İŞLETMELERDE BİLGİ GÜVENLİĞİ İÇİN WEB TABANLI BİR UYGULAMANIN GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

NABİ KOÇ

MERSİN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME BİLGİ YÖNETİMİ
ANABİLİM DALI

MERSİN
KASIM – 2017

İŞLETMELERDE BİLGİ GÜVENLİĞİ İÇİN WEB TABANLI BİR UYGULAMANIN GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

NABİ KOÇ

MERSİN ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

İŞLETME BİLGİ YÖNETİMİ
ANABİLİM DALI

Danışman
Prof. Dr. Cemile ÇELİK

İkinci Danışman
Yrd. Doç. Dr. Evrim Ersin KANGAL

MERSİN
KASIM – 2017

ONAY

Nabi KOÇ tarafından Prof. Dr. Cemile ÇELİK danışmanlığında hazırlanan "İşletmelerde Bilgi Güvenliği İçin Web Tabanlı Bir Uygulamanın Geliştirilmesi" başlıklı bu çalışma, aşağıda imzaları bulunan jüri üyeleri tarafından oy birliği ile Yüksek Lisans Tezi olarak kabul edilmiştir.

Görevi	Ünvanı, Adı ve Soyadı	İmza
Başkan	Prof. Dr. Cemile ÇELİK	.....
Üye	Yrd. Doç. Dr. Ufuk ORHAN	.....
Üye	Yrd. Doç. Dr. Mehmet Ali AKTAŞ	.....

Yukarıdaki Jüri kararı Sosyal Bilimler Enstitüsü Yönetim Kurulu'nun ..15.11.2017..... tarih ve ..2017..... /..17..... sayılı kararıyla onaylanmıştır.

Prof. Dr. Süleyman DEĞİRMEN
Sosyal Bilimler Enstitü Müdürü

Bu tezde kullanılan özgün bilgiler, şekil, tablo ve fotoğraflardan kaynak göstermeden alıntı yapmak 5846 sayılı Fikir ve Sanat Eserleri Kanunu hükümlerine tabidir.

ETİK BEYAN

Mersin Üniversitesi Lisansüstü Eğitim-Öğretim Yönetmeliğinde belirtilen kurallara uygun olarak hazırladığım bu tez çalışmasında,

- Tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- Görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlâk kurallarına uygun olarak sunduğumu,
- Başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- Atıfta bulunduğum eserlerin tümünü kaynak olarak kullandığımı,
- Kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- Bu tezin herhangi bir bölümünü Mersin Üniversitesi veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı,
- Tezin tüm telif haklarını Mersin Üniversitesi'ne devrettiğimi

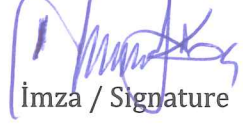
beyan ederim.

ETHICAL DECLERATION

This thesis is prepared in accordance with the rules specified in Mersin University Graduate Education Regulation and I declare to comply with the following conditions:

- I have obtained all the information and the documents of the thesis in accordance with the academic rules.
- I presented all the visual, auditory and written informations and results in accordance with scientific ethics.
- I refer in accordance with the norms of scientific works about the case of exploitation of others' works.
- I used all of the referred works as the references.
- I did not do any tampering in the used data.
- I did not present any part of this thesis as an another thesis at Mersin University or another university.
- I transfer all copyrights of this thesis to the Mersin University.

2 Kasım 2017 / 2 November 2017



İmza / Signature

NABİ KOÇ

Öğrenci Adı ve Soyadı / Student Name and Surname

ÖZET

Verilere dayalı bilgiler, işletmelerin en değerli varlığıdır ve önemi her geçen gün artıyor. Bununla birlikte, işletmeler için hayati önem taşıyan bilgileri hedef alan siber saldırılar da bu eğilime paralel olarak artmaktadır. Bu nedenle, yeterli bilgi güvenliğinin sağlanması, gizliliğin korunması, hizmetin sürekliliği, bilginin erişilebilirliğinin sağlanması, personel ve kurumsal kaynaklardaki verilerin korunması, ekonomik kayıpların en aza indirilmesi iş açısından önemlidir. Bu çalışmada, kuruluşu bilgi güvenliği ihlalleri ile ilişkili saldırılara karşı korumak için web tabanlı bir uygulama geliştirilmiştir. Uygulama sırasıyla C Sharp ve ASP programlama dillerinde yazılmış ana program ve web sayfasından oluşmaktadır. Ayrıca, Microsoft SQL ortamını kullanarak bir veritabanı tasarlanmıştır. Uygulama, yetkisiz kişilerin dosyaların içeriğini görüntülemesini önleyen Windows dosya gezgini işlevine benzer bir işlev yapısını içerir. Uygulama ayrıca, kullanıcıların yetkilerine uygun olarak verilere erişmesine ve işverenlerin veritabanında bulunan verileri bu yetki çerçevesinde kullanmasına izin verir. Bu arada, kurumsal çalışma süresince ilgili bilgiler önceden tanımlı alanlarda muhafaza edildiğinden, yetkisiz erişimin sağlanması mümkün değildir. Uygulama Mersin ilinde bulunan, emlakçılık, mobilya perakendeciliği ve bilgisayar satış ve bakımı alanlarında faaliyet gösteren üç farklı işletme tarafından test edilmiştir. Programın kuruluş ve kullanımıyla ilgili olarak şirket çalışanlarından olumlu ve olumsuz geri bildirimler alınmış ve bu geri bildirimler sonuçlar bölümünde değerlendirilmiştir.

Anahtar Kelimeler: Bilgi güvenliği ve web tabanlı uygulama.

Danışman: Prof. Dr. Cemile ÇELİK, Mersin Üniversitesi, İşletme Bilgi Yönetimi Anabilim Dalı, Mersin

İkinci Danışman: Yrd. Doç. Dr. Evrim Ersin KANGAL, Mersin Üniversitesi, Bilgisayar Teknolojisi ve Bilişim Sistemleri Ana bilim Dalı, Mersin

ABSTRACT

The Development Of A Web-Based Application For Information Security In Enterprises

Information based on the data is the most valuable asset of enterprises and its importance has been growing every day. However, cyberattacks targeting information crucial for enterprises have also been increasing, paralleling this trend. For this reason, providing adequate information security, maintaining privacy, continuity of service, ensuring the accessibility of information, protecting data on personnel and intuitional resources, minimizing economic losses are extremely critical from the business point of view. In this study, a web-based application has been developed for protecting enterprise from attacks related to the information security violations. The application consists of the main program and the web page written in C Sharp and APS programming languages, respectively. Furthermore, a database has been designed by using the Microsoft SQL environment. The application includes a function structure similar to the Windows file explorer that prevents unauthorized persons from viewing the contents of files. The application also allows users to access data according to the user's authorization and keeps the unauthorized usage of employers in database. Meanwhile, it can be interactively accessed from outside since the information related to the enterprise during the runtime is kept in the pre-defined areas. The application has been tested by three different companies operating in real estate, furniture retailing and computer sales and maintenance in the province of Mersin.. We get positive and negative feedbacks related to the installation and usage of the program from the company employers and they have been discussed in results and discussion sections.

Keywords: Information Security and the web-based application.

Advisor: Prof. Dr. Cemile ÇELİK, Mersin University, Department of Business Information Management, Mersin

Second Advisor: Yrd. Doç. Dr. Evrim Ersin KANGAL, Mersin University, Department of Computer Science and Information Systems, Mersin

TEŞEKKÜR

Yüksek lisans eğitimine başladığım ilk günden itibaren, sadece tez çalışmasında danışmanım olarak değil, bölüm ile ilgili tüm konularda çok değerli yardımlarını esirgemeyen, üniversite ile ilgili bütün gelişmelerde öncesinden bilgi veren, yönlendiren ve bütün eğitimimle yakından ilgilenen, çok kıymetli saygıdeğer hocam Prof. Dr. Cemile ÇELİK'e en içten duygularımla teşekkür eder, sonsuz minnet ve şükranlarımı sunarım. Çok kıymetli hocamın yardımları, esirgemeyip paylaştığı engin bilgi ve tecrübesi, her fırsatta çalışmamızın gidişatını yönlendirmesi ve adeta bir dost yaklaşımıyla sunduğu harika danışmanlığı sayesinde bu çalışma öncelikle fikir olarak ortaya çıkmış, sonrasında planlanarak uygulama aşamasına geçilmiş ve uzun bir çalışmanın sonucunda tamamlanmıştır. Bir kez daha kendisine sonsuz teşekkür ve minnetlerimi sunarım.

Yürütülen bu çalışma üzerinde büyük emeği olan, teknik danışmanlığı ile çalışmamıza artı değer katan, bir anlamda çalışmanın çerçevesine yön veren ve her aşamasında çok ciddi katkılar sağlayan Yrd. Doç. Dr. Evrim Ersin KANGAL hocama da çok teşekkür ederim. Hocamın bilhassa gecenin geç saatlerinde, hatta bazen tez sahibi olarak benim uykuda olduğum zaman dilimlerinde, kendisi uyumayıp, çalışmanın incelemesini gerçekleştiren, gerekli gördüğü yerlerde düzeltmeler yapan, bu özverisi ve çalışma disipliniyle beni kendisine hayran bırakan Yrd. Doç. Dr. Evrim Ersin KANGAL hocama da bir kez daha teşekkür ederim.

Ayrıca bu çalışma esnasında uygulamanın geliştirilmesi konusunda yardım ve desteklerini esirgemeyen Mersin Üniversitesi Bilgisayar Teknolojileri ve Bilişim Sistemleri Lisans Programı son sınıf öğrencilerinden Muhammed Acar'a da teşekkür ederim.

Tez çalışması süresince gösterdiği sabır ve verdiği her türlü destek ile sürekli yanımda olan, en kritik anlarda verdiği moral ve sağladığı motivasyon ile tezin aşama kaydetmesinde ve nihayetinde bitirilmesinde büyük katkısı olan, dünyalar tatlısı iki kızımız Ayşe Tuğba ve Deniz Alya'nın annesi, çok kıymetli eşim Hatice KOÇ'a da en özel ve en içten teşekkürlerimi ve minnetlerimi sunarım.

Son olarak tez savunma sınavımda jüri üyesi olarak görev alan Yrd. Doç Dr. Mehmet Ali AKTAŞ ve Yrd. Doç. Dr. Ufuk ORHAN hocalarıma da tez çalışmasının son düzeltmelerinde verdikleri destek ve emek için çok teşekkür ederim.

İÇİNDEKİLER

TABLOLAR DİZİNİ

ŞEKİLLER DİZİNİ

KISALTMALAR

Kısaltma / Simge	Tanım
DBIR	Data Breach Investigations Report (Verizon 2015)
ISO	International Standards of Organisations (Uluslararası Standartlık Örgütü)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BSI	British Standards Institute (İngiliz Standart Enstitüsü)
PUKÖ	Planla – Uygula – Kontrol et – Önlem al Döngüsü
WPF	Windows Presentation Foundation
XAML	eXtensible Application Markup Language
XML	eXtensible Markup Language
SQL	Structured Query Language
MSSQL	Microsoft Structured Query Language
MYSQL	My Structured Query Language
VTYS	Veritabanı Yönetim Sistemi
ASP	Active Server Pages
MAC Adresi	Media Access Control Address
IOS	iPhone / iPad Operating System
CRM	Customer Relationship Management
PDKS	Personel Devam Kontrol Sistemi
CobIT	Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknoloji İçin Kontrol Hedefleri)
ITIL	Information Technologies Infrastructure Library (Bilgi Teknolojisi Altyapı Kütüphanesi)

1. GİRİŞ

Latince bir sözcük olan "informatio" kelimesinin kökünden türemiş olan "bilgi" sözcüğü, günlük hayatımızda çok fazla kullanılmasına rağmen, bu sözcüğün tanımını yapmak oldukça zor ve karmaşıktır. Çok eski tarihlerden beri kullanılıyor olması dahi, "bilgi" sözcüğünün tanımında ortak bir görüş birliğine varılmasını sağlayamamıştır. Esasında bu durum "bilgi" sözcüğünün çok geniş anlamlar içermesinin doğal bir sonucudur. Tüm çağlar boyunca var olagelen "bilgi" tüm bu zaman dilimi boyunca adeta yaşayan ve gelişen canlı bir organizma gibi, anlamını her geçen gün daha da genişletmiş ve bu yüzden yeniden tanımlanmaya olan ihtiyacı günümüze kadar devam ettirmiştir (Uçak, 2010: 705-722).

Antik Yunan "bilgi" sözcüğünü tanımlamaya yönelik çabaların başladığı ilk dünyadır. Sokrates'e göre "bilgi" doğuştan gelmektedir. Sadece bu "bilginin" hatırlanması ve açığa çıkarılması gerekmektedir. Bunun için de tartışma yöntemini önerir. Platon bilgiyi "Doxa" ve "Episteme" olarak iki ayrı türe ayırmıştır. "Doxa" doğruluğu şüpheli olan yanlış bilgiyi ifade etmektedir. "Episteme" ise, doğru bilgiyi ifade eder. Platon'a göre "Doxa" duyu organlarımızla, "Episteme" ise aklımızda elde ettiğimiz bilgidir. Descartes ise bu konuda bilginin kaynağının yalnızca insan aklı olduğunu ileri sürmektedir. Descartes'te Sokrates gibi insanın zihninde doğuştan bilgi olduğunu kabul eder (Çelikhol, 2015: 161-162, Yıldırımer, 2013: 97–129).

Bilgi kelimesi sözlüklerde geçen en genel ifadesiyle insan aklının erişebileceği gerçek ve ilkelerin tamamı şeklindedir. Bilgi araştırma, öğrenme ve gözlemlerle elde edilen her türlü gerçek kavramların tümüne verilen addır. "Bilgi" Amerikalı ünlü sosyolog Daniel Bell'e göre ise, belirli bir sistem dâhilinde, herhangi bir iletişim aracı kullanılarak diğer şahıslara aktarılan doğru bir deneyimi ya da tecrübenin sonucunu gösteren, fikirlerle ilgili düzenli ve sistematik ifadelerin tamamıdır (Çağtürk, 2006, Çoban, 1997: 79-119)

Bilginin çağımıza ismini vermesi, tüm çağlar boyunca önemini sürekli artırmasının ve çağımızla birlikte artık doruk noktada bir öneme sahip olmasının olağan bir sonucudur. Bilgi çağı olarak adlandırılan çağımızda iletişim araçlarının gelişmesi ve son olarak bilişim teknolojilerinde yaşanan müthiş boyutlardaki ilerleme, bilginin dünyanın her bir köşesine hızlı bir şekilde ulaşmasına ve tüm toplumlar arasında hızla yayılmasına olanak sağlamıştır (Bensghir, 1996: 10-17).

Çağımızda bilgi teknolojilerinde yaşanan hızlı gelişme bilginin üretimini, kullanımını ve yaygınlaşmasını önemli ölçüde artırmaktadır. Dünyanın her geçen gün küreselleşmesi, bir diğer ifadeyle dünya milletlerinin ekonomik, siyasi ve iletişim bakımından birbirlerine yakınlaşarak bir bütün olması, bilgiyi işletmeler için en değerli varlık haline getirmiştir. Üretim, hizmet ve tüketim süreçlerinde bilgi, en değerli ve üstün rekabet sağlayan varlıktır. Günümüz rekabet ortamında ancak bilgiyi yönetebilenler ve bilgi güvenliğini sağlayabilenler başarıyı

yakalayacaklardır. Tüm bu gelişmelere bağlı olarak bilgiye yönelik tehditler de çok büyük oranda artış göstermektedir.

1.1. Çalışmanın Amacı

Bugünün teknolojik koşullarında bilgiye yönelik korsanlık girişimleri ve bilgi hırsızlıkları her geçen gün artmaktadır. Bu gelişmelerle birlikte bilgi güvenliği hassasiyeti ve bu konuda alınacak önlemler büyük önem kazanmıştır. Bu noktada çalışmanın amacı, kamu ve özel sektör ayırımı gözetmeksizin tüm kurum ve kuruluşların en kritik öneme sahip varlıkları olan bilgiye yönelik tehdit ve saldırılar karşısında oluşabilecek riskleri en aza indirmek ve yaşanabilecek tehlikelere karşı çözüm bulmaktır. Bu amaç doğrultusunda işletme bilgi güvenliğini sağlayacak olan web tabanlı bir program geliştirilmiştir. Geliştirilen bu program, işletme bilgi güvenliği aşamalarının ve güvenlik politikalarının tek bir kontrol merkezi üzerinden yönetilmesine olanak sağlayacaktır.

Bu çalışmanın işletmelere sağlayacağı katkılar aşağıda maddeler halinde sıralanmıştır.

1. İşletmelerin bilgi güvenliği risklerini en aza indirmek.
2. Bilgi güvenliği tehditleri sonucu oluşabilecek tehlikelere karşı önlem almak.
3. İşletme bilgi güvenliğini tek merkezden kontrol ederek, BGYS'ni kolaylaştırmak.
4. İşletme bilgi güvenliği kuralları oluşturmak ve bu kurallara uyulmasını sağlamak.
5. Bilgi güvenliği açıkları sonucu oluşabilecek maddi ve manevi zararları minimize etmek.

1.2. Çalışmanın Önemi

Bu konuda yapılan yazın taramasında, işletme bilgi güvenliği alanında yapılan akademik çalışmalar arasında genellikle bilgisayar ağları güvenliğinin önemine değinildiği ve bu yönde çalışmalar yapıldığı görülmüştür. Ayrıca günümüzde küreselleşmenin boyutu göz önünde bulundurulduğunda, işletmelerin sınır ötesindeki işletmelerle iletişim kurmaları ve onlarla ortaklıklar kurarak iş yapmalarıyla birlikte bilgi güvenliğine yönelik tehditlerde her geçen gün büyük bir artış yaşanmaktadır. Özellikle internet kullanımının tüm dünya üzerinde yaygınlaşması ile beraber bu riskler daha da artmıştır. İşletmenin profesyonel yönetici transfer etmesi ile yönetim şeklinin değişmesi, işletmenin yeni ortaklıklar kurmasıyla yeni teknolojilere

kavuşması, işletmelerde yeni bir bilgi birikiminin oluşmasına neden olmaktadır. Sayılan tüm bu sebepler aslında bilgi alış verişinin bir sonucudur. Bilgi alış verişinin çok yoğun ve çok hızlı bir şekilde gerçekleşmesi ile işletmelerin bilgi güvenliğine olan hassasiyetlerini ve bu konuya verdikleri önem artmaktadır. Tüm bu sebeplerden dolayı bilgi güvenliği özellikle 21. Yüzyılda uygulamacılar ve akademisyenler arasında önemli bir araştırma ve çalışma alanı olmuştur (Johnson, 2007: 5, Chang, 2007: 438-458).

Günümüzde bilgi güvenliğine yönelik saldırlar iki temel unsur üzerinde vücut bulmaktadır. Bunlardan ilki dışarıdan etkileyen başlıca tehditler olup, aşağıda maddeler halinde sıralanmıştır.

1. **Virüsler (Viruses):** Virüs yazılımları diğer bilgisayar yazılımlarının hizmet ettiği amaçlardan farklı olarak, kötü niyetle ve sızdığı bilgisayara zarar vermesi amacıyla hazırlanmış olan zararlı yazılımlardır. Virüsler genellikle, kullanıcıların internet veri havuzuna erişmeleri ile bulaşmakta ve bilgisayarda beklenmeyen ve istenmeyen olaylara sebep olan programlar olarak tanımlanmaktadır. Virüsler eriştikleri bilgisayar üzerinde, dosya silebilme, dosya içeriğini değiştirebilme ve kopyalayabilme özellikleri ile en büyük tehditlerdendir (Şahinaslan, 2013: 17).
2. **Solucanlar (Worms):** İsmini aldıkları solucanlara benzer şekilde, bilgisayara bulaştıklarında sistem üzerinde zararlı bir delik açarak yerleşen bu zararlı yazılımlar, kendilerini kopyalama özelliklerine sahiptirler. Bu özelliklerinden dolayı bilgisayarın işleyişini yavaşlatarak zarar vermektedirler (Şahinaslan, 2013: 18).
3. **Truva Atı (Trojan):** Bu zararlı yazılımlar solucanlardan farklı olarak kendilerini kopyalayıp çoğalmazlar. Girdikleri bilgisayarda kendisini gönderen kişinin komutlarını yerine getirmek için tasarlanmışlardır. Gönderen kişinin amacına göre bilgisayardaki bilgiler kaybedilebilir ve bilgisayar diski tamamen kullanılamaz hale gelebilir (Şahinaslan, 2013: 19).
4. **Tuş Kaydedici (Keylogger):** Keylogger zararlı yazılımları bulaştıkları bilgisayarda klavyeden basılan her tuş bilgisini kaydedip, bu bilgiyi kendisini yöneten merkeze göndermesi ile bilinmektedirler. Bu şekilde klavyeden girilen tüm bilgiye erişebilirler ve e-posta şifreleri, banka şifreleri, kredi kartı numaraları gibi hayati önem taşıyan kişisel bilgileri çalabilmektedirler (Erol, Şahin, Yılmaz, ve Haseski, 2015: 76-77).
5. **Casus Yazılım (Spyware):** Bilgisayar kullanıcısının haberi olmaksızın bilgi toplayan casus yazılımlar ise spyware olarak adlandırılmaktadır. Bulaştığı bilgisayar üzerinde istediği her türlü bilgiye ulaşabilmekte ve elde edebileceği bu bilgiler üzerinde istediği işlemleri yapabilmektedirler. En büyük bilgi hırsızlığı yazılımlarıdır (Canbek ve Sağıroğlu, 2006: 125).

Diğer tehlike ise kurum içerisinden gelebilecek saldırılardır. Literatürde yapılan çalışmalara bakıldığında bilgi güvenliğini tehdit eden en büyük tehlike sanılanın aksine işletme dışından değil, işletme çalışanlarının yanlış eylem ve davranışlarda bulunmasıdır (Johnson, 2007: 5).

İşletme içinden gelebilecek tehditleri iki farklı kategoride değerlendirmek mümkündür. Bunlar; çalışanların iyi niyetli olmalarına rağmen yanlış hareket etmeleri sonucunda oluşan tehlikeler ve çalışanların tamamen kötü niyetli olarak sebep olabileceği tehlikelerdir. İşletme dışından gelebilecek tehlikelere karşı alınacak önlemler arasında anti-virüs programlarının kullanımı ve firewall güvenlik yazılımlarının kullanımları sayılabilir. Ancak içerden gelebilecek tehlikelerde özellikle kötü niyetli çalışanların sebep olabileceği tehditler için alınabilecek önlemler sınırlıdır. Bu konuda en iyi çözüm ise çalışanların bilgiye erişimleri için yetki seviyelerinin belirlenmesi ve yetkisi olmayan çalışanların her türlü bilgiye erişmelerini engellemek olacaktır.

Bu çalışma kapsamında geliştirilen bilgi güvenliği programı, kullanıcılar için değişik seviyelerde yetki seviyesi belirlenerek, her kullanıcının kendisine tanımlanmış olan yetki seviyesine göre bilgiye erişmesine olanak sağlaması fikri üzerine kurulmuştur. Ayrıca işletme bilgi güvenliği sadece bilgisayar ağlarının güvenliğinin sağlanması olarak değerlendirilmeyip, bilgi güvenliğinin bir bütün olarak ele alınması ve bir kontrol merkezinden yönetilmesi amaçlanmıştır. Bu özelliğiyle çalışma yazın için bir özgünlük taşımaktadır.

1.3. Tez Çalışmasının Planı

Bu tez çalışması dört bölümden oluşmaktadır. Çalışmanın giriş bölümünde, bilginin tanımı ve tarihsel gelişimi, teknolojik gelişmelere bağlı olarak bilginin yaygınlaşması, bilgiye yönelik tehditler ve bilgi güvenliği konuları üzerinde durulmuştur. Çalışmanın birinci bölümünde "Çalışmanın Amacı", "Çalışmanın Önemi" ve "Tez Çalışmasının Planı" alt başlıkları yer almaktadır.

İkinci bölümde, "Bilgi Güvenliği ve Yönetimi" konusu tanımlanarak, bu alanda yaşanmakta olan problemlerin genel tespiti yapılmış, bu konudaki araştırmaların önemine değinilmiş ve bilgi güvenliği ile ilgili yazında yer alan tanımlamalara yer verilmiştir. Bilgi güvenliğinin sağlanması konusunda temel gereklilikler açıklanmış ve bu konuda bazı ilkelerin uygulanması önerilmiştir. Bilgi güvenliği yönetim sisteminin uygulanması aşamasında uluslararası bir yol haritası hükmünde olan ISO 27001 standardı açıklanmıştır. Bu bölümde son olarak BGYS (Bilgi Güvenliği Yönetim Sistemi) kurulumu ve uygulanması aşamaları açıklanmıştır.

Tez çalışmasının üçüncü bölümünde, programın geliştirilmesi esnasında kullanılan araçlar, uygulamayı geliştirme süreci, programın yönetimi ve kullanıcı yetkilerinin tanımlanma aşamaları, uygulama menüleri ve özellikleri açıklanmıştır. Ayrıca programın uygulanması ile tüm kullanım detayları geniş bir şekilde anlatılmıştır.

Son bölümde ise çalışmanın genel bir değerlendirmesinden oluşan sonuç bölümü yer almaktadır. Bu bölümde toplumlar arasında bilgi transferinin artmasına paralel olarak bilgiye yönelik hassasiyetin ve dolayısıyla bilgi güvenliğinin öneminin de aynı oranda artmakta olduğu açıklanmıştır. Bilgi güvenliği alanında yapılmış çok sayıda akademik çalışmanın olmasına rağmen, bu çalışmaların güvenliği sağlamaya yönelik somut bir yazılım ortaya koymadığı tespit edilmiş ve çalışmanın amacının bu eksikliği gidermek üzerine inşa edildiği belirtilmiştir. Çalışmanın bu yönüyle diğer bütün çalışmalardan farklı olduğu açıklanmıştır.

Yine son bölümde bilgi güvenliğini sağlamaya yönelik programın, geliştirme aşamaları ve bu esnada kullanılan programlama dilleri açıklanmıştır. Programın bilgi güvenliği konusundaki en önemli işlevleri anlatılarak, bazı temel güvenlik fonksiyonları hakkında bilgi verilmiştir.

2. BİLGİ GÜVENLİĞİ VE YÖNETİMİ

İşletmeler için "bilgi yönetimi" kavramı son yıllarda özellikle bilginin işletmeler için değeri düşünüldüğünde birçok kişi ve organizasyon tarafından üzerinde araştırma yapılan konuların başında gelmektedir. İşletmeler rekabet üstünlüklerini, en temel kurumsal kaynakları olarak gördükleri "bilgi" ile sağlamaktadırlar. Bu noktada işletmelerin ellerinde bulundurdukları bilgiyi, düzenli ve sistemli bir yapı içinde yönetmesi büyük önem kazanmaktadır (Fussell, 2005: 2977).

Bilgi yönetimi, işletmenin amaçları doğrultusunda başarıyı yakalaması için, bilginin nasıl elde edilip ortaya çıkarılabileceğini, nasıl kullanılabileceğini ve yönetebileceğini belirleyen sistematik bir süreçtir. Bu süreçte düzenlenerek kayıt altına alınan bilginin doğru zamanlarda, sadece doğru kişilerin ve istenilen yerden ulaşılabilmesini sağlamak da bilgi yönetiminin temel gerekliliklerinden bir tanesidir (Atılgan, 2009: 201-212, Kandemirli, 2007: 38).

İşletmelerde bilgi güvenliğinin tam ve doğru bir şekilde sağlanabilmesi için aşağıda tanımları yapılmış olan üç temel ilkenin uygulanması gerekmektedir (TS GUIDE 13268-2, 2006: 3-13).

- **Bilginin gizliliği (Confidentiality):** Bilgiye yalnızca yetkili olan kişilerce erişimin sağlanması ve yetkisiz kişiler tarafından erişime izin verilmemesi "gizlilik" ilkesini oluşturmaktadır.
- **Bilginin bütünlüğü (Integrity):** Bilginin çıktığı noktadan alıcısına teslim edilinceye kadar geçen süreçte herhangi bir değişime uğramadan hedefine ulaşması "bütünlük" ilkesini ifade etmektedir.
- **Bilgiye erişilebilirlik (Availability):** Erişilebilirlik ilkesi ise bilgiyi kullanmaya yetkili olan kişilerin istedikleri anda bilgiye ulaşabilmesi anlamına gelmektedir.

2.1. Bilgi Güvenliğinin Önemine Genel Bir Bakış

Bilgi güvenliği en kısa ve genel tanımıyla, yazılı, sözlü veya dijital ortam gibi farklı ortamlardaki bilginin gizlilik, bütünlük ve erişilebilirlik/kullanılabilirlik bakımından teminat ve garanti altına alınması ve bu güvencenin sürekliliğinin sağlanması olarak tanımlanabilir. Başka bir ifade ile bilgi güvenliği, bilgilerin yetkisi olmayan kişiler tarafından izinsiz olarak erişimlerinden, kendilerine ait olmayan bu bilgiyi kullanmalarından, bilginin işletmeye özel durumunun sona erdirilip umuma açık hale getirilmesinden, tamamen ortadan kaldırılmasından, değiştirilmesinden veya zarar verilmesinden korunmasıdır. Bilgi güvenliği yönetimi ise, bilginin güvende tutulması ile söz konusu bilgiye erişimin güvenli bir şekilde sağlanması olarak açıklanabilir. Bunu sağlamak için işletmeler, yönetimleri tarafından sınırları

çizilerek onaylanmış olan bir çerçeve dâhilinde, ayrıca çeşitli güvenlik politikalarıyla sınırları belirlenmiş olan bir güvenlik yönetimi planlayarak uygularlar (Çetin, 2010: 41-46).

Amerika'nın önde gelen telekomünikasyon firmalarından Verizon, her sene "Verizon Data Breach Report" adlı bir çalışma yayınlamaktadır. Firmanın 2015 yılında yayınladığı rapora göre, bilgi güvenliği konusunda aralarında Türkiye'nin de bulunduğu, 95 ülkeden bilgi güvenliği olayları ele alınmış ve bunların arasında kayda değer 63.437 bilgi güvenliği ihlali olayı incelenmiş ve 1.367 vakada ciddi ve geri döndürülemeyen veri kaybı yaşandığı tespit edilmiştir (Şentürk, Çil, ve Sağıroğlu, 2016: 39-51).

Kamu kuruluşları, bankalar, seyahat acenteleri gibi birçok kurum ve kuruluş tarafından kişisel bilgilerimizin veri bankalarında tutuluyor olması, bilgi güvenliğine yönelik birçok riski beraberinde getirmektedir. İlk olarak 2009 yılında Bitcoin ile para, elektronik ortama taşınmış ve dijital para devri böylece başlamıştır. Dünyada ilk olarak Estonya devleti resmi dijital para birimi olarak Estcoin'i kullanmaya başlayacağını açıklamıştır. Bu ve benzeri gelişmeler bilgi güvenliğinin ne derece büyük bir öneme sahip olduğunu ortaya koyan örneklerden bir tanesidir.

İşletmelerde bilgi birikiminin oluşturduğu büyük ve kıymetli verilerin her geçen gün artması, cep telefonu ve tablet gibi mobil cihazlar üzerinden bu veriye erişimin kolaylaşması, internet ortamındaki bulut sistemlerinin kullanılmaya başlanması gibi sebeplerden dolayı bilgi güvenliğinin daha büyük bir öneme ulaştığı gözlemlenmektedir. Örneğin Gartner tarafından 2016 yılında yapılan araştırmada sunduğu rapora göre; 2015 yılında bilgi güvenliğini sağlamaya yönelik yapılan harcamaların toplamı 75 milyar $'a ulaşmıştır. Bilgi güvenliği konusunda otorite kabul edilen uzmanların ortak görüşüne göre, dünya genelinde bilgi güvenliğine harcanan paranın 2018 yılında 101 milyar $'a ve 2020 yılında ise 170 milyar $'a ulaşması öngörülmektedir. Söz konusu rakamların büyüklüğü göz önünde bulundurulduğunda, işletmeler açısından bilgi güvenliğinin ne derece önemli olduğu bir kez daha ortaya çıkmaktadır (Gartner Inc. Stamford, 2016: 66).

2.2. Bilgi Güvenliği Tanımları

Amerikalı psikoloji profesörü Maslow'un yazmış olduğu ihtiyaçlar hiyerarşisinde insanların güvenlik gereksinimi, fizyolojik gereksinimlerden hemen sonra ikinci sırada yer almaktadır. Ancak bilgi güvenliği söz konusu olduğunda bu sıralamaya uygun davranıldığını söylemek pek mümkün değildir. Bireyler veya işletmeler, bilgi güvenliği ihlalleri sonucu karşılaşabilecekleri kimlik hırsızlığı, kişisel bilgilerinin ve işletme sırlarının çalınması ile ifşa edilmesi, bilgi varlıklarının silinerek yok edilmesi, değiştirilmesi veya yetkisiz olarak kullanılması ve benzeri sorunlar karşısında büyük çapta maddi ve manevi zarara uğrayabilirler (Siponen, 2000: 31-41) .

İşletmelerde bilgi güvenliğinin tam olarak sağlanması, sadece bilişim uzmanlarının ve yöneticilerin sorumluluğunda olan bir konu değildir. İşletmede çalışan bütün personelin bilgi güvenliğinin sağlanmasında ortak sorumluluğu bulunmaktadır. İşletmelerde bilgi güvenliğinin sağlanmasında en önemli faktörlerden birisi de her şeyden önce çalışanlara bilgi güvenliğinin önemine yönelik eğitimler verilerek, bilgi güvenliğinin önemine olan inancın sağlanması ve bilgi güvenliği bilincinin oluşturulmasıdır. Çünkü alınan tüm önlem ve tedbirlere rağmen her şey eninde sonunda insan faktörüne dayanmaktadır (Thomson, Solms ve Louw, 2006: 7-11).

Yazında bilgi güvenliği ile ilgili yapılan yazın taramasında elde edilen tanımlamalar aşağıda tablo halinde sunulmaktadır:

Tablo 1: Bilgi Güvenliği Tanımları Tablosu

YAYINLAYAN	YILI	YAYIN ADI	BİLGİ GÜVENLİĞİ TANIMI
Gürol Canbek Şeref Sağıroğlu	2006	"Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme"	"Bilgi güvenliği, "bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önleme olarak" tanımlanır (Canbek ve Sağıroğlu, 2006: 165)."
Türk Standartları Enstitüsü	2002	"Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri"	"Bilgi güvenliği; bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunu garanti etme (gizlilik), bilginin ve işleme yöntemlerinin doğruluğunu ve bütünlüğünü temin etme (bütünlük) ve yetkili kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişebileceklerini garanti etme (erişilebilirlik) olarak tanımlanmaktadır (Türk Standartları Enstitüsü, TSE-TS ISO/IEC 17799, 2002: 17)."

Basie von Solms	2000	"Information Security – The Fourth Wave"	"Bilgi güvenliği kurumsal BT (Bilgi Teknolojileri) kaynaklarının erişilebilirlik, bütünlük ve gizliliği üzerindeki risk etkilerinin azaltılarak disiplinize edilmesidir (Solms, 2000: 168)."
The Institute of Internal Auditors	2006	"Information Technology Controls"	"Bilgi güvenliği; iş devamlılığını sağlamak, iş hasar ve zararlarını asgari düzeyde tutmak ve yatırım geri dönüşü ve getirilerini ve iş fırsatlarını azami düzeye çıkartmak amacıyla, bilgiyi çok çeşitli tehditlere karşı korur (The Institute of Internal Auditors, 2006: 33)."
Charles P. Pfleeger	1997	"The Fundamentals of Information Security"	"Bilgi güvenliği yalnızca yetkili tarafların veriyi görmesini ve işlem yapmasını (gizlilik), yasal yollardan kodları ve veriyi değiştirmesini (bütünlük), ihtiyacı olduğunda verilere veya programlara erişmesinin (erişilebilirlik) sağlanmasıdır (Pfleeger, 1997: 14)."
Irene N. Shegai	2003	"Some Aspects of Information Security Problems"	"Bilgi güvenliği bilgi ve onu destekleyen (taşıma, depolama, işleme, vb.) altyapının kazara veya kasıtlı olarak doğal veya yapay tehditler aracılığıyla gelebilecek zararlardan korunması anlamına gelmektedir (Shegai, 2003: 33.)"
Yılmaz Vural	2007	"Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri"	"Bilgiye sürekli olarak erişilebilirliğin sağlandığı bir ortamda, bilginin göndericisinden alıcısına kadar gizlilik içerisinde, bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden bütünlüğünün sağlanması ve güvenli bir şekilde

			iletilmesi süreci bilgi güvenliği olarak tanımlanabilir (Vural, 2007: 89)."
Bahadır M. Kandemirli	2012	"Bilgi Teknolojileri Güvenliği Ve Sigorta Şirketinde Iso/Iec 27001 Standartları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uygulaması"	"Bilgi güvenliği, bilgiyi ve bilgi sistemlerini yetkilendirilmemiş erişimden, kullanımdan, ifşa edilmesinden, kesintiye uğramasından, modifiye edilmesinden veya yok olmaktan korumaktır (Kandemirli, 2007: 38)."
Sunay Kahraman	2006	"Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi Ve Aselsan A.Ş.'de Uygulaması"	"Bilgi Güvenliği, bilginin gizliliğinin, bütünlüğünün ve elverişliliğinin korunması olarak ifade edilmektedir (Kahraman, 2010: 37)."

2.3. Bilgi Güvenliği Yönetim Sistemi

British Standards Institute (BSI) tarafından 1998 yılında yayınlanan BS 7799-2 standardında Bilgi Güvenliği Yönetim Sistemi (BGYS) ifadesi ilk kez kullanılmıştır. Daha sonraki zamanlarda bu standart, Uluslararası Standartlar Kurumu (ISO) tarafından kabul edilerek ISO/IEC 27001:2005 olarak yayınlanmıştır (Vural ve Sağıroğlu, 2008: 507-522).

Bilgi güvenliğini sağlam temeller üzerinde oturtmak, güvenlik politikalarını planlamak, aşamalarını tasarlamak, gerçekleştirmek, işletmek, takip etmek, kontrol etmek ve devamlılığını sağlamak, işletme yönetim sisteminin bir parçası ve Bilgi Güvenliği Yönetim Sistemi (BGYS) olarak tanımlanmaktadır (Türk Standartları Enstitüsü, TS GUIDE 13268-2, 2006).

ISO 27001 standardı, ülkelere göre özelleştirilmiş tanımlara yer verilmeyen ve tüm dünya ülkeleri için geçerli olan genel tanımların bulunduğu, uluslararası kabul görmüş bir Bilgi Güvenliği Yönetim Sistemini uygulama standardıdır. Bu standarda göre bilgi güvenliği sadece bilişim sistemlerinin güvenliğini sağlamaya yönelik eylemlerden ibaret değildir. Bunun yanı sıra, kâğıt üzerinde yazılı olan ya da sözlü olarak paylaşılan tüm bilgilerin güvenliğini de kapsamaktadır. Bu standarda uyulmaması durumunda, işletmelerde bilginin zarara uğraması ya da değiştirilmesi gibi durumlar meydana gelebilir. Bu durum ise işletmenin, piyasadaki pazarını ve itibarını kaybetmesine, müşterileri, iş ortakları ve hissedarları karşısında güven ve

saygınlığını yitirmesine, yasal yaptırımlarla karşılaşmasına ve en sonunda maddi kayba neden olabilmektedir (Gülmüş, 2010).

Bu bağlamda ISO 27001, uygulanacak bir takım kontrol mekanizmaları yardımıyla, işletmelere bilgi güvenliğini doğru bir şekilde yönetebilecekleri ve etkinliğini ölçebilecekleri standart bir çözüm sunmaktadır. Söz konusu standart, ticari kuruluşlar, küçük, orta ve büyük çaplı kamu kurumları, kar amaçlı olmayan vakıf ve dernek gibi tüm kurum ve kuruluşları kapsar. Özellikle elektronik imza konusunda hizmet veren servisler, finans kuruluşları, sigorta şirketleri, hastaneler, bilgi teknolojileri alanında hizmet veren kuruluşlar ve elektronik ticaret yapmakta olan şirketlerde BGYS'nin uygulanması önemli bir zorunluluktur.

Bir kuruluş ya da şirketin BGYS standardının gerekliliklerini yerine getirerek uygulaması ve güvenlik sertifikasını alması, işletmeye ait bilgilerin korunmasında güvenliği yüzde yüz garanti altına aldığı anlamına gelmemektedir. Aslında bu sertifikaya sahip olunmasının anlamı, şirketin bilgi güvenliğinin hangi seviyede sağlandığının, bu konuda tespit edilen zayıf yönlerinin, risklerinin, risk sonuçlarına göre alınabilecek önlemlerin, şirket yöneticileri tarafından bilindiği ve takip edildiğidir (Şentürk, Çil, ve Sağıroğlu, 2016: 39-51).

2.4. Bilgi Güvenliği Yönetim Sisteminin Yönetimi ve Kurulumu

BGYS işletme genel yönetim sisteminin bir parçasıdır. Bu sistemin uygulanması ile işletmelerde bilgi güvenliği organizasyonunu kurmak ve gerçekleştirmek, bu yapıyı işletmek, sürekli takip etmek, gerekli kontrolleri sağlamak ve yapının sorunsuzca işlemesini temin etmek üzere gerekli önlemler alınmış olmaktadır. BGYS'nin kurulmasıyla, muhtemel tehdit ve risklerin belirlenmesi, işletme bilgi güvenliği politikalarının oluşturulması, denetimlerin ve bu konuda yapılan çalışmaların kontrol edilerek uygun yöntemlerin geliştirilmesi, kurumsal yapıların kurulması ve yazılım/donanım güvenlik fonksiyonlarının yerine getirilmesi gerekmektedir. Tüm bunları sağlamak için ise bir dizi denetimin üç farklı aşamada yapılması gerekmektedir. Bu aşamalar şunlardır (Türk Standartları Enstitüsü, TSE-TS ISO/IEC 17799, 2002: 17).

1. Aşama: Bilgi güvenliğinin kapsamının belirlenmesi ve politika geliştirilmesi.

2. Aşama: Bilgi güvenliğini sağlama yolundaki risklerin değerlendirilmesi, belirlenmesi, analiz edilerek derecelendirilmesi, işlenmesi ve kontrol edilmesi.

3. Aşama: Bilgi güvenliği risklerinin kabul edilerek onaylanması, işletme üst yönetiminin onayı ve uygulanabilirlik belgesinin alınması.

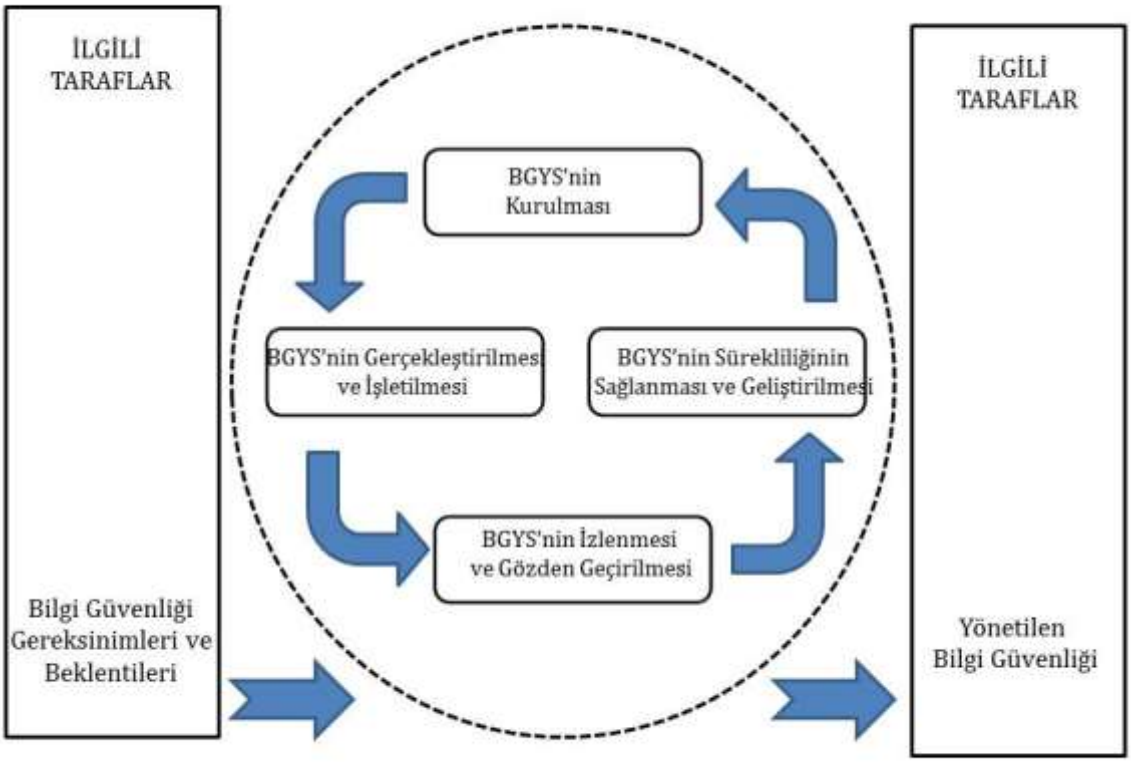
BGYS standartlarının uygulanması aşamasında sırasıyla takip edilmesi gereken yol;

- BGYS'nin kurulumu,
- Gerçekleştirilmesi,
- İşletilmesi,

- İzlenmesi,
- Gözden geçirilmesi,
- Kontrol edilmesi,
- Gerekli önlemlerin alınması,
- Sürekliliğinin Sağlanmasıdır.

Söz konusu aşamalar aşağıda yer alan Tablo 2'deki PUKÖ döngüsünde (Planla – Uygula – Kontrol et – Önlem al) yer almaktadır.

Tablo 2: PUKÖ Döngüsü Tablosu



Aşağıda yer alan Tablo 3'te ise PUKÖ döngüsünü oluşturan "Planla", "Uygula", "Kontrol Et", ve "Önlem Al" terimlerinin bu döngü içinde ne anlama geldikleri açıklanmıştır.

Tablo 3: Planla – Uygula – Kontrol Et – Önlem Al (PUKÖ) Döngüsü Açıklamaları

P	**PLANLA** (BGYS'nin Kurulması)	BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi
U	**UYGULA** (BGYS'nin gerçekleştirilmesi ve işletilmesi)	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi
K	**KONTROL ET** (BGYS'nin izlenmesi ve gözden geçirilmesi)	BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi
Ö	**ÖNLEM AL** (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)	Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve öneleyici faaliyetlerin gerçekleştirilmesi

- **Planla:** BGYS politikasının belirlenmesi, bu konuda işletmenin amaçlarının ve hedeflerinin belirlenmesi, tüm bu işlemlerin uygulanacağı süreçler ve uygulama aşamasında kuralların ve prosedürlerin geliştirilmesidir.
- **Uygula:** Planlama aşamasında belirlenen politikanın uygulanması, gerekli kontrollerin sağlanması, süreçlerin takip edilmesi ve prosedürlerin gerçekleştirilmesidir.
- **Kontrol Et:** BGYS politikasının uygulanma performansının değerlendirilmesi, amaçlara uygun hareket edilip edilmediğinin kontrolü, sürecin ilerlemesinin değerlendirilmesi ve sonucun ilgililere rapor olarak sunulmasıdır.
- **Önlem Al:** Bir önceki aşamada sunulan raporun işletme üst yönetimi tarafından gözden geçirilerek, çıkacak sonuçlara göre düzeltici ve önleyici faaliyetlerin gerçekleştirilmesidir (Kılıç ve Göçgöl, 2010).

2.5. Yazın Taraması

Bilgi güvenliği konusunda yapılan yazın taramasında akademik dünyada konuyla ilgili çok sayıda çalışmanın yürütüldüğü tespit edilmiştir. Bilgi güvenliği alanında yapılan çalışmaların genellikle bilgi güvenliği yönetim sistemleri, bilişim sistemleri ve bilgisayar ağları güvenliği, bilgi güvenliği risklerinin değerlendirilmesi, bilgi güvenliği bilinçlendirme eğitimleri ve yaşanan bilgi güvenliği problemleriyle ilgili durum tespitleri başlıklarında yapıldığı anlaşılmıştır. Konuyla ilgili ülkemizdeki araştırmacılar tarafından yapılmış olan çalışmalardan bazılarına aşağıda yer verilmiştir.

Keser ve Güldüren tarafından 2015 yılında Bilgi Güvenliği Farkındalık Ölçeği Geliştirme Çalışması adıyla yürütülen çalışmada, bilgi güvenliği konusunda alınabilecek tüm tedbir ve önlemlere rağmen insan faktörünün bu konuda bilinçlendirilmesi gerektiği belirtilmiştir. Söz konusu çalışmada yükseköğretim kurumlarında çalışmakta olan akademik personelin bilgi güvenliği konusunda bilinç ve farkındalık düzeylerinin belirlenebileceği bir ölçek geliştirilmiştir (Keser ve Güldüren, 2014).

Erkan (2006), işletmelerde uygulanan bilgi güvenliği yönetim aşamalarının otomasyonu konusunda araştırma yapmış ve ISO/IEC 27001:2005 standardına uygun olarak belgelendirilmiş bir bilgi güvenliği yönetim sisteminin kurulabilmesi için yürütülmesi gereken işlemlerin mümkün olabildiğince otomatik olarak yapılabilmesi konusunda önerilerde bulunmuştur (Erkan, 2006).

Kahraman (2006) tarafından yürütülen çalışmada ise kurumların TS ISO/IEC 27001standardında bilgi güvenliği yönetim sistemini kurmaları için gerekli olan bilgi risklerinin belirlenmesi teknikleri üzerinde durulmuştur. Ayrıca belirlenen bu risklerin önlenmesi için ihtiyaç duyulan her türlü teknoloji, politika ve kurallar açıklanmıştır (Kahraman, 2010).

Vural (2007), bilgi güvenliğini genel çerçevesi itibariyle araştırmış ve incelemiş, kurumsal bilgi güvenliğinin ve bilgi güvenliği standartlarının bir değerlendirmesini yapmıştır. Ayrıca çalışmasında kurum ve kuruluşlar için bilgi güvenliğini tehlikeye sokan tehditleri belirlemeye çalışmıştır. Çalışma kapsamında Türkiye'deki bilişim hukuku incelenerek, web uygulamalarının güvenliği üzerinde durulmuştur (Vural, 2007).

Ülkemizde henüz yeni olarak uygulanmaya başlayan e-devlet portalının kullanımı çerçevesinde, kurum ve kuruluşların bilişim sistemleri konusundaki mevcut durumlarını araştırmış olan Yıldız (2007), ISO/IEC 27001:2005 güvenlik standardı çerçevesinde söz konusu kurumlarda bilgi güvenliği yönetim sisteminin hangi aşamalardan geçirilerek oluşturulduğunu belirlemeye çalışmıştır (Yıldız, 2007).

Çetinkaya (2008), kurum ve kuruluşların bilgi güvenliğini uygulama başarılarını belirlemek ve ISO/IEC 27001:2007 bilgi güvenliği standartları kurallarının kullanıldığı web tabanlı bir test aracı geliştirilmesi üzerine çalışmıştır. Geliştirilen test aracı ile muhataplarına güvenlik alanında bazı sorular yöneltilmekte ve alınan cevapların değerlendirilmesiyle güvenli, az güvenli veya tamamen güvensiz ve benzeri sonuçlar içeren bir bilgi güvenliği durum raporu sunulmaktadır (Çetinkaya, 2008).

Kurum ve kuruluşların bilgi güvenliği sağlamlık seviyelerini incelemiş olan Aydoğmuş (2010), bu konuda ISO/IEC 27001:2005 standardı ile gösterdikleri uyumu değerlendirmiştir. Yapılan bu değerlendirme sonucunda işletmelerin uyguladığı bilgi güvenliği aşamalarının uluslararası standartlara uygun olup olmadığı konusunda bir sonuç açıklanmıştır (Aydoğmuş, 2010).

Mete (2010), Bilgi Güvenliği Yönetim Sistemini standartlara uygun olarak kurmayı ve yönetmeyi amaçlayan bilgi işlem merkezi yöneticileri için, kurumlarında bilgi güvenliği kültürü oluşturabilmelerini ve uluslararası ISO/IEC 27001 standardı için Türkçe bir kılavuz hazırlanması konusunda çalışmalar yapmıştır. Hazırlanan bu kılavuz ile özellikle bilgi işlem merkezlerinde ISO/IEC 27001 standartları kapsamında yapılması gereken çalışmalar açıklanmıştır (Mete, 2010).

Bingöl (2010) yürüttüğü çalışmada ise BGYS kurulması çalışmalarının açık kaynak koda sahip programlar üzerinden takip edilmesi halinde, sistemin kuruluş sürecinin yönetim maliyetinin düşeceğini belirtmiştir. BGYS kurulumu yapmayı hedefleyen bir kurumun, kurulum sürecinde nasıl bir sisteme ihtiyacı olacağının belirlenmesi konusunda çalışmalar yapmıştır. Yürütülen bu çalışma ile BGYS kurulum aşamalarının belirlenen bir sistematik çerçevesinde yapılması halinde sürecin ilerlemesinde daha sağlıklı sonuçlar alınacağı belirtilmiştir (Bingöl, 2010).

ABC A.Ş. isimli işletmede Kandemirli (2012) tarafından yapılmış olan çalışmada, bilişim sistemleri ve bilgi teknolojileri konusunda tüm dünyada yaygın olarak kullanılmakta olan ISO 27001, CobIT (Control Objectives for Information and Related Technology) ve ITIL (Information Technologies Infrastructure Library) bilgi güvenliği yönetimi süreçlerini incelemiştir. Bu üç farklı bilgi güvenliği standartları arasındaki farklar ve benzerlikler ortaya konarak, birbirlerine karşı üstün ve/veya zayıf yanları açıklanmıştır (Kandemirli, 2007).

Çin Kültür Üniversitesi Bilgisayar Bilimleri Bölümünden Chang-Lung Tsai, Uei-Chin Lin, Allen Y. Chang ve Chun-Jung Chen tarafından 2012 yılında yürütülen çalışmada ise bilgi güvenliğini sağlamanın en güvenli yönteminin bilgisayar tabanlı internet bulut sistemlerinin kullanılması olduğu ileri sürülmüştür. Bu çalışmada bilginin, en güvenli şekilde internet bulut sistemlerinde tutulması ve söz konusu bulut sistemine, birkaç aşamadan oluşan son derece güvenli bağlantılarla erişim sağlanarak kullanılması üzerinde durulmuştur (Chang-Lung, T. Uei-Chin, Allen ve Chun-Jung, 2012).

Bandyopadhyay 2006 yılında Amerika'daki Teksas Üniversitesinde yürüttüğü doktora tezinde, siber güvenlik risklerinin en az seviyeye indirgenmesi amacıyla siber güvenlik yatırımlarının getireceği fayda ve siber sigorta kullanımını incelemiştir. Ayrıca sonraki çalışmalar için deneye dayalı analizlerin yapılmasını önermiştir. Söz konusu doktora tezi çalışmasında, siber güvenlik yatırımlarının indirgenmesi için yapılacak yatırımların işletme için bir kârlılık yatırımı olmayacağını, ancak yetkisiz sızma sonucu oluşabilecek bilgi kayıplarının sebep olabileceği maddi kayıpları en aza indireceğini belirtmiştir (Bandyopadhyay, 2006).

Amerika'nın Alabama eyaletindeki Auburn Üniversitesinde Jourdan tarafından yürütülen doktora tezinde, bilgi güvenliği uzmanlarıyla yapılan görüşmeler ışığında bilgi güvenliği risk analizi süreçleri araştırılmıştır. Tez çalışması sonucunda risk analiz süreçlerinin

dinamiklerini daha iyi anlamak ve uygulamalarını iyileştirmek için yapılacak akademik çalışmaların devam etmesini önermiştir (Zachariah, 2010).

Claunch ve McMillan Healtcare Financial Management adlı dergide yayınlanan makalelerinde, son yıllarda siber saldırılardan kaynaklanan kayıp ve zarar maliyetlerinin artmakta olduğuna dikkati çekerek, 2010-2011 döneminde sadece tıp sektörü için %10 olan kayıp maliyetinin %32 oranında artış gösterdiğini belirtmiştir. Wyoming Tıp Merkezi'nde gerçekleştirdikleri vaka çalışmasında işletmenin bilgiye dayalı tüm varlıklarını kapsayan bir risk analizi çalışması yaparak, ilgili tıp merkezinin en uygun değerde siber güvenlik yatırımıyla, güvenlik seviyesini önemli derecede artırabildiğini açıklamıştır (Claunch ve McMillan, 2013).

Son olarak 2014 yılında düzenlenen 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı'nda H. Şentürk, C. Z. Çil ve Ş. Sağıroğlu tarafından yapılan "Siber Güvenlik Ekonomisi Üzerine Literatür İncelemesi" adlı sunumda, işletmelerin bilgi güvenliği alanındaki risklerinin ekonomik anlamda tüm boyutlarıyla belirlenmesi amacıyla bir çalışma yapılmıştır. Bu çalışmada yaşanması muhtemel güvenlik saldırılarının ekonomik maliyetinin ölçülmesi, bu konuda alınabilecek güvenlik teknolojisi önlemlerinin etkinliğinin belirlenmesi ve en uygun güvenlik yatırımlarının tespit edilmesi konularında incelemeler yapıldığı belirtilmiştir. Çalışmanın sonuç kısmında ise konuyla ilgili yapılan yazın taraması sonucu açıklanarak, siber güvenlik maliyet ekonomisi alanında yapılan çalışmalarda farklı yaklaşımların ortaya konulduğu ve dolayısıyla bu konuda genel olarak kabul edilmiş standart bir model veya yöntemin bulunmadığı tespit edildiği açıklanmıştır (Şentürk, Çil ve Sağıroğlu, 2014).

3. İŞLETMELERDE BİLGİ GÜVENLİĞİ İÇİN WEB TABANLI BİR UYGULAMA GELİŞTİRİLMESİ

3.1. Programın Geliştirme Araçları

Programın geliştirilmesi esnasında aşağıda açıklamaları yapılan sekiz farklı program geliştirme araçlarından faydalanılmıştır.

C Sharp

En genel tanımıyla C Sharp bir bilgisayar programlama dilidir. Günümüze kadar birçok programa dili geliştirilmiştir. Özellikle 20. ve 21. yüzyıllarda insanların hayatını kolaylaştırmak adına çok yaygın bir şekilde programlama dillerinin geliştirildiği zaman aralıkları olmuştur. Tüm programlama dilleri arasında özellikle nesnel bir diğer ifadeyle görsel programlama dilleri arasında iki programlama dili insanlık için ön plana çıkmıştır. Bu dillerin birincisi diğer dillerle ortak bir platformda çalıştırılabilen Java'dır. İkincisi ise .net programlama kütüphanesi ile eşleştirilebilen, tüm programlama dilleriyle ortak bir alanda programlanabilme özelliği ve kolay kod yazma yapısıyla ön plana çıkan C Sharp programlama dilidir. C Sharp programlama dili Microsoft tarafından geliştirilmiştir (Süzen ve Taşdelen, 2013: 122-131).

Kullanımın yaygın olması ve pek çok programcı tarafından kullanılıyor olması sebebiyle, C Sharp tabanlı bir programın geliştirilmesi aşamasında uzman programcılardan yardım almak oldukça kolaydır.

C# programlama dilini diğer bazı programlama dillerinden ayırt eden birkaç tane özelliği vardır. Bu özellikler aşağıda maddeler halinde sıralanmıştır.

- C Sharp programlama dilinin öğrenilmesi kolaydır.
- Bu programlama dilinden program yazılımı aşamasında oldukça yüksek verim elde edilmektedir. Diğer programlama dillerinde oluşan bazı hataların bu dilde önüne geçilmiştir.
- Görsel ve nesne tabanlı programlamayı desteklemektedir. Bu sayede büyük çaplı projeler hızlı bir şekilde geliştirilebilir.
- Güncel ve modern bir programlama dilidir. İnternet çağının gerektirdiği tüm programlama gereksinimlerini barındırdığı özellikleri sayesinde desteklemektedir.
- Bu programlama dilinin kaynağının dünyanın en saygın ve büyük bilişim firmalarından biri olan Microsoft firmasının olması kullanıcılara güven vermektedir.

- Başlangıçta 2 yıl süresince lisans ücreti talep edilmemektedir.

Tüm bu sebepler göz önünde bulundurularak tez çalışmamız çerçevesinde geliştirmiş olduğumuz bilgi güvenliği uygulaması C Sharp programlama dili kullanılarak geliştirilmiştir.

Windows Presentation Foundation

Windows Presentation Foundation, yeni nesil windows form oluşturma teknolojisi olarak adlandırılmaktadır. Standart windows form uygulamasından farkı ise, daha üstün bir performans, veri bağlama özelliği, tarayıcıda çalışabilme olanağı ve kolay tasarım imkanı sağlaması en öne çıkan özelliklerindendir. Windows Presentation Foundation (WPF), Microsoft tarafında geliştirilmiş yeni bir görsel tasarım sistemidir. WPF etkileyici ve işlevsel görsel tasarımlar yapılmasına olanak sağlamaktadır. WPF ile yapılan program tasarımları XAML (eXtensible Application Markup Language) olarak adlandırılan ve XML benzeri bir işaretleme dili ile oluşturulur. WPF ile birlikte kullanıcı ara yüzü ile yazılımın geliştirildiği platform birbirinden ayrılmıştır. Bu özellik sayesinde üzerinde çalışılan uygulamalar daha esnek ve kolay değiştirilebilmekte ve görsel açıdan daha zengin tasarlanabilmektedir. Bu sayede yazılımcının da üzerinde çalışmakta olduğu programa daha fazla zaman ayırmasına imkân vermektedir (Aktaş, 2013).

Tez projemizin uygulama tasarımı aşamasında WPF platformu kullanılmış ve sunmakta olduğu kolaylıklardan ve teknolojik imkânlardan faydalanılmıştır.

MS Visual Studio

MS Visual Studio, Microsoft tarafından geliştirilmiş ve Windows tabanlı işletim sistemlerinde çalıştırılmak üzere uygulama geliştirmemize yarayan bir yazılımdır. Diğer bir ifadeyle program geliştirme araçlarından birisidir denilebilir. Bu yazılım, üzerinde tamamen kodlar kullanılarak programlar geliştirilebildiği gibi, görsel bir şekilde de yazılım ara yüzü geliştirmemize imkân vermektedir. Bu büyük avantajı sayesinde de, kısa zamanda daha güzel ara yüzlü uygulama programları geliştirmek mümkün olabilmektedir.

Tez çalışmamız esnasında geliştirdiğimiz uygulama programının yazım aşamasında, MS Visual Studio yazılımından faydalanılmıştır.

Microsoft Blend

Microsoft Blend, geliştirilmesi amaçlanan uygulama türünün özelliklerini harmanlayan, web ve masaüstü uygulamaları için grafik ara yüzler oluşturulmasına imkan sağlayan Microsoft tarafından geliştirilmiş programlama tasarım aracıdır. Microsoft Blend, Silverlight ve Windows Presentation Foundation uygulamaları için geliştirme ve tasarım ortamıdır. Kişisel ara yüz tasarımları yapmak için MS Blend oldukça kullanışlıdır. Görsel tasarımcılar için işlevsel, iş akışlarının rahat kontrol edilebildiği bir geliştirme platformudur.

Geliştirdiğimiz bilgi güvenliği programının tasarımında Microsoft Blend tasarım aracı kullanılmıştır (Yumrutaş, 2014: 38-46).

Microsoft SQL

Microsoft SQL kavramının ne anlama geldiğini açıklamadan önce veritabanı kavramının tanımlanması gerekmektedir. Veritabanı birbiriyle ilişkili bilgilerin tutulduğu, söz konusu verilerin kullanım amaçlarına göre düzenlendiği ve son olarak bu verilerin mantıksal ve fiziksel olarak tanımlarının bulunduğu bilgi depolarıdır (Demirol ve Baykara, 2013).

Veritabanı; en sade anlamıyla belirlenmiş bir düzende bilgilerin yer aldığı veri topluluğudur. Daha geniş anlamıyla ise birbirleriyle ilişkili verilerin tekrar edilmediği ve çok amaçlı olarak depolandığı yapıya veritabanı denir. SQL (Structured Query Language), veri tabanlarında bulunan verilen üzerinde seçme, silme ve güncelleme gibi işlemleri yapmak için kullanılan bir sorgulama dilidir (Altıntaş, 2016: 7).

Microsoft SQL veritabanı sorgulama dili, bilişim uzmanları tarafından en çok tercih edilen veritabanı yazılımıdır. Veritabanlarının hayata geçirilmesini ve yönetilmesini sağlayan, aynı zamanda büyük çaplı kurumsal veritabanlarının da yönetilebildiği bir veritabanı yönetim sistemidir. Program tasarımcıları öncelikle bir veritabanı sistemi seçmelidirler. Bu seçim programın ihtiyaçlarına göre değişiklik göstermekle birlikte, Oracle, Access, MSSQL ve MYSQL veritabanı sistemlerinin en çok bilinenleri ve kullanılanlarıdır. Geliştirmiş olduğumuz güvenlik yazılımında veritabanı sistemi olarak MSSQL tercih edilmiştir.

Veritabanı sistemi olarak MSSQL seçilmişse, bu veritabanını oluşturmak, yönetmek ve tasarlamak için bir veri tabanı yönetim sistemine (VTYS) ihtiyaç duyulmaktadır. Bu alanda hizmet eden değişik programlar geliştirilmiş ve programcıların kullanımına sunulmuştur. Bunlardan bir tanesi de Microsoft firması tarafından geliştirilmiş olan SQL Server 2008 Express Edition'dır.

SQL Server 2008 Express Edition

Microsoft tarafından geliştirilmiş bir veritabanı yönetim sistemi olan SQL Server 2008 Express Edition programı ücretsiz kullanılabilmektedir. Ayrıca kullanımı oldukça pratik, yönetimi sade ve kolay, özellikle küçük boyutlu veritabanı ihtiyaçları için kullanımı yaygın olarak tercih edilmektedir. Ayrıca küçük çaplı uygulamalarda SQL Server lisans maliyetini karşılama zorunluluğundan kurtulmak için de tercih edilebilir. SQL Server 2008 Express Edition, sadece Microsoft işletim sistemleri üzerinde çalıştırılabilen kişisel bazlı olarak kişiye özel veya sunucu tabanlı olarak genel kullanım amaçlı olarak çalıştırılabilen bir veritabanı yönetim sistemidir.

Microsoft tarafından sağlanan tüm bu kolaylıklar göz önünde bulundurularak, uygulamamızda Microsoft SQL Server 2008 Express Edition programından faydalanılmıştır (Tosun ve Özdamar, 2015).

ASP

ASP web sayfası tasarımları yapmak amacıyla kullanılan ve Microsoft firması tarafından geliştirilmiş olan bir programlama dilidir. Active Server Pages'in kısaltılmış şekli olan ASP, dilimizde "Aktif Sunucu Sayfaları" anlamında kullanılmaktadır. ASP programlama dili, Microsoft Windows işletim sistemi üzerinde IIS (Internet Information Services / İnternet bilgi servisleri) ile çalıştırılabilen bir dildir. Sunucu tarafında çalıştırılması ile ortaya çıkan veriler HTML olarak internet tarayıcınız (Örneğin; Google Chrome, Firefox, Internet Explorer veya Opera) tarafından anlamlandırılır ve gösterilir. ASP dili ile kodlanan sitelere dinamik web siteleri de denmektedir (Akçakaya, 2006).

Geliştirilen uygulamanın web sayfası tasarımları ve uygulamaya konulan dinamik web sayfası ASP programlama dili kullanılarak hayata geçirilmiştir.

.Net

.Net Microsoft tarafından geliştirilen, herhangi bir programlama dilinden ve çalıştırılacak işletim sisteminden bağımsız olarak uygulama geliştirmeyi sağlayan ve bu anlamda yazılımcıya özgürlük sunan bir platformdur. .Net bir programlama dili değildir. Bunun aksine pek çok sayıda programlama dili ile yazılım geliştirmeye olanak sağlayan bir platformdur. .Net platformunun desteklediği programlama dillerinden bir tanesi de Visual

Studio'dur. Geliştirdiğimiz bilgi güvenliği programı Visual Studio kullanılarak yazıldığından, .Net platformundan yararlanılmıştır (Çayırlı ve Aslantaş, 2005).

3.2. Programın Geliştirilmesi

"İşletmelerde bilgi güvenliği için web tabanlı bir uygulama geliştirilmesi" başlığı altında yapmakta olduğumuz yüksek lisans tezi projesi kapsamında geliştirdiğimiz bilgi güvenliği programı, web uygulaması ve Windows işletim sistemi üzerinde çalışacak olan ana program olmak üzere iki aşamadan oluşmaktadır. Söz konusu program, akademik dünyada bu alanda yapılmış ilk çalışma olması sebebiyle benzer çalışmalardan oldukça farklıdır. Bilgi güvenliği başlığı altında birçok çalışma yapılmış ancak daha önce yapılmış olan hiçbir çalışmada, bilgi güvenliğini pratikte sağlamaya yönelik somut bir program geliştirilmemiştir.

Bu çalışma ise, tam olarak bu eksikliğin farkında olunması sonucu ortaya çıkmış ve projelendirilerek uygulanmıştır. Ancak yapılan tüm bu çalışmalar ve önlemlere rağmen, zincirin son halkası olan insan faktörünün göz ardı edilmemesi gerekmektedir.

Bilgi güvenliği risklerinden ve tehditlerinden korunmanın en iyi yolu, güvenliği sağlamaya yönelik bilişim teknolojilerine yatırım yaparak, bu teknolojileri daha fazla kullanmaktan önce, işletme çalışanlarının bilgi güvenliği konusunda bilinçlendirilmesi sağlamaktan geçmektedir. Bunun yanında işletmenin ihtiyacının olduğu tespit edilen güvenlik teknolojilerini de kullanmak gerekmektedir. İnsan etkenine bağlı olan bilgi güvenliği risklerini tamamen ortadan kaldırmak çoğu zaman mümkün olmamaktadır. Ancak iyi planlanarak uygulanacak bir bilgi güvenliği farkındalık etkinliği ile güvenlik risklerinin kabul edilebilir makul bir seviyeye indirilmesi sağlanabilir (Baykara ve Karadoğan, 2013).

Bilgi ve iletişim teknolojileri ile birlikte geliştirilen elektronik uygulamalar bir yandan hayatın akışını ve işleyişini kolaylaştırırken diğer yandan daha önce hiç karşılaşılmamış güvenlik tehditlerini ve dolayısıyla yeni suç tipleri ile karşı karşıya kalınmasını beraberinde getirmektedir. Son 15-20 yılda bilgi güvenliğine olan ilgi, dünyada olduğu gibi ülkemizde de çok büyük bir artış göstermiş ve buna paralel olarak bu alanda ülkemizde yapılan araştırmalarda artmıştır. Bilgi güvenliği konusundaki araştırmalar, problemleri daha çok teknik bakış açısıyla ele alıp, insan faktörünü göz ardı etmektedir. Kurumsal ve kişisel bilgilerin güvenliğini sadece bilişim sistemleri üzerinde alınabilecek güvenlik önlemleriyle (Firewall [güvenlik duvarı], VPN [sanal özel ağ], IPS-IDS [saldırı tespit/önleme sistemi], anti-virüs, internet içerik kontrolü yazılımı vb.) sağlamak mümkün değildir. Ayrıca işletme çalışanlarının da güvenlik bilincine sahip olması gerekmektedir (Keser ve Güldüren, 2014: 1167-1184).

Programın geliştirilmesi aşamasında, herhangi bir işletmenin bilgi güvenliğini sağlayabilmesi için yapılması gereken tüm aşamalar düşünülmüştür. Uygulamanın kullanımı ile

işletme bilgi güvenliğini maksimum düzeyde sağlamış ve bu konudaki riskleri minimize etmiş olacaktır.

Daha önce program geliştirme araçlarında açıklandığı gibi, program "C Sharp" programlama diliyle yazılmıştır. Uygulamanın geliştirilmesi aşamasında programlama ortamı olarak "Windows Presentation Foundation" kullanılmıştır. Geliştirme ortamı olarak "Visual Studio", program tasarımında ise, "Microsoft Blend" kullanılmıştır. Uygulama veri tabanı "Microsoft SQL" üzerinde oluşturulmuştur. Web uygulaması ise, ASP ve .Net kullanılarak geliştirilmiştir. İşletim sistemi üzerinde çalışacak olan program ana ekranı ve kullanıcı taleplerinin iletilmesi işlemlerinin gerçekleştirileceği web uygulaması, aynı veritabanı kullanılarak tasarlandığı için, web uygulaması üzerinden girilecek olan herhangi bir yetki talebi eş zamanlı olarak "Kullanıcı Yetkileri ve Erişim Güvenliği" menüsü altında görülebilecektir. Yetkili kullanıcı tarafından bu talepler değerlendirilecek ve gerekli görülen onaylama veya bekletme işlemleri bu menü üzerinden yapılabilecektir. Bu konu üçüncü bölümde yer alan 3.2.4. ve 3.2.5.2. numaralı alt başlıklarda daha detaylı bir şekilde açıklanacaktır.

3.2.1. Program Mimarisi

Program mimarisi 4 temel katmandan oluşmaktadır. Bu katmanlar şunlardır.

1. Veritabanı katmanı
2. Uygulama katmanı
3. Web uygulaması katmanı
4. Sunuş katmanı

5. Tablo 4: Program Mimarisini Oluşturan Katmanlar

Yukarıda yer alan Tablo 4'te görüldüğü gibi program mimarisini oluşturan tüm katmanlar birbiri ile iletişim halindedir. Program içeriğinde bulunan tüm bilgiler, veritabanında tutulmakta, uygulama katmanı ihtiyacı olan tüm bilgiye veritabanı üzerinden ulaşmakta, web uygulama katmanında yapılan her bir işlem veritabanı üzerinden uygulama katmanı ile paylaşılmakta ve son olarak sunuş katmanında programın tüm fonksiyonları kullanıcıların hizmetine sunulmaktadır.

3.2.2. Veritabanı Tasarımı

Veritabanı program mimarisinde yer alan katmanlardan bir tanesidir. Program içeriğinde yer alan tüm bilgiler veritabanı üzerinde tutulmaktadır. Programın geliştirme araçlarında açıklandığı üzere, veritabanı olarak Microsoft SQL kullanılmıştır. Dolayısıyla veritabanı tasarımında Microsoft SQL veritabanına ait tablolama yapısı kullanılmıştır. Veritabanında yer alan tüm tabloların ihtiyaç duydukları veriye erişim sağlayabilmeleri için tablolama yapısında var olan tüm tablolar birbirlerine sınırsız erişim hakkına sahiptirler.

Kullanıcı tanımları, kullanıcı şifreleri, bilgisayar MAC adresi bilgisi, kullanıcı yetki seviyesi, talep durumu, kullanıcı süresi gibi tüm bilgiler veritabanı üzerinde farklı tablolarda tutulmakta ve programın kullanımı esnasında ihtiyaca göre cevap vermektedir.

3.2.3. Program Akış Diyagramı

Tablo 5: Program Akış Diyagramı

Program akış diyagramı yukarıdaki Tablo 5'te görüldüğü gibidir. İlk olarak program ana ekranından veya web uygulaması üzerinden programa erişim sağlanması gerekmektedir. Programın web uygulamasına, İnternet Explorer, Google Crome veya Firefox gibi standart bir web istemcisi kullanılarak erişim sağlanıp kullanılabilir. Program ana ekranı ise, Windows işletim sistemine sahip herhangi bir bilgisayar üzerinde çalıştırılabilir.

Program ana ekranına veya web uygulaması ana sayfasına erişim sağlandıktan sonra, program yöneticisi tarafından oluşturulmuş olan, kullanıcı adı ve şifre bilgisi ile programa giriş yapılabilir. Programa giriş sağlandıktan sonra, kullanıcı kendisine tanımlanmış olan yetki seviyesine göre programın fonksiyonlarını kullanmaya başlayabilir.

Kullanıcı tarafından programda yapılan her bir işlem programın veritabanında tutulmaktadır. Tutulan bu veriler sonuç veya rapor olarak kullanılabilir.

3.2.4. Programın Yönetimi ve Kullanıcı Yetkileri

Program üzerinde farklı yetki seviyelerine sahip kullanıcılar oluşturulmuştur. Bu yapının kurulmasındaki amaç ise, bilgiye erişiminin sadece söz konusu bilgiye ihtiyacı olan kullanıcılarla sınırlandırılması ve böylelikle oluşabilecek bilgi güvenliği risklerinin azaltılmasıdır. Aşağıda detayları açıklanmış olan bu 3 farklı yetki seviyeleri ayrı kategorilerde değerlendirilmiş ve kullanıcı yetkileri buna göre belirlenmiştir. Söz konusu yetki seviyeleri şunlardır.

1. Tam Yetkili Kullanıcı: İşletme yönetim kurulu ve üst yönetim kadrosunun kullanımına sunulacak olan yetki seviyesidir. Uygulamanın tüm fonksiyonlarını kullanmakta tam yetkiye sahiptir. Programın kullanımında en üst seviyede yetkilendirmeyi ifade etmektedir.
2. Standart Yetkili Kullanıcı: İşletme departman / birim yöneticilerinin kullanımına sunulan yetki seviyesidir. Bu yetki seviyesine sahip bir kullanıcı, sadece kendi departmanı ve birimi ile ilgili tüm fonksiyonlarda tam yetkiye sahiptir. Ancak diğer departman ve birimlerin fonksiyonlarına ve dosyalarına herhangi bir müdahalede bulunamazlar.
3. Kısıtlı Yetkili Kullanıcı: En alt yetki seviyesine sahip kullanıcı tipidir. Departmanlarda ve birimlerde çalışmakta olan bölüm yöneticisi dışındaki tüm kullanıcıların yetki seviyesidir. Yalnızca kendi bölümü ile ilgili fonksiyonları kullanabilir ve dosyalara erişim sağlayabilir. Bunun dışında bölüm yöneticilerinin onayı ile yetki seviyeleri değiştirilip, bir üst yetki seviyesine çıkarılabilir.

3.2.5. Programın Menüleri ve Fonksiyonları

Programın geliştirilmesi iki temel aşamadan meydana gelmektedir. Birinci aşamada kişisel bilgisayarlar üzerinde çalışacak olan bilgi güvenliği uygulaması geliştirilmiştir. İkinci aşamada ise, uygulamanın kullanımı esnasında ortaya çıkabilecek bazı yetkilendirme taleplerinin değerlendirilebilmesi ve karşılanması amacıyla web sayfası geliştirilmiştir.

Programın web uygulaması üzerinden, işletme dışında olabileceği düşünülen program kullanıcılarının, bulundukları dış ortamdan programa erişimlerinin sağlanabilmesi amacıyla

programın indirilmesi mümkündür. Kullanıcılar programı web uygulaması üzerinden indirip, kendi kişisel bilgisayarlarında kullanabilirler. Ancak bunu yapabilmeleri için öncelikle yine web uygulaması üzerinden yöneticilerine ve/veya program yöneticisine bu taleplerini iletmelidirler. Bu şekilde işletme dışında kullanmak istedikleri bilgisayarlarının MAC adres bilgisini ileterek, onay talep etmelidirler. Yöneticileri ve/veya program yöneticisi tarafından verilecek onay sonrasında, kullanıcılar işletme dışından da programa erişim sağlayıp kullanabilirler.

3.2.5.1. İşletme Bilgi Güvenliği Temel Yükümlülükler ve Programa Giriş

Şekil 1: Program Ana Sayfası Görünümü

Program ana sayfasının görünümü yukarıda yer alan Şekil 1'de görüldüğü gibidir. Program çalıştırıldığı bilgisayar üzerinde Windows işletim sistemi özellikleri kullanılarak başlangıçta otomatik olarak açılmakta ve bilgisayar ekranını tamamen kaplamaktadır. Bu şekilde kullanıcının, program üzerinde kendisine tanımlanmış yetkileri dışında, bilgisayar üzerinden herhangi bir güvenlik açığına sebebiyet vermesinin önlenmesi amaçlanmaktadır.

Program ilk olarak çalıştırıldığında, ana ekranın sol tarafındaki program işlem menülerinden ilk sırada yer alan "İŞLETME BİLGİ GÜVENLİĞİ TEMEL YÜKÜMLÜLÜKLER ve PROGRAMA GİRİŞ" menüsünün arka planı yeşil renkte görülmekte, diğer menülerin arka planları ise kırmızı renkte görülmektedir. Bu renklerin anlamı; programa ilk giriş

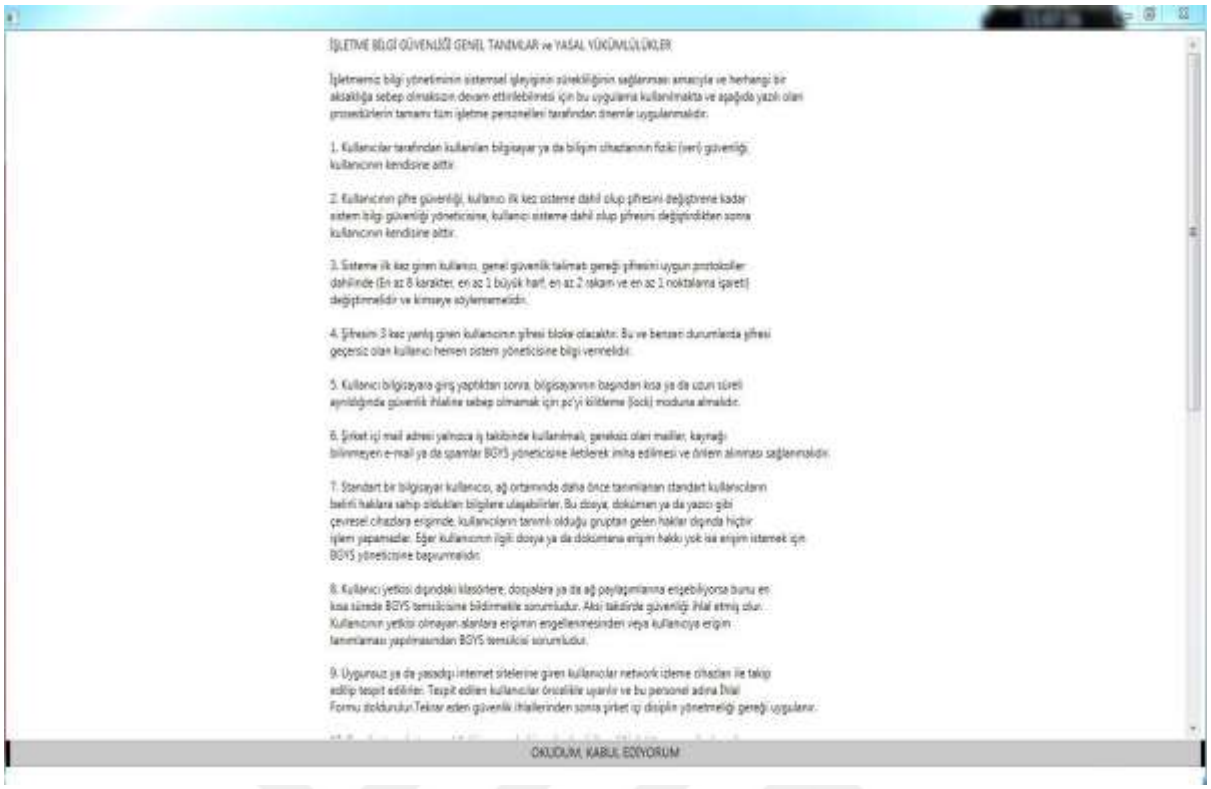
aşamasındayken sadece "yeşil" renkli arka plana sahip menüye giriş yapılabileceğini, "kırmızı" renkte arka plana sahip diğer tüm menülerin ise bu aşamada kullanılamayacağını ifade etmektedir. Diğer tüm menülerin aktif olması ve kullanılabilir duruma gelebilmesi için, program veritabanında tanımlı herhangi bir kullanıcının, kullanıcı ismi ve parolasını yazarak programa giriş yapması ile mümkün olabilmektedir.

Kullanıcıların programa henüz giriş yapmadıkları ana sayfa görünümünde arka plan rengi kırmızı olan herhangi bir menüye tıklayıp, giriş yapmaya çalıştıklarında karşılarına aşağıda yer alan Şekil 2'de görüldüğü gibi "Önce Giriş Yapmalısınız" uyarısının yer aldığı pencere açılmaktadır.

Şekil 2: "Önce Giriş Yapmalısınız" Uyarı Penceresi Görünümü

Başlangıçta aktif olarak kullanılabilir durumda olan ve yeşil arka plan rengine sahip tek menü olan "İŞLETME BİLGİ GÜVENLİĞİ TEMEL YÜKÜMLÜLÜKLER ve PROGRAMA GİRİŞ" menüsüne tıklandığında aşağıda yer alan Şekil 3'te görülen bilgi ve uyarı penceresi açılmaktadır.

Programa giriş yapmak isteyen kullanıcıdan, pencerenin en alt kısmında yer alan "OKUDUM KABUL EDİYORUM" yazısının yer aldığı butona basarak onay vermesi talep edilmektedir. Kullanıcı söz konusu onay butonuna basmadan, programa giriş penceresi açılmamaktadır.



Şekil 3: Program Giriş Uyarı ve Bilgilendirme Penceresi Görünümü

Açılan bu pencere ile program kullanıcılarına aşağıda yer alan uyarılar ve bilgilendirmeler yapılmaktadır.

İŞLETME BİLGİ GÜVENLİĞİ GENEL TANIMLAR ve YASAL YÜKÜMLÜLÜKLER

İşletmemiz bilgi yönetiminin sistemsel işleyişinin sürekliliğinin sağlanması amacıyla ve herhangi bir aksaklığa sebep olmaksızın devam ettirilebilmesi için bu uygulama kullanılmakta ve aşağıda yazılı olan kuralların tamamı tüm işletme personelleri tarafından önemle uygulanmalıdır.

1. Kullanıcıların kullandıkları bilgisayarın ve diğer bilişim sistemleri cihazlarının fiziki güvenliği, kullanıcıların sorumluluğu altındadır.

2. Kullanıcının programa giriş esnasında kullanacağı şifrenin güvenliği, kullanıcı ilk kez sisteme giriş yapıp şifresini değiştirene kadar bilgi güvenliği yöneticisine, kullanıcı sisteme giriş yaptıktan sonra ise kendisine aittir.

3. Sisteme ilk kez giriş yapan kullanıcı, güvenlik talimatı uyarınca şifresini belirlenmiş olan kurallara uygun bir şekilde (En az 8 karakter, en az 1 büyük harf, en az 2 rakam ve en az 1 noktalama işareti) değiştirmelidir ve kimseyle paylaşmamalıdır.

4. Şifresini 3 kez yanlış giren kullanıcının şifresi bloke olacaktır. Bu ve benzeri durumlarda şifresi geçersiz olan kullanıcı hemen sistem yöneticisine bilgi vermelidir.

5. Kullanıcı sisteme giriş yaptığında, kullandığı bilgisayarın başından kısa ya da uzun süreli ayrılması gerektiği durumlarda, güvenlik ihlallerine yol açmamak için bilgisayarını kilit (lock) moduna almalıdır.

6. Şirket içi elektronik posta adresi yalnızca iş ile ilgili konularda kullanılmalı, kaynağı bilinmeyen elektronik posta ya da spamlar BGYS yöneticisine iletilerek imha edilmesi ve önlem alınması sağlanmalıdır.

7. Kullanıcılar işletme bilgisayar ağı üzerinde BGYS yöneticisi tarafından tanımlanmış olan yetki seviyesine göre belirli haklara sahip oldukları bilgilere ulaşabilirler. Bu dosya, doküman ya da yazıcı gibi cihazlara erişimlerinde, kullanıcılar tanımlı olan yetkileri dışında işlem yapamazlar. Eğer kullanıcının ihtiyaç duyduğu dosya ya da dokümana erişim hakkı yok ise erişim istemek için BGYS yöneticisine başvurmalıdır.

8. Kullanıcı yetkisi olmayan dosyalara veya klasörlere erişebildiğini tespit etmesi durumunda, bunu en kısa sürede BGYS temsilcisine bildirmekle sorumludur. Bunun aksi belirlendiği takdirde, bilgi güvenliğini ihlal etmiş sayılır. Kullanıcının yetkisi olmayan alanlara erişimin engellenmesinden veya kullanıcıya erişim tanımlaması yapılmasından BGYS yöneticisi sorumludur.

9. Uygun olmayan içeriğe sahip web sayfaları veya yardımcı araçlar kullanılarak yasa ile yasaklanmış internet sitelerine giren kullanıcılar bilgisayar ağları izleme cihazları ile takip edilip tespit edilirler. Tespit edilen kullanıcılara ilk seferinde uyarı yapılır ve bu personel adına ihlal formu doldurulur. Tekrar eden güvenlik ihlallerinin tespit edilmesi halinde ise işletme disiplin talimatı uygulanır.

10. Kullanıcılar internet ortamında tanımadığı kimse ya da kimselerden gelen içeriğini bilmediği doküman veya dosyaları "İşletme Güvenlik Talimatı" gereği kesinlikle açmamalıdır.

11. Yetkisi olmayan kullanıcıların kullandıkları bilgisayara program yükleme, güncelleme veya herhangi bir programı kaldırmak gibi genel güvenlik talimatına aykırı davranmaları kesinlikle yasaktır.

12. Kullanıcılar, BGYS yöneticisinin bilgisi olmadan kendilerine tahsis edilmiş bilgisayar dışında şirket içindeki diğer bilgisayarları ve veri taşıma disklerini (harici diskler), genel güvenlik talimatı gereğince kesinlikle kullanmamalıdır.

13. Kullanıcılar, bilgisayarların kurumsal olduğunu unutmamalı, bütün müzik ve resim dosyaları kısıtlanmalıdır. Bilgisayarlarda müzik, resim vs. dosyaları bulundurulmamalı var ise silinmelidir.(Sistem merkezden yönetilebilir durumdadır, bir süre sonra bu işler sistem tarafından otomatik yapılacaktır.

14. Kullanıcılar, istenmeyen e-postalara uyarak hiçbir şey satın almamalı ve hiçbir hayır kurumuna bağış yapmamalıdır.

15. Kullanıcılar zincir e-postaları iletmemelidir. E-posta adreslerinin kimler tarafından görüleceğinin denetlenememesinden dolayı asılsız haberlerin veya virüslerin yayılmasına maruz kalabiliriz.

16. Gönderilecek e-postaların boyutu bir defada 6 MegaByte'ı geçmemelidir. Bu boyuttan büyük e-postalar sistemde yavaşlığa ve aynı zamanda mail kotalarının dolmasına sebep olacağından azami dikkatli olunmalıdır.

17. Bilgisayarlara hiçbir şekilde lisanssız program kurulumu gerçekleştirilmemelidir. Lisanssız yapılan kurulumların, kurulumu yapan kişiye hukuki anlamda hapis cezasına kadar varan yaptırımları bulunmaktadır.

18. Firma içinde yaşanan bilgisayar ya da yazılımlar ile ilgili sorunlar çok önemli ve acil değilse ilgili departmana e-posta yolu ile bildirilmelidir.

19. Şirket çalışanları bilgi işlem ve bağlı tüm sistemlerin genel güvenliği kapsamında, mesailerinin sonunda hafıza kartı, cd, dvd, harici disk ya da şirket bilgilerini içeren her türlü belgelerini (dosya, klasör, ve benzeri gizlilik içeren yazılı doküman) açıkta bulundurmamalıdır.

20. Şirket yönetimi, işletme içinde kullanılan bilgi sistemleri cihazlarının güvenliğinden, işletme içi bilgilerin gizliliğinden, bütünlüğünden ve erişilebilirliğinden, ayrıca bilgi güvenliği ihlallerinde yapılması gereken işlemlerden tüm çalışanlarla birlikte müştereken sorumludur.

Okudum, Kabul Ediyorum

Yukarıda yazılı olan kuralların ihlal edildiğinin tespit edilmesi halinde işveren haklı sebeple iş akdinin feshi hakkını saklı tutmaktadır (ISO Belgesi, 2017).

Programa giriş yapmak isteyen herhangi bir kullanıcı, yirmi maddeden oluşan bu uyarı penceresinin en alt kısmında yer alan "OKUDUM, KABUL EDİYORUM" butonuna basarak onay vermesi gerekmektedir. Onay verme işlemi sonrasında aşağıda yer alan Şekil 4'te görülen, kullanıcı adı ve şifre bilgisinin talep edildiği programa giriş penceresi açılmaktadır.

Şekil 4: Programa Giriş Penceresi Görünümü (Kullanıcı Adı ve Şifre Ekranı)

Programa giriş penceresi üzerinden herhangi bir kullanıcı kendisine tanımlanmış olan kullanıcı adı ve parola bilgilerini kullanarak programa giriş yapabilmektedir. Giriş yapıldıktan sonra "İşletme Bilgi Güvenliği Temel Yükümlülükler ve Programa Giriş" menüsü otomatikman ekrandan kalkmaktadır. Başarı ile giriş yapmış olan kullanıcılar kullanımları süresince bu menüyü artık görüntüleyelemezler.

Program üzerinde üç farklı kullanıcı yetki seviyesi tanımlanmıştır. Bu yetki seviyeleri aşağıda maddeler halinde sıralanmıştır.

1. Tam Yetkili Kullanıcı
2. Standart Yetkili Kullanıcı
3. Kısıtlı Yetkili Kullanıcı

Programa 1 numaralı yetki seviyesi olan "Tam Yetkili Kullanıcı" ile giriş yapıldığında aşağıda yer alan Şekil 5'te görüldüğü gibi programın 8 farklı menüden oluşan tüm işlem menüleri kullanılabilir durumdadır.

Şekil 5: Tam Yetkili Kullanıcı İle Giriş Ekranı Görünümü

Programa 2 numaralı yetki seviyesi olan "Standart Yetkili Kullanıcı" ile giriş yapıldığında ise aşağıda yer alan Şekil 6'da görüldüğü gibi programın bazı işlem menüleri kullanılabilir durumdadır. Bu yetki seviyesine sahip bir kullanıcı programa giriş yaptığında, program işlem menülerinden sadece aşağıda maddeler halinde yazılı olan 5 adet menü program ana ekranında görülecektir. Bu durumda olup da tam yetkisi olmayan kullanıcılar, yetkili olmadıkları program işlem menülerini göremeyecekler ve dolayısıyla bu menüler üzerinde herhangi bir işlem yapamayacaklardır. Standart yetki seviyesine sahip bir kullanıcı programa giriş yaptığında görebileceği ve işlem yapabileceği program menüleri aşağıdaki gibidir.

- Anti-Virüs Uygulaması
- Firewall Uygulaması
- İşletme Uygulama Programları
- Veri Erişim Güvenliği ve Yedekleme İşlemleri

Şekil 6: Standart Yetkili Kullanıcı İle Giriş Ekranı Görünümü

Son olarak programa 3 numaralı yetki seviyesi olan "Kısıtlı Yetkili Kullanıcı" ile giriş yapıldığında ise aşağıda yer alan Şekil 7'de görüldüğü gibi programın işlem menülerinden sadece üç tanesi kullanılabilir durumdadır. Kısıtlı yetkili kullanıcı hesabı ile programa giriş yapan kullanıcıların kullanımına açık olan 2 adet menü şunlardır.

- İşletme Uygulama Programları
- Veri Erişim Güvenliği ve Yedekleme İşlemleri

Şekil 7: Kısıtlı Yetkili Kullanıcı İle Programa Giriş Ekranı

Program ana ekranının sol üst köşesinde yer alan insan şekli ve hemen altında bulunan yazılı metin; programa hangi kullanıcı isminin giriş yaptığını göstermektedir. Resmin sağ üst köşesinde yer alan rakam ise giriş yapan kullanıcının yetki seviyesini ifade etmektedir. Burada 1 rakamı, tam yetkili kullanıcıyı, 2 rakamı standart yetkili kullanıcıyı ve 3 rakamı ise kısıtlı yetkili kullanıcıyı ifade etmektedir.

Ekran görüntüsünün sol tarafında yer alan program işlem menülerinin hemen üst kısmında, programa giriş yapan kullanıcının (kullanıcı 1) yetki seviyesi "FULL" ve hemen yanında ise programdan çıkış butonu yer almaktadır. Ancak burada belirtmemiz gerekir ki; programımızda güvenlik önlemleri açısından iki farklı çıkış butonu bulunmaktadır.

Bunlardan bir tanesi sol taraftaki program işlem menülerinin üst kısmında yer alan "ÇIKIŞ" yazılı olan butondur. Bu "ÇIKIŞ" butonu ile kullanıcı programdan sadece giriş yaptığı kullanıcı ismini çıkarabilmektedir. (LOGOUT) Yani bu "ÇIKIŞ" butonu ile programı kapatarak, tamamen çıkış yapmak mümkün değildir. Programdan tamamen çıkış yaparak, programı kapatmak ve bilgisayar ana ekranını görebilmek, kullanıcıların yetkilerinde değildir. Programdan tamamen çıkmak için ana ekran görüntüsünün sağ üst kısmında yer alan programdan çıkış butonu kullanılabilir. (EXIT) Söz konusu çıkış butonuna basıldığında, aşağıdaki Şekil 8'de yer alan bilgi menüsü açılmaktadır.

Şekil 8: Programdan Çıkış Butonu ve Parola Ekranı

Açılan bu bilgi menüsünün üzerinde "SADECE PROGRAM YÖNETİCİSİ ÇIKIŞ YAPABİLİR" şeklinde bir uyarı notu yer almaktadır. Program yöneticisinin yetkili parolasını girmesi ile programdan çıkış yapılabilmektedir. Yönetici dışındaki diğer tüm kullanıcılarda bu yetki bulunmamaktadır. Dolayısıyla yönetici dışındaki hiçbir kullanıcı programdan çıkış yapamamaktadır.

Program ana ekranının sağ tarafında ise, Windows işletim sisteminde yer alan ve tüm bilgisayar kullanıcıların ihtiyaç duyacağı birçok yardımcı programın kısa yolu yer almaktadır. Ana ekranın sağ tarafında bulunan işletim sistemine ait bu programlar, tüm yetki seviyesindeki kullanıcılar için aynıdır ve bu kısma tüm kullanıcılar herhangi bir kısıtlama ile karşılaşmadan erişip kullanabilmektedirler. Bu alanda yer alan programlar şunlardır.

1. Microsoft Paint
2. Microsoft Word
3. Microsoft Excel
4. Microsoft Power Point
5. Microsoft Access
6. Microsoft One Note
7. Acrobat Reader
8. Notepad

9. Hesap Makinesi
10. İnternet Explorer
11. Microsoft Outlook

Son olarak program ana ekranı sağ üst köşesinde saat ve tarih bilgilerinin yer aldığı aktif bir buton bulunmaktadır. Programın bu menüsüne erişim tüm yetki seviyelerindeki kullanıcılar için standarttır. İşletim sistemine ait olan bu yardımcı programlar, yetki seviyesine bakılmaksızın tüm kullanıcılar tarafından erişim sağlanıp kullanılabilir durumdadır.

Şekil 9: İşletim Sistemi Yardımcı Program Açılış Görünümü

3.2.5.2. Kullanıcı Yetkileri ve Erişim Güvenliği

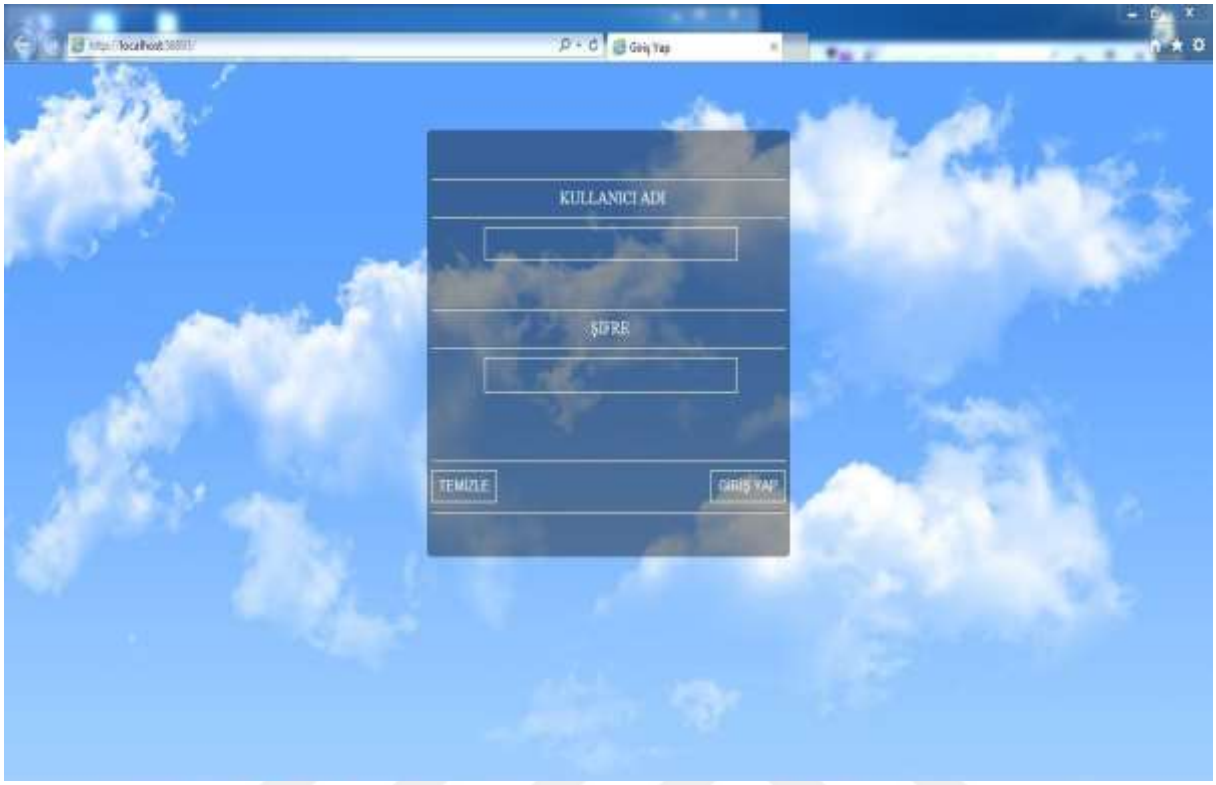
Şekil 10: Kullanıcı Yetkileri Penceresi

Programın yukarıdaki Şekil 10'da görülen "Kullanıcı Yetkileri ve Erişim Güvenliği" menüsüne sadece yetki seviyesi 1 olan "Tam Yetkili Kullanıcılar" erişebilmektedirler. Tam yetkili kullanıcıların, işletmede müdür/amir pozisyonunda olacağı varsayımı ile bu kullanıcılara altlarında çalışmakta olan personellerinin yetkilerini değiştirme, düzenleme ve görüntüleme yetkisi verilmiştir.

Bu menü üzerinden programa giriş yapma yetkisi olan tüm kullanıcıların, kullanıcı isimleri, parolaları, kullanmakta oldukları bilgisayarın ismi, yetki seviyeleri, personelin bölümü ve talep durumu gibi detaylar görüntülenmektedir.

Yetki seviyesi kısıtlı yetkili kullanıcı olan herhangi bir kullanıcının, mevcut yetki seviyesinin bir üst seviye olan standart yetkili kullanıcıya yükseltilmesi yönünde bir talebi olabilir. Aynı şekilde işletme dışında bulunan herhangi bir kullanıcı, dışardan erişim sağlayıp işletme bilgi güvenliği programını kullanma ihtiyacı duyabilir. Bu gibi durumlarda programla uyumlu olarak çalışmakta olan web uygulaması devreye girmektedir. Bu web uygulaması üzerinden kullanıcılar yetki taleplerini iletebilecekler ve bu talepleri "Kullanıcı Yetkileri ve Erişim Güvenliği" menüsü üzerinden yetkili amirleri tarafından görüntülenerek değerlendirilip

sonuçlandırılacaktır. Web uygulamasının giriş ana sayfa görünümü aşağıdaki Şekil 11'de görüldüğü gibidir.



Şekil 11: Web Uygulaması Giriş Görünümü

Web uygulamasına giriş yapabilmek için de program veritabanı üzerinde tanımlanmış olan geçerli bir kullanıcı adı ve şifre bilgisine ihtiyaç vardır.

Yetki seviyesini onaylama yetkisi olan yönetici, talebin ve personelin durumunu göz önünde bulundurarak dilerse, yetki talebini belirli bir süre için de onaylayabilir. Örneğin yetki seviyesi değiştirilecek olan kullanıcın yetkisini 3 gün, 7 gün veya 10 gün olacak şekilde onaylayabilir. Belirli süreli yetki onayı kullanıldığında, belirlenen süre sonunda yetki seviyesi program tarafından otomatik olarak iptal edilmektedir.

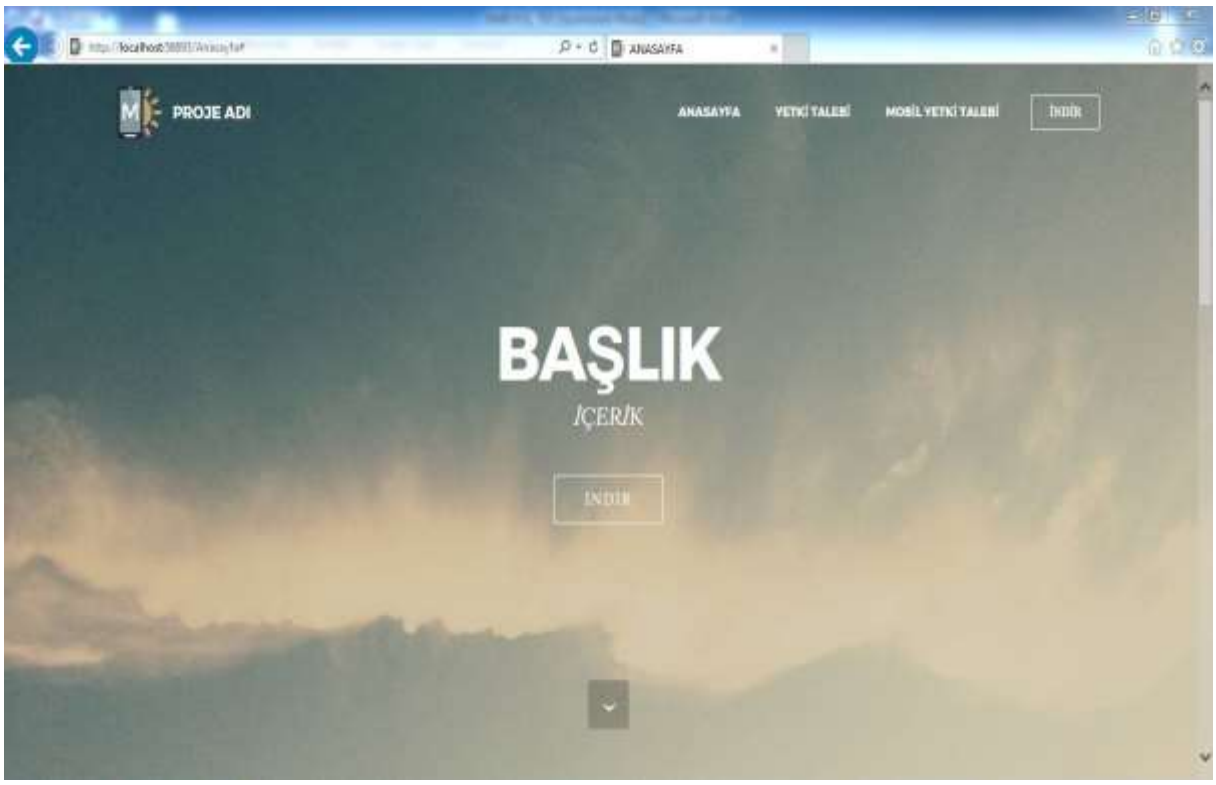
Yukarıda yer alan Şekil 10'da görüldüğü gibi "KULLANICI YETKİLERİ" penceresi üzerinde "BEKLEMEYE AL" ve "KAYDET" butonları yer almaktadır. Web sayfası üzerinden kullanıcılar yetki taleplerini girdiklerinde, girmiş oldukları bu talepleri programın "Kullanıcı Yetkileri ve Erişim Güvenliği" menüsü altında görüntülenmektedir. Bu alanda yetkili olan kullanıcı bu talepleri onaylayabilir veya yetkilerini beklemeye alabilir.

Kullanıcı yetkisinin beklemeye alınması ise, söz konusu kullanıcı yetki seviyesi onaylanıncaya kadar programa giriş yapamaz anlamına gelmektedir. Bu güvenlik önlemi programa erişim güvenliğinin gereklerinden bir tanesi olarak programda uygulanmıştır.

Web uygulaması işletmeye ait olacağı varsayılan *www.işletmealanadı.com.tr/program* alan adı üzerinden erişilip çalıştırılacaktır. Ancak bu aşamada yerel bilgisayar üzerinden yayın

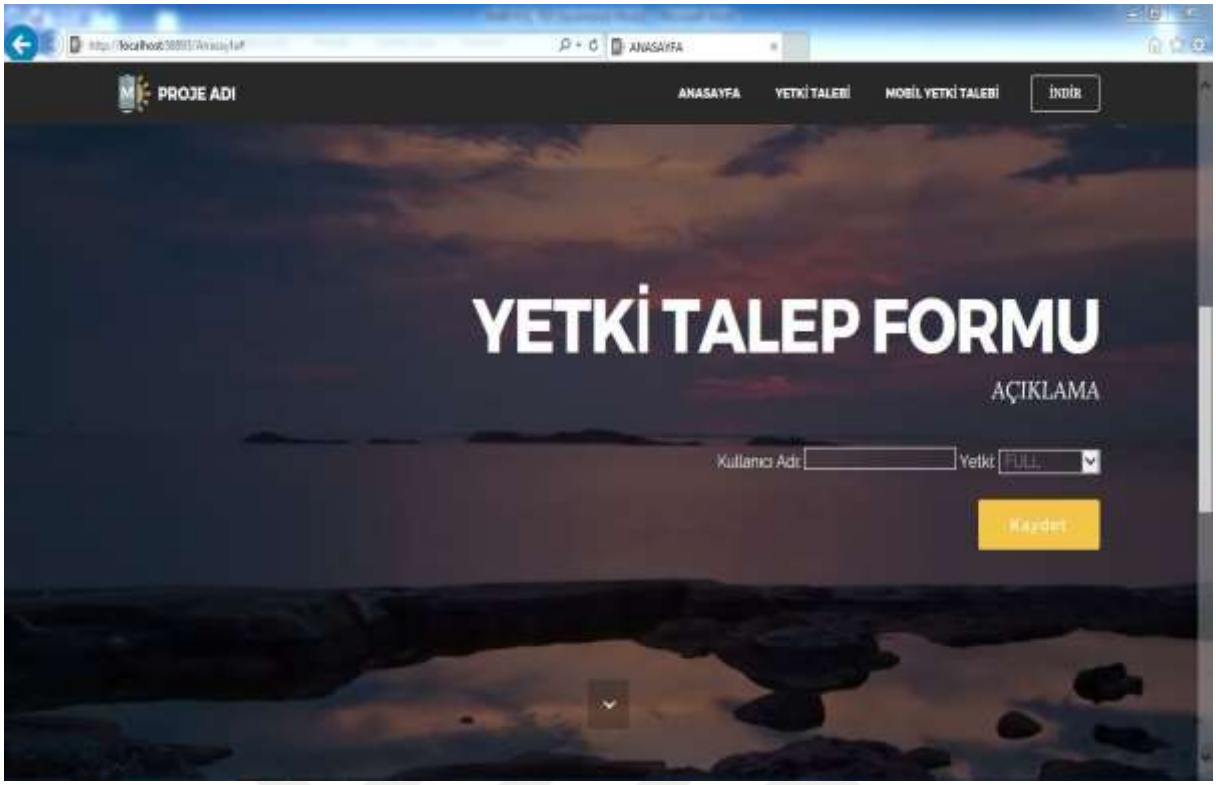
yapacak şekilde ayarlanmış olan ve *http://localhost:56893/Anasayfa#* sayfasından erişilebilmektedir. Web uygulaması üzerinden aşağıda yer alan Şekil 12'de görüldüğü gibi kullanıcıların yapabilecekleri işlemler şunlardır.

- Programın web uygulaması üzerinden indirilerek, bilgisayar ortamında kurulması ve kullanılmaya başlanması
- Kullanıcıların bir üst seviyede yetki talebinde bulunabilmesi
- Kullanıcıların programa mobil akıllı cihazları üzerinden erişim sağlayıp kullanabilmeleri için yetki talebinde bulunması



Şekil 12: Web Uygulaması Ana Sayfa Görünümü

Program kullanıcıları talep edecekleri yetki talebi değişikliği isteklerini web uygulaması ana sayfasında bulunan "YETKİ TALEBİ" butonuna basarak aşağıda yer alan Şekil 13'te görüldüğü gibi, açılan "YETKİ TALEBİ FORMU" sayfasında, kullanıcı adını ve talep ettiği yetki seviyesini seçip, "KAYDET" butonuna basarak kolaylıkla yapabilmektedir. Kurduğumuz bu dinamik yapı ile kullanıcılar şirket dışında iken bile yetki talebinde bulunabileceklerdir.



Şekil 13: Web Uygulaması Yetki Talebi Sayfası Görünümü

3.2.5.3. Anti – Virüs Uygulaması

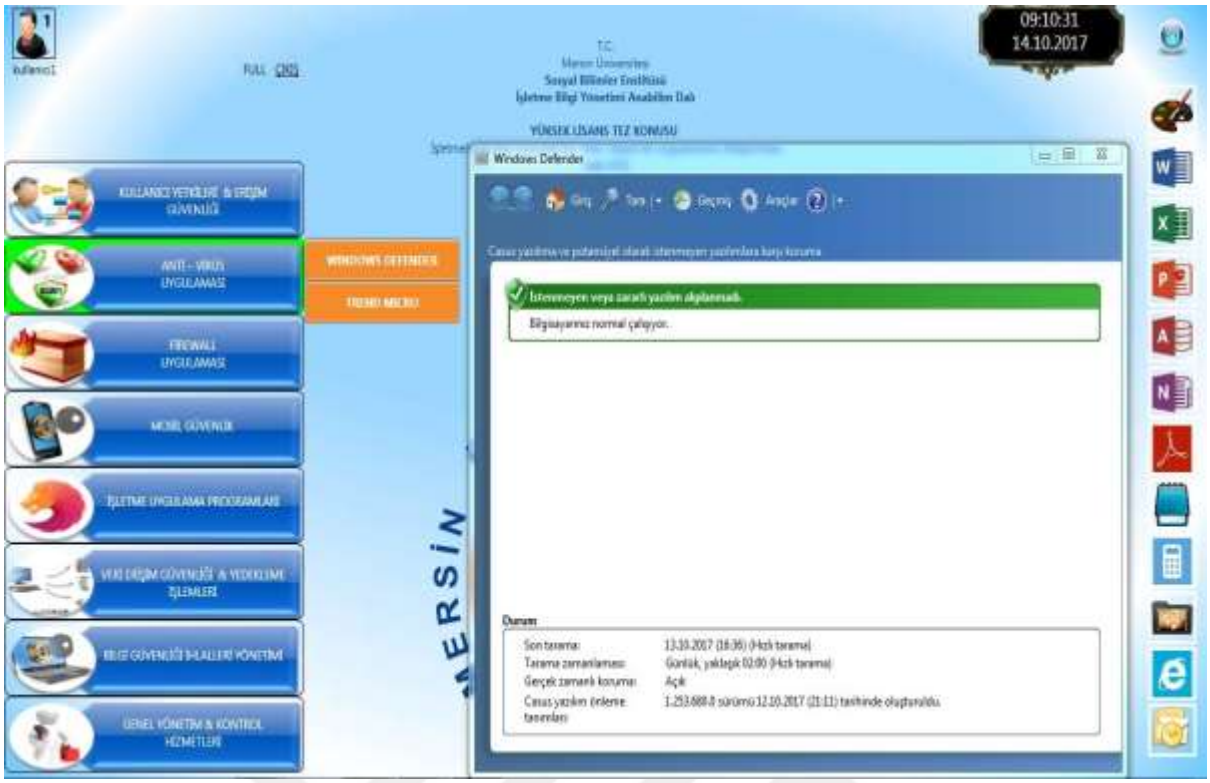
Şekil 14: Anti-Virüs Uygulaması Penceresi Görünümü

Anti-Virüs programları bilgisayar virüslerine karşı yazılmış, temizleme ve kurtarma işlemlerini yerine getiren koruyucu programlara verilen genel isimdir. Anti-virüs programları bilgisayar virüslerini bulmak, karantina altına almak veya silmek için çeşitli yöntemler izlerler. Her anti-virüs programının bünyesinde bir virüs veritabanı bulunur ve bu veritabanı sıklıkla güncellenerek, en yeni virüslere karşı önlemler alınır. Anti-virüs programlarının en yaygın olarak kullanılan markaları şunlardır.

- Eset
- Norton
- McAfee
- Avira
- Panda Security
- Trend Micro
- Windows Defender

Programımız bir işletme bilgi güvenliği programı olmakla birlikte, bir anti-virüs programı değildir. Ancak anti-virüs programı olmadan bilgiyi güvende tutmak günümüzde neredeyse imkansız hale gelmiştir. Bu nedenle program menülerine yukarıda yer alan Şekil 14'te görüldüğü gibi "ANTİ-VİRÜS UYGULAMASI" menüsü eklenmiştir.

Bu menü açılır pencerelere sahip dinamik yapıda tasarlanmış olan bir menüdür. Menünün üzerine gelindiğinde iki farklı pencere seçeneği açılmaktadır. Bu pencerelerden birisi Windows işletim sisteminde bulunan Microsoft firmasının ürettiği ve işletim sistemi ile birlikte ücretsiz olarak kullanılmasına izin verdiği "Windows Defender" anti-virüs programıdır. Diğeri ise programımızın kullanılmakta olduğu bilgisayar üzerinde kurulu olan "Trend Micro" adlı anti-virüs programıdır. Pencereler arasında seçim yapılarak tıklandığında ise, aşağıdaki Şekil 15'te görüldüğü gibi "Windows Defender" anti-virüs uygulamasının yönetim ekranı açılmaktadır.



Şekil 15: Anti-Virüs Uygulama Menüsü Açılır Pencereler – Windows Defender

Diğer pencere seçeneğiyle bilgisayarımızda kurulu ve kullanılmakta olan “Trend Micro” seçildiğinde ise, aşağıdaki Şekil 16’da yer alan Trend Micro anti-virüs programının ara yüzü açılmaktadır. Kullanıcılar açılan bu yönetim ekranında istedikleri işlemleri yapabilmektedir.

Şekil 16: Anti-Virüs Uygulama Menüsü Açılır Pencereler – Trend Micro

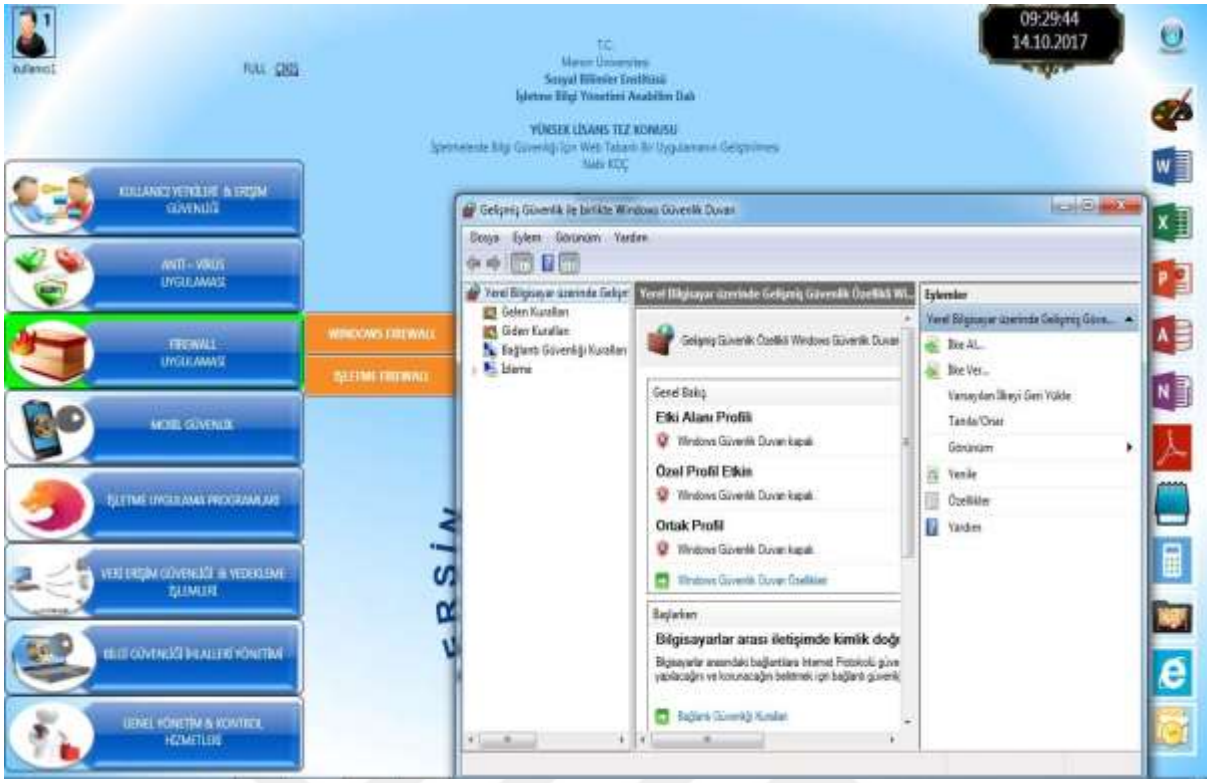
Kullanıcılar açtıkları her iki anti-virüs programları pencerelerinden de diledikleri işlemleri gerçekleştirebilirler. Windows Defender programı üzerinden bilgisayarı virüslere karşı tarama, işletim sistemi güncelleştirmelerinin kontrolü, geçmişte tespit edilmiş ve karantinaya alınmış virüs bilgileri ve bunun gibi tüm işlemleri yapabilirler. Açılan bir diğer pencere olan Trend Micro anti-virüs programı penceresi üzerinden de, Windows Defender programına benzer şekilde virüs tarama, programın güncellenmesi ve söz konusu programın sunmuş olduğu virüs günlüklerinin ve geçmişinin görüntülenmesi gibi buna benzer diğer bütün özelliklerini kullanabilmektedirler.

3.2.5.4. Firewall Uygulaması

Şekil 17: Firewall Uygulaması Açılır Pencere Görünümü

Programın uygulama menülerinden bir diğeri "Firewall (Güvenlik Duvarı) Uygulaması" menüsüdür. Menünün görünümü yukarıda yer alan Şekil 17'de görüldüğü gibidir. En genel tanımıyla firewall; bilgisayarımızı, tabletinizi veya akıllı telefonunuzu internetten gelebilecek zararlı yazılım tehlikelerine karşı koruyan bir kalkandır. İnternet ortamında veriler bilgisayarlar arasında dolaşmaktadır. Firewall ise, bu verilerin güvenli olup olmadığını kontrol eder ve güvenli olmayan verilere karşı bizleri korur. Günümüzde birçok modern işletim sistemi üzerinde bir firewall mutlaka bulunmaktadır. Windows işletim sistemi üzerinde de, "Windows Firewall" adında bir güvenlik duvarı uygulaması bulunmaktadır.

Bilgi güvenliği konusunda güvenlik duvarı çözümlerinin çok yaygın bir şekilde kullanılıyor olması sebebiyle programımız üzerinde aynı bir menü olarak "FIREWALL UYGULAMASI" menüsü yer almaktadır. Kullanıcılar bu menüyü seçtiklerinde yukarıda yer alan Şekil 15'te görüldüğü gibi, karşılarına iki farklı açılır pencere ekranı gelmektedir. Bunlardan ilki olan "WINDOWS FIREWALL" penceresi seçildiğinde ise, Windows işletim sistemi içerisinde yer alan firewall programı açılmaktadır. Aşağıda yer alan Şekil 18'de görülebileceği üzere bu ekran üzerinden kullanıcılar Windows firewall programının tüm özelliklerini kullanabilmektedirler.



Şekil 18: Firewall Uygulama Menüsü Açılır Pencereler – Windows Firewall

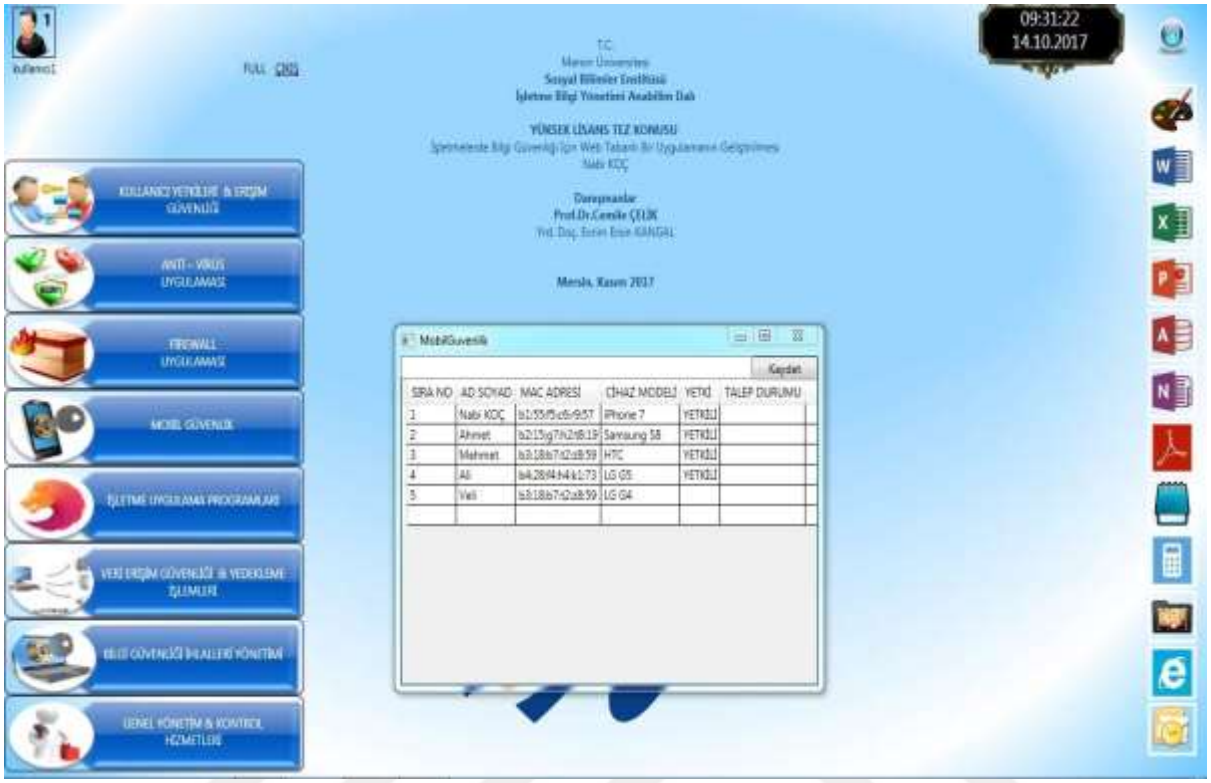
Firewall uygulama menüsünde yer alan ikinci açılır pencere "İŞLETME FIREWALL" seçeneğiyle ise, günümüzde birçok işletmenin bilgisayar sistemleri ağında kullanılmakta olan güvenlik duvarı çözümüne, program üzerinden erişim sağlamak mümkün olabilmektedir. Bu firewall ise işletmenin tercihine göre günümüzde en yaygın olarak kullanılmakta olan aşağıdaki firewalllardan birisi olabilir.

- Check Point Firewall
- Cisco Pix Firewall
- FortiNet Firewall
- Sonicwall Firewall
- Zyxel Firewall

3.2.5.5. Mobil Güvenlik

Programda yer alan mobil güvenlik menüsü, program kullanıcılarının mobil akıllı cihazlarından, programın web uygulamasına erişmelerine imkân sağlamak amacıyla tasarlanmıştır. Programın akıllı cihazlarda kullanılabilmesi için geliştirilmiş IOS (iPhone / iPad Operating System) veya Android tabanlı bir sürümü bulunmamaktadır. Bu menü üzerinden

kullanıcılar cep telefonu veya tabletleri üzerinden web sayfasına erişip, web sayfası üzerinden taleplerini yöneticilerine veya program yöneticisine iletebilirler.



Şekil 19: Mobil Güvenlik Menüsü Görünümü

Ancak projemizin temeli bilgi güvenliği esaslarına göre şekillendirildiği için, web sayfası uygulamasına erişim sağlayabilmek için akıllı cihazlarının MAC adresi bilgisi program üzerinde tanımlı olmalıdır. Aksi takdirde veritabanı üzerinde yer alan tablo yapısında, MAC adresi, kullanıcı adı eşleşmesi gerçekleşmeyecek ve kullanıcı hiçbir şekilde sisteme giriş yapamayacaktır.

Yetkili olan kullanıcılar bu menüye giriş yaptıklarında yukarıda yer alan Şekil 19'da görüldüğü gibi "Mobil Güvenlik" penceresi açılmaktadır. Bu pencere üzerinde tanımlı kullanıcıların ADI – SOYADI, MAC ADRESİ, CİHAZ MODELİ, YETKİ ve TALEP DURUMU gibi bilgiler yer almaktadır.

Günümüz teknoloji dünyasında birçok işletme, kullanmakta oldukları programlara cep telefonu ve tablet gibi akıllı cihazlardan erişim sağlanmasına olanak tanımayı tercih etmektedir. Bu özellik ile işletme çalışanları bilgisayara bağımlı kalmaksızın işletme dışından işlerini takip edebilmektedirler. İşletmenin kullanmakta olduğu varsayılan, mobil cihaz uygulama özelliği olan herhangi bir yazılıma erişim sağlanması gerektiğinde, bu talep programımız üzerinden MAC adresi – kullanıcı adı eşleştirmesi sağlandıktan sonra mümkün olabilecektir.

3.2.5.6. İşletme Uygulama Programları

Şekil 20: İşletme Uygulama Programları Açılır Menüsü Görünümü

"İşletme Uygulama Programları" adlı program menüsü açılır pencerelere sahip, dinamik yapıda tasarlanmış bir menüdür. İşletme kullanmakta olduğu tüm programları bu menüye yerleştirip, kullanıcıların hizmetine sunabilir. Kullanıcılar bu menüye giriş yaptıklarında, karşılarına yukarıda yer alan Şekil 20'de görülen pencereler çıkmaktadır. Programda bu menü üzerinde 5 farklı pencere yer almaktadır. Bu pencereler şunlardır.

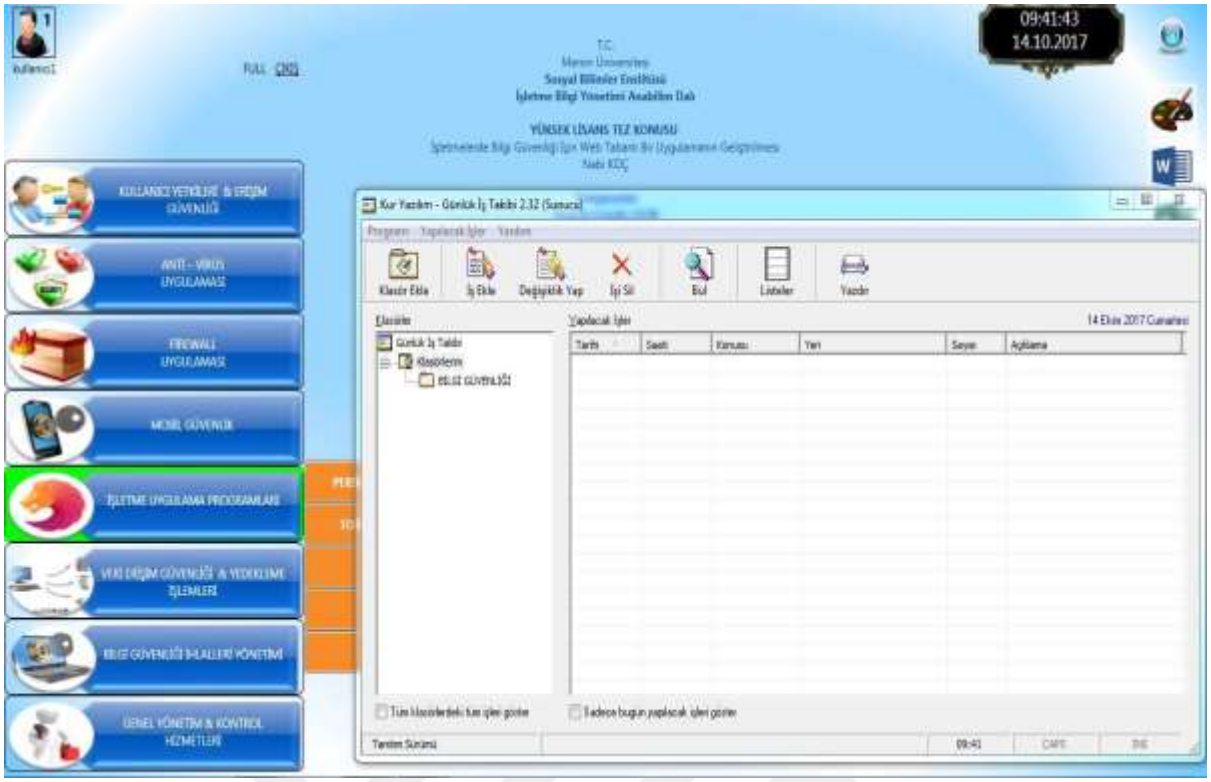
1. PERSONEL İLETİŞİM
2. TOPLANTI TAKİP
3. CRM (MÜŞTERİ YÖNETİMİ)
4. LOGO
5. PDKS

Söz konusu menünün birinci açılır penceresi olan "PERSONEL İLETİŞİM" penceresi seçildiğinde, kullanıcıların karşılarına aşağıda yer alan Şekil 21'de görülen pencere açılmaktadır.

Şekil 21: İşletme Uygulama Programları Menüsü - Personel İletişim Penceresi Görünümü

Kullanıcılar personel bilgilerini tutmakta olan bu yardımcı yazılım üzerinden işletmede çalışan tüm personellerle ilgili ihtiyaç duyabilecekleri bilgilere ulaşıp kullanabilmektedirler. Bu yazılım üzerinden personellerin iletişim bilgileri, e-posta adresi ve bunun gibi tüm bilgiler kullanıcıların hizmetine sunulmaktadır.

Menü üzerinde yer alan ikinci açılır pencere ise, "TOPLANTI TAKİP" penceresidir. Kullanıcılar bu pencereye giriş yaptıklarında karşılarına aşağıda yer alan Şekil 22'de görülen günlük iş takibi yapmaya imkân veren yazılımın ara yüzü açılmaktadır.



Şekil 22: İşletme Uygulama Programları Menüsü - Toplantı Takip Penceresi Görünümü

Toplantı takip işlevine sahip bu yardımcı yazılım ile kullanıcılar, herhangi bir toplantı veya iş belirleyip, bunu söz konusu yardımcı yazılıma kaydederek iş planı yapabilmektedirler. Söz konusu yazılım ile kayıt altına alınan toplantı bilgisi öncesinde talep edilmesi halinde belirlenen zaman aralığında kullanıcıya uyarı mesajı verilmesi sağlanarak, olası aksamaların önüne geçilmesi mümkündür.

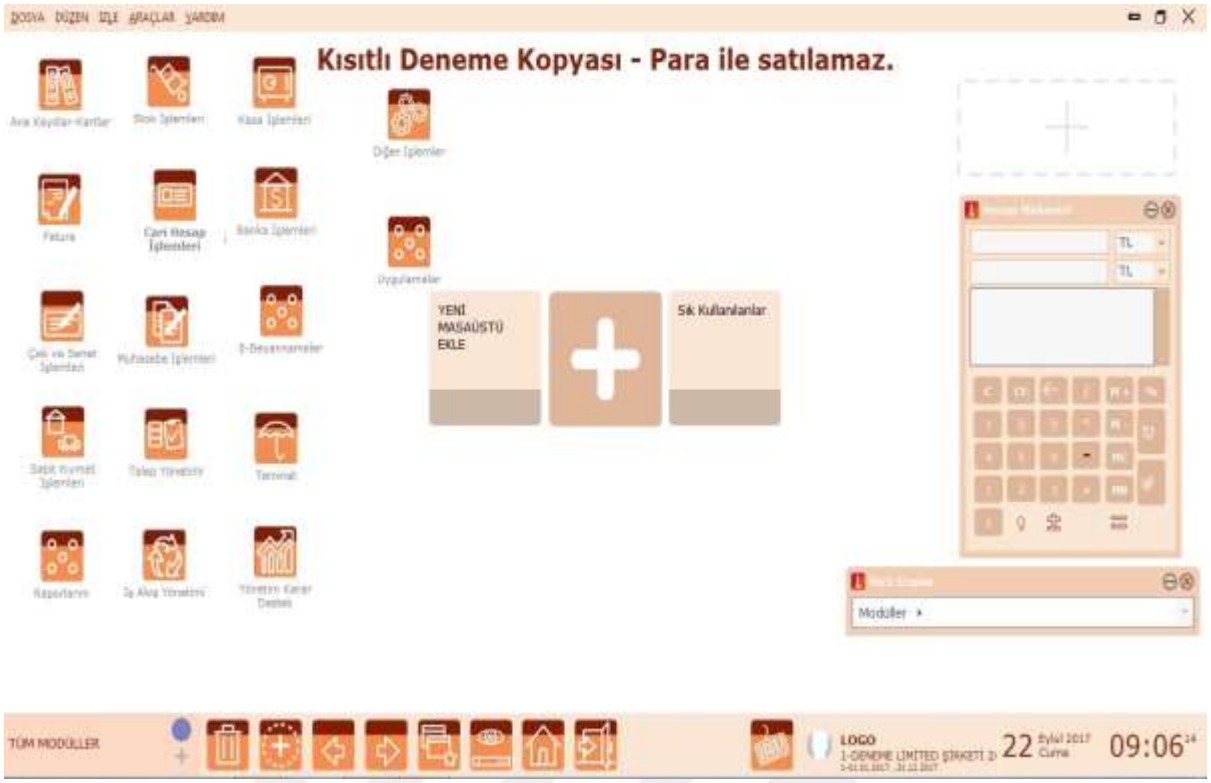
İşletme uygulama programları menüsü üzerinde yer alan üçüncü açılır pencere ise "CRM" penceresidir. Kısaca CRM'i; Türkçe ifadesi ile Müşteri İlişkileri Yönetimini (CRM: Customer Relationship Management) müşteriyi tanımak, müşteri ihtiyacını anlamak, ona uygun hizmetler ve ürünler geliştirmek ve bu bilginin organizasyon içinde paylaşılması olarak tanımlayabiliriz. Herhangi bir işletmenin ticari faaliyetlerinde en çok ihtiyaç duyacağı yardımcı yazılımlardan birisi de CRM yazılımlarıdır. Bu sebeple program üzerinde işletme uygulama programları menüsüne CRM yazılımı eklenmiştir.

Kullanıcılar "CRM" açılır penceresine giriş yaptıklarında, karşılarına aşağıda yer alan Şekil 23'te görülen true bilgi yönetim sistemleri adlı yazılımın ara yüz ekranı gelecektir.

Şekil 23: İşletme Uygulama Programları - CRM Açılır Penceresi Görünümü

Açılan CRM yazılımı üzerinden kullanıcılar, müşteri yönetimi konusunda yazılımda yer alan tüm özellikleri kullanabilmektedir.

Bu menü üzerinde bulunan dördüncü açılır pencerede ise, her işletmenin mutlaka kullanmak durumunda olduğu muhasebe yazılımı bulunmaktadır. Programda muhasebe yazılımı olarak ülkemizde oldukça yaygın bir şekilde kullanılmakta olan Logo muhasebe yazılımı kullanılmıştır. Kullanıcılar bu pencereye giriş yaptıklarında karşılarına aşağıda yer alan Şekil 24'te görülen Logo muhasebe yazılımının ara yüz ekranı gelmektedir.



Şekil 24: İşletme Uygulama Programları Menüsü - Logo Penceresi Görünümü

Kullanıcılar söz konusu muhasebe yazılımı üzerinden, yazılımın kendilerine sunduğu tüm muhasebe hizmetlerinden faydalanabilmektedirler.

İşletme uygulama programları menüsünde yer alan son açılır pencere ise PDKS (Personel Devam Kontrol Sistemi) penceresidir. Kullanıcılar PDKS penceresine giriş yaptıklarında karşılarına aşağıda yer alan Şekil 25'te görülen personel devam kontrol sistemi yazılımı gelmektedir.

Şekil 25: İşletme Uygulama Programları - PDKS Görünümü

Günümüzde birçok işletmede PDKS çözümleri yaygın olarak kullanılmaktadır. Bu yazılımlar üzerinden personellerinin işe geliş ve gidiş saatlerini, fazla mesai işlemlerini ve en sonunda personelin ücretinin hesaplanması işlemleri gerçekleştirilmektedir.

3.2.5.7. Veri Erişim Güvenliği ve Yedekleme İşlemleri

Programın yedinci menüsü olan Veri Erişim Güvenliği ve Yedekleme İşlemleri menüsü ile kullanıcıların tüm önemli veri dosyalarını, programın yöneticisi tarafından belirlenen ortak bir alanda tutmalarını zorunlu kılan bir menüdür. Bu menünün görünümü aşağıda yer alan Şekil 26'da görüldüğü gibidir.

Şekil 26: Veri Erişim Güvenliği ve Yedekleme İşlemleri Menüsü Görünümü

Bu menüye giriş yapan kullanıcılar yetkilendirildikleri ortak klasörlere erişim sağlayabilirler. Yukarıda yer alan Şekil 26'da tüm ortak klasörlere erişim sağlandığı görülmektedir. Bunun sebebi ise programa tam yetkili kullanıcı olan "Kullanıcı 1" ile giriş yapılmış olmasıdır. Kullanıcı 1 tüm ortak klasörlere erişme yetkisine sahiptir.

Aşağıda yer alan Şekil 27'te görüldüğü gibi, programa tam yetkili bir kullanıcı dışında, örneğin standart yetkiye sahip olan "Kullanıcı 2" ile giriş yapıldığında, sadece yetkili olduğu klasörler beyaz renkte ve erişilebilir durumda olacaktır. Kırmızı renkteki klasörlere bu yetki seviyesindeki bir kullanıcı giriş yapamayacaktır.

Kullanıcı 2'nin yetkili olup erişebileceği üç klasör bulunmaktadır. Bu klasörler şunlardır.

- Ortak/Raporlar
- Ortak/Log
- Ortak/MUHASEBE

Burada kullanıcı 2'nin muhasebe bölümünde çalışan bir personel olduğu düşünülerek, sadece kendi bölümüne ait klasöre erişim yetkisi verilmiştir.

Şekil 27: Veri Erişim Güvenliği ve Yedekleme İşlemleri - Standart Yetkili Kullanıcı Görünümü

Son olarak Veri Erişim Güvenliği ve Yedekleme İşlemleri menüsüne en az yetki seviyesine sahip olan "Kullanıcı 3" ile giriş yapıldığında ise aşağıda yer alan Şekil 28'de görüldüğü gibi sadece Ortak/Raporlar ve Ortak/Log klasörlerine erişim yetkisine sahip olduğu görülecektir. Bu iki ortak klasör dışındaki tüm klasörlere erişim yetkileri yoktur ve bunun ifadesi olarak diğer tüm klasörler kırmızı renktedir.

Şekil 28: Veri Erişim Güvenliği ve Yedekleme İşlemleri Menüsü - Kısıtlı Kullanıcı Giriş Görünümü

3.2.5.8. Bilgi Güvenliği İhlalleri Yönetimi

Şekil 29: Bilgi Güvenliği İhlalleri Yönetimi Menüsü Görünümü

Programın Bilgi Güvenliği İhlalleri Yönetimi menüsünün görünümü yukarıda yer alan Şekil 29'da görüldüğü gibidir. Bu menünün amacı herhangi bir bilgi güvenliği ihlalinin tespit edilmesi durumunda bunun en hızlı şekilde program yöneticine bildirilmesinin sağlanmasıdır. Böylece ilgili güvenlik açığı için gerekli görülen tedbirlerin en hızlı şekilde alınması amaçlanmış ve varsa zararın en az seviyede tutulması hedeflenmiştir.

Yukarıda yer alan Şekil 27'de görüldüğü üzere tam yetkili kullanıcı seviyesindeki kullanıcıların karşılaştıkları olumsuz bir durumu program üzerinden en hızlı şekilde program yöneticisine iletmesini sağlamaktadır. Açılan ekranda problemi yazan kullanıcı, gönder butonu ile mesajını en kısa ve hızlı yoldan ilgili kişiye iletebilmektedir.

3.2.5.9. Genel Yönetim ve Kontrol Hizmetleri

Programın son menüsü olan Genel Yönetim ve Kontrol Hizmetleri menüsüne giriş yapıldığında, aşağıda yer alan Şekil 30'da görülen ekran açılmaktadır. Bu menüye sadece tam yetkili kullanıcıların giriş yetkisi bulunmaktadır. Bu menü üzerinden açılan ekran ile kullanıcılar aşağıdaki işlemleri gerçekleştirebilirler.

- Yeni kullanıcı tanımlanması (Tam Yetkili, Standart Yetkili ve Kısıtlı Yetkili)
- Kullanıcıların şifrelerinin belirlenmesi
- Gelen yetki taleplerinin değerlendirilmesi ve gerçekleştirilmesi
- Belirli süreliğine yetkilendirme işlemlerinin yapılması
- Program üzerinde bulunan herhangi bir kullanıcının silinmesi
- Kullanıcılar üzerinde yapılan değişikliklerin kaydedilerek uygulanması

Şekil 30: Genel Yönetim ve Kontrol Hizmetleri Menüsü Görünümü

4. PROGRAMIN TEST EDİLMESİ

4.1. Birinci Test Çalışması

Program ilk olarak Mersin ili Yenişehir ilçesi sınırları içerisinde 25 yıllık köklü bir gayrimenkul firması olan Aspark Gayrimenkul Limited Şirketinde 25 - 29 Ekim 2017 tarihleri arasında 5 gün süresince test edilmiştir. İşletme bünyesinde kullanılmakta olan 3 farklı bilgisayara programın kurulumu yapılmış ve firma çalışanları tarafından programın bütün özellikleri kullanılarak uygulamalı olarak test edilmesi sağlanmıştır.

Aspark Gayrimenkul firmasında yapılan uygulamalı test çalışması esnasında aşağıda yer alan Şekil 31'de görüldüğü gibi ASPARK1, ASPARK2, ASPARK3 adlarında 3 farklı kullanıcı oluşturulmuştur. Söz konusu kullanıcılardan ASPARK1 kullanıcısı yönetim tarafından kullanılan ve tam yetki seviyesine sahip bir kullanıcıdır. ASPARK2 kullanıcısı muhasebe personeli tarafından kullanılan standart yetki seviyesine sahip bir kullanıcıdır ve son olarak ASPARK3 kullanıcısı ise firma sekretaryası tarafından kullanılan ve kısıtlı yetki seviyesine sahip bir kullanıcıdır.

Şekil 31: Programın Aspark İşletmesinde Uygulamalı Olarak Test Edilmesi

Uygulamalı test çalışması sırasında işletme çalışanları programın, Anti-Virüs, Firewall, İşletme Uygulama Programları, Veri Erişim Güvenliği ve Yedekleme İşlemleri gibi tüm özelliklerini kullanıp test etme imkânı bulmuştur. Aşağıda yer alan Şekil 32'de görüldüğü gibi, firma çalışanları daha önce sadece kullandıkları bilgisayar üzerinde kayıt altına aldıkları tüm belgeleri programın kullanımı ile birlikte ortak klasör altında kayıt altına almaya ve dolayısıyla yedeklemeye başlamıştır. Bu sayede firmanın müşteri portföyü kayıtları gibi önemli bilgileri yedeklenerek koruma altına alınmıştır.

Ayrıca aşağıda yer alan Şekil 32'nin sol üst köşesinde yer alan kullanıcı ikonundan görülebileceği üzere programa ASPARK1 (Tam Yetkili Kullanıcı – Yönetici) kullanıcısı ile giriş yapılmıştır. Program özelliklerinden olan "Veri Erişim Güvenliği ve Yedekleme İşlemleri" menüsü kullanılarak ortak klasör altında "ASPARK MÜŞTERİ LİSTELERİ" adlı bir klasör oluşturulmuştur. Bu ve benzeri oluşturulabilecek klasörlerin içerisine firmanın önem arz eden belgeleri kopyalanmış ve bu anlamda bilgi güvenliği sağlanmıştır.

Şekil 32: Aspark İşletmesi Yedekleme İşlemleri Görünümü

Şekil 33: Aspark İşletmesi Kullanıcıları ve Yedekleme Klasörleri Görünümü

Yukarıda yer alan Şekil 33'te görüldüğü gibi uygulamalı test çalışması esnasında işletme çalışanları ASPARK1 kullanıcı adı ile programa giriş yaptıklarında, program ana ekranında yer alan bütün menüleri kullanım yetkisine sahip olmuştur. Ayrıca "Yönetim" adlı ana klasör altında "Aspark Yönetim" adında oluşturdukları klasöre erişim sağlandığı da yine Şekil 33'te görülmektedir.

ASPARK2 kullanıcı adıyla giriş yaptıklarında ise tam yetkili kullanıcıdan farklı olarak program ana ekranının sol kısmında yer alan menülerden sadece 4 tanesi kullanılabilir durumdadır. Bu kullanıcının "Muhasebe" adlı ana klasör altında oluşturduğu "Aspark Muhasebe" klasörü firmaya ait belgeleri kayıt altına alarak yedekleyebileceği alanı ifade etmektedir.

Son olarak ASPARK3 kullanıcı adı ile giriş yapıldığında ise program ana ekranının sol kısmında bulunan fonksiyonlardan sadece 2 tanesi kullanılabilir durumdadır. Söz konusu kullanıcı kısıtlı yetkiye sahip olması sebebiyle "Raporlar" adlı genel klasöre erişim sağlayabilmekte ve bu alanda oluşturduğu "Aspark Belgeler" klasörü altına tüm önemli belgelerini kayıt altına alarak kullanabilmektedir.

4.2.Birinci Test Çalışması Sonucunda Tespit Edilen Eksiklikler

Programın test edildiği Aspark Gayrimenkul şirketi tarafından programda belirlenen eksiklikler şunlardır.

1. Program ana ekranının sol kısmında bulunan işletim sistemi yardımcı programlarının içerisinde Photo Shop veya Corel Draw gibi fotoğraf düzenlemeyi sağlayan herhangi bir program bulunmamaktadır. Ancak bu programlar işletmenin en çok kullanım ihtiyacı duyduğu programlardandır.
2. Programın web uygulamasının kullanılabilmesi için şirket web sayfasının tamamen yenilenmesi ve web sayfası ile program veritabanının ortak bir platformda buluşturulması gerekmektedir. Bu durum şirkete ek maliyet getirecektir.
3. Programa girişte kullanılan şifrelerde büyük / küçük harf duyarlılığı bulunmamaktadır.
4. Programın özelliklerinden olan dosya gezginindeki ortak alanda yer alan klasörler için herhangi bir erişim yetkisi talebi olduğunda, bu işlemi program içinden yapmak mümkün olmamaktadır. Söz konusu yetki sadece veritabanı üzerinden verilebilmektedir. Dolayısıyla bu durum ise programın yönetimini zorlaştırmaktadır.
5. Programın "Bilgi Güvenliği İhlalleri Yönetimi" menüsü üzerinden gönderilen mesajlar, tüm kullanıcıların ekranında otomatik olarak çıkmalıdır. Ancak buradan sadece tam yetkili kullanıcılar mesaj atabilmekte ve gönderilen mesajı da sadece bu yetki seviyesindeki kullanıcılar görebilmektedir. Bu durum programın tespit edilen en büyük eksikliğidir.

4.3. İkinci Test Çalışması

Program ikinci olarak Mersin ili Yenişehir ilçesinde yerleşik bulunan ve yaklaşık 30 yıldır mobilya perakendeciliği alanında Bellona Mobilya bayisi olarak faaliyet gösteren Boğaziçi Mobilya Limited Şirketinde test edilmiştir. 3 -7 Kasım 2017 tarihleri arasında 5 gün süresince gerçekleştirilen test çalışması esnasında program, işletmede bulunan 3 farklı bilgisayara kurulumu yapılmış ve şirket çalışanlarının kullanmaları sağlanmıştır.

Test çalışması süresince şirket çalışanlarının kullanımı için program üzerinde YÖNETİM, MUHASEBE ve SATIŞ adlarında üç kullanıcı tanımlanmıştır. Bu kullanıcılardan YÖNETİM, tam yetkili kullanıcı olarak, MUHASEBE standart yetkili kullanıcı olarak ve son olarak SATIŞ ise kısıtlı yetkili kullanıcı olarak tanımlanmıştır.

Aşağıda yer alan Şekil 34'te söz konusu işletmede yapılan test çalışması esnasında oluşturulan kullanıcılar görülmektedir.

Şekil 34: Programın Boğaziçi Mobilya İşletmesinde Uygulamalı Olarak Test Edilmesi

İşletme çalışanları tarafından programın kullanımı ve test edilmesi esnasında, programda yer alan bütün özellikler kullanılmıştır. İşletme Eset adlı anti-virüs uygulamasını kullanmaktadır ve programa bu uygulamanın yönetim ekranı yerleştirilerek "Anti-Virüs Uygulaması" menüsü altında firmanın kullanmakta olduğu Eset anti-virüs programı çalıştırılmıştır. Firmanın herhangi bir firewall uygulaması kullanmadığı tespit edilmiş ve sadece program ana sayfasında kısa yol olarak tanımlı olan windows firewall uygulamasını kullanmakta olduğu anlaşılmıştır.

Boğaziçi Mobilya firması sadece LKS muhasebe programı kullanmaktadır. Bunun dışında kullandığı başka bir program bulunmamaktadır. Bu sebeple programın "İşletme Uygulama Programları" menüsüne LKS muhasebe programı yerleştirilmiş ve bu menü üzerinden söz konusu muhasebe programına erişim yapmaları sağlanmıştır.

Firma çalışanları test çalışması boyunca en önemli firma bilgisinin kullanılmakta olan muhasebe programının veritabanı dosyası olduğunu ifade etmiş ve söz konusu dosyanın yedeklenmesi gerektiği belirtilmiştir. Bu talep üzerine programın "Veri Erişim Güvenliği ve Yedekleme İşlemleri" menüsü altında yer alan özellikler açıklanmış ve muhasebe programı veritabanının yedeklenmesi yapılmıştır.

Aşağıda yer alan Şekil 35'te firma çalışanları tarafından muhasebe programı LKS'nin yedeklenmesi görülmektedir.

Şekil 35: Boğaziçi Mobilya İşletmesi Yedekleme İşlemleri Görünümü

Bu işlem sonrasında firmanın en değerli belgesi olan LKS muhasebe programı veritabanı yedek dosyası oluşturulmuş ve muhasebe kayıtlarında veri kaybı yaşanması durumunda gerekli önlem alınmıştır.

İşletme yönetimi ve çalışanları tarafından programın kullanımının oldukça pratik olması sebebiyle olumlu geri bildirimler alınmıştır. Programın işletme bünyesinde kullanıma uygun olduğu ve başarılı bulunduğu ifade edilmiştir.

4.4. İkinci Test Çalışması Sonucunda Tespit Edilen Eksiklikler

Programın Boğaziçi Mobilya firmasında 5 gün süresince yapılan test çalışması sonucunda firma yöneticileri ve çalışanları tarafından aşağıdaki eksiklikler tespit edilmiş ve tarafımıza bildirilmiştir.

1. Programın ana sayfasında sol üst köşede yer alan kullanıcı ikonuna, programı kullanmakta olan kullanıcı tarafından istenilen herhangi bir resmin konulabilmesi için bir özellik bulunmamaktadır. Bu özelliğin eklenmesi programın görselliğini daha güzel bir hale getirebilir.

2. Firma internet bağlantılarında genellikle Google Chrome programını kullanmaktadır. Ancak program ana sayfasının sol tarafında bulunan yardımcı programlar arasında söz konusu program bulunmamaktadır.
3. Firma muhasebe programı üzerinden müşterileri için fatura, ödeme makbuzu ve sipariş formu gibi bazı çıktılar almak zorundadır. Ancak söz konusu formların her biri farklı özelliklerde yazdırılmaktadır. Bu yüzden çıktısı alınması planlanan formun formatına göre yazıcı ayarlarında değişiklik yapmak gerekmektedir. Ancak program ana sayfasında yardımcı programlar kısmında yazıcı ayarları için erişim bulunmamaktadır.
4. Firma programa bir müşteri takip özelliği eklenmesini talep etmiştir. Eklenecek bu fonksiyon ile firma müşterilerinin iletişim bilgileri ve fotoğraflarının programda kayıtlı olmasını ve böylelikle ismini hatırlamadıkları bir müşterilerini programda yer alacak olan fotoğraf ve diğer bilgilerinden kontrol ederek bilgi edinmelerinin sağlanması programdan en önemli talepleridir.
5. Programın el terminali tarzında bir bilişim aracı üzerinde mobil olarak çalıştırılmasının sağlanması firmanın bir diğer talebidir. Bunun sağlanması ile birlikte örneğin işletmenin 5. Katında müşterileri ile ilgilenmekte olan bir satış temsilcisinin soracağı herhangi bir konu hakkında telefona ihtiyaç duymadan program üzerinden mesaj atarak, yine program üzerinden cevap alması ve bu cevabı müşterilerine anında iletmesi firma açısından talep edilen bir diğer özellik olmuştur.

4.5. Üçüncü Test Çalışması

Program son olarak Mersin ili Yenişehir ilçesinde 16 yıldır bilgisayar satışı ve bilgisayar tamiri/bakımı alanında faaliyet göstermekte olan Aydın Bilgisayar işletmesinde 3 – 7 Kasım 2017 tarihleri arasında 5 gün boyunca test edilmiştir. Test süresi boyunca program, firmada bulunan 4 farklı bilgisayara kurulmuş ve firma çalışanları tarafından bütün özelliklerinin kullanılması sağlanmıştır.

Test çalışması boyunca firma çalışanlarının kullanması amacıyla program üzerinde, AB-Yönetici-1, AB-Yönetici-2, AB-Muhasebe ve AB-Destek adlı 4 farklı kullanıcı oluşturulmuştur. Oluşturulan bu kullanıcılardan AB-Yönetici-1 ve AB-Yönetici-2 adlı kullanıcılar tam yetkiye sahip bir kullanıcı tipi olarak, AB-Muhasebe adlı kullanıcı standart yetkiye sahip bir kullanıcı olarak ve son olarak AB-Destek adlı kullanıcı ise kısıtlı yetkiye sahip bir kullanıcı olarak oluşturulmuştur.

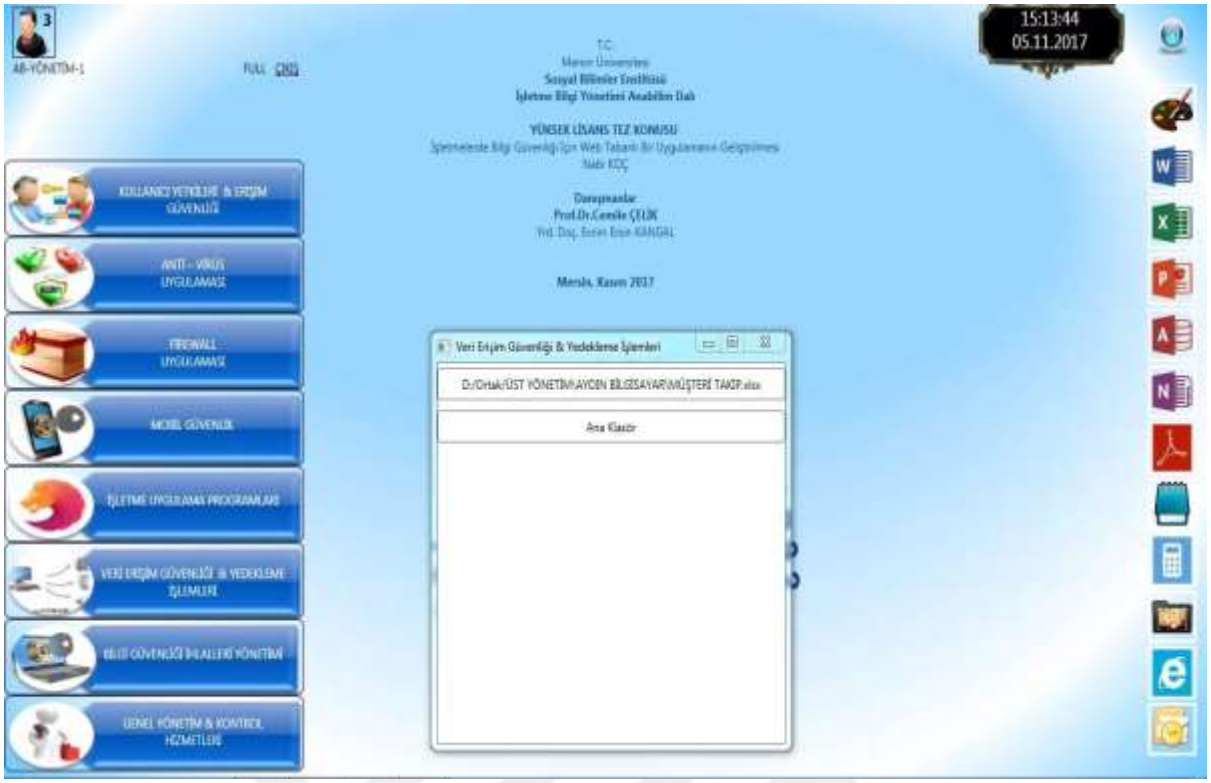
Aşağıda yer alan Şekil 36'da Aydın Bilgisayar firmasında yapılan test çalışması esnasında firma çalışanlarının kullanımları için program üzerinde oluşturulmuş olan kullanıcılar görülmektedir.

Şekil 36: Programın Aydın Bilgisayar İşletmesinde Uygulamalı OIarak Test Edilmesi

Programın test edilmesi aşamalarında tüm fonksiyonları firma yönetici ve çalışanları tarafından kullanılarak test edilmiştir. Firma anti-virüs uygulaması olarak Norton Anti-Virüs uygulamasını kullanmaktadır. Programda yer alan "Anti-Virüs Uygulaması" menüsüne söz konusu uygulama yerleştirilmiş ve personelin bu menü üzerinden uygulamaya erişimleri sağlanmıştır. Firma firewall uygulaması olarak ise Pfsense adındaki uygulamayı kullanmaktadır. Söz konusu firewall uygulaması programın "Firewall Uygulaması" menüsü altına yerleştirilmiş ve personelin kullanımına sunulmuştur.

Aydın Bilgisayar firması uygulama programı olarak sadece windows işletim sisteminde yer alan veya sonradan yüklenmiş olan bazı yardımcı uygulama programlarını kullanmaktadır. Ayrıca firma müşterilerini takip etmek amacıyla bir excel listesi kullandığını beyan etmiştir.

Test çalışması esnasında firma tarafından kullanılan söz konusu excel listesinin yedeklemesi gerçekleştirilmiştir. Aşağıda yer alan Şekil 37'de Aydın Bilgisayar firmasında yapılan dosya yedekleme çalışması görülmektedir.



Şekil 37: Aydın Bilgisayar İşletmesi Yedekleme Görünümü

Aydın Bilgisayar firmasında yapılan test çalışması esnasında firmanın müşteri bilgilerini tuttuğu excel listesi yukarıda yer alan Şekil 37'de görüldüğü üzere yedeklenerek bu anlamda firmanın bilgilerinin güvenliği sağlanmıştır.

Son olarak firma çalışanlarının kullanımı için program üzerinde oluşturulan 4 farklı kullanıcının, programı kullanmaları esnasında yaptıkları program giriş ekranı aşağıda yer alan Şekil 38'de görülmektedir.

Şekil 38: Aydın Bilgisayar İşletmesi Kullanıcılar Program Giriş Ekranı Görünümleri

Programın kullanımı sonrasında firma çalışanları tarafından özellikle görsel hali oldukça beğeni kazanmıştır. Programın toplam boyutunun 66 MB büyüklüğünde olması, taşınması ve başka bilgisayarlara kurulması sırasında büyük kolaylık sağlayacağı için ayrıca beğenilen bir başka özelliği olmuştur.

4.6. Üçüncü Test Çalışması Sonucunda Tespit Edilen Eksiklikler

Programın Aydın Bilgisayar firmasında 5 gün süresince test edilmesi sonucunda firma yöneticileri ve çalışanları tarafından tespit edilerek tarafımıza bildirilen eksiklikler ve talepler aşağıda maddeler halinde sunulmuştur.

1. Aydın Bilgisayar firması müşterilerine teknik destek sağlamak için Team Viewer, Alpemix ve windows uzak masa üstü bağlantısı gibi bir bilgisayardan başka bir bilgisayara ekran görüntüsü aktarılmasını ve bu yöntemle karşı taraftaki bilgisayara müdahale edilmesini sağlayan yardımcı programları kullanmaktadır. Ancak programın sol kısmında yer alan yardımcı programlar kısmında uzak masa üstü bağlantısı sağlayan herhangi bir uygulama bulunmamaktadır.

2. Programa bir özellik daha eklenerek müşteri takibinin yapılabileceği bir menü geliştirilebilir. Bu menü sadece müşterilerin iletişim bilgileri ile firmada yaptırdıkları işlemleri içerecektir.
3. Programda güncelleme özelliği bulunmamaktadır. Programın yeni bir sürümünün olması durumunda, tüm kullanıcıların tek tek dolaşılarak programın bir üst sürüme yükseltilmesi gerekecektir. Ancak program ana sayfasına bir güncelleme butonu konularak, yeni bir sürümün yayınlanması halinde, söz konusu güncelleme işleminin kullanıcının kendisi tarafından yapılması sağlanabilir.
4. Programın herhangi bir hata veya arıza sonucu çalışmadığı durumlarda, bilgisayar masa üstü görüntüleneceğinden kullanıcılar böyle durumlarda bilgisayarın bütün özelliklerini kullanabilir duruma gelebilirler. Bu senaryo göz önünde bulundurularak önlem alınmalıdır.
5. Programın herhangi bir hatadan dolayı hiç çalışmadığı ve eksik çalıştığı durumlar için program ana sayfasında bir resetleme veya yeniden yükleme butonu bulunmamaktadır. Söz konusu butonun konulması halinde problemle karşılaşan herhangi bir kullanıcı öncelikle programı yeniden çalıştırmayı deneyerek problemini hızlıca çözmeyi deneyebilir.
6. Program ana ekranının sol kısmında bulunan yardımcı programlar arasında yazıcı ayarlarının değiştirilebileceği özellik bulunmamaktadır. Söz konusu özellik tüm kullanıcılar tarafından sıklıkla kullanılmakta olduğu için program ana sayfasına eklenmelidir.

5. SONUÇLAR

Günümüzdeki teknolojik gelişmeler ve özellikle internetin tüm dünyada her geçen gün daha yaygın bir şekilde kullanılmaya başlanması sebebiyle, neredeyse bütün toplumlar birbirleri ile iletişim halindedir. Toplumlararası gerçekleşen bilgi transferleri, tüm dünya için bilgi güvenliğinin önemini her geçen gün artırmaktadır. Ülkemizde bilgi güvenliği alanında danışmanlık hizmeti vermekte olan firmaların verdiği istatistiğe göre işletmelerin % 87'si güvenlik riski taşımaktadır. Konunun uzmanı Gartner gibi otoritelerin yapmış oldukları araştırmalar sonucunda işletmelerin bilgi güvenliği alanında yapacakları harcamaların önümüzdeki yıl itibariyle 100 Milyar $ eşiğini aşacağı açıklanmıştır. Aynı şekilde son yıllarda yaşanan bilgi güvenliği ihlalleri sonucu oluşan maddi kayıpların miktarı da milyar dolarlar seviyesinde telaffuz edilmektedir (Gemci ve Bay, 2010: 198-202).

Bu noktada Türkiye'de Tübitak Ulakbim sistemi üzerinde, "bilgi güvenliği" anahtar kelimesi ile yapılan araştırmada çok fazla sayıda akademik yayın yapıldığı tespit edilmiştir. Bunun yanı sıra YÖK akademik arama motorunda yapılan araştırmada 416 adet yayın yapıldığı tespit edilmiş olup bu yayınların 71 adedinin tez çalışması olduğu görülmüştür. Söz konusu tezlerin taranması neticesinde bilgi güvenliğini sağlamaya yönelik yazılım tabanlı bir tez çalışmasına rastlanmamıştır. Ancak Kültür Üniversitesi Fen Bilimleri Enstitüsünde "Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi" adlı bir yüksek lisans tezi yürütülmüştür. Yürütülen bu tez çalışmasında, işletmelerin bilgi güvenliği gereksinimleri ele alınarak, kurumların bilgi güvenliği altyapısının sorgulanmasına yönelik bir test aracı geliştirilmiştir.

Bu tez çalışmasında, akademik alanda bilgi güvenliği konusunda yapılan araştırmalardan farklı olarak, bilgi güvenliğini sağlamaya yönelik bir program geliştirilmiş ve bu alanda riskleri en aza indirecek şekilde tasarlanarak hayata geçirilmiştir. Bu yönüyle çalışmanın akademik dünya için yenilikçi bir yaklaşım sergilediği düşünülmektedir. Çalışma ile işletmeler, bilgi güvenliğini sağlamaya yönelik önlemleri üst seviyede almış ve bu alandaki riskleri en aza indirmiş olacaktır. Böylece bu konuda yaşanabilecek ihlaller sonucu oluşabilecek maddi ve manevi zararların önlenmesine katkı sağlayacaktır.

Tez çalışması kapsamında geliştirilen program iki aşamalı olarak tasarlanmıştır. Birinci aşamada, işletme içinde bulunan personellerin kullanımı için C Sharp programlama dili kullanılarak ve Microsoft Windows işletim sistemi üzerinde çalışan ana program geliştirilmiştir. İkinci aşamada ise gerek iş görüşmesi, toplantı, iş seyahati gibi nedenlerden dolayı işletme dışında bulunacak olan personelin internet üzerinden, gerekse işletme içindeki personelin yerel ağ üzerinden program veritabanına erişip, programla ilgili yetki taleplerini değerlendirme ve karşılamaya olanak sağlayan bir web uygulaması geliştirilmiştir.

Bilgi güvenliğini sağlamaya yönelik olması nedeniyle programın geliştirilmesindeki amaçlardan biri, programın çalıştırılması ile birlikte, kullanıcının, program üzerinde kendisine tanımlanmış yetkileri dışında, bilgisayar üzerinden herhangi bir güvenlik açığına sebebiyet vermesinin önlenmesi amacıyla bilgisayar ekranını kaplaması ve bu yolla kullanıcılara bazı kısıtlamalar getirmesidir. Ayrıca programa giriş aşamasında yasal yükümlülüklerin yerine getirilmesi bağlamında, güvenlik önlemlerinin yer aldığı 20 maddelik bilgilendirme formu onaya sunulmuştur.

Bilgi güvenliği denilince akla ilk gelen güvenlik mekanizmaları olan anti-virüs ve güvenlik duvarı (firewall) uygulamaları iki farklı menü olarak programda yer almaktadır. Program kullanıcıları, söz konusu güvenlik programlarının bütün fonksiyonlarını program üzerinden kullanabilmektedir. Buna ilave olarak programda yer alan bir diğer menü olan "İşletme Uygulama Programları" menüsü altında personelin işi gereği ihtiyaç duyup kullanmak isteyebileceği personel iletişim, toplantı takip, müşteri yönetimi, muhasebe ve personel kontrol gibi yardımcı yazılımlar yer almaktadır. Programa söz konusu menünün eklenmesindeki amaç, kullanıcıların program ekranında yer alan özellikler dışında başka bir fonksiyona ihtiyaç duymalarının önüne geçmek ve böylelikle tüm işlemlerin program üzerinden yapılmasını sağlayarak olası bir güvenlik ihlaline engel olmaktır.

Geliştirilen bu program, işletme için *en kritik öneme sahip bilgileri,* tüm kullanıcıların ulaşabilmesine sınırlandırma getirerek, sadece yetkili kişilerin, belirlenen yetki çerçevesinde erişmelerine izin vermektedir. Program içerisinde oluşturulabilen "tam yetkili" veya "kısıtlı yetkili" gibi değişik seviyelerdeki kullanıcı tipleri ile hangi kullanıcının hangi bilgilere ulaşabileceği net olarak belirlenmektedir. Bu özelliği ile program, en temel güvenlik fonksiyonunu yerine getirmekte ve bu özellik programın en önemli işlevi olarak değerlendirilmektedir.

Programda yer alan "Veri Erişim Güvenliği ve Yedekleme İşlemleri" menüsü, işletmenin sahip olduğu verilere erişimin güvenli bir şekilde sağlamasının yanı sıra kullanıcıların tüm önemli veri dosyalarını, programın yöneticisi tarafından belirlenen ortak bir klasörde yedeklenmesine olanak sağlamaktadır. Buna bağlı olarak programın Windows işletim sisteminin dosya gezgini özelliğine benzeyen bir fonksiyonu bulunmakta ve bu fonksiyon ile kullanıcılar sadece yetkili oldukları klasör ve dosyalara erişebilmektedir. Bu özellik; kullanıcı hataları veya personelin yanlış işlemleri sonucu oluşabilecek veri kayıplarını önlemeyi amaçlamaktadır.

Program menülerinden birisi olan "İşletme Uygulama Programları" menüsünün içeriğinde beş adet yardımcı yazılım bulunmaktadır. Bu sayı işletmenin ihtiyacına göre opsiyonel olarak talep edilen miktarda artırılabilir. Ayrıca programa giriş yaptıktan sonra

program ana ekranının sol üst köşesinde yer alan kullanıcı ikonuna gerçek kullanıcı resimleri yerleştirilerek, programın daha güzel bir görsele sahip olması sağlanabilir.

Son olarak program, üzerinde yer alan mesaj paneli ile herhangi bir kullanıcının bilgi güvenliği ihlali ile karşılaşması durumunda, bunu en hızlı şekilde bilgi güvenliği yöneticisine bildirmesine olanak sağlamaktadır. Böylelikle karşılaşılan bilgi güvenliği tehdit ve ihlallerine karşı alınacak önlemlerin en hızlı şekilde uygulanmasına fırsat vermektedir. Bu özelliği de programın önemli işlevlerinden birisidir.

Program 3 farklı işletme ortamında her işletmede birden fazla bilgisayara kurulumu yapılarak, 5'er gün süresince işletme çalışanları tarafından kullanılarak test edilmiştir. Bu test çalışmaları sonucunda şirket çalışanları tarafından programın kullanım kolaylığı sağladığı yönünde olumlu görüşler alınmakla birlikte, programda tespit edilen bazı eksiklikler de ayrıca maddeler halinde bildirilmiştir. Tespit edilen bu eksiklikler tarafımızdan değerlendirilmiş ve programın bir üst sürümünde giderilmesini yönünde gerekli çalışmanın yapılmasına karar verilmiştir.

ÖNERİLER:

1. Programa işletme yerel ağı üzerinde yer alan bir terminal sunucu üzerinde çalıştırılarak, işletme içinden veya işletme dışından interaktif olarak söz konusu terminal sunucuya bağlantı sağlanarak erişilebilir ve böylelikle program her noktadan kullanıma hazır hale getirilebilir.
2. Programa giriş esnasında kullanılan şifrelerin, günümüzde birçok kurum tarafından kullanılan ve bu alanda üst seviyede güvenlik sağlayan "*elektronik şifrematik*" sistemi üzerinden alınması sağlanarak, bu konuda güvenlik önlemleri daha ileri bir seviyeye taşınabilir. Ayrıca bu sayede şifrelerin kayıp edilmesi, unutulması veya başkasının eline geçmesi gibi olumsuz durumların yaşanması da engellenmiş olacaktır.
3. Program içerisinde yer alan ve kullanıcıların üzerinde çalıştıkları belgelerin kayıt altına alındığı ortak klasörde yer alan bütün dosyaların, belirlenecek zaman aralıklarında program tarafından otomatik olarak anti-virüs taramasından geçirilerek, söz konusu dosyalara virüs ve benzeri zararlı yazılımların bulaşmasının ve dosyaların zarar görmesinin önüne geçilebilir.
4. Program kullanıcılarının tüm dosyalarını kayıt altına aldıkları ortak klasörün, program tarafından başka bir fiziksel kayıt ortamına yedeklenmesi sağlanarak, iki aşamalı yedekleme sistemi kurabilir ve bu şekilde ortak klasörün bulunduğu kayıt diskinin arızalanması gibi durumlarda karşılaşılabilecek veri kayıpları engellenebilir.
5. Program ana ekranının sol kısmında yer alan işletme yardımcı programları alanı dinamik bir yapıya kavuşturulabilir. Böylelikle kullanıcı ihtiyaç duyduğu yardımcı programları kendisi seçip ekranına taşıyarak kullanabilir.

6. Test çalışmasının yapıldığı işletmelerin çalışanları tarafından bildirilen eksikliklerin tamamı giderilerek, program bir üst sürüme yükseltilebilir.

KAYNAKLAR

[1]. Akçakaya, V. (2006). *Eğitimciler için yeni bir web aracı*. Yayımlanmamış yüksek lisans tezi, Balıkesir Üniversitesi, Balıkesir.

[2]. Aktaş, F. (2013). *Hastane otomasyon projesi.* Yayımlanmamış yüksek lisans tezi, Dumlupınar Üniversitesi, Kütahya.

[3]. Altıntaş, V. (2016). *Veri tabanı yönetim sistemleri*. Akademik Veritabanları Eğitimi Seminerinde sunulan bildiri. Celal Bayar Üniversitesi, Manisa.

[4]. Atılgan, D. (2009). Bilgi yönetimi kavramı ve gelişimi: Görüşler*. Türk Kütüphaneciliği, 23*, 201-212.

[5]. Aydoğmuş, E. (2010). *Assessment of information security maturity levels and ISO/IEC 27001:2005 compliance of organizations in Turkey*. Yayımlanmış yüksek lisans tezi, İstanbul Teknik Üniversitesi, İstanbul.

[6]. Bandyopadhyay, T. (2006). M*itigation and transfer of information security risk: Investments in financial instruments and technology*. Yayımlanmamış doktora tezi, Teksas Üniversitesi, ABD.

[7]. Baykara, M. Daş, R. ve Karadoğan, İ. (2013). *Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi.* 1. International Symposium on Digital Forensics and Security (ISDFS'13) sempozyumunda sunulan bildiri. Fırat Üniversitesi, Elazığ ve Sütçü İmam Üniversitesi, Kahramanmaraş.

[8]. Bensghir, K. T. (1996). Bilişim teknolojileri ve örgütsel değişim. *Türkiye ve Ortadoğu Amme İdaresi Enstitüsü*, *1(274)*, 10-17.

[9]. Bingöl, U. (2010). *ISO 27001 bilgi güvenliği yönetim sistemi otomasyonu*. Yayımlanmış yüksek lisans tezi, Sakarya Üniversitesi, Sakarya.

[10]. Canbek, G. ve Sağıroğlu, Ş. (2006). *Kötücül ve casus yazılımlar: Kapsamlı bir araştırma.* Ankara: Gazi Üniversitesi Bilimsel Araştırmalar Merkezi.

[11]. Canbek, G. ve Sağıroğlu, Ş. (2006). Bilgi, bilgi güvenliği ve süreçleri üzerine bir inceleme. *Politeknik Dergisi*, 9(3), 165-174.

[12]. Chang, S. E. and Lin C. S. (2007). Exploring organisational security culture for information security management. *Industrial Management & Data Systems, 3(107)*, 438– 458.

[13]. Chang-Lung, T. Uei-Chin, L. Allen, Y. C. and Chun-Jung, C. (2012). Information security issue of enterprises adopting the application of cloud computing. *National Science Magazine*, 3, 645-649.

[14]. Çağtürk, A. T. (2006). B*ilgi toplumuna dönüşüm sürecinde e-yaşam olanakları ve e-devletin gerekliliği üzerine bir araştırma.* Yayınlanmamış yüksek lisans tezi, Onsekiz Mart Üniversitesi, Çanakkale.

[15]. Çayırlı, M. ve Aslantaş, A. (2005). *Microsoft .net vizyonunun incelenmesi ve bilgisayar teknolojisi ve programlama eğitimi ile entegrasyonu için bir rehber çalışması*. Isparta: Süleyman Demirel Üniversitesi Keçiborlu Meslek Yüksek Okulu.

[16]. Çelikhol, S. (2015). Aristoteles'te etik göreciliğin eleştirisi. *Erzincan Üniversitesi Sosyal Bilimler Enstitüsü Dergisi (ERZSOSDER)*, 1, 161-162.

[17]. Çetin, H. (2010). İşletme bilgi güvenliği yönetim sistemleri. *Göller Bölgesi Aylık Hakemli Ekonomi ve Kültür Dergisi,* 41-46.

[18]. Çetinkaya, M. (2008). Bilgi güvenliği yönetim sistemi altyapısının değerlendirilmesi için bir test aracı geliştirilmesi. Yayımlanmış yüksek lisans tezi, İstanbul Kültür Üniversitesi, İstanbul.

[19]. Claunch, D. and McMillan, M. (2013). Determining the right level for your IT security investment. *Healthcare Financial Management, 5*, 100-103.

[20]. Çoban, H. (1997). *Bilgi toplumuna planlı geçiş: gelecekten kaçılamaz, bilgi toplumuna planlı geçiş için stratejik planlama ve yönetim bilgi sistemi uygulanması*. İstanbul: İnkılap Kitabevi.

[21]. Demirol, D. Daş, R. ve Baykara, M. (2013). *Sql enjeksiyon saldırı uygulaması ve güvenlik önerileri.* 1. International Symposium on Digital Forensics and Security (ISDFS'13) sempozyumunda sunulan bildiri. Fırat Üniversitesi, Elazığ.

[22]. Erkan, A. (2006). An automated tool for information security management system. Yayımlanmış yüksek lisans tezi, Orta Doğu Teknik Üniversitesi, Ankara.

[23]. Erol, O. Şahin, Y. L. Yılmaz, E. ve Haseski, H. İ. (2015). Kişisel siber güvenliği sağlama ölçeği geliştirme çalışması. *International Journal of Human Scienses*, 12,2.

[24]. Fussell, R. S. (2005). Protecting information security availability via self-adapting intelligent agents. Military Communications Conference sunulan bildiri. IEEE, 2977S.

[25]. Gartner Inc. Stamford, ABD, (2016). *Gartner reveals top predictions for it organizations and users in 2017 and beyond.* Gartner Symposium/ITxpo. 10 Ekim 2017 tarihinde http://www.gartner.com/technology/research.jsp adresinden alınmıştır.

[26]. Gemci, C. ve Bay, Ö. F. (2010). Yapay zeka temelli bilgi güvenliği yönetim sistemi yaklaşımı. *Gazi Üniversitesi Bilişim Enstitüsü*, *2,* 198-202.

[27]. Gülmüş, M. (2010). K*urumsal bilgi güvenliği yönetim sistemleri ve güvenliği.* Yayımlanmamış yüksek lisans tezi, Yıldız Teknik Üniversitesi, İstanbul.

[28]. ISO Belgesi, (2017). B*ilgi güvenliği genel kurallar ve yasal yükümlülükler.* 11 Ekim 2017 tarihinde www.iso-belgesi.net adresinden alınmıştır.

[29]. Johnson, M. E. and Goetz E. (2007). Embedding information security into the organization. *IEEE Security & Privacy, 3*, 5.

[30]. Kahraman, S. (2010). Y*önetimde bilgi güvenlik sisteminin yapısı işleyişi ve Aselsan A.Ş.'de uygulaması.* Yayımlanmamış yüksek lisans tezi, Anadolu Üniversitesi, Eskişehir.

[31]. Kandemirli, B. M. (2007). *Bilgi teknolojileri güvenliği ve sigorta şirketlerinde ISO/IEC 27001 standartları çerçevesinde bilgi güvenlik yönetim sistemi uygulaması*. Yayımlanmış yüksek lisans tezi, Yıldız Teknik Üniversitesi, İstanbul.

[32]. Keser, H. ve Güldüren, C. (2014). Bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Kastamonu Üniversitesi, Kastamonu Eğitim Dergisi, 23(3),* 1167-1184.

[33]. Kılıç, Ç. M. ve Göçgöl, O. (2010). T*ürkiye'deki işletmelerin bilgi güvenliği yönetim sistemi alt yapısının değerlendirilmesi.* İstanbul: Bahçeşehir Üniversitesi Mühendislik Fakültesi Araştırma Projesi Yayını.

[34]. Mete, H. (2010). ISO/IEC 27001 Bilgi güvenliği yönetim sisteminin bilgi işlem merkezlerinde uygulaması. Yayımlanmış yüksek lisans tezi, Sakarya Üniversitesi, Sakarya.

[35]. Pfleeger, C. P. (1997). The fundamentals of information security. Software and IEEE, 14, 1-14.

[36]. Shegai, I. (2003). Some aspects of information security problems. *The IEEE Siberian Conference on Control and Communications (SIBCON-2003)*. Tomsk.

[37]. Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. Information Management & Computer Security, *1(8),* 31-41.

[38]. Solms, V. B. (2000). Information security – the fourth wave. *Computers & Security 25*, 165-168.

[39]. Süzen, A. A. ve Taşdelen, K. (2013). Kinect teknolojisi kullanılarak engelliler için ev otomasyonu. *SDU International Technologie Science – Computer Technologies, 2(5),* 122-131.

[40]. Şahinaslan, Ö. (2013). S*iber saldırılara karşı kurumsal ağlarda oluşan güvenlik sorunu ve çözümü üzerine bir çalışma.* Yayımlanmamış doktora tezi, Trakya Üniversitesi, Edirne.

[41]. Şentürk, H. Çil, C. Z. ve Sağıroğlu Ş. (2016). Siber güvenlik yatırım kararları üzerine literatür incelemesi. *Politeknik Dergisi*, *19(1),* 39-51.

[42]. Şentürk, H. Çil, C. Z. ve Sağıroğlu, Ş. (2014). S*iber güvenlik ekonomisi üzerine literatür incelemesi,* 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansında sunulan bildiri. İstanbul.

[43]. The Institute of Internal Auditors, (2006). I*nformation technology control.* IAA GTAG, Florida.

[44]. Thomson, K. L. Solms, R, V. and Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security*, *10*, 7-11.

[45]. Tosun, Ö. N. ve Özdamar, S. (2015). O*nline alışveriş web sitesi*. Yayımlanmamış yüksek lisans tezi, İstanbul Kültür Üniversitesi, İstanbul.

[46]. TS GUIDE 13268-2, (2006), *TS ISO/IEC 27001'e göre bilgi güvenliği yönetim sistemi (BGYS) gerçekleştirmeler*. Türk Standartları Enstitüsü, Ankara.

[47]. TSE-TS ISO/IEC 17799, (2002). *Bilgi teknolojisi-bilgi güvenliği yönetimi için uygulama prensipleri.* Türk Standartları Enstitüsü, Ankara.

[48]. TS ISO/IEC 27001, (2006). B*ilgi teknolojisi – güvenlik teknikleri – bilgi güvenliği yönetim sistemleri: Gereksinimler*. Türk Standartları Enstitüsü, Ankara.

[49]. Uçak, N. Ö. (2010). Bilgi: Çok yüzlü bir kavram. *Türk Kütüphaneciliği Hakemli Yazılar*, *4(24),* 705-722.

[50]. Vural, Y. ve Sağıroğlu Ş., (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi*, *23(2),* 507-522.

[51]. Vural, Y. (2007). *Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri.* Yayımlanmamış yüksek lisans tezi, Gazi Üniversitesi, Ankara.

[52]. Yıldırımer, Ş. (2013). İbn sînâ ve Descartes'ın bilgi anlayışları bakımından karşılaştırılması. *Çanakkale Onsekiz Mart Üniversitesi İlahiyat Fakültesi Dergisi*, *2(22),* 97 - 129.

[53]. Yıldız, B. (2007). B*ilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetim standartlarının uygulanması*. Yayımlanmış yüksek lisans tezi, Gebze Yüksek Teknoloji Enstitüsü, Gebze.

[54]. Yumrutaş, H. İ. (2014). Coğrafi bilgi sistemi tabanlı kentsel altyapı yönetim sistemi yazılımı tasarımı. *El-Cezeri Fen ve Mühendislik Dergisi, 1(2),* 38-46.

[55]. Zachariah, J. S. (2010). A*n investigation of organizational information security risk analysis*. Yayımlanmamış doktora tezi, Auburn Üniversitesi, ABD.

ÖZGEÇMİŞ

Adı Soyadı **:** Nabi KOÇ

E-posta **:** nabikoc@gmail.com

Öğrenim Durumu **:** Lisans

DERECE	BÖLÜM / PROGRAM	ÜNİVERSİTE	YIL
Ön Lisans	Bilgisayar Programcılığı	Ege Üniversitesi	1997-1999
Lisans	İktisat	Anadolu Üniversitesi	2001-2006
Yüksek Lisans	İşletme Bilgi Yönetimi	Mersin Üniversitesi	Halen
Doktora			