıp uygun olmayan değerler atanırsa veri tabanı çalışmaz hale getirilebilir. Bu nedenle sadece veri tabanı altında çalışan hesaba kayıt defterinde düzenleme, silme yetkisi verilmeli bir değişiklik yapılmadan önce de muhakkak sistem yedeklenmelidir. Kayıt defteri düzenleyicisi ile kayıt defteri anahtarına erişim izni olan kullanıcılar listelenmeli ve gereksiz erişim izinleri tespit edilirse bunlar kaldırılmalıdır.

HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE\KEY_HOME_NAME
HKEY_LOCAL_MACHINE\SOFTWARE\ORACLE
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

7.4. Veri Şifreleme

Veriler hem bilgisayar ağ trafiğinden geçmesi hem de işletim sisteminde dosyalarla saklanıyor olmasından dolayı veri tabanı kullanıcısı olmayan kötü niyetli kişiler tarafından ele geçirilme riski ile karşı karşıyadır. Ağdaki trafiğin dinlenmesi ve işletim sisteminde

saklanan verilere yetkisiz erişimlerin gerçekleşmesini önlemek için veri şifreli saklanmalı ve veri tabanı trafiği de şifrelenmelidir.

Veri şifreleme bir bilginin belirli algoritmalara göre şifrelenerek yalnızca yetkili kişiler tarafından okunabilmesine olanak tanıyan kodlama işlemidir. Bir bilgi şifrelendiğinde ulaşılmaz hale gelmiş olmaz ancak yetkisiz kişilerin eline geçtiğinde anlaşılabilir bir içerik bulmalarını büyük oranda engeller. Bilgiler kriptografik algoritmalar kullanılarak şifrelenir ve sadece yetkilendirilen kullanıcı verilen anahtarla veriyi kolayca çözer ancak şifreleme yönteminin kolay tahmin edilebilir basit bir algoritma olması, anahtarların kısa olması veya anahtar bilgisinin ifşa edilmesi gibi durumlarda şifrelenmiş veri de güvende olmaz.

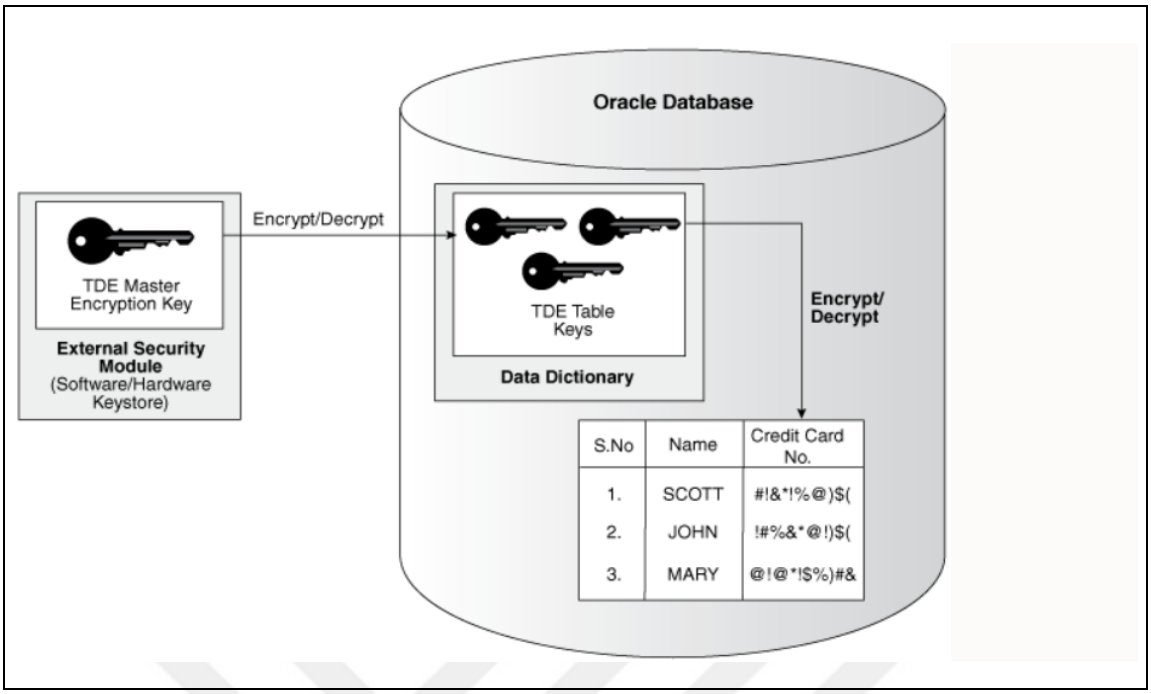
Veri tabanına çoğunlukla uzaktan bağlantılar ile bağlanıldığından veri tabanı trafiği bilgisayar ağlarından Oracle ait bir network teknolojisi olan TNS(Şeffaf Ağ Alt Katmanı) protokolü ile TCP/IP paketleri ile geçmektedir. Veri tabanı trafiği, oturum kimlik bilgisi, sorgu ve sorgudan dönen cevap yani verinin kendisinden oluşmaktadır. Trafiği dinlemek isteyen kötü niyetli kişiler çeşitli uygulamaları kullanarak trafiğin içini okumakta ve böylece oturum bilgilerini, verinin kendisini ele geçirebilmektedir. Bu tür istismarların önüne geçebilmek için ağ ve istemci sürücülerinin SSL/TLS (Güvenli Soket Katmanı/Taşıma Katmanı Güvenliği) protokolünü kullanarak trafik şifreleme yapılandırmalarını yaptığı ve bilgilerin gizliliğini korumak için güvenli kabul edilen TLS1.2 ve TLS1.3'ün kullanıldığı kontrol edilmelidir ve uzak bağlantılar için VPN kullanılarak veya SSH protokolü ile tünelleme yapılarak trafiğin şifreli geçmesinin sağlanması gerekmektedir.

VPN (Virtual Private Network), birçok farklı protokol ve teknolojiyi bir arada kullanarak istemciyi fiziksel olarak bulunmadığı yerdeki bir ağa şifreli iletişim yaparak güvenli bir tünel kurarak eriştirmektedir. Bu tünel içindeki verileri, araya girip trafiği dinlemek isteyen kişi şifreli görür ve güçlü kriptolar kullanıldıysa içeriği anlaşılır hale getiremez ve böylece trafiğin güvenli hale gelmesi sağlanır. SSH tünelleme ile de istemci yerel bir TCP portuna trafiği gönderir tünelleme aracı bu porta gelen işlemleri uzak sunucu IP adresi ve portuna SSH protokolü ile tüm trafiği şifreleyerek yönlendirir. Windows işletim sistemi kurulu olan yerel makineden Linux işletim sistemi kurulu olan veri tabanı sunucusuna Putty uygulaması gibi uygulamalar kullanılarak, çoğu Linux işletim sistemi kurulu olan makinelerde ön tanımlı gelen SSH istemcisi ile tünelleme işlemi yapılabilmektedir.

Diskteki veya veri tabanındaki veriler ağ trafiğindeki verilerden daha uzun ömürlüdür ve verilerin doğrudan veri tabanından çalınma oranı ağ trafiğinden çalınma oranından çok daha fazladır. Bu nedenle depolama ortamı, test veri tabanı ve gerçek veri tabanındaki verilerin şifrelenmesi daha üzerinde durulması gereken bir konudur. Verilerin korunması için oracle birçok çözüm geliştirmiştir. Oracle Advanced Security (ASO) ile birlikte gelen Transparent Data Encryption (TDE) ve Data Redaction en yaygın olarak kullanılan yöntemlerdir. Transparent Data Encryption (TDE) yöntemi ile uygulamalarda değişiklik yapılmadan veriler fiziksel olarak saklandıkları datafile'larda şifrelenerek tutulur böylece kötü amaçlı kişiler datafile'lara ya da backup'lara erişse dahi verilerin güvenliği zarar görmez. TDE, bir tablo sütununda saklanan verinin şifrelenmesini sağladığında bu veriye erişim yetkisi olan kullanıcı verinin şifreli olduğunu dahi anlamadan herhangi bir şifreyi çözme işlemi gerçekleştirmeden veriyi şeffaf haliyle görür. Veri şifreleme ve şifre çözme veri tabanının kendisi tarafından yönetilir bu nedenle yetkili kullanıcı diskte şifreli tutulan bir veriyi SQL sorguları ile çektiğinde düz metin olarak görür.

Oracle, şifreleme anahtarlarını bir güvenlik modülünde veri tabanının dışında yalnızca güvenlik sorumlusu tarafından erişilebilecek şekilde saklamayı önermektedir eğer şifreleme anahtarı şifrelenen veri ile aynı yerde saklanıyorsa yetkisiz kişilerin verileri okuması çok kolay olur. Bu nedenle şifre anahtarlarının nerede tutulduğu kontrol edilmelidir. Ayrıca şifreleme anahtar yönetimi Bilgi Güvenliği felaket kurtarma planlarında da yer almalı, yedekleme prosedürlerinde şifreleme özellikleri ile beraber şifre anahtarı yönetimi de bulunmalıdır ki bu sayede felaket anında yedekten veri tabanı dönüldüğünde şifreli verilerde kurtarılabilsin.

TDE ile tablo alanı veya sütun bazında şifreleme yapılabilmektedir. Eğer tablo alanı şifrelenecek ise tabloanlanının sıkıştırılmamış olması, eğer kolon şifrelenecek ise kolonun çok güncellenmeyen anne kızlık soyadı, tc numarası gibi verileri içeriyor olması önerilmektedir. Eğer yabancı anahtarlı kolon şifrelenecekse ya da indeksli ve çok sayıda kolon şifrelenecekse o zaman tablo alanı şifrelemesi tercih edilebilir.



Şekil 7.22. Şeffaf veri şifreleme [55]

Transparent Data Encryption(Şeffaf veri şifreleme) işlemi yapılırken öncelikle şifreleme esnasında kullanılacak anahtarın saklanacağı bir dizin oluşturulur ve anahtar veri tabanında bir sözlük tablosunda saklanır. Şekil 7.22'de de görüldüğü üzere sözlük tablosundaki kolon anahtarları da ana şifreleme anahtarı ile birlikte veri tabanı dışında harici bir güvenlik modülünde saklanır. Harici güvenlik modülü(cüzdan) ile anahtarları, veri tabanından da ayırarak yalnızca güvenlik sorumlusunca erişilebilen veri tabanı yöneticisinin dahi erişemediği güvenli bir yapı oluşturulmuştur [55].

Anahtarın saklanacağı dizini belirledikten sonra Sqlnet.ora dosyasının içerisine giderek aşağıdaki satırlar eklenerek wallet location parametresine cüzdan yeri atanır.

ENCRYPTION_WALLET_LOCATION =
(SOURCE = (METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /oracle/product/db/network/admin/wallet))))

Anahtarın saklanacağı dizin hazırlandıktan sonra şifreleme ve şifreyi çözmek işlemi için kullanılacak ana şifreleme anahtarı aşağıdaki komutla oluşturulur. En az 8 karakterden oluşan güçlü bir şifre verilmesi önerilmektedir.

