İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL GÜVENLİK İNCELEMESİ VE BİR ÇÖZÜM ÖNERİSİ

YÜKSEK LİSANS TEZİ

Ayşe Bilge İnce

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Haziran 2016

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

KURUMSAL GÜVENLİK İNCELEMESİ VE BİR ÇÖZÜM ÖNERİSİ

YÜKSEK LİSANS TEZİ

Ayşe Bilge İnce
(504121509)

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Doç. Dr. Berk Canberk
Eş Danışman: Prof. Dr. Eşref Adalı

Haziran 2016

İTÜ, Fen Bilimleri Enstitüsü'nün 504121509 numaralı Yüksek Lisans / Doktora Öğrencisi Ayşe Bilge İnce, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "Kurumsal Güvenlik İncelemesi ve Bir Çözüm Önerisi" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Berk Canberk** İstanbul Teknik Üniversitesi	.....
Eş Danışman :	**Prof.Dr. Eşref Adalı** İstanbul Teknik Üniversitesi	.....
Jüri Üyeleri :	**Yard. Doç. Dr. A. Cüneyd Tantuğ** Yıldız Teknik Üniversitesi	.....
	Prof. Dr. İbrahim Soğukpınar Gebze Teknik Üniversitesi	.....

Teslim Tarihi : 02 Mayıs 2016
Savunma Tarihi : 23 Haziran 2016

Tüm aileme,

ÖNSÖZ

Tez boyunca bana destek olan hocalarım Prof. Dr. Eşref Adalı ve Doç.Dr. Berk Canberk'e, her problemde bana elinden gelen tüm desteği veren eşim Mehmet Dursun İnce'ye ve her çıkmaza girdiğimde yanımda olup, beni rahatlatan aileme ve arkadaşlarıma çok teşekkür ederim.

Haziran 2016

Ayşe Bilge İnce
Araştırma Görevlisi

İÇİNDEKİLER

Sayfa

KISALTMALAR

BG : Bilgi Güvenliği
İS : İçeriden Saldırı
IP : İnternet Protokolü
BGS : Baş Gizlilik Sorumlusu
BT : Bilgi Teknolojileri
İST : İçeriden Saldırı Tespiti
HDBS : Hizmet Dışı Bırakma Saldırısı
EVA : Elektronik Veri Aktarımı
SDAGE : Sistem Yöneticisi, Denetim, Ağ, Güvenlik Enstitüsü
DB : Doğrusal Bağlanım
DYM : Destek Yöney Makinesi
TSDYM : Tek-Sınıflı Destek Yöney Makinesi
DHDBS : Dağıtık Hizmet Dışı Bırakma Saldırısı
Tİ : Tek İmza
STS : Saldırı Tespit Sistemi
SÖS : Saldırı Önleme Sistemi

TÜRKÇELEŞTİRİLMİŞ KISALTMALAR

BG : IS
İS : ITh
IP : IP
BGS : CPO
BT : IT
İST : ITD
HDBS : DOS
EVA : EDI
SDAGE : SANS
DB : LR
DYM : SVM
TSDYM : OCSVM
DHDBS : DDOS
Tİ : SSO
STS : IDS
SÖS : IPS

TÜRKÇELEŞTİRİLMİŞ TERİMLER

Gizlilik	**:** Confidentiality
Bütünlük	**:** Integrity
Erişebilirlik	**:** Availability
İçeriden Saldırı Tespiti	**:** Insider Threat Detection
Baş Gizlilik Sorumlusu	**:** Chief Privacy Officer
Eylem Tutanağı	**:** Log
Üst Bilgi	**:** Metadata
Bilişim Uzayında Saldırı	**:** Cybercrime
Bilişim Uzayında Savaş	**:** Cyberwarfare
Yanlış Olumlu Oranı	**:** False Positive Rate
Hizmet Dışı Bırakma Saldırısı	**:** Denial of Service
Elektronik Veri Aktarımı	**:** Electronic Data Interchange
Sistem Yöneticisi, Denetim, Ağ, Güvenlik Enst.	**:** SysAdmin, Audit, Network Security Institute
Deneme Yanılma Saldırısı	**:** Intrusion Detection Sys.
Doğrusal Bağlanım	**:** Brute-Force Attack
Destek Yöney Makinesi	**:** Support Vector Machine
Tek-Sınıflı Destek Yöney Makinesi	**:** One-Class Support Vector Machine
Dağıtık Hizmet Dışı Bırakma Saldırısı	**:** Distributed Denial of Service
Tek İmza	**:** Single Sign-on
Saldırı Tespit Sistemi	**:** Intrusion Detection Sys.
Saldırı Önleme Sistemi	**:** Intrusion Prevention Sys.
Bal Küpü	**:** Honeypot
Güvenlik Duvarı	**:** Firewall

ÇİZELGE LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

KURUMSAL GÜVENLİK İNCELEMESİ VE BİR ÇÖZÜM ÖNERİSİ

ÖZET

Bilgi ve bilgisayar güvenliğini iki ortam için farklı düşünmek gerekir; Bireysel kullanım amaçlı bir bilgisayarın güvenliği söz konusu olduğunda, bilgisayara girme ve bu bilgisayarda bulunan veriler üzerinde işlem yapabilme akla gelmektedir. Kurumsal bilgi sisteminin güvenliği söz konusu olduğunda, çok sayıda bilgisayardan oluşan bir yapının güvenliği düşünülmelidir. Bilgisayar sayısının çokluğu ve bunların birbirine yerel bilgisayar ağı (YBA) ile bağlı olmaları; YBA üzerinde başka donanımların bulunması, kurumsal bilgi sisteminin güvenliğini karmaşık hale sokmaktadır.

Kurumların koruması gereken varlıkları, verileri, kaynakları ve özellikle de saygınlıklarıdır. Özellikle toplumda saygın konumu olan üniversiteler, bankalar ve kamu kuruluşlarının birinde olabilecek bir güvenlik açığı, bu kuruluşa olan güveni çok sarsar. Örneğin, İnternet bankacılığındaki bir güvenlik açığının toplum tarafından öğrenilmesi, müşterilerin o bankadaki hesaplarını kapatmasına neden olabilir. Ya da İTÜ gibi saygınlığı ön planda tutan ve tutması da gereken bir kurumun sistemindeki bir güvenlik açığının kullanılıp veri çalınması, okulun itibarını yerle bir edecek ve okula duyulan güveni de sarsacaktır. Bugün Türkiye'de hala üniversiteler için belirlenmiş zorunlu bir güvenlik politikası bulunmamaktadır, ancak önümüzdeki dönemlerde bu standartların belirlenmesi kaçınılmaz olacaktır.

Bir kurumun güvenlik politikası belirlenmeye karar verildiğinde, incelemeye, ilk olarak kurum içi bilgi sisteminin yapısını tanımayla başlanmalıdır. Kurum içi bilgi sistemlerine zaman içinde sürekli eklemeler yapıldığı için, donanımların görev ve işlevleri unutulabilmektedir. Bu nedenle, sistem içindeki tüm donanımların ve yazılımların konumları ve işlevleri ortaya konmalıdır. Bu öğrenme aşamasının ardından, bilgi güvenliğini artıracak birimler konusunda çalışmalar yapılmalıdır.

Bu bağlamda, tezde İTÜ Otomasyon Sistemi için incelemeler yapılmış ve bu incelemeler sonucunda, muhtemel güvenlik açıklıklarının olabileceği yerler saptanmaya çalışılmış, ileride güvenlik sorunu yaşanmaması için alınması gereken önlemler yöneticiye bildirilmiştir. Sistemde güvenlik açıklığı olup olmadığı temel güvenlik sorgulama çalışmalarıyla ve sınayarak ortaya çıkarılmıştır. Bu önlemler ve standartların belirlenmesi aşamasında ISO 27001 politikalarından ve 27002 yönergelerinden yararlanılmıştır.

Yukarıda anlatılanlar dış kullanıcılardan kaynaklanan sorunlardır, ancak bilgi güvenliği sistemlerinin genel özelliklerinden bilindiği üzere iç kullanıcılardan kaynaklanan sorunlar da yaşanabilmektedir. Tezin amacı hem iç hem de dış kullanıcıların sebep olacağı güvenliği bozucu davranışların ortaya çıkarılmasıdır. Bu yüzden, ikinci aşamada Otomasyon Sistemleri için öğrencinin notlarının girişi, notların değişmesi durumunda düzeltimi ve mezuniyet durumu gibi oldukça hassas durumlar incelenmiştir. Bu gibi durumların dikkate alınmaması en hafif hali ile

haketmediği notu alan öğrencilerin bulunması ve en ağır hali ile de belki de okula hiç kayıt olmamış öğrencilerin mezun olması ile sonuçlanacaktır.

Bu problemlerin yaşanmadığı hiç yaşanmayacağı anlamına gelmediği için öncesi yaşanabilecek güvenlik problemlerini en aza indirmek amacıyla Not Girişi, Not Düzeltimi ve Mezuniyet Durumu Kontrolünü güvenli hale getirebilmek amacıyla bir sistem önerilmiştir. Sisteme göre öğretim üyesi not girişini masa üstü bir uygulama üzerinden internete bağlı olmaksızın gerçekleştirecek ve sonrasında bunun EVA (Elektronik Veri Aktarımı) ya da XML formatında hem kendisi için bir kopyasını saklayacak hem de kendi fakültesinin veri tabanına gönderecek ve buradan da şifreli bir haberleşme ile Öğrenci İşleri veri tabanı ile paylaşılacaktır. Not Düzeltimi içinse bu işlem bir karar yazışması ile birlikte gerçekleştirilir. Bu yüzden not düzeltme işlemini gerçekleştiren öğretim üyesi not belgesini EVA ya da XML formatında fakülteye gönderir. Fakülte önce not değişimi için gelen yazışmayı kendi yazışma veri tabanına kaydeder, not belgesini de not için oluşturulmuş olan veri tabanına kaydedip, sonrasında not belgesini ve yazışmayı şifreleyerek öğrenci işleri ile arasında kurulan güvenli bağlantı aracılığıyla öğrenci işlerine gönderir. Öğrenci işlerinde yazışma delil olması için yazışma veri tabanına, not belgesi de öğrenci veri tabanına kaydedilecektir. Öğrencinin mezuniyet durumunda ise, hem fakülte veri tabanındaki hem de öğrenci veri tabanındaki notlar karşılaştırılır ve eğer ikisi birbirinin aynısı ise, "öğrenci mezun olabilir" bilgisi verilir. Eğer farklılıklara rastlanırsa, "öğrenci mezun olamaz" bilgisi döner ve bu aşamada farklılık sorgulaması işlemleri başlatılır. Not düzeltme yazıları da elektronik belge haline getirileceği için yapılan tüm not değişikliklerinin de bir resmi tutanağı üretilmiş olacaktır. Bu tutanak hem fakültede hem de öğrenci otomasyon sisteminde tutulacağı için de bir araştırma sırasında karşılaştırma olanağına sahip olunacaktır.

Son aşamaya gelindiğinde eylem tutanakları üzerinde çalışıldı ve Otomasyon Sistemine karşı gerçekleştirilecek içeriden tehditleri tespit edecek bir karar destek yazılımı geliştirilmiştir. Karar destek yazılımını oluşturabilmek için bir kural listesi hazırlanmıştır.

Tez 5 ana bölümden oluşmaktadır: Giriş bölümü ile çalışılan konu ve çevresel faktörleri genel detayları ile anlatılması amaçlanmıştır. Bir sonraki bölümde Kurumsal Güvenlik kavramı üzerinde durulmuştur. 3. bölümde güvenlik açıklıklarının araştırması yapılmıştır. Daha güvenli sistem oluşturmak için önerilerde bulunulmuştur. 4. bölümde yetkili kişilerin davranışlarından kalkılarak sınıflandırmaları, her sınıfı karakterize eden özelliklerin ortaya çıkarılması, bunun sonucu olarak da aykırı davranışta bulunanların saptanması yapılmıştır. Ortaya çıkan sonuçlara bakarak yetkilendirmelerin nasıl yapılması konusunda bir öneri listesi oluşturulmuştur. Bu aykırı davranış biçimlerinin bulunması için eylem tutanaklarından yararlanılarak aykırı davranışları ortaya çıkaran bir karar destek yazılımı geliştirilmiştir. Bu geliştirilen yazılım İTÜ Otomasyon Sisteminin kullanması için verilmiştir. Son olarak da Sonuç ve Öneriler kısmı yer almaktadır.

ENTERPRISE SECURITY ANALYSIS AND A SOLUTION PROPOSAL

SUMMARY

Over the past half a century, organizations have implemented information systems for managing their business processes. These information systems have now evolved into as commonly known as enterprise information systems. Computer and Information Security are needed to think in a different way for two circumstances. When personel computers' security is concerned; access to computer and can operate on data on this computer comes to mind. On the other hand, when security of enterprise information system comes to mind, a structure which consist of lots of computers, should be concerned. Enterprise networks, today carry a range of mission critical communications. The sheer number of computers to be connected to each other with local computer network; the presence of other hardwares on it, makes complicate the security of enterprise information systems.

Enterprise information security architecture is a key component of information security processes. Organizations amass a great deal of confidential information about their employees and users. Most of this information is now collected, processed and stored in an online warehouses and transmitted across networks to other online devices. Organizations should protect their datas, sources and especially their reputation. When a vulnerability found in system and some confidential datas are leaked by a black hat hackers from this kind of organizations which has respected positions in society like universities, banks and public institutions, is undermine the confidense in these organizations. It will be a massive damage for any organizations who faced with these problems. For instance, when society learns a vulnerability show up in internet banking application, sooner or later it will cause customers cancel their accounts in bank. Or, if a hacker found a vulnerability and theft datas and leaked from the systems an institution like İTÜ, will bring down the reputation of the school and will also undermine the confidense of the school in the eyes of public. Today, there is still no mandatory security policy for universities in Turkey, but it would be unevitable in the coming period. Because, managing the security of enterprise information systems has become a critical issue in this century. Hacktivism and cyber warefares are spreading all over the world. One day, if one of the universities officers computer turns out to be used as a zombie computer for an attack to an organization; it would be a big scandal not only for public citizens, but also for all country. To illustrate of this, it is obviously known that all officers are admin on their computers and some days their children plays games on these computers, especially flash games. And most of these games carried malwares, flash games are the most common one. When user starts and play the game, malware locate itself sneaky in operating system and some of them transform computer as a zombie to use future attacks, some of them taking videos of desktop and stores all

key actions of users. In a nutshell, for all these reasons, universities should have standard security policy and they should comply with all specifications, carefully.

Security can not be managed, unless it can be measured. The need for metrics is important for assessing the current security status, to develop operational best practices. To develop an organization's security policy, the review should be made and it should be started firstly with the diagnosis of in-house information systems to find metrics. Because of the fact that, there is continuous additions to in-house information systems, tasks and functions of the hardwares can be forgotten in times. Therefore, the positions and functions of all hardwares and softwares should be put forth. After this learning phase, some works about units which will improve of information security and its awareness should be made. In this context, examinations for İTÜ Automation System (a.k.a Student Affairs) have been made and as a result of this examination, it is tried to determine the possible security vulnerabilities and also determined precautions are reported to the manager to prevent from the security problems in the future, in these thesis. It is revealed with basic security questioning and examining the system, whether a vulnerability exist or not. Besides, security performance measurement by using standardized metrics gained increasingly interest during the last years with the help of guidelines, code of practices and standards accepted widely over the world. Therefore, the policy of ISO 27001 and instructions of 27002 are used to determine precautions and standards. By preparing these a policy for university, it is aimed to be as possible as protected from the external attack. All organizations need to build an information security architecture to keep secure their systems and all organizations should keep in their mind that information security policy is not an option instead it is an obligation in this era.

Those described above are mentioned about problems which are caused by external users, but there can be problems arising from internal users as it is known as the general characteristics of the information security system. The aim of this thesis is to reveal the security disruptive behavior will arise because of both internal and external users. Therefore, in second phase extremely sensitive situations like student Grade Entrance, Grade Correction and Graduation Status Controls are investigated for Automation System. The existence of students who don't deserve their notes in lightest form and in the graduation of the students even did not record in school with the most severe form of result the ignoring such cases. Because of not experienced these kind of problems don't mean it will never be, studies are conducted in order to minimize problems that may arise in future. A system is recommended to make more secure of Grade Entrance, Correction and Graduation Status Control. According to the recommended system, while teaching staff will enter notes, they'll make it on a desktop application which is not connected to internet. After that, the application create note document as EVA or XML format and both they will store original documents in application and send a copy to the database of own Faculty. Finally, Faculty will share the document with encrypted connection with Student Affairs' database.

Besides, that Grade Correction is carried out with decision correspondence document. Hence faculty member who made the grade correction sends grade documents to the faculty as EVA or XML format. Faculty, store grade correction correspondense its related database firstly, then stores grade document to its related database. Finally, faculty sends both documents to Student Affairs through secure connection line established between two sides to be stored also in there. Securiy Affairs stores those documents to related databases to be an evidence for future.

Grade documents will be stored in grade databases and correction correspondence document will be stored in correspondense databases; so there will be two databases in there, too. In the case of a student's graduation, both Faculty database and Automation database will cross-check with each other, and if both results are same then "student can graduate" information will be send to Student Affairs. Otherwise, they will be informed with a message which carries "student can't graduate. Results do not match." Right after, an investigation will be started to understand the reason of different grade results. Storing Grade Correction Correspondece document as an electronic format in both Faculty database and Automation database, makes any investigation easier.

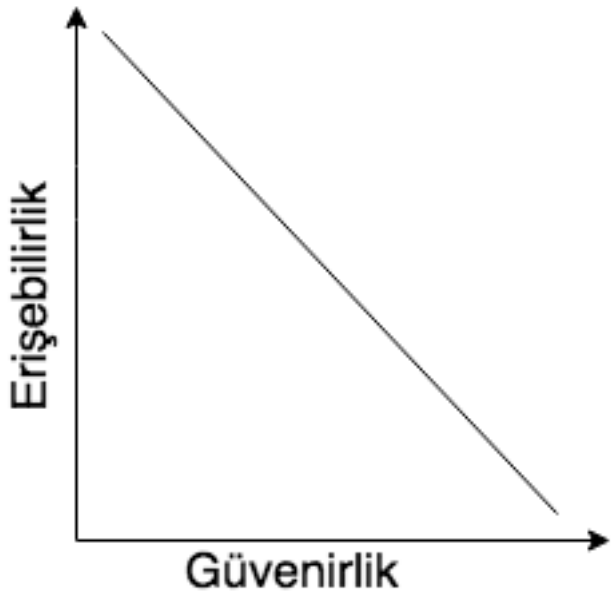
In final stage, a decision support software developed. It works with log files which have taken from Student Affairs Department and it aims to investigate insider threat in Automation System. Coverage of this work may be one of the following: it can be a student who sell lessons in a black market or it can be lecturer who abuse system with his/her powers, even it can be a Student Affairs' officer who change students' grade exchange with money. Some metric rules are needed to be created to develope a decision support machine software. In this stage software aims to find authenticated user who abused the Automation's system.

The thesis consists of five main sections: first of all it begins with Introduction Section that aims to express main details of studied subject and its environmental factors. Next Section dwell on Enterprise Information Security Concept and expresses it in some detail based on known standards which are specified by Standardization Organizations like SANS, ISO etc. In Section Three an investigation made to find vulnerability in system. A questionare is prepared for Student Affairs officers and according to their answers actions are taken and possible vulnerabilities are determined. After that based on possible vulnerability points, counter measures are spesified to build more secure system. Counter measures are prepared as suggestions list and it is delivered, right after that. In Fourth Section authorized users behaviours investigated from logs and tried to create characterization for each classes according to metric rules. In this work, it is aimed to find improper actions and abusements has been acted by authorized users. Thus, results which ensued from possible improper action, are examined and another list prepared to examine whether there is an bad action had been made by users. Decision Support Software creates lists according to log files from Automation System to ensue those improper action. The software is delivered to İTÜ Automation System to be used. Eventually, Final Section is consist of conclusions and recommendations. Besides of all conclusions about above sections, this section includes recommended system to make more secure Grade Entrance, Correction and Student Graduation stages. Also why recommended system is more secure than the current one is explained in details.

1. GİRİŞ

Güvenlik, iyi durumdaki bilgi ve yapının hırsızlık, veri değişikliği, bilgiyi bozma, servislerin açıklarına karşı korumasını sağlamaktır[2]. Günümüzde popüler çalışma alanlarından olan Bilgi Güvenliği (BG), bilgilerin izinsiz kullanımından, izinsiz açıklanmasından, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma veya bilgilere yapılacak olan izinsiz erişimleri engellemekle ilgilenen bilim dalıdır [1].

Bilginin güvenliği gizlilik, bütünlük ve erişebilirlik ilkelerine sıkı sıkıya bağlıdır. Bu ilkelerden bir ya da bir kaçının zarar görmesi halinde güvenlikten bahsetmek mümkün değildir. Şekil 1.1'de görüldüğü gibi güvenlik ve erişebilirlik birbirlerine ters orantılıdırlar, kullanılan sistem ne kadar güvenliyse erişilebilirliği de o kadar zordur. Bu yüzden ikisi için de doğru bir oran yakalanmalıdır. Örnek olarak kullandığımız parolalar düşünülebilir. İdeal bir parolanın uzunluğu 5 ila 8 karakter uzunluğunda olmalıdır; daha uzunu hatırlamak için zor, daha kısası içinse saldırganların şifreyi tahmin etmesi kolaydır[3].



Şekil 1.1 : Erişebilirlik – Güvenilirlik

1.1 Bilişim Teknolojileri (BT) Sistemlerinin Güvenliği

İnternetin kullanımı beraberinde Bilişim Teknolojilerinde güvenlik sorununu da ortaya çıkarmıştır. Bu sorunların nitelik ve niceliği her geçen gün artmakta; buna karşın önlemler de aynı hızda gelişmektedir. Durum artık kedi fare oyununa dönüşmüş, teknolojinin gelişiminin artışı işlenen suçları da giderek daha etkili ve tehlikeli bir hale getirmiştir.

Bu noktada sorulması gereken sorulardan bir tanesi de güvenlik açıklarının neden oluştuğu olmalıdır. Temel, basit ve sık sık karşılaşılan sebepleri sıralayacak olursak:

- Dışarıdan satın alınmış yazılımda güvenlik açıklığı olması, içerideki tüm sistemi de savunmasız bırakabilir. Üstelik satın alan kurum ya da kuruluş bunu genellikle bilemez. Elbette bu açıklar kurumun kötü niyetli olmasından değil, genellikle çalışan yazılımcıların güvenlik hakkında bilgili olmamasından kaynaklanmaktadır.
- Satın alan firma ya da yazılımı yapan kurum satıştan önce güvenlik sınamasından geçirmemiş olabilir.
- İleriki teknolojiler için tasarlanmamış olabildikleri için, ilerleyen teknolojiye entegrasyon aşamasında güvenlik açığı oluşabiliyor.

Bilişim sistemlerinin kaynaklarını veya bilgileri elde etme, değiştirme, bozma veya yalanlama amacıyla yapılan her türlü çalışma bilişim sistemine saldırı olarak kabul edilmektedir. Bilişim sistemlerine yapılan saldırılar, giderek etkisini artırmaktadır. Saldırılar, bireysel bilgisayarlara yapılabildiği gibi, kurumlara, kuruluşlara ve güvenlik birimlerine yönelik yapılmaktadır. Bu nedenle, *Bilişim Uzayında Saldırı* ya da *Bilişim Uzayında Savaş* gibi yeni tanımların yapılması gerekmiştir. Buna göre;

Bilişim uzayını kullanarak bir kuruluşun çalışmasını kesintiye uğratmak, engellemek, bozmak veya bilgi sistemini veya altyapısını kötü amaçla kullanmak veya verilerin bütünlüğünü bozmak veya çalmak amacıyla yapılan saldırılar bilişim saldırısı olarak kabul edilmektedir.

1.1.1 Saldırı türlerinin sınıflandırılması

Bilişim sistemlerine yapılan saldırılar farklı açılardan sınıflandırılmışlardır. Bu sınıflandırmalar aşağıda tanımlanmış ve açıklanmıştır:

Etkin ve ya Edilgen saldırılar: Etkin saldırılar bilgi sisteminin çalışması üzerinde etkili olurlar ve kaynaklar üzerinde değişiklik yapabilirler. Edilgen saldırılar, genelde bilişim sisteminde bulunan bilgileri öğrenmeyi amaçlar. Bu tür saldırılar sistem kaynaklarını bozmayı ya da değiştirmeyi amaçlamazlar. Dolayısıyla, etkin saldırıların kötü niyetli olduğu açıktır [22].

İçeriden ya da Dışarıdan Saldırılar: Adından da anlaşılacağı gibi, kuruluşta görevli ve yetkili bireylerin yaptıkları saldırılar *iç saldırı* olarak tanımlanır. İç saldırılar, kuruluşun bilgisayarı üzerinden yapılabilmektedir. Yetkili ya da yetkisiz bireylerin sisteme dışarıdan yaptıkları saldırılar *dış saldırı* olarak tanımlanır. Dışarıdan yapılan saldırılar, genellikle İnternet üzerinden yapılmaktadır. Dış saldırganlar değişik düzeyde yeteneklere sahip birey ya da topluluklar olabilmektedir. Günümüzde bu amaçla örgütlenmiş birlikler, firmalar, teröristler bulunmaktadır [22].

Saldırı Kaynağına göre Saldırılar: Bu sınıflandırma, saldırının yapıldığı kaynağı tanımlanmaktadır. Bir ya da birden çok bilgisayar tarafından yapılan saldırılar; *tekil saldırı*lar ve *dağıtık saldırı* olarak tanımlanmaktadır [22].

Açıklardan Yararlanma: Saldırıların bazıları bilgi sistemlerindeki açıklardan yararlanmayı hedeflerler. Bu tür saldırılar, bilgisayar ağını ve ana bilgisayarları hedeflerler [22].

Donanıma Yönelik Saldırılar: Bu tür saldırılar, bilgisayar ve çevre birimlerini ele geçirmeyi (bir anlamda çalmayı) amaçlarlar. Bu saldırılar bilgi sisteminin çalışma mantığını değiştirebilir [22].

1.2 Kurum İçi Güvenlik

Bu alan kendi içerisinde bir çok alt alana ayrılmaktadır ve bunlardan birisi de şüphesiz kurum içerisindeki kullanıcıların şüpheli hareketlerini tespit etmeyi amaçlayan, İçeriden Saldırı Tespitidir(İST).

Türkiye'de pek de üzerinde durulmayan bu konuyla ilgili Amerika Birleşik Devletleri (ABD) 1999 yılından beri çalışmaktadır [12]. 2001 yılında bilinen ilk

büyük içeriden saldırı FBI tarafından yakalanmıştır. Bir AB ordu askerinin içeriden aldığı gizli bilgileri Rusya'ya sattığı tespit edilmiştir[9]. Türkiye'de ise bu konuyla alakalı özel bir yasa hala bulunmamaktadır[15].

Bilginin değeri her geçen gün arttığı için onun güvenliğini sağlamak da önemli hale gelmiştir. Bu yüzden organizasyonlar çalışanlarına roller ve sorumlulukları görevler ayrılığı prensibine göre atamışlardır. Bu prensibe göre süreçler ve sistemler, kritik bir işlemin tek bir personel veya destek hizmet kuruluşu tarafından girilmesi, yetkilendirilmesi ve tamamlanmasına imkan vermeyecek şekilde tasarlanır. Etkin bir görevler ayrılığı ortamının tesis edilebilmesi için veriler üzerinde etkileri olabilecek süreçleri yürütecek personele, sadece üzerine atanan görevleri yürütmeye yetecek kadar yetki verilmelidir[10]. Bu bağlamda bilgi güvenliğini sağlamak için bir organizasyonda olması gereken roller ve sorumlulukları sıralayacak olursak[3]:

Üst Yönetim: Bilgi kaynaklarının tamamının korunmasından sorumludurlar.

Süreç Sahipleri: Uygun güvenlik önlemlerinin kurumsal politika ile tutarlılığından sorumludurlar.

Kullanıcılar: Aşağıda sıralanan maddeleri içeren organizasyonun güvenlik politikasını uygularlar:

- Güvenlik politikalarını okuyup kabul etmek,
- Oturum kimlik ve parolasının gizli olduğundan emin olmak,
- Kullanmadığında terminal'inin oturumunu kapatmak,
- Şüpheli güvenlik ihlallerini rapor etmek,
- Kapıları kilitli, giriş anahtarlarının gizli tutarak ve tanınmadık kişileri sorgulayarak fiziksel güvenliği sağlamak,
- Yürürlükteki yasa ve yönetmeliklere uygun hareket etmek,
- Gizli bilgilere ilişkin gizlilik düzenlemelerine bağlı kalmaktır.

Veri Sahipleri: Bilgiler için veri sınıflandırma seviyesini belirleyip böylece gizlilik, bütünlük ve erişebilirlik ilkeleriyle bağlantılı olarak uygun kontrol seviyesini belirlemekle görevlidirler.

Baş Gizlilik Yöneticisi (BGY): Şirketin müşterileri ve çalışanlarının korunması gereken gizlilik meselelerini koruyacak politikaları açıkça ifade etmek ve uygulamaktan sorumludurlar.

Bilgi Güvenliği (BG) Güvenlik Komitesi: Güvenlik kılavuzu, politikası ve prosedürleri tüm organizasyona etki eder ve yönetim kurulu, güvenlik yönetimi, bilgi güvenliği personeli ve hukuk müşavirleri gibi son kullanıcıların önerilerini ve desteğini almalıdır. Bu nedenle, çeşitli yönetim seviyelerini temsil eden bireyler, bu konuları tartışmak için, güvenlik uygulamaları oluşturmak için bir komitede toplanmaktadırlar. Komite uygun bir iş tanımı ile resmi olarak kurulur ve her toplantıda takip edilmek üzere eylem maddeleri kaydetmekle görevlidirler.

Güvenlik Uzmanları ve Danışmanları: Kurumun güvenlik politikasının, standartlarının ve süreçlerinin tasarım, uygulamaya koyma, yönetim ve gözden geçirilmesi aşamalarına yardımcı olmak ve onları yayınlamakla görevlidirler.

Bilgi Teknolojileri (BT) Geliştiricileri: BG uygulamalarını geliştirmekle görevlidirler.

BG Denetçileri: BG amaçlarının etkinliği ve uygunluğu üzerine bağımsız güvence yönetimi temin etmekle görevlidirler.

Dış Parçalar: Müşterileri, hizmet sağlayıcı, destek sağlayıcı ve yazılım sağlayıcılardan oluşur.

Organizasyon içerisindeki her parçanın bu yapıya göre bilgi güvenliğini sağlamak için görevi bulunmaktadır. Parçalar içerisindeki anahtar rol BG Denetçilerinde bulunmaktadır. BG denetçileri gizlilik etki analizi yapmalı ve değerlendirmelerin yönetim tarafından yerine getirilip getirilmediğini kontrol etmelidirler. Bu değerlendirmeler:

- iş süreçleri ile alakalı kişisel kimlik bilgilerinin belirlemeyi,
- kişisel bilgilerin toplanması, kullanılması, açıklanması ve yok edilmesinin belgelenmesinin sağlanması,
- gizlilik riskini ve bu riski azaltmak için gerekli seçenekleri anlamaya dayalı bilinçli politika, operasyonlar ve sistem tasarımı yapmak için bir araçla yönetim sağlanması,
- hem teknik hem de yasal ilgili yönetmeliklere uygun kalıcı bir format ve yapısal bir süreç oluşturulması,
- gizlilik sorunları için hesap verebilirliğin var olduğundan emin olunması,
- gizlilik uyumları için bilgi sistemlerinin yeniliklerinin ve düzeltmelerinin azaltılmasından oluşan kavramsal ve gereksinim analizi aşamasından son

tasarım onaylanmasına, fon bulmasına, geliştirilip, uygulamaya geçirilmesi ve iletişim aşamasına kadar gizliliğin de düşünüldüğünden emin olmak için bir çatı sağlanmasıdır.

Roller kendilerine atanan sorumlulukları oldukça titiz bir şekilde yerine getirse de en başta erişebilirlik ve güvenilirlik konusu içerisinde bahsettiğimiz parolanın özelliklerinin doğru şekilde belirlenmesi de bilginin güvenliğinin sağlanması açısından çok önem arz etmektedir. Sistem oluşturulduğunda tüm kullanıcılara bir başlangıç parolası atanmalıdır ve bu başlangıç parolası kişiye özel olarak mutlaka güvenlik yöneticisi ya da sistem tarafından otomatik olarak atanmalı ve içerdiği karakterler rastgele olmalıdır. Kullanıcı adı ve parolanın mutlaka doğru kullanıcının eline geçtiğinden emin olunmalı ve eğer atanan başlangıç parolası belli bir süre boyunca kullanılmazsa sistem tarafından hesap askıya almalıdır. Kullanıcı sisteme ilk kez giriş yaptığı anda parolası değiştirilmeye zorlanmalıdır. Eğer kişi parolasını sisteme giriş esnasında belli bir sayıda yanlış giriyorsa, genellikle bu rakam 3'tür, kullanıcının hesabı yine otomatik olarak pasif hale getirilmelidir. Eğer kullanıcı hesap bilgilerinden herhangi birini unuttuğu için hesabı pasif duruma getirildiyse sistem yöneticisine hesabı aktifleştirmesi için bilgi vermelidir. Parolalar şifrelenmiş olarak ya da özetleri alınmış olarak saklanmalı ve hiçbir ortamda gösterilmemelidirler. Ayrıca periyodik olarak değiştirilmelidirler ve bu periyod parola sahibinin bilgi erişiminin önem seviyesine göre kısa ya da uzun olmalıdır. Parolanın değiştirilmesi gerektiğinde mutlaka kullanıcıların kendileri tarafından ve kendi makineleri üzerinden değiştirilmelidir. Çalışmalar göstermiştir ki kullanıcılar kendilerine uyarı verilmediği sürece parolalarını değiştirmek konusunda titiz davranmamaktadırlar, bu yüzden değişim tarihi yaklaştığında kullanıcılara bildirim gönderilmelidir. Parola değişimi esnasında da tıpkı başlangıç aşamasında olduğu gibi parolanın belli bir yapısı olmalıdır ve bu yapı şu şekilde olmalıdır:

- İdeal bir parolanın uzunluğu 5 ila 8 karakter uzunluğunda olmalıdır. Daha azı tahmin etmek için kolay daha fazlası da hatırlamak için zordur.
- Parola sayı, büyük, küçük harf ve özel karakterlerin minimum 3 çeşit kombinasyonundan oluşmalıdır.
- Parola özellikle kişi ile alakalı herhangi bir bilgi(isim, soy isim, doğum yeri vs.) içermemelidir.

- Aynı parolanın tekrar kullanılabilmesi için son kullanılmasının üzerinden en az 1 yıl geçmiş olmalıdır.
- Kullanıcı sisteme eriştikten sonra belli bir süre boyunca işlem yapmıyorsa oturumu sonlandırılmalıdır.
- Kimlik doğrulamanın bilgi güvenliği açısından çok önemli olduğu düşünülürse, bu aşamada kullanılacak şifreleme teknikleri, güncel durum itibariyle literatürde kabul görmüş ve güvenilirliğini yitirmemiş algoritmalar göz önünde bulundurularak seçilmelidir.
- Kullanılacak şifreleme anahtarları, ilgili algoritmalar için anahtarın geçerli olacağı ve kullanabileceği zaman zarfında kırılmayacak şekilde uzun seçilmelidir. Geçerliliğini yitirmiş, çalınmış veya kırılmış şifreleme anahtarlarının kullanılabilirliği engellenmelidir[3].

Ayrıca kimlik doğrulama mekanizmasının başarısız kimlik doğrulama teşebbüsleri hakkında, ilgilinin sisteme ilk girdiği anda bilgi vermesi, başarısız teşebbüslerin belli bir sayıya ulaşması halinde ise ilgili kullanıcının erişimini engellemesi ya da başarısız kimlik doğrulama teşebbüsleri sonrasında bu teşebbüsü gerçekleştiren kişiye yanlış girilen kullanıcı bilgisi veya parolası ile ilgili örneğin böyle bir kullanıcının sistemde olmadığı veya parolanın yanlış girildiği gibi gereksiz bilgi vermemesi gerekmektedir[10].

1.2.1 İçeriden yapılan soygun örnekleri

Parasal işlemlerin yoğun olduğu, bankacılık, perakendecilik ve hizmet sektörlerinde yaşanmış bazı örnekler incelemeye değer. Bu tür soygunları yapanlar, genellikle kuruluşun bilgi sistemleri bölümlerinde çalışanların içinden çıkmaktadır. İçeriden yapılan soygunlara ilişkin bazı örnekler aşağıda sunulmuştur:

1.2.1.1 Salam dilimi

Hesaplamalarda yapılan çok küçük değişiklikler ile yapılan soygunlara, soygununun çok küçük parçalar halinde yapılması nedeniyle *Salam Dilimi* türü soygun adı verilmektedir. 1970-90 arası yaşanmış birkaç örnek bulunmaktadır. Örneklerden biri şöyledir: Bir bankanın bilgi sistemleri bölümünde programcı olarak çalışan biri müşterilerin birikimleri için verilecek faizleri hesaplayan programda küçük bir değişiklik yapar. Bilindiği gibi, günlük ya da aylık hesaplanan faizler kuruşuna kadar

hesaplanır; ancak belli bir değerin altındaki değerler yuvarlanır. Örneğin 5 kuruşun altındakiler sıfıra, üstündekiler 10 kuruşa yuvarlanır diyelim. Bu yuvarlatma işleminden müşterilerin haberi vardır ve miktar çok küçük olduğu için önemsemezler. Bu gerçeği bilen programcı, 10 kuruşun altında kalan faizleri sıfıra yuvarlatır; böylece atılan miktarları kendi çekebileceği özel bir hesaba aktarır. Bu işlemi her zaman değil, rastgele zamanlarda yaptığı düşünülürse yakalanma olasılığının da çok düşük olacağı açıktır. 1 milyon müşterisi olan bir bankada bu yöntemle, bir faiz hesaplaması sonunda yaklaşık 50.000,TL nin çalınabileceği kolayca söylenebilir [22].

Salam dilimi türü soygunlara ilişkin bir başka örnek, bir araba kiralama firmasında 1993 te yaşanmıştır. Firmanın bilgi sistemleri bölümünde çalışan bir programcı, ödeme sisteminde küçük bir değişiklik yaparak, araçların yakıt deposunu yaklaşık 20 litre daha büyük olarak tanımlamıştır. Müşteriler aracı geri getirdiklerinde, yakıt deposunu dolu olarak teslim etmediklerinde kendilerinden eksik yakıt için bir ödeme yapmaları istenmektedir. Araçların yakıt depoları olduğundan büyük tanımlandığı için müşteriler, gereğinden fazla para ödemek zorunda kalmaktadır. Müşteriden istenen eksik yakıt bedeli ile gerçek eksik yakıt bedeli arasındaki fark, programda değişiklik yapan kişinin hesabına aktarılmaktadır. Böylece yakıt deposunu tam doldurmadan geri getiren müşterilerden eksik 5-20 litre yakıt bedelinin alındığı saptanmıştır. Bu türde dolandırılan müşteri sayısı yaklaşık 47.000 dir [22].

Salam dilim türü çok sayıda soygunun yapıldığı bilinmektedir. Yönetim ve müşteriler tarafından fark edilmesi çok zor olan bu tür soygunlar rastlantı sonucu ya da bazı şüpheler üzerine yoğun araştırmaların sonunda bulunabilmektedir. Salam dilimi türü soygunlar, kuruluş içinden soygunların yapılabileceğini göstermesi açısından önemlidir. Ayrıca sezilmeleri ve ortaya çıkarılmaları çok zordur. Bu tür soygunları önlemenin yolu, program geliştiriciler tarafından hazırlanan programların işletmeye alınmadan önce güvenlik birimi tarafından ayrıntılı biçimde incelenmesi ve sınanmasıdır. Bu aşamayı geçmeden işletmeye alınmamasıdır [22].

1.2.1.2 Uzaktan erişim

Banka, borsa, maliye ve benzeri kuruluşlar, iş hacimleri nedeniyle büyük boy bilgisayarlar ile hizmet vermektedirler. Bu tür kuruluşların bilgisayarları için zaman içinde güncelleme ve bakım hizmeti gerekmektedir. Bakım ve güncelleme hizmetleri

genellikle kuruluş dışından sağlanmaktadır. Bu tür hizmetlerin sağlanabilmesi için ya bir uzman, kuruluşun bilgi sistemlerinin bulunduğu yere gelerek çalışır ya da sisteme uzaktan erişerek bu hizmeti vermeye çalışır. Her iki durumda da uzmanın sisteme girebilmesi için yetki verilmesi gerekir. Bu yetkinin, bazı durumlarda en üst düzeyde olması gerekir. Çünkü yapacağı güncelleme ve bakım bu yetkiyi gerektirir [22].

Böylesine yetkilendirilmiş bir dış kaynak uzmanı, daha sonra aynı sisteme girebildiğini fark eder. Kendisine verilmiş olan kullanıcı kimliği ve parolanın hâlâ geçerli olduğunu görür. Eğer uzman kötü niyetli ise sistem üzerinde her türlü değişikliği yapabilir. Eriştiği sistem bir bankanın sistemi ise para aktarımında bulunabilir. Maliyenin sistemi ise borçlarını silebilir. Askerlik şubesine ilişkin ise, kendisini askerlik görevini yapmış olarak gösterebilir. Aklımıza gelebilecek her türlü işlemi yapabilir [22].

Geçmişte ve günümüzde bu tür sorunlar yaşanmaktadır. Teknik zorunluluk nedeniyle verilen bu yetkiler, bakım ve güncelleme işlemi tamamlandığında hemen iptal edilmeli ya da sistemin sahibinin yetkisi ve gözetiminde yapılmalıdır [22].

1.2.1.3 Bomba

İçerden yapılan başka tür bilişim suçlarına bir örnek olarak *bomba* örneği verilebilir. Adından da anlaşılacağı gibi bomba etkisi yapacak programların bilgi sistemi içine yerleştirilmesi ve zamanı geldiğinde etkin hale getirilmesi eylemidir. Bomba türü yazılımlar, bilgi sistemleri bölümünde program geliştiriciler tarafından hazırlanır. Amaçları, çalıştıkları kuruluştan mutsuz bir şekilde ayrıldıklarında, kuruluşa zarar vermektir. Bu nedenle saatli bomba örneğinde olduğu gibi bir program hazırlarlar ve bu programı, sistemde sürekli çalışan bir programın içine gömerler. Kuruluş içinde çalıştıkları süre içinde bomba programın patlama zamanını ertelerler. Mutsuz bir ayrılmadan belli bir süre sonra bomba program etkin hale gelir ve programı hazırlayanın belirlediği zararları vermeye başlar. Örneğin veri tabanındaki verileri değiştirebilir; verileri silebilir; programları akışını değiştirebilir ya da çalışmaz kılabilir [22].

Bomba türü programlar, dışarıdan satın alınan programların içinde de olabilmektedir. Özellikle lisans bedellerinin ödenmemesi durumunda etkin hale gelecek biçimde kurgulanırlar [22].

Bomba türü saldırıları önlemenin, program geliştiriciler tarafından hazırlanan programların işletmeye alınmadan önce güvenlik birimi tarafından ayrıntılı biçimde incelenmesi ve sınanmasıdır. Bu aşamayı geçmeden işletmeye alınmamasıdır. Dışarıdan sağlanan programların kaynak kodları her zaman görülemeyeceği için bu tür sınamalardan geçirilmeleri zordur. Ancak zaman sınamasından geçirmek oldukça kolaydır [22].

1.3 Tezin Amacı

Her BT sisteminin mutlaka bir açığı vardır, açığı olmadığı söylenene inanılmaz fikriyle yola çıkmış olan güvenlik saldırılarını gerçekleştirenler, bu güne kadar haklı çıkmışlardır. "Hırsıza Kilit Vurulmaz" ve her BT sisteminin açığı vardır ve var kabul edilir. Bu ana fikir ile belirlenen tezin amacı, İTÜ gibi çok kullanıcılı dağıtık bir sistemin incelemesini yapmak ve bunun sonucunda olabilecek saldırılara karşı güvenlik önerisinde bulunmaktır. Çalışmada örnek olarak İTÜ öğrenci otomasyon sistemi ele alınmıştır.

Kullanıcılar dört grupta toplanmıştır, bunlar: öğretim üyesi, öğrenci, yetkili, sistem ve veri tabanı yetkilisidir. öğretim üyesi ve öğrenci sistemi dışarıdan kullananlar; yetkili, sistem ve veri tabanı yetkilisi de sistemi içeriden kullanan kullanıcılar olarak ele alınmıştır.

Yapılacak çalışma da üç aşamada gerçekleştirilecektir. Öncelikle bu kullanıcı grupları için, sistemi kullananların tamamının kullanım örüntüsünün çıkarılması gerekmektedir. Sonrasında derslerin örüntüsünün çıkarılması ve en son da sistem açıklıklarının saptanması gerçekleştirilecektir. Bu örüntüler çıkarılırken saldırı olarak kabul edilebilecek bazı durumlar da göz önünde bulundurulacaktır. Örneğin, öğrenci için dışarıdan saldırı yapabilmesi, Hizmet Dışı Bırakma Saldırısı (HDBS) yapıp sistemi bloke etmesi ya da izin verilen zamanlar dışında sistemi kullanabilmesi gibi durumlar saldırı olarak kabul edilmiştir. Öğretim Üyesi için en basitinden VF girişi ile alakalı izin kaldırılmasının unutulması sebebiyle hocanın sistemi öğrencinin mağdur olacağı şekilde kullanabilmesi aslında sisteme yapılmış bir saldırıdır ve tezde de saldırı olarak kabul edilmiştir. Sistem ne kadar mükemmel olursa olsun, yetki verme ya da bir yetkiyi kaldırmanın zamana bağlı olduğu durumlar bulunmaktadır; bu sistemi yöneten çalışanların unutmaları halinde yukarıda belirtilen açıklıkların olması ve bunların kullanılması kaçınılmazdır.

1.4 Kaynak Araştırması

İçeriden saldırıyı tespit etmek üzere yapılan çalışmalarda farklı disiplinler bir araya getirilerek, başarılı tespit mekanizmaları yapılmaya çalışılmıştır.

[5] numaralı çalışmada denetimli öğrenme ve akış madenciliği bir arada kullanılması denemişlerdir. Denetimli öğrenme olarak diğerlerinden daha başarılı buldukları için Tek-Sınıflı Destek Yöney Makinesi'ni (TSDYM) kullanmışlardır. Başarımı yeterli buldukları dışında miktar belirtmemişlerdir. Bu çalışmada model oluşturulduktan sonra çalışma boyunca aynı model kullanılmış ve tüm testler bu model ile yapılmıştır. İleriki çalışmalar için önerileri kullanıcı geri dönüşüne göre modeli de sürekli geliştirerek bu çalışmayı yapmak olmuştur.

[7]'nin yaptığı çalışmada da denetimli öğrenme yöntemini kullanmıştır ancak bu çalışma özellikle Elektronik Sağlık Sistemi için yapılmıştır. Çalışmanın amacı sisteme şüpheli erişimleri tespit etmektir. Çalışma iki model şeklinde ele alınmıştır; ilki için 1291 etiketlenmiş olaya Doğrusal Bağlanım (DB) ve Destek Yöney Makinesi (DYM) uygulanmıştır. İkinci model için de imza ve kural tabanlı bir filtreleme tekniği uygulanmıştır. İlk modelden %96 başarım, ikinci modelden de %99,8 başarım elde edilmiştir. Sonuç olarak, olayları etiketlemenin çok büyük zaman kaybına sebep olduğundan ve pozitif durumların çok az olduğu için başarımı etkilediğinden bahsetmişler ancak başarımı daha iyi hale getirmek için bir öneride bulunmamışlardır.

[8] çalışmalarında süreç madenciliği ve istatistiği bir arada kullanmışlardır. Süreç modeli çıkarma ve sürecin yapısını oluşturma işlemi için sistem eylem tutanağından faydalanmışlar, yapılar oluşturulduktan sonra her işlem örneği için sayısal bir vektör oluşturulup, istatistiksel bilgiler kullanılarak vektörlerin aykırı değerleri belirlenmiştir. Sonrasında bu belirlenen aykırı işlemleri gerçekleştiren kullanıcılar şüpheli olarak belirlenmişlerdir. Önerilen yöntem kontrol yapıları ve döngüler içeren bir süreç modeli üzerinde çalışıldığında %85'in üzerinde başarım alınırken, döngü içermeyen bir süreç model üzerinde çalıştırıldığında ise %90'ın üzerinde başarım elde edilmiştir. Diğer yandan kendi alanları içerisindeki diğer çalışmalarla karşılaştırıldığında daha az yanlış olumluluk oranı içerdiği görülmüştür.

[6] numaralı çalışmanın amacı, iş akışlarını bu iş akışlarına katkıda bulunan bilgi türlerini elde etmek ve bu iş akışları içerisindeki sapmaları tanımlamak amacıyla bir

organizasyon içerisindeki bilgi akışını analiz etmektir. Çalışma belge için bir yol oluşturmak için dosyaların hareketlerini zaman ile birleştirerek belgelerin hareketlerini inceleyen bir sistem oluşturulmuştur. Belgenin yolu, hareketlerini ve zaman içerisindeki gelişimini içeriyor ve bu yolları bir alt kümesi olan kurumsal süreçleri temsil eden bir örüntü içerisinde grupluyor. Sonrasında organizasyon içerisindeki belgeleri inceliyor ve bu belgelerin hem içerik hem de üst veri benzerlikleri üzerinden oluşturduğu bilgi akışlarını kendisine referans noktası olarak kabul ettikten sonra bu referans noktasına göre belgelerin benzerliklerini analiz ediyor ve bu analiz sonucunda bir harita oluşturuyor. Eğer haritada bir sapma tespit edilirse potansiyel zararlı davranış olarak rapor ediliyor. Çalışmanın sonuç bölümünde her hangi bir başarım miktarından ya da ileriye yönelik bir öneriden söz edilmemiştir.

1.5 Tezin Katkısı

İTÜ'nün otomasyon sistemi dağıtık bir bilgi sistemidir. Bu tarz bir sistemin yönetilmesi de dağıtık olması sebebiyle oldukça güçtür. Ayrıca sistem ile alakalı yaşanmış sorunlar olduğu ve bunların zaman içinde giderildiği bilinmektedir.

Örneğin;

1. Lisans öğrencileri arasında ders satışı olduğu tespit edilmiştir. Öğrenciler alabileceklerinden fazla dersi alarak, para karşılığında dersi almak isteyen öğrencilere satış yaptıkları duyulmaktadır.
2. Dönem dışında öğrencilerin derse kayıt oldukları duyulmaktadır.
3. Öğretim üyelerinin dönem dışında not girişi ve değişimi yapabildikleri duyulmaktadır.
4. Öğretim üyelerinin dönem dışında sınava giriş hakkını kısıtladıkları duyulmaktadır.

Bu ve buna benzer sorunların yaşandığı ve sorunların kaynakları bilindiği için çözülebildiğini biliyoruz.

Şu kesin ki hiçbir bilişim sisteminin %100 güvenli olmadığı varsayımından kalkarak, İTÜ Öğrenci Otomasyon Sisteminde güvenlik açığı araştırması yapılmıştır. Sistemde güvenlik açıklığı olup olmadığı temel güvenlik sorgulama çalışmalarıyla ve sınayarak ortaya çıkarılmıştır.

Yukarıda anlatılanlar dış kullanıcılardan kaynaklanan sorunlardır, ancak bilgi güvenliği sistemlerinin genel özelliklerinden bilindiği üzere iç kullanıcılardan kaynaklanan sorunlar da yaşanabilmektedir. Tezin amacı hem iç hem de dış kullanıcıların sebep olacağı güvenliği bozucu davranışların ortaya çıkartılmasıdır.

Son aşamaya gelindiğinde eylem tutanakları üzerinde çalışılacak ve Otomasyon Sistemine karşı gerçekleştirilecek içeriden tehditleri tespit edecek bir karar destek yazılımı geliştirilmiştir. Karar destek yazılımını oluşturabilmek için bir kural listesi hazırlanmıştır.

1.6 Tezin İçeriği

Tez 5 ana bölümden oluşmaktadır: Giriş bölümü ile çalışılan konu ve çevresel faktörleri genel detayları ile anlatılması amaçlanmıştır. Bir sonraki bölümde Kurumsal Güvenlik kavramı üzerinde durulmuştur. 3. bölümde güvenlik açıklıklarının araştırması yapılmıştır. Daha güvenli sistem oluşturmak için önerilerde bulunulmuştur. 4. bölümde yetkili kişilerin davranışlarından kalkılarak sınıflandırmaları, her sınıfı karakterize eden özelliklerin ortaya çıkarılması, bunun sonucu olarak da aykırı davranışta bulunanların saptanmıştır. Ortaya çıkan sonuçlara bakarak yetkilendirmelerin nasıl yapılması konusunda bir öneri listesi oluşturulmuştur. Bu aykırı davranış biçimlerinin bulunması için eylem tutanaklarından yararlanılarak aykırı davranışları ortaya çıkaran bir karar destek yazılımı geliştirilmiştir. Bu geliştirilen yazılım İTÜ Otomasyon Sisteminin kullanması için verilmiştir. Son olarak da Sonuç ve Öneriler kısmı yer almaktadır. Çalışma saygınlığı olan bir kurum için yapıldığı için bazı çalışmalar tez kitabı kapsamına dahil edilmemiştir.

2. KURUMSAL GÜVENLİK

Bilgi ve bilgisayar güvenliğini iki ortam için farklı düşünmek gerekir; Bireysel kullanım amaçlı bir bilgisayarın güvenliği söz konusu olduğunda, bilgisayara girme ve bu bilgisayarda bulunan veriler üzerinde işlem yapabilme akla gelmektedir. Kurumsal bilgi sisteminin güvenliği söz konusu olduğunda, çok sayıda bilgisayardan oluşan bir yapının güvenliği düşünülmelidir. Bilgisayar sayısının çokluğu ve bunların birbirine yerel bilgisayar ağı (YBA) ile bağlı olmaları; YBA üzerinde başka donanımların bulunması, kurumsal bilgi sisteminin güvenliğini karmaşık hale sokmaktadır.

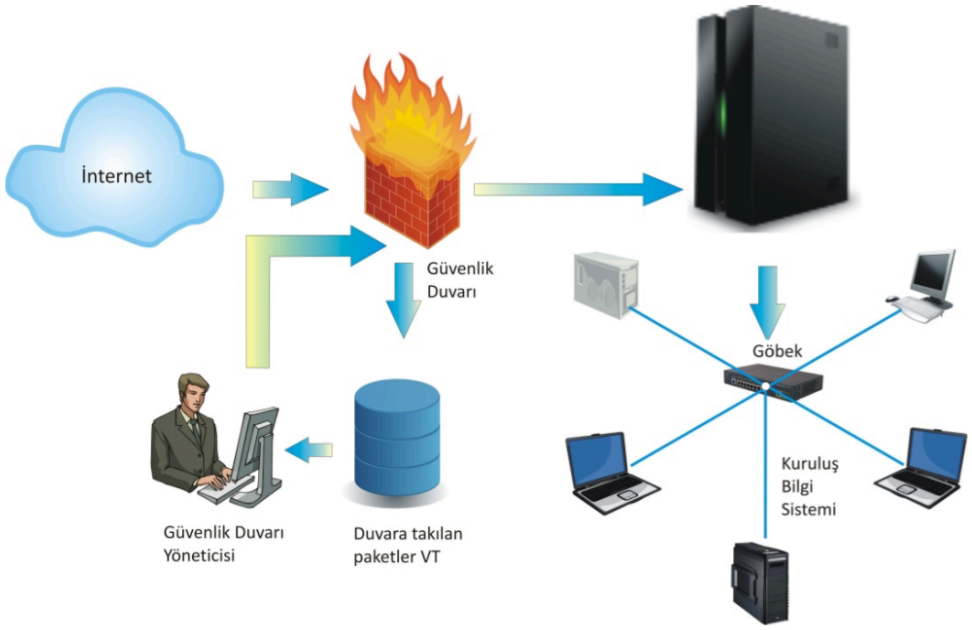
Kurumların koruması gereken varlıkları, verileri, kaynakları ve özellikle de saygınlıklarıdır. Kurumun sahibi olduğu bilgi sistemi, yetkili ya da yetkisiz kişiler tarafından kendi amaçları için kullanılamamalıdır. Örneğin, bir kurum çalışanı özel belgelerini ve verilerini diskteki boş alanda saklamaya kalkışabilir. Aynı tür girişim, kurum ile ilgisi olmayan