ALTER SYSTEM SET ENCRYPTION KEY IDENTIFIED BY "RbYn2*w9";

Ana şifreleme anahtarını aktif etmek için de aşağıdaki komut çalıştırılır.

ALTER SYSTEM SET ENCRYPTION WALLET OPEN IDENTIFIED BY "RbYn2*w9";

Şifreleme için anahtar oluşturulduktan sonra şifrelenecek nesne belirtilmeli ve ENCRYPTION anahtar kelimesi ile AES192,3DES168, AES128, AES256 kriptolama algoritmaları ile daha güvenilir tablolar kolonlar, tablo alanları hazırlanır. Aşağıdaki örnekte personel isimli tablo ilk yaratılırken sicil numarası kolonun şifreli olarak saklanması encrypt anahtar kelimesi ile sağlanmıştır.

CREATE TABLE Personel
(isim CHAR(15) NOT NULL,
soyisim CHAR(15) NOT NULL,
sicil INT NOT NULL ENCRYPT);

Bu tabloya veri eklenirken standart insert işlemi gerçekleştirilir. Fakat sicil kolonu encrypt değerinde olduğundan aşağıda gönderilen '11111111111' değeri diske şifreli yazılır.

INSERT INTO Personel (isim, soyisim, sicil, adres) VALUES ('Rabia', 'Yıldız','111111111111');

Tablo oluşturulduktan sonra da bir kolona şifre konulabilmektedir. Örneğin personel tablosunun isim alanına da şifre konulması gerektiğinde kullanılacak komut aşağıdaki gibi olmalıdır:

ALTER TABLE Personel MODIFY isim ENCRYPT;

Tablonun bir kolonundaki şifreyi çözmek o kolonu diskte şifresiz tutmak içinde aşağıdaki komut çalıştırılmalıdır:

ALTER TABLE Personel MODIFY sicil DECRYPT;

Kolonu şifrelemek için kullanılan algoritmayı değiştirmek için aşağıdaki komut çalıştırılmalıdır:

ALTER TABLE Personel REKEY USING 'AES256';

Yetkisiz veya görmesini istemediğimiz kullanıcıların veri tabanındaki her veriyi görmesini fiziksel değişiklik yapmadan önlemenin yolu da Oracle Data Redaction'dır. Oracle Advanced Security(ASO) ile birlikte gelen Oracle Data Redaction ve Transparent Data Encryption arasındaki en önemli fark Data redaction'ın fiziksel olarak veri maskesi yapmayıp " DBMS_REDACT " paketi yardımı ile çağrılan verileri belirlenen yönteme göre kullanıcı özelinde maskelemesidir. Böylece hassas veriler veri tabanından döndürülürken bizim seçeceğimiz Full, Partial, Regular Expression ve Random maskeleme yöntemlerinden biri ile maskelenmektedir. Bu maskeleme yöntemlerine kısaca değinirsek:

Full redaction'da etkilenen kolonda bulunan tüm değerler etkilenir dbms_redact.full default değeri '0' dır örneğin bir kart numarası kolonuna full redaction uygulanırsa yetkisiz kullanıcılar farklı bir değer ataması yapılmadı ise kart numarası alanını "0" olarak görebilirler. Ancak full redaction verinin tipine göre değişkenlik göstermektedir örneğin karakter veri tipi tutulan kolonun sorgu sonucu "0" değil boşluk olarak gösterilir.

Partial redaction'da etkilenen kolondaki değerlerin tamamı değil belirli bir kısmı düzenlenebilir örneğin 16 hanelik kart numarasının ilk 12 hanesine "1" veya "*" gibi değerler ile gösterilirken son 4 hanesi mevcut halini koruyabilir.

Regular expressions, farklı tipteki karakter değerlerini düzenlemek için kullanılır bu nedenle yalnızca karakter veri tiplerine sahip kolonların kullanımına uygundur. Örneğin farklı karakter sayılarına ve değerlerine sahip e_posta adreslerinin yer aldığı kolona uygulanarak [hidden]@example.com şeklinde düzenlenilerek, verinin tam haline erişmesi istenilmeyen kullanıcılara maskelenerek gösterilebilir.

Random redaction, en çok tercih edilen yöntemdir. Kolonun veri tipinin ne olduğu fark etmeden her sorgu sonucunda veriye farklı bir random karaktetlerden oluşan değer döndürmektedir ve sürekli benzersiz bir değer döndürülmesi veri güvenliği için önemli bir husustur.

Buraya kadar anlatılanlardan görüldüğü üzere veri şifreleme ile bilgi güvenliğinin en önemli hususlarından biri olan bilgilere izinsiz veya yetkisiz erişimlerden, bilgilerin ifşa edilmesinden, değiştirilmesinden, yok edilmesinden veriler korunmakta ve veri mahremiyeti sağlanmaktadır.

7.5. Veri Tabanı Etkinliklerini Denetleme ve Yedekleme

Veri tabanında saklanan verilerin öneminden dolayı kötü niyetli saldırganları ve yetkisiz kullanıcıların verilere erişimini belirleyebilmek, veri tabanlarının güvenliğini sağlamak için kullanıcıların veri tabanı eylemleri izlenmeli ve kaydedilmeli yani denetlenmelidir. Veri tabanı etkinliklerinin denetimi ile:

- Sorunlu işlemler kayıt altına alınarak sorunlu işlemi yapan kullanıcıların hesap verilebilirliği sağlanır ve kullanıcılarda bir caydırıcılık oluşturulur.
- Ayrıcalıklara sahip olan kullanıcılar bu haklarını kötüye kullanıyorlarsa onlar teptit edilir ve kullanıcılardan ayrıcalıkları geri alınır.
- Hangi sistemlere kim, nasıl, ne zaman erişti, yöneticiler ve kullanıcılar tarafından yürütülen işlemler ve değişiklikler neler takip edilir, veri tabanı yöneticileri için şeffaflık sağlanır.
- Kullanılan veya kullanılmayan nesneler ile ilgili log verileri toplanabilir böylece güvenliğin yanı sıra performanslı veri tabanları hazırlanır.

Oracle veri tabanlarında, her türlü veri tabanı objesinin, SQL cümleciklerinin, ağ ve çok katmanlı faaliyetlerin denetlenmesinin yanında spesifik veri tabanı faaliyetlerini denetlemek için kullanılan fine grained auditing yöntemi de vardır. Fine grained denetleme ile oluşan aksiyonlar veya bu aksiyonların oluştuğu zaman gibi belirlenilen durumlara göre özelleştirilmiş audit işlemleri yapılır.

Oracle veri tabanında denetleme işlemini yapmak için başlatma parametreleri, AUDIT ve NOAUDIT SQL ifadeleri kullanılır. AUDIT_TRAIL sistem parametresi ile audit kayıtlarının nerede ve nasıl saklanacağı belirlenir. AUDIT_TRAIL'e değer ataması yapıldıktan sonra bu değişikliğin geçerli olabilmesi için veri tabanının kapatılıp açılması gerekmektedir. AUDIT_TRAIL'e atanabilecek değerler aşağıda listelenmektedir:

- NONE: Veri tabanı yönetim sisteminde audit denetimini devre dışı bırakır.
- DB: Veri tabanındaki bütün denetimler SYS şemasında DBA_AUDIT_TRAIL görünümünde kayıt altına alınır.
- OS: Denetim kayıtları işletim sisteminde belirtilen bir dosyada saklanır.
- DBA EXTENDED: Denetim kayıtları sorgu değişkenleri ile birlikte daha detaylı veri tabanında tutulur.

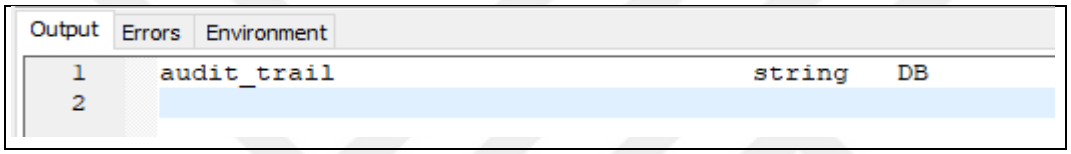
- XML: Denetim kayıtları işletim sisteminde XML türünde tutulur.
- XML EXTENDED: Denetim kayıtları sorgu değişkenleri ile birlikte daha detaylı XML türünde tutulur.

AUDIT_TRAIL parametresine atanacak değer belirlendikten sonra aşağıdaki komut ile atanmalıdır:

ALTER SYSTEM SET AUDIT_TRAIL=DB SCOPE=SPFILE;

Yukarıdaki komutla DB parametre değeri atanmıştır.

SHOW PARAMETER AUDİT_TRAİL;



Şekil 7.23. Audit_trail parametre değeri

Show parameter audit_trail komutu çalıştırıldığında audit_trail parametresinin son değeri Şekil 7.23 sorgu çıktısında görüldüğü üzere ekrana gelecektir.

Aşağıdaki komut çalıştırıldığında SYS şeması altındaki dba_audit_trail görünümünde sorguda tanımlanan kullanıcı takip edilebilir hale gelecektir.

AUDIT SELECT ANY TABLE BY 'UTLU' BY SESSION;

Aşağıdaki komutta belirtilen UTLU şemasının PERSONEL tablosundaki her türlü güncelleme ve silme işlemleri takip edilebilir hale gelir.

AUDIT UPDATE, DELETE ON UTLU .PERSONEL ;

Yukarıda standart audit işlemlerine örnekler verilmiştir ancak hassas tablolardaki sadece hassas kayıtları okuyan kullanıcıların takip edilmesinin gerektiği durumlarda fine grained auditing ile özelleştirilmiş denetimler yapılır. Veri tabanı yöneticileri bilgi güvenliğine de uygun stratejide detaylı denetim kayıtlarını DBMS_FGA paketinde oluşturabilir.

Denetlenmek istenen veri tabanı nesneleri için kural konfigürasyonu çalıştırılıp veri tabanı yönetim sistemi denetlemeye hazır hale getirildikten sonra SYS şemasının AUD$ tablosuna kayıtlar gelmeye başlayacaktır.

Buraya kadar olan kısımda denetim parametrelerinin açılması ve denetleme işleminin gerçekleştirilmesine değinildi fakat nelerin denetlendiğinin bilinmesi de önemli bir husustur. Veri tabanında yapılan her işlemi denetlemek elimizde çok fazla veri birikmesine, veri tabanında performans problemlerine ve sistem kaynaklarının tükenmesine sebep olur. Bu nedenle de sadece gerekli görülen işlemler için gereken süre kadar denetlemeler yapılmalı ihtiyaç duyulmayan denetleme işlemleri kaldırılmalıdır. Bunları belirlemek için de audit tespiti gerekli sorgular ile yapılmalıdır.

Hangi yetkiler kullanıldığında veri tabanında audit yapıldığı aşağıdaki sorgu ile öğrenilir:

SELECT * FROM sys.dba_priv_audit_opts;

Hangi nesnelerin veri tabanında audit yapıldığı aşağıdaki sorgu ile öğrenilir:

SELECT * FROM sys.dba_obj_audit_opts;

Çalıştırılan hangi komutların veri tabanında audit yapıldığı aşağıdaki sorgu ile öğrenilir:

SELECT * FROM dba_stmt_audit_opts;

Denetleme işlemi için tutulan veriler, veri tabanında hızla büyüdüğünden günümüz teknolojisinde artık denetleme işlemi için ayrı bir katman, farklı bir veri tabanı sunucusu oluşturulmaktadır. Oracle veri tabanı yönetim sisteminde; işletim sisteminden, veri tabanından, dosya sisteminden toplanan tüm denetim verilerinin Oracle Audit Vault ve Database Firewall ile esnek ve kapsayıcı bir şekilde izlenmesi sağlanmıştır. Oracle Audit Vault and Database Firewall ile bir çok veri tabanından gelen denetim verileri tek bir merkezde toplanıp bunlardaki SQL trafiği, yetkisiz erişimler takip edilebilir. Oracle Audit Vault and Database Firewall pek çok ürünü destekelemektedir Oracle veri tabanı, Microsoft SQL Sunucu, IBM DB2 for LUW, SAP Sybase ASE, Oracle MySQL veri tabanları bunlardan başlıcalarıdır. Audit Vault denetim verileri için merkezi ölçeklenebilir, güvenli bir depolama alanı sunmakla beraber raporlama, uyarma ve politika yönetimi için ideal bir platformdur.

Database Vault ile hassas verilere, ayrıcalıklı kullanıcılardan bile istenmeyenlerin erişimleri kısıtlanabilir. Böylece tüm veri tabanı yöneticileri veya ayrıcalıklara sahip olan her kullanıcı veri tabanındaki bütün verilere erişemez, hassas verilerin çalınması ve uygulamalarda yetkisiz değişikliklerin yapılması da önlenir. Veri tabanında hangi kullanıcıların neleri yapabileceği, veri tabanlarına ne zaman erişebileceği de kontrol altına alınır.

Oracle Database firewall, ağ katmanında kurulumu yapıldığından ağ üzerinde ilk korunma mekanizması sağlar böylece yaşanabilecek ağ hataları, SQL enjeksiyonu ve veri tabanındaki diğer zararlı durumlar Database firewall ile engellenebilir. Database firewall, ağ katmanından veri tabanı gitmekte olan SQL sorgularını analiz, izleme, bloklama, değiştirme ya da hiçbir işlem yapmadan direk veri tabanına iletme görevi görmektedir. Geliştirilen özel yapısı ile veri tabanına ulaşması istenilmeyen sorgular belirlenebilmekte, SQL'in yapısını inceleyerek SQL enjeksiyon saldırılarını tespit edebilmekte, bu saldırıları bloklayıp eğer istenirse belirlenen kişilere mail atabilmektedir. Oracle bu ürünleri ile veri tabanı güvenliğini çok yüksek seviyelere çıkarabilmekte bu nedenle de Database firewall, Audit Vault ve Database Vault üçlüsünü tavsiye etmektedir.

Veri tabanı yönetim sistemleri başlığı altında yedekleme ve geri dönüş alt başlığında yedeklemenin gerekliliğine ve yedekleme türlerine detaylıca yer verilmişti. Oracle veri tabanı yedeklemesini farklı bir bakış ile gerçekleştirebildiğini, işletim sistemi seviyesinde, yedekleme ve kurtarma aracı RMAN ile ve mantıksal yöntemlerle yedekleme yapabildiğini belirtmektedir.

İşletim sistemi seviyesinde yani fiziksel yedek alma işlemi; veri dosyaları, redolog dosyaları ve kontrol dosyalarının işletim sistemi komutları ile yedeklenmesidir. Bu yedekleme veri tabanı servislerinin kapalı olduğu NOARCHIVELOG modu veya veri tabanı servislerinin açık olduğu ARCHIVELOG modunda olmak üzere iki şekilde yapılabilmektedir.

NOARCHIVELOG modunda veri tabanı çalışırken arşivleme işlemi devre dışı bırakılır ve klasik kopyalama mantığı ile kapatılan veri tabanının veri dosyaları, redolog dosyaları, kontrol dosyaları başka disk ortamına yedeklenir. Bu yedekleme yöntemi; yedek alınırken veri tabanının kapatılması gerektiğinden veri tabanının sürekli açık kalması gerekmeyen, bütün veri dosyaları, redolog dosyaları, kontrol dosyalarının teker teker yedeği alınacağından veri tabanında verisi az olan, arşivleme yapılmadığından iki yedek arasında yapılan işlemler kaybolacağından veri tabanında bir miktar veri kaybını tolere edebilecek

kurum ve kuruluşlar tarafından kullanılmalıdır. NOARCHIVELOG modunda çalışan bir veri tabanında yedekten geri yükleme gerektiğinde sadece veri tabanı kapalı iken alınan tam yedekler kullanılacağından düzenli ve sık aralıklarla yedek alınmalı fakat sistem sürekliliği ve performans kaybını önlemek için bu işlem geceleri yapılmalıdır.

ARCHIVELOG modunda çalışan veri tabanında, redo log günlüklerinin arşivlenmesi etkin olur. Veri tabanında yapılan değişiklikler redo log dosyalarına yazıldığından veri dosyaları, redolog dosyaları, kontrol dosyalarının tek tek kopyalanması gerekmez. Archivelog modunda yedekleme işlemleri veri tabanı kullanımdayken yapılabilir ve arşivlenmiş redo günlüğü dosyaları sayesinde yedekten geri dönmek gerektiğinde tüm commit edilmiş verileri kurtarabilir bu nedenle iş sürekliliğinin kesintiye uğramaması gereken ve veri kaybının kabul edilebilir görünmediği kurumlarda archivelog modunda yedekleme işlemi yapılmalıdır. Archivelog modu oracle veri tabanının nomount aşamasında aşağıdaki komutun çalıştırılması ile set edilebilir:

ALTER DATABASE ARCHIVELOG;

Archivelog modu aktifleştirildikten sonra tek tek veri dosyalarının mantıksal düzeydeki karşılığı olan tablo alanlarının kopyalarının alınması gerekir.

ALTER TABLESPACE <tabloalan_adı> BEGIN BACKUP;

Tüm veri dosyaları için yukarıdaki komutu tek tek çalıştırıp yedekleme işlemini tamamladıktan sonra aşağıdaki komut çalıştırılır.

ALTER TABLESPACE < tabloalan_adı > END BACKUP;

Kontrol dosyalarının kopyalanması işlemi için de aşağıdaki komut çalıştırılır.

ALTER DATABASE <SID> BACKUP CONTROLFILE TO <kopyalanacağı_dizin_adı>

Oracle veri tabanı, dışarı veri aktarımı(export) ve içeri veri alma (import) komut modunda çalışan yardımcı programları ile mantıksal yedekleme yapmaktadır. Bu yöntemde, log dosyaları ya da kontrol dosyaları yedeklenmeden veri tabanı nesneleri, verilerin anlık görüntüsü işletim sistemi dosyası haline dönüştürülerek yedeklenmektedir ve yedek alırken veri tabanı kapatılmak zorunda değildir. Dışarı aktarılan veri yedekleri import işlemi ile

içeri aktarılmaktadır. Mantıksal yedekleme yönteminin avantajları; günlük, haftalık vb. tarihe göre yedek almak kolay olduğundan bu yedekler ile veri tabanının durumunu, gelişimini takip etmek daha kolaydır. Veri tabanı nesnelerinin yedekleri, veri tabanı verilerinin anlık görüntüsü alınabildiğinden bir uygulamaya ait istenilen nesneler başka bir ortama kolayca aktarılabilir. Veri tabanı versiyon değişikliklerinde verileri taşımada, veri tabanları arasında veri kopyalamada kullanılabilir.

Yedekleme ve kurtarma aracı, Recovery Manager yani RMAN ile veri tabanının tamamı, tablo alanları, kontrol dosyaları, arşiv logları yedeklenebilir. RMAN, işletim sisteminden bağımsız bir araçtır. İşletim sistemi seviyesindeki yedeklemelerde boş alanlarında yedeği alınıyordu RMAN boş alanların yedeğini almayarak daha performanslı bir yapı sunmaktadır. Ayrıca blok seviyesinde yedekleme yapabildiğinden blokları değişenleri sadece değişen kısımları yedekleyen, incremental yedekleme seçeneğini de sunmaktadır. RMAN aracı ile tek tek el ile yapılan yedekleme işlemleri otomatik hale getirilebilmekte, veri tabanının düzenli yedeği alınabilmekte ve arıza anlarında arşiv logları otomatik uygulanıp sistemi kurtarma işlemi gerçekleştirilebilmektedir. RMAN ile standart bir yedekleme şöyle alınır:

RMAN kullanımında, yedeklenen veri tabanının kontrol dosyaları kullanımından ziyade yedekten dönme işlemlerini ve takibi kolaylaştırdığından katalog veri tabanı tercih edilmelidir. Tüm değişikliklerin çevrimiçi kaydedilmesi için yedeklenecek veri tabanı archivelog moduna alınmalıdır. Veri tabanının istenilen şekilde yedeklenmesini sağlayacak olan RMAN'ın kendi sorgu dilinde yedeklemeyi yapacak sorgu ve de hangi tip level0, level1 gibi RMAN yedeğinin alınacağını belirleyen ve buna göre yedekleme başlamadan RMAN sorgularını hazırlayan işletim sistemi sorguları veri tabanı yöneticisi tarafından hazırlanmalıdır. Hazırlanan RMAN sorgusu ile yedekleme yapacak ve sonucunu veri tabanı yöneticilerine mail ile bildirecek sorgu da veri tabanı yöneticisi tarafından hazırlanır.

Yedekleme politikasında dikkate alınması gereken en önemli husus veri tabanın en kısa sürede kurtarılabilmesidir. Politika belirlenirken, ne kadarlık veri kaybı tolere edilebilir, veri tabanının kurtarılması için geçecek ortalama süre ne kadar olur, yedekleme süresi ne kadar faktörleri dikkate alınmalıdır. Veri tabanında sıfır kesinti olması gerekli ise sadece veri tabanı asla yeterli olmayacaktır, replikasyon, paralel sunucu gibi yöntemler muhakkak kullanılmalı, archivelog modu hep aktif tutulmalıdır. Veri tabanına tablo alanı, veri dosyası yani yapısal herhangi bir değişiklik yapılacaksa veri tabanının o işlemden önce yedeği alınmalı, arşiv logların kaybolması veya bozulması ihtimaline karşı birden fazla yerde arşiv

logların yedeği tutulmalı, son alınan yedeğin kaybolması veya bozulması ihtimaline karşın eski veri tabanı yedekleri de saklanmalıdır.

Yedekten kurtarma gereken durumlarda istenilen zamana en hızlı şekilde dönebilmek için en önemli şart en yakın yedeğin ve arşiv logların sistemde sağlam olmasıdır. Eğer yedek alınma tarihi eski ise arşiv loglarında boyutları büyük ise bu veri tabanı kurtarma hızını olumsuz etkiler. Bu nedenle alınan yedekler kontrol edilmelidir. Yedeklerin doğru alındığını kontrol edebilmek için çalıştırılması gereken sorgu aşağıdadır:

```
SELECT start_time,
end_time,
input_type,
status
FROM V$RMAN_BACKUP_JOB_DETAILS
ORDER BY 1 DESC;
```

START_TIME	END_TIME	INPUT_TYPE	STATUS
31-OCA-22	31-OCA-22	ARCHIVELOG	COMPLETED
31-OCA-22	31-OCA-22	DB INCR	COMPLETED
30-OCA-22	30-OCA-22	ARCHIVELOG	COMPLETED
30-OCA-22	30-OCA-22	DB INCR	COMPLETED
29-OCA-22	29-OCA-22	ARCHIVELOG	COMPLETED
29-OCA-22	29-OCA-22	DB INCR	COMPLETED
28-OCA-22	28-OCA-22	ARCHIVELOG	COMPLETED
28-OCA-22	28-OCA-22	DB INCR	COMPLETED
27-OCA-22	27-OCA-22	ARCHIVELOG	COMPLETED
27-OCA-22	27-OCA-22	DB INCR	COMPLETED
26-OCA-22	26-OCA-22	ARCHIVELOG	COMPLETED
26-OCA-22	26-OCA-22	DB INCR	COMPLETED
25-OCA-22	25-OCA-22	ARCHIVELOG	COMPLETED

Şekil 7.24 Günlük yedekleme

Şekil 7.24'de görüldüğü üzere günlük yedeklemenin başlangıç ve bitiş tarihi, tipi ve yedeğin başarılı bir şekilde tamamlanıp tamamlanmadığı soru sonucu ile görülebilmektedir. Yedeğin kaç dakika sürdüğü, yedeğin boyutu bilgileri de görülmek istenildiğinde sorgunun select kısmı aşağıdaki şekilde düzenlenmelidir:

```
SELECT start_time,
end_time, input_type,status,
output_bytes_display,
time_taken_display
FROM V$RMAN_BACKUP_JOB_DETAILS
ORDER BY 1 DESC;
```

Veri yedekleme cihazlarının çalınması veya yedeklenen verilere yetkisiz erişimlerin gerçekleşmesi ile hassas veriler ifşa edilebilir. Veri tabanı kopyalarını korumak için güvenli bir mekanizma geliştirilmeli, tüm veri tabanları ve ilgili yedeklemeler için kurum bir envantere sahip olmalıdır. Bu varlık envanterinde, kurum bünyesindeki tüm veri tabanlarına ait donanım ve yazılım bilgileri, varlığın sahibinin kim olduğu, bilgi sınıflandırması yapılarak erişim haklarının belirlenmesi, saklanma koşulları ve depolama için kullanılan medya desteğinin nasıl elden çıkarılacağı yani imhanın nasıl yapılması gerektiği konuları kurumsal bilgi güvenliği politikalarına göre belirlenmelidir.

Kötü niyetli kişiler, veri tabanında bulunan hassas bilgilere erişmek için işletim sistemi dosyalarını ve yedekleme ortamlarını hedef alır. Bu ortamlara erişmek saldırganlar için veri tabanlarına erişmekten daha kolaydır. Çünkü pek çok kurumda veri tabanlarının yedeklerinin tutulduğu ortamlarda gerekli denetimlerin ve kontrollerin olmadığı bilinmektedir. Oracle'da yedekleme verilerinin ifşa edilmesini önlemek için veri şifreleme başlığı altında anlatılan gelişmiş veri tabanı şifreleme yöntemleri ile veri tabanı yedekleri şifrelenmelidir.

7.6. Veri Tabanı Özelinde Hazırlanabilecek Bilgi Güvenliği Dokümanları

Kurum ve kuruluşlar, iş süreçlerinin planlanması, uygulanması ve iyileştirilmesi amacıyla bilgi güvenliği yönetim sistemi kapsamında hazırlanan yol gösterici politika, prosedür ve talimatlar ile süreçlerin nasıl geçekleştirileceğini belirlemektedir.

Politikalar, üst yönetim tarafından desteklenen resmi talimat ve beyanlar ile bilgi güvenliği hedeflerinin yansıtıldığı dokümanlarken prosedürler ise, sık tekrarlanan bilgi güvenliği ile ilgili görevi gerçekleştirmek için adım adım talimatlar içeren dokümanlardır [1].

Bilgi güvenliği yönetiminde, yönetim, BGYS ekibi, teknik personel, kurum personeli gibi çeşitli roller bulunmakta ve Kurum Üst yönetimi tarafından bu rollere BGYS ile ilgili görevler için sorumlu ve yetkililerin ataması yapılmalıdır. Veri tabanı sorumluları da üst

yönetimce uygun bulundukları bir rolde diğer roller ile uyumlu çalışmalar yürüterek kurumsal bilgi güvenliği olgunluk düzeyini üst seviyelere çıkarmayı hedeflemelidir. Bu süreçte; bilgi güvenliği kapsamında yer alan veri tabanındaki verilerin güvenliğinin ve sürekliliğin sağlanması için Ek-1 ve Ek-2'de kılavuz olması amacıyla hazırlanan taslak dokümanlara yer verilmiştir.

8. SONUÇ, TARTIŞMA VE ÖNERİLER

Bilgi toplumu olmak ve bilgi çağında yaşamak, işlerin sürdürülebilmesi için yoğun şekilde bilgi kullanımını bir ihtiyaç haline getirmiş bilgiye olan bu ihtiyaçta, bilginin korunması gerekliliğini gündeme getirmiştir. Bilginin silinmesi, tahrip edilmesi, bütünlüğünün bozulması, gizliliğin zarar görmesi, erişilebilirliğinin sağlanamaması gibi bilgiye yönelik saldırılardan meydana gelecek aksaklıkları en aza indirmek için bilgi güvenliğinin sağlanması zorunla hale gelmiştir.

Yapılan araştırmalar sonucunda, bilgi güvenliği ve veri tabanı konusunda kendimiz daha çok bilgi edinip, daha iyi eğitilmeyi sağlamış olduk. Araştırmaya başlamadan önce yapılan literatür taramaları, çalışmamızı belli bir noktaya kadar getirmemize olanak sağlıyor fakat ihtiyacımız olanı bulamayıp varmak istediğimiz sonuca varamadan eksik bırakıyordu. Bu nedenle bizi sonuca ulaştıracak her türlü kaynağı ve edindiğimiz tecrübe ve bilgileri kullanarak bir çalışma gerçekleştirmeyi hedefledik.

ISO27001 Bilgi Güvenliği Yönetim Sistemi standardı gerekliliklerini yerine getirerek sertifika sahibi olan kurumlar; gizlilik, bütünlük, erişilebilirlik ve güvenliğe verdiği önemi uluslarası geçerliliğe sahip bağımsız kuruluşlar tarafından bağımsız denetim ve farklı zamanlarda yapılan kontroller ile ispatlamış olurlar. Bu standardın gerekliliklerini yerine getiren bir kurumda her süreç önceden belirlenmiş ve üst yönetim onayından geçmiş politika, prosedür ve talimatlar ile yürütülür, kurum personeline ve 3. Taraflar ile yapılan sözleşmelerde vasıtası ile kurum dışı çalışanlara kurum bilgi güvenliği yapısı hakkında bilgiler verilir. Bunlar, iş sürecinde bilgi güvenliğine yönelik yaşanan bir olumsuzluk karşısında kurumun elini güçlendirebilecek belge niteliği taşımakta, yasal mevzuatlardan dolayı yaşanabilecek sorunlara karşı da bizleri koruma altına almaktadır. Bu sertifika ile, üst yönetim, teknik personel hatta kurumla ilişkisi olan her birey ya da şirket kısacası ilgili olduğu her kesim güvence altına alınmış olur [4].

Bilişim ve İnovasyon Derneği tarafından yayınlanan Siber Güvenlik Raporu incelendiğinde bilgi güvenliğine yönelik önerilerin olay yönetimi, bilgi güvenliği yönetim sistemi, güvenlik ve sızma testleri, iş sürekliliği yönetim sistemleri, yerli donanım ve yazılım teşvik edecek politikalar üzerinde durulurken farkındalık eğitim konusuna kısaca yer verildiği görülmektedir [56]. Gerçekleştirilen bilimsel araştırmalarla birlikte teknolojik ürün oluşturulması yönünde büyük emek ve harcamalar yapılmaktadır oysa ki bunlar son

kullanıcıların bilgi güvenliğine yönelik yeterli farkındalığa ulaşmadığı takdirde tek başına bilgi güvenliğini sağlamak için yeterli olmadığını ve zincirin en zayıf halkası olarak tanımlanan insanların bilgi güvenliğine yönelik eğitimler alması ve bilgi güvenliğini benimsemelerinin önemi ortaya çıkmıştır. Bilgi Güvenliği Derneği, bireylerde bilgi güvenliğine yönelik arzu edilen seviyede davranış gelişmemesinin sebebini; kurum ve kuruluşların son 30 yıl içerisinde bilgi güvenliği farkındalığı konusunu, özgü araç ve teknolojinin tanıtımı ve kullanımına dair faaliyetler kapsamında yürütmelerine bağlamıştır. Arzu edilen yönde davranış değişikliği olması için bilgi güvenliği farkındalık eğitimlerinin bilgilendirme aşamasını takiben uygun davranışın içselleştirme faaliyetlerini de kapsaması gerektiği ve eğitimlerin hedef kitlesinin geniş tutulması için en uygun ortamın çevrimiçi öğrenme ortamları olduğu sonucuna varılmıştır [57].

Deloitte GFSI(Global Financial Service Industry) firması 2007 yılında 32 ülkeden 170'in üzerinde finans kuruluşu ile anket gerçekleştirmiştir. Ankete katılan kuruluşların %50'si birinci önceliklerinin erişim ve kimlik yönetimi olduğunu ifade etmiş ve en yaygın iç denetim bulgularının birinin erişim ve kimlik yönetimi ile ilgili olduğu ortaya çıkmıştır. Bunlar hassas bilgiler içeren veri tabanı ve sistem yönetim araçlarına ilgili personel dışında erişimin olması, gereğinden fazla verilmiş yetkilerin alınması, görev değişimi ve sonlanması ardından verilen yetkilerin silinmemesi, denetim kayıt izlerinin eksikliği, yazılım geliştiricilerin üretim ortamında ve canlı veri tabanlarında gereğinden fazla yetkisinin olması olarak gösterilmiştir [58]. Erişim kontrolünün sistemdeki hareketleri takip ederek ve denetimi sağlayarak bilgiyi tutarlılık ve bütünlük içinde depolayabilen ve işleyebilen bir güvenlik hizmetidir. Bilgi güvenliği üzerinde yapılan çalışmalarda erişim kontrolü, kimlik doğrulama ve denetimin bir arada düşünülerek her bir yöntemin güçlü noktasının bir araya getirilip koordineli bir yaklaşımla yürütülmesine ihtiyaç vardır [59].

SANS'ın yayınlamış olduğu Bilişim Teknolojileri Güvenlik Harcamaları Raporuna göre kuruluşlar, erişim ve kimlik doğrulama, zararlı yazılımları engelleme, uç nokta güvenliği, kablosuz ağ güvenliği, veri sızdırma ve kayıp önleme, log yönetimi teknolojilerine kaynaklarının büyük çoğunluğu harcamaktadır [60]. Gartner Bilgi Güvenliği Harcama Raporu ise dünya genelinde bilgi güvenliği yazılım ve servislerine 2017 yılında 101.544 milyar dolar harcandığını açıklamış ve bu harcamanın 2019 yılında %8.7 büyüyeceği tahmininde bulunmuştur [61]. Levi siber suç eğilimlerini incelediği çalışmasında; Avustralya, Kanada, Almanya, Hollanda, İsveç, İngiltere ve Amerika gibi gelişmiş ülkelerdeki çevrimiçi dolandırıcılık vakalarının önemli oranda artış gösterdiğine ortaya

koymuştur [62]. Buda gösteriyor ki yapılan bu harcamalar bilgi güvenliği yönetimi konusunda teknik çözümlerden öteye gitmemiştir.

Bilgi güvenliğinin kurumlarda sağlıklı ve dinamik gerçekleştirilmesi için en önemli kural, tüm kurum personelinin süreç hakkında bilgi sahibi olması ve özellikle teknik personelin ISO27001'in kurumsal teknik süreçler üzerinde uygulanabilir olduğunu anlamalarını sağlamaktır. Kurum çalışanlarının tamamı iş süreçlerinde bilgi güvenliğinden bağımsız hareket etmemelidir. Fakat orta-büyük ölçekli kurumlarda bilgi güvenliği departmanlarının, daha küçük ölçekli kurumlarda bilgi güvenliği ekiplerinin kurulması ve bilgi güvenliği çalışmalarını onların yürütüyor olmasından dolayı diğer çalışanlar bilgi güvenliği konusunu o birimlerin göreviymiş gibi düşerek iş süreçlerinde bilgi güvenliğini dikkate almayabiliyorlar. Bu noktada yapılması gereken tüm çalışanlara bilgi güvenliği sorumluluğunun herkesin görevi olduğunu hatırlatmak ve bilgi güvenliğini sahiplenmelerini sağlamaktır. Herath ve Rao alanyazında yapılan çalışmaların çoğunlukla bilgi güvenliği uzmanlarına yönelik olmasını eleştirmiş ve bilgi güvenliği farkındalığının son kullanıcılar üzerinde çalışılması gerekliliğinin önemini vurgulamıştır [63].

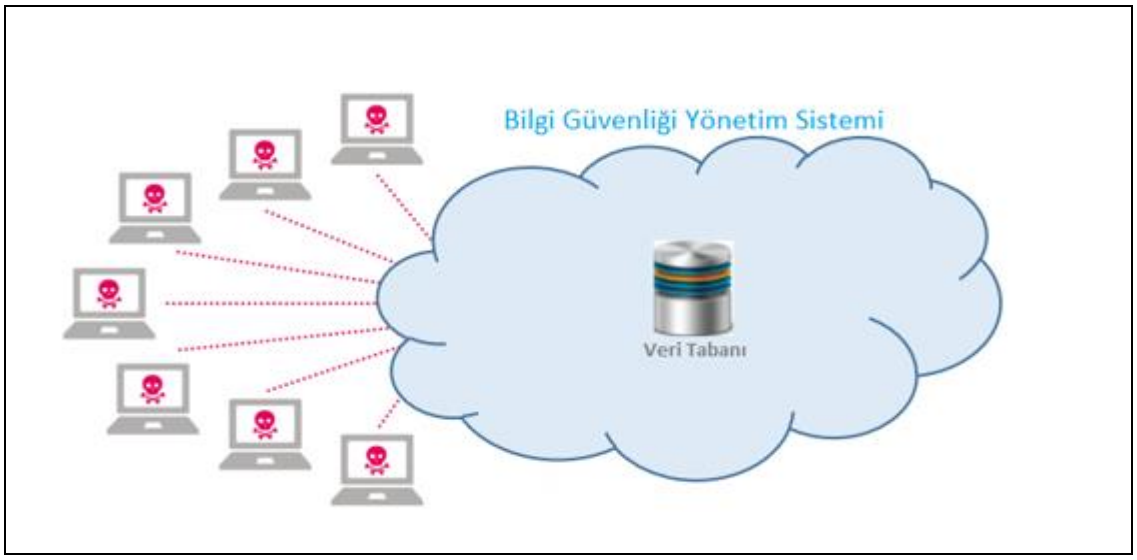
Bilgi güvenliği yönetim sisteminin önündeki en büyük engel bilgi işlem personellerinin bile sürecin dışında kalmak istemeleridir. Kurumlar bilgi güvenliği ile ilgili süreçleri, teknolojik gelişmeleri ve çözümleri ya kurumların bilgi güvenliği ekiplerine ya da kurum dışından hizmet aldıkları danışmanlık firmalarına aktararak bilgi güvenliğini sağlamaya çalışmaktadırlar. Danışmanlık firmalarının sadece sertifika alabilmeyi hedef alarak kurumların çoğunda benzer bir bilgi güvenliği yönetim sistemi oluşturması, bilgi güvenliği ekiplerinin de diğer personelden yeterli desteği alamadığından bazı süreçlerin ya çok yavaş ilerlemesi ya da ilerleyememesinden BGYS sağlıklı ve dinamik bir şekilde sağlanamamaktadır [10]. Bu nedenle bilgi güvenliği sürecini tüm kurum personeli özellikle de bilgi işlem personeli benimsemeli BGYS içerisinde yer almalı ve sorumluluk hissetmelidir. Örneğin, kurumun veri tabanı sorumlusu bilgi güvenliğinin de kendi sorumluluk alanına girdiğini ve görevi olduğunu kabullenir ise verilerin okunması, silinmesi, güncellenmesi, saklanması gibi işlemlerin tek önceliği olmadığını bu işlemleri güvenlik gereksinimleriyle birlikte yürütülmek zorunda olduğunu kabul eder ve her bilgi işlem personeli bu görev bilincine ulaşır ise bilgi güvenliği sağlanabilir ve bilgi güvenliği riskleri asgari düzeye indirilebilir.

Bilgi güvenliği konusunda farklı alan ve ihtiyaçlara göre tasarlanmış pek çok farklı standart ve pek çok çalışma mevcut. Ancak yapılan araştırmalarda, bu çalışmaların çoğunda bilgi güvenliğine yönelik hep benzer konulara değinildiği, benzer kriterler üzerinde durulduğu görülmüştür. Bilgi güvenliğinin dinamik ve sürekliliğinin sağlanabilmesi için; bütünsel yaklaşıma dayanan ama daha özelleştirilmiş alt başlıklara hitap eden güvenlik kontrollerini içeren çalışmalara ihtiyaç duyulmaktadır. Bu çalışmamızda; bilgi güvenliği yönetim sistemini ve hassas verilerin tutulduğu veri tabanlarının sürece uyumlu hale getirilmesinin önemini açıklamaya çalıştık.

Kurumların, her geçen gün ilerleyen teknolojiyi kullanarak saldırganların oluşturacakları tehdit ve risklere karşı bilgi varlıklarını koruyabilmesi için bilgi güvenliği yönetim kavramını ve gerekliliklerini anlayabilmeleri, gerekllilikleri yerine getirerek riskleri gidermeleri ve kabul edilebilir seviyelere düşürmeleri gerekmektedir.

Veri tabanları, etkili veri getirme ve saklama özellikleri ile hassas verilere hızlı ve doğru bir erişim imkanı sunduğundan günümüzün en önemli araçlarından biridir. Birçok kurum yaptığı işlerle ilgili veri yığınına sahiptir ve kurumların başarısı bu veri yığınlarından doğru ve güvenilir verilere hızlı erişim sağlamaları ve onları analiz etmelerine bağlıdır. Diğer yandan, veri tabanlarının uygulamaların görünmeyen arka tarafında bulunması bu sistemlere ulaşılmasının güç olduğu fikrini düşündürtmekte ve veri tabanlarının güvenliği ikinci planda kalabilmektedir. Gelişen teknoloji ile birlikte yeni saldırı teknikleri de gelişmektedir bu olası tehditlere karşı gerekli güvenlik önlemlerinin alınmaması veya alınacak önlemlerin sistemin bütünlüğü bozacağı endişesi güvenlik açıklarına neden olabilmektedir.

Çalışmamızda, güvenlik açıklarından dolayı dünya genelinde yaşanan en önemli veri tabanı saldırılarına örnekler verilip bu saldırılar sonucunda sadece maddi kayıplar değil itibar zedelenmelerinin de yaşanıldığına değinilmiştir. Bilginin ve verileri tutan veri tabanlarının güvenliği sağlanmadıkça bu olaylar artarak yaşanmaya devam etmektedir. Bilgi güvenliği ana başlığı altında bilgi güvenliğinin temel unsurları ve bilgi güvenliği yönetim sistemi ile ilgili bilinmesi gereken temel kavramlara ve ilgili süreçlere değinilerek bilgi güvenliğinin kavranması hedeflenmiştir. Bilgi güvenliği kavramının benimsenmesi ve 27001 gerekliliklerinin veri tabanı sistemlerine uygulanabilmesinin sağlanması ile sistemlerin güvenliğini makul seviyeye çekmek mümkün olabilmektedir. Şekil 8.1’de BGYS ile veri tabanının tehditlerden korunması gösterilmektedir.



Şekil 8.1. Bilgi güvenliği yönetim sistemi ile veri tabanının koruma altında olması

Veri tabanında açıklıklar varsa saldırganlar bu açıklıkları kullanarak veri tabanına zarar verebilir. ISO 27001 bilgi güvenliği yönetim sistemi gereksinimleri veri tabanında uygulandığında zafiyet oluşturabilecek açıklıklar giderilmiş olacak ve Şekil 8.1'de görüldüğü üzere tehditler uygun koşulları bulamadığından veri tabanına zarar veremeyecektir.

Tezin beşinci bölümünde ISO 27001 Standardı ekler bölümü kontrol amaçları ve kontrolleri ele alınıp devamında bu kontrol maddeleri başlangıç noktası kabul edilerek veri tabanı yönetim sistemini doğrudan veya dolaylı ilgilendiren gerekliliklerin veri tabanına nasıl uygulanabileceği sınıflandırılarak altı ana başlıkta altıncı bölümde ele alınmaktadır. Çizelge 8.1'de 27001 kontrol amaçları, veri tabanına uygulanması gereken setler ile eşleştirilmiştir.

Çizelge 8.1. 27001 kontrol amaçlarının veri tabanı setleri ile eşleşmeleri

	Veri Tabanı Genel Kontrolleri ve Kurulum Adımları	**Veri Tabanı Kullanıcı Hesap Güvenliği Kontrolleri**	**İşletim Sistemi Güvenliği Kontrolleri**	**Veri Şifreleme**	**Veri Tabanı Etkinliklerini Denetleme ve Yedekleme**	**Veri Tabanı Özelinde Hazırlanabilecek Bilgi Güvenliği Dokümanları**
A.5 Bilgi Güvenliği Politikaları						
A.6 Bilgi Güvenliği Organizasyonu		✓			✓	
A.7 İnsan Kaynakları Güvenliği		✓				✓
A.8 Varlık Yönetimi					✓	
A.9 Erişim Kontrolü		✓	✓	✓	✓	
A.10 Kriptografi				✓		
A.11 Fiziksel ve Çevresel Güvenlik				✓		
A.12 İşletim Güvenliği	✓		✓	✓	✓	
A.13 Haberleşme Güvenliği				✓	✓	✓
A.14 Sistem Temini, Geliştirme ve Bakımı	✓		✓	✓		

Çizelge 8.1 (devam). 27001 kontrol amaçlarının veri tabanı setleri ile eşleşmeleri

	Veri Tabanı Genel Kontrolleri ve Kurulum Adımları	**Veri Tabanı Kullanıcı Hesap Güvenliği Kontrolleri**	**İşletim Sistemi Güvenliği Kontrolleri**	**Veri Şifreleme**	**Veri Tabanı Etkinliklerini Denetleme ve Yedekleme**	**Veri Tabanı Özelinde Hazırlanabilecek Bilgi Güvenliği Dokümanları**
A.15 Tedarikçi İlişkileri		✓				✓
A.16 Bilgi Güvenliği İhlal Olayı Yönetimi					✓	
A.17 İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları			✓	✓	✓	
A.18 Uyum	✓	✓		✓		

Altı ana başlıkta ele alınan 27001 kontrol amaçlarının veri tabanında uygulanması, tezin üçüncü bölümünde değinilen en sık rastlanan veri tabanı güvenlik tehditlerini önleyen kontrolleri de kapsamaktadır. Bu kontroller, güvenlik tehditlerine tam anlamıyla engel olamasa da veri tabanı güvenlik tehlikelerine karşı alınacak tedbirleri anlayıp, öğrenerek bu saldırılara karşı kurumların iş süreçlerine en az sorun ile devam edebilmesini ve bilgi varlıklarının korunmasını sağlayabilmektedir.

Çizelge 8.2'de veri tabanı güvenlik tehditleri ile veri tabanına uygulanması gereken setler ilişkilendirilmiştir.

Çizelge 8.2. Veri tabanı güvenlik tehditleri ve veri tabanı setleri ile eşleştirilmesi

	Veri Tabanı Genel Konrolleri Ve Kurulum Adımları	**Veri Tabanı Kullanıcı Hesap Güvenliği Kontrolleri**	**İşletim Sistemi Güvenliği Kontrolleri**	**Veri Şifreleme**	**Veri Tabanı Etkinliklerini Denetleme Ve Yedekleme**	**Veri Tabanı Özelinde Hazırlanabilecek Bilgi Güvenliği Dokümanları**
Aşırı ve Kullanılmayan Yetki Tehdidi		✓				
Yetki Suistimali Tehdidi		✓				
SQL Enjeksiyon Tehdidi	✓	✓	✓	✓		
Kötü Amaçlı Yazılım Tehdidi	✓					
Zayıf Denetim Takibi Tehdidi					✓	
Yedek Verinin İfşa Olma Tehdidi				✓	✓	
Yanlış Yapılandırma ve Güvenlik Açığı Tehdidi	✓	✓	✓		✓	

Çizelge 8.2 (devam). Veri tabanı güvenlik tehditleri ve veri tabanı setleri ile eşleştirilmesi

	Veri Tabanı Genel Kontrolleri Ve Kurulum Adımları	**Veri Tabanı Kullanıcı Hesap Güvenliği Kontrolleri**	**İşletim Sistemi Güvenliği Kontrolleri**	**Veri Şifreleme**	**Veri Tabanı Etkinliklerini Denetleme ve Yedekleme**	**Veri Tabanı Özelinde Hazırlanabilecek Bilgi Güvenliği Dokümanları**
Yönetilmeyen Hassas Veri Tehdidi	✓				✓	
Hizmet Dışı Bırakma Tehdidi				✓	✓	
Sınırlı Güvenlik Uzmanlığı ve Eğitimi						

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri sertifikasına sahip olmak isteyen kurumlar ya da BGYS'yi yapılarında dinamik ve kusursuz işletmek isteyen kurumlarda veri tabanı sorumlularının, 27001 standardı gerekliliklerinin asgari düzeyde veri tabanında nasıl uygulanacağı konusunda yol gösteren setlere sahip olması BGYS' yi veri tabanında daha etkin kılmaktadır. Bulgular ve yorumlar bu çalışmanın en önemli bölümünü oluşturmaktadır ve burada bahsedilen 27001 gerekliliklerinin veri tabanı sistemlerine uygulanması için hazırlanan setlerin; kurumların bilgi güvenliği yönetim sisteminin uygunluğunun denetimini yapan denetçiler, veri tabanı yöneticileri, sistem üzerinde değerlendirme yapacak kişiler ve veri tabanı güvenliği konusunda bilgi sahibi olmak isteyen kişiler tarafından kullanılması amaçlanmıştır. Veri tabanı yönetim sistemleri pek çok katmanla birlikte çalıştığından uygulama, işletim sistemi ve ağ katmanlarının işleyişi hakkında da bilgi sahibi olunması faydalı olacaktır. Veri tabanıyla doğrudan veya dolaylı etkileşimde olan her bir katmanı kapsayacak şekilde veri tabanında uygulanacak kontrol ve gereksinimler standartta tanımlanan kontrol maddeleri ile eşleştirilip altı gruba ayrılarak bir metodoloji oluşturulmuştur. Bu çalışmada anlatılan veri tabanında uygulanacak adımların her biri tüm kurum yapılarında uygulanamayabilir, çünkü her kurum kendine özgü farklı sistemlere sahip olabilmektedir.

Bu çalışmanın, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri sertifikasyon sürecinde yer alacak birçok veri tabanı sorumlusunun, veri tabanı yönetim sisteminde asgari gerçekleştirmesi gereken gereklilikleri belirlemesi, standardı anlama ve özümseme aşamasında yaşayacağı problemleri ve belirsizlikleri en aza indirgemesi için rehber bir kaynak olarak kullanılabileceği ümit edilmektedir. Diğer yandan herhangi bir otorite tarafından BGYS ve veri tabanı yönetim sistemlerini birlikte ele alan böyle kapsamlı bir yönetmelik yayınlanmamış olması nedeniyle bu tezin bu alanda yapılacak çalışmalara bir çerçeve oluşturması açısından önem arz etmesi beklenmektedir.

Bu tez çalışmasında, ISO27001 kontrol amaçlarının veri tabanına uygulanması aşamasında Oracle veri tabanı sistemi ele alınmış, veri tabanı sisteminin kurulumu, yapılandırması ve güvenlik adımları uygulamalı olarak Oracle veri tabanında işlenmiştir. ISO 27001 gerekliliklerinin veri tabanlarına uygulanması çalışmaları veri tabanının tipine göre farklılıklar gösterir. Benzer bir konuda çalışma yapılmak istenirse aynı konu, yaygın kullanıma sahip olan Microsoft SQL Server, MySQL, PostgreSQL veri tabanları üzerinden örneklerle çalışmalar yürütülebilir. Bunun yanında bu çalışmada ISO27001 gereklilikleri veri tabanı yönetim sistemleri ele alınarak incelenmiştir, BGYS içerisinde yer alan diğer sistemler için de kontrol maddelerinin uygulanabilirliği incelenebilir. Bu tarz çalışmaların bilgi güvenliği araştırmalarına katkı sağlayacağı düşünülmektedir.

Kurum ve kuruluşların üst düzeyde bilgi güvenliğini ve iş sürekliliğini sağlamaları, BGYS'nin etkinliğini yüksek seviyede tutmaları için standartlar çerçevesinde teknik önlemlerin uygulanmasının, yönetimsel, hukuksal önlemlerin alınmasının yanında teknik personel başta olmak üzere en zayıf halka olarak tabir edilen insanların bilgi güvenliği sürecini; kanıksaması, öğrenmesi, sahiplenmesi ve rutin hale getirmesi gerekmektedir. Bunun için de, BGYS kurmak isteyen kurumlar; tamamen danışmanlık ve eğitim firmalarına bağımlı kalmadan, eğitimlerle insanları bilinçlendirip sürecin bir parçası olmaya istekli hale gelmesini ve doğru güvenlik çözümlerinin doğru yer, zamanda kullanılmasını sağlayarak gereksiz tedbirler ile insanlar üzerinde olumsuz etki yaratmadan, bilgi güvenliğinin zaman içinde kurum kültürü haline gelmesini hedeflemelidir.

KAYNAKLAR

1. Tuygun, M., Çakır, H. (2019*). Iso27001 Bilgi Güvenliği Yönetim Sistemi Standardının Kamu Kurumlarına Uygulanabilirliğinin Araştırılması: Ankara İli Örneği,* Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara.

2. İnternet: KamuNet Ağına Bağlanma ve KamuNet Ağının Denetimine İlişkin Usul ve Esaslar Hakkında Tebliğ (2017,24 Haziran). *Resmi Gazete (Sayı:30103).* URL: https://www.resmigazete.gov.tr/eskiler/2017/06/20170621-15.htm, Son Erişim Tarihi: 15.10.2020.

3. Adalı, E. (2016). *Bilgisayar ve Bilgi Güvenliği Yönetimi, Bilgisayar ve Bilgi Güvenliği*. İstanbul: Özkaracan Matbacılık, 29-37.

4. Akay, İ. G. (2014). *Bilgi Güvenliği Yönetim Sistemleri: Bilgi Güvenliği Uygulama Mülakatları,* Yüksek Lisans Tezi, *Bilecik* Şeyh Edebali Üniversitesi, Bilecik.

5. Ottekin, F. (2011). BGYS ve BGYS Kurma Deneyimleri. *6. Kamu Kurumları Bilgi Teknolojileri Güvenlik Konferansı,* Ankara.

6. Baykara, M., Daş, R., Karadoğan, İ. (2013). Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, *1st International Symposium on Digital Forensics and Security (ISDFS'13),* 1-15, Elazığ.

7. Henkoğlu, T. (2015). *Hassas Bilgi Varlıklarının ve Kişisel Verilerin Hukuksal Düzenlemeler ile Korunması ve Bu Kapsamda Üniversiteler için Bilgi Güvenliği Politikasının Geliştirilmesi,* Doktora Tezi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Ankara

8. İnternet: Başaranoğlu, İ.E. (2016). Bilgi Güvenliği Unsurları. *Siber Portal.* URL: https://www.siberportal.org/blue-team/securing-information/bilgi-guvenligi-unsurlari-cia-ve-digerleri/, Son Erişim Tarihi: 25.10.2020.

9. Canbek, G., Sağıroğlu, Ş. (2006). Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme. *Politeknik Dergisi*, 9(3), 165-174.

10. Çek, E. (2017). *Kurumsal Bilgi Güvenliği Yönetişimi ve Bilgi Güvenliği İçin İnsan Faktörünün Önemi,* Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü, İstanbul.

11. İnternet: Curphey, M. (2002). Access Control and Authorization, A Guide to Building Secure Web Applications. URL: https://www.cgisecurity.com/owasp/html/ch05.html, Son Erişim Tarihi: 03.11.2020.

12. Ersoy,E.V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı Tanımlar ve Örnek Uygulamalar.* Ankara: ODTÜ Yayıncılık, 8.

13. İnternet: COBIT. *ISACA*. URL: https://www.isaca.org/resources/cobit, Son Erişim Tarihi: 13.11.2020.

14. Raflesia, S.P., Surendro, K., ve Passarella, R. (2017). The user engagement impact along information technology of infrastructure library (ITIL) adoption. *in 2017 International Conference on Electrical Engineering and Computer Science (ICECOS).* Palembang, Indonesia.

15. İnternet: *International Organization for Standardization*. URL: https://www.iso.org/, Son Erişim Tarihi: 05.12.2020.

16. İnternet: *European Committee for Standardization.* URL: https://www.cen.eu/cen/pages/default.aspx, Son Erişim Tarihi: 07.12.2020.

17. İnternet: Hakkımızda. *Türk Standardları Enstitüsü.* URL: https://www.tse.org.tr/Hakkimizda?ID=2&ParentID=1, Son Erişim Tarihi: 10.12.2020.

18. İnternet: TÜRKAK Hakkında. *T.C. Dışişleri Bakanlığı Türk Akredıtasyon Kurumu.* URL: https://www.turkak.org.tr/kurumsal/hakkinda.html, Son Erişim Tarihi: 21.12.2020.

19. ISO/IEC (2015). ISO/IEC:27006 Bilgi Güvenliği Yönetim Sistemlerinin Denetim ve Belgelendirmesini Sağlayan Kuruluşlar İçin Şartlar.

20. ISO/IEC (2017). ISO/IEC:27003 Bilgi Güvenliği Yönetim Sistemleri - Rehberlik.

21. ISO/IEC (2016). ISO/IEC:27004 İzleme, Ölçüm, Analiz ve Değerlendirme.

22. ISO/IEC (2017). ISO/IEC:27007 Bilgi Güvenliği Yönetim Sistemleri Denetimi İçin Rehber.

23. Gülmüş, M. (2010). *Kurumsal Bilgi Güvenliği ve Yönetim Sistemleri ve Güvenliği*, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, İstanbul.

24. Erdağı, E. (2017). *Veri tabanı Güvenlik Riskleri,Şifreleme Algoritmaları Ve Enjeksiyon Modelleri,* Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi Bilişim Enstitüsü, Ankara.

25. İnternet: Stack Exchange Inc (2021). URL: https://insights.stackoverflow.com/survey/2020/, Son Erişim Tarihi: 05.01.2021.

26. Connolly, T., Begg, C. (2015). A Practical Approach to Design. *Implementation and Management Sixth Edition*, Pearson, 135s.

27. Potineni, P. (2021). Backup and Recovery User's Guide, 21c. *U.S. Oracle,* 1-14.

28. Ashdown, L., Keesling, D., Kyte, T. (2020), Oracle Database Database Concepts, 21c. *U.S. Oracle,* 8-13.

29. Balter, A. (2003). *Access Masaüstü Uygulamaları Geliştirme: Uzman Çözümler*. İstanbul: Sistem Yayıncılık, 94.

30. Riordan, R. M. (2002). *Microsoft SQL Server 2000 Programlama*. Ankara: Arkadaş Yayınevi, 516.

31. İnternet: The 15 biggest data breaches of the 21st century. *CSO.* URL: https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html, Son Erişim Tarihi: 12.02.2021.

32. İnternet: Bilgi Güvende. URL: https://bilgiguvende.com/2019-siber-saldirilar/,ilgi Güvende, Son Erişim Tarihi: 12.02.2021.

33. Özbilgin, İ. G., (2003). Bilgi Teknolojileri Denetimi ve Uluslararası Standartlar. *Sayıştay Dergisi*, 49, 123-127.

34. Vural, Y., Sağıroğlu, Ş. (2010). Veri tabanı Yönetim Sistemleri Güvenliği: Tehditler ve Korunma Yöntemleri. *Politeknik Dergisi*, 13(2), 71-81.

35. İnternet: SQL injection. *PortSwigger.* URL*:* https://portswigger.net/web-security/sql-injection, Son Erişim Tarihi: 12.02.2021.

36. Kalman, S. (2003). *Web Security Field Guide*. Indianapolis: Cisco Press, 36-37.

37. Dlamini, M. T., Eloff, J. H., & Eloff, M. M. (2009). Information security: The moving target. *Computers & Security*, 28(3-4), 189-198.

38. Luo, X. R., Zhang, W., Burd, S., & Seazzu, A. (2013). Investigating phishing victimization with the Heuristic–Systematic Model: A theoretical framework and an exploration. *Computers & Security*, 38, 28-38.

39. Yiğit, T., Akyıldız, M. (2014). Sızma Testleri İçin Bir Model Ağ Üzerinde Siber Saldırı Senaryolarının Değerlendirilmesi. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 18 (1).

40. Hekim, H., Başıbüyük, O. (2013). Siber Suçlar Ve Türkiye'nin Siber Güvenlik Politikaları*. Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.

41. Bostan, A., Şengül, G. (2018). *Siber Güvenlik Farkındalığı Oluşturma. Siber Güvenlik ve Savunma.* Ankara: Grafik Yayınları, 145-163.

42. Çetin, H. (2014). Kişisel Veri Güvenliği Ve Kullanıcıların Farkındalık Düzeylerinin İncelenmesi. *Akdeniz Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 14(29), 86-105.

43. Eminağaoğlu, M. Ve Gökşen, Y. (2009). Bilgi Güvenliği Nedir, Ne Değildir, Türkiye' de Bilgi Güvenliği Sorunları ve Çözüm Önerileri. *Dokuz Eylül Üniversitesi Sosyal Bilimler Dergisi*, 11(4), 1-15.

44. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151-156.

45. King, K.E. (2017). *Examine the relationship between information technology governance, control objectives for information and related technologies, ISO 27001/27002, and risk management*, Ph.D., Capella University, Minneapolis, USA.
46. Gencer, K. (2015). *ISO 27001 Kapsamında Kurumsal Bilgi Güvenliğine Dinamik Bir Yaklaşım,* Yüksek Lisans Tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, Afyon.

47. Shoraka, B. (2011). *An Empirical Investigation of the Economic Value of Information Security Management System Standards*, Ph.D., Nova Southeastern University, Florida, USA.

48. Aktaş, K. (2020). *ISO 27001 Bilgi Güvenliği Yönetim Sistemi: Erişim Kontrol Politikası Üzerine Bir İnceleme,* Yüksek Lisans Tezi, Doğuş Üniversitesi, İstanbul.

49. ISO/IEC (2017). ISO/IEC:27001 Bilgi Güvenliği Yönetim Sistemleri - Gereksinimler.

50. İnternet: Huey, P. (2014). Database Security Guide, 11gRelease 1. URL: https://docs.oracle.com/cd/E11882_01/network.112/e36292.pdf, Son Erişim Tarihi: 12.08.2021.

51. Ingram, A. , Shaul, J. (2007). *Practical Oracle Security*. U.S. : Elsevier Science & Technology Books, 148-155.

52. Demir, B. (2010). *Oracle Veritabanı Güvenliği*, Yüksek Lisans Tezi, Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, Kocaeli.

53. Bryla, B.,Loney, K. (2008). *Oracle Database 11g DBA Handbook*. U.S: Oracle Press, 55-68.

54. İnternet: Oracle Database Online Documentation 11g Release 2. *Oracle Help Center*, URL: https://docs.oracle.com/cd/E11882_01/network.112/e10835/listener.html, Son Erişim Tarihi: 05.11.2021.

55. İnternet: Oracle Database Advanced Security Guide 19c. *Oracle Help Center, URL:* https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/introduction-to-transparent-data-encryption.html#GUID-547EA215-9576-4C61-A414-3DA3287692A4, Son Erişim Tarihi: 15.11.2021.

56. İnternet: Kurtul, A., Zeyveli, F., İnce, Y., Yıldız, K., Yüce, H., & Yakaryılmaz, F. (2020). Siber Güvenlik Raporu [Technical]. *Bilişim ve İnovasyon Derneği*, URL: http://www.bilisiminovasyon.org.tr/webfiles/userfiles/files/siber_guvenlik_raporu.pdf Son Erişim Tarihi: 21.01.2022.

57. Bostan, A., & Şengül, G. (2018). *Siber Güvenlik Farkındalığı Oluşturma*. Ankara: Grafiker Yayınları.

58. İnternet: Özgirgin, K. B., (2007). Rol Tabanlı Erişim Kontrolü. *Deloitte,* URL: https://docplayer.biz.tr/2492956-Rol-tabanli-erisim-kontrolu.html, Son Erişim Tarihi: 07.02.2022.

59. Sandhu, R. S., & Samarati, P. (1994). Access control: principle and practice. *IEEE communications magazine*, 32(9), 40-48.

60. Filkins, B. (2016). IT Security Spending Trends. *SANS Institute Information Security Reading Room*, 1-23.

61. İnternet: Moore, S., & Keen, E. (2018). Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019. *GARTNER*. URL: https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019, Son Erişim Tarihi: 11.02.2022.

62. Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change*, *67*(1), 3-20.

63. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.

EKLER

EK 1: Kurumsal Oracle Veri tabanı Bilgi Güvenliği ve Çalışma Prosedürü

ABC KURUMU

ORACLE VERİ TABANI BİLGİ GÜVENLİĞİ VE ÇALIŞMA PROSEDÜRÜ

1. Amaç

Bu prosedürün amacı, "BGYS Kapsam Dokümanı"nda belirtilen, ABC Kurumunun Oracle veri tabanının çalışma kuralları, güvenlik önlemleri, tüm yazılım geliştiricilerin veri tabanları üzerindeki erişim ve işlemlerinde uyulması gereken kuralları ve kontrol edilmesi gereken noktaları tanımlamak üzere hazırlanmıştır.

2. Kapsam

Bu prosedür, "BGYS Kapsam Dokümanı"nda belirtilen, ABC kurumu iş ve işlemleri kapsamında kullanılan verilerin tutulduğu Bilgi İşlem Merkezi sorumluluğunda bulunan Oracle veri tabanlarında yapılan ve yapılacak tüm faaliyetleri kapsar.

3. Sorumluluk

Bu prosedürün uygulanmasından 5. maddeden itibaren bahsi geçen kişiler sorumludur.

4. Kısaltmalar ve Tanımlar

Terim	Tanım/Açıklama
BGYS	Bilgi Güvenliği Yönetim Sistemi
Kurum	ABC Kurumu
DBA	Database Admin (Veri tabanı Yöneticisi)

5. Kurumsal Oracle Veri Tabanı Bilgi Güvenliği ve Çalışma Prosedürü

ABC Kurumu bünyesinde bulunan Oracle veri tabanlarında aşağıdaki başlıklarla toplanan iş ve işlemler doğrulanmalıdır

5.1. Veri Tabanı Kullanıcıları ve Yetkilendirme

(1) Yazılım geliştiriciler; Oracle veri tabanı üzerinde iş ve işlemlerini yapabilmesi için "Kurumsal Oracle Veri Tabanı Kullanıcı Taahhütnamesi ve Başvuru Formu" ile kullanıcı talebinde bulunur.

(2) Veri tabanında hiçbir kullanıcı "DBA" yetkisi talep edemez.

(3) Veri tabanında kullanıcılara sadece gerektiği kadar yetki verilir.

(4) Oracle veri tabanında oluşturulan kullanıcıların parola politikası aşağıdaki gibidir:

(a) Parolalar, 8 karakterden daha az karakterden oluşmaz.

(b) Parolalar, en az bir harf, bir rakam ve özel bir işaret içermelidir.

(c) Parolalar, sözlükte yer alan kelimeler olmamalıdır. Güvenlik için tahmin edilmesi ve bulunması zor olan (İsim veya soyisim, kimlik numarası, telefon numarası gibi parolalar seçilmemelidir), kullanıcı hakkında bilgi içermeyen parolalar seçilmelidir.

(d) Parolalar gizli tutulmalı, başkaları ile paylaşılmamalı ve otomatik sistem girişleri sırasında kaydedilmemelidir.

(e) Parolalar düzenli olarak ve parolanın güvenliğinin tehlikeye düştüğü düşünüldüğü her durumda değiştirilmelidir.

(f) Parolalar, 90 gün aralıklarla değiştirilmeli ve üç önceki parola ile aynı parola tekrar verilmemelidir.

(5) Veri tabanı üzerinde PUBLIC objesinde kritik nesne ve verilerin paylaşımı yapılmaz.

(6) SYSDBA ve SYSOPER yetkileri veri tabanı yöneticileri dışındaki kullanıcılara verilmez.

(7) Uygulama geliştirmek amacıyla oluşturulmuş hiçbir veri tabanı kullanıcısına veri tabanı objeleri üzerinde "any" yetkisi verilmez.

(8) Hiçbir veri tabanı kullanıcısı kendi objeleri üzerinde "WITH ADMIN", "WITH GRANT OPTION" yetkilendirmeleri yapamaz.

5.2. Yazılım Geliştirme Ortamı ve Test Veri tabanı

(1) Uygulamaların geliştirme ve gerçek ortamları birbirinden farklıdır. Geliştirme ortamında; uygulamanın geliştirileceği yazılım ve veri tabanına erişim yapılacak programlar bulunur, gerçek ortamda sadece uygulamanın çalışır son hali bulunur.

(2) Yazılım geliştirilirken ve test işlemleri yapılırken test veri tabanı kullanılmalı ve gerçek ortamda bu işlemler yapılmamalıdır. Bu tür işlemlerin gerçek ortamda yapılması durumunda oluşan veri kaybı ve veri bozulması ilgili kişilerin sorumluluğundadır.

(3) Gerçek veri tabanı için tanımlı bütün güvenlik tedbirleri test veri tabanı için de uygulanır.

5.3. Log Tutma İşlemi

(1) Yazılım geliştiriciler, uygulamanın kullanıcı şifrelerini veri tabanında standartlara ve bilgi güvenliği politika amaçlarını da karşılayacak kriptoloji tekniklerine uygun bir kriptoloma yöntemi ile şifreleyerek saklamalıdır.

(2) Yazılım geliştiriciler, kritik olduğu düşünülen tablolardaki tüm işlemleri, bu işlemi yapan kullanıcı ve erişim bilgilerini detaylı bir şekilde loglar.

(3) Kullanıcı, ilgili uygulama aracılığı dışında uygulamanın tablolarında ki veriler üzerinde değişiklik ve erişim yapamaz. Uygulama verilerinde Update, Insert, Select gibi işlemlerin yalnızca uygulama aracılığıyla yapılması bunun dışında veriye müdahaleye izin verilmemesi ve yazılım geliştiricilerin uygulamayı bu şekilde geliştirmesi gerekmektedir.

(4) Veri tabanında uygulamaya ait bütün veriler uygulama tarafından ya da 3.parti bir yazılım tarafından hiçbir şekilde silinemez. Eğer ilgili kayıt uygulama tarafından kullanılmayacak ise ya da görünmemesi gereken bir veri ise; veri maskeleme yöntemleri kullanılarak ilgili kaydın görünmemesi sağlanabilir.

6. İlgili Dokümanlar

6.1. İç Kaynaklı Dokümanlar

(1) BGYS Kapsam Dokümanı

(2) Kurumsal Oracle Veri tabanı Kullanıcı Başvuru Formu

6.2. Dış Kaynaklı Dokümanlar

(1) TS ISO/IEC 27001:2017 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler

EK 2: Kurumsal Oracle Veri Tabanı Kullanıcı Taahhütnamesi ve Başvuru Formu

KURUMSAL ORACLE VERİ TABANI KULLANICI TAAHHÜTNAMESİ ve BAŞVURU FORMU

1. AÇIKLAMA

Kurumsal politikamız gereği kurum verilerimizin tutulduğu veri tabanındaki verilerin sürekliliğini ve güvenliğini sağlamak amacıyla Bilgi İşlem Merkezi bilgi sistemlerine veri ve bilgi girişi ile bunlara erişim konusunda yetkilendirmeler yapmak, hata ve usulsüzlükleri önlemek, tespit etmek, düzeltmek ve bu işlemleri sağlayacak mekanizmalar oluşturmakla yükümlüdür. Bu amaçla kurumsal veri tabanı üzerinde **"Kurumsal Oracle Veri tabanı Güvenlik ve Çalışma Prosedürü"** nde belirtildiği üzere bazı kurallar oluşturulmuştur. Bu kurallar çerçevesinde kullanıcı; aşağıda belirtilen maddelerde yer alan hususları taahhüt etmek zorundadır.

2. TAAHHÜT EDİLEN HUSUSLAR

(1) Kullanıcının; Bilgi İşlem Merkezi'nce tarafına verilmiş olan "Veri Tabanı Kullanıcı Adı ve Şifre"sini başka bir şahıs ile paylaşması yasaktır.

(2) Kullanıcı, kendisine verilen görevleri yerine getirebilmek maksadı ile sınırlı olacak şekilde ve **"Kurumsal Oracle Veri Tabanı Güvenlik ve Çalışma Prosedürü"** nde belirtilen kurallar ve politikalar doğrultusunda iş ve işlemlerini gerçekleştirecektir.

(3) Anayasamızın 20'nci maddesinde "Herkes, özel hayatına ve aile hayatına saygı gösterilmesini isteme hakkına sahiptir. Özel hayatın ve aile hayatının gizliliğine dokunulamaz." denilmektedir. Kullanıcı, bu kapsamda veri tabanında bulunan bilgiler özel hayatın gizliliğine zarar verecek şekilde kullanmayacaktır.

(4)6698 sayılı Kişisel Verilerin Korunması Kanunu ile belirtilen Kişisel Verilerin, kanun kapsamında ifade edildiği şekilde kullanımı esastır, kanuna aykırı şekilde paylaşımları yapılamaz. Bu hususlara riayet edilmez ise, kullanıcı, kanunun 17 ve 18. maddelerinde yerini bulan yaptırımlardan sorumludur.

(5) Kullanıcı, 5237 sayılı Türk Ceza Kanunu 134-140 maddeleri ve kurumsal güvenlik politikamızın sorumlulukları gereği kurum verilerinin gizliliğinden ve güvenliğinden sorumludur.

(6) Kullanıcı, kurumla ilgili her türlü gizli bilgiyi muhafaza etmek ve korumak için üst seviyede özen gösterecek ve yalnızca iş kapsamında kendisine verilen görevler için kullanacak, idarenin yazılı onayı olmadan herhangi bir üçüncü kişi veya kurum/kuruluşa açıklamayacaktır.

(7) Sistemden edinilen bilgiler hiçbir yerde yayınlanmayacak, elektronik veya basılı olarak yetkisiz kişilere verilmeyecek, iş süreçleri dışında hiçbir amaç için kullanılmayacaktır.

(8) Bilgi İşlem Merkezince, kullanıcının yükümlülüklerini yerine getirmediğini tespit etmesi halinde tek taraflı olarak haklarını iptal etme hakkına sahiptir.

(9) Kullanıcı, iş kapsamında erişim sağladığı sistemleri/bilgileri, yetki dahilinde ya da yetkisini aşarak kendisine ya da başkasına çıkar sağlamak amacıyla kullanamayacağı gibi, bu bilgi işleme sistemlerinden programları, verileri veya herhangi bir unsuru hukuka aykırı olarak ele geçirme, değiştirme, tahrip etme, silme, sistemin işlemesine engel olma veya yanlış işlemesini sağlama gibi davranışlarda bulunamaz, bunları her ne sebeple olursa olsun kullanmaz, nakledemez, çoğaltamaz.

(10) Kullanıcı, gizli bilginin yetki dışı kullanıldığını/ifşa edildiğini veya bu taahhütnamenin herhangi bir şekilde ihlal edildiğini tespit etmesi halinde derhal idareyi bilgilendirecektir.

(11) Bu Taahhütnamede yer alan yükümlülükler, Gizli Bilginin kullanıcı ile paylaşıldığı ilk andan itibaren yürürlüğe girecektir.

Bu taahhütname ile verilen yetkilere ilişkin yukarıda yer alan yükümlülükleri kabul ettiğimi beyan ve taahhüt ederim. Ayrıca, bu işlemle ilgili görevimden ayrıldığımda, en geç 1 iş günü içinde Bilgi İşlem Merkezine görevden ayrıldığım bilgisini ileteceğimi taahhüt ederim. ../../20..

Veri Tabanına Erişim Gerekçesi	
Uygulama Adı ve Uygulama ile İlgili Bilgi	

Kullanıcı Bilgisi	**Birim Yetkilisi**
TC No	TC No
Adı Soyadı	Adı Soyadı
Görev Yeri	Görev Yeri
Tel	Tel
(imza)	*(imza)*

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: YILDIZ, Rabia
Uyruğu	: T.C.
Doğum tarihi ve yeri	:
Medeni hali	:
Telefon	:
e-posta	:

Eğitim

Derece	Eğitim Birimi	Mezuniyet Tarihi
Yüksek lisans	Gazi Üniversitesi / Bilişim Sistemleri	Devam ediyor
Lisans	Selçuk Üniversitesi / Bilgisayar Mühendisliği	2015
Lise	İncirli Lisesi	2009

İş Deneyimi

Yıl	Yer	Görev
2018-Halen	Kültür Bakanlığı	Mühendis

Yabancı Dil

İngilizce

Tezden Üretilen Yayınlar

1. Yıldız, R. (2022). ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemleri Gereksinimlerinin Veri Tabanı Sistemlerinde Uygulanması. V. Internatıonal New York Academıc Research Congress, Full Text Book, 128-135.

GAZİLİ OLMAK AYRICALIKTIR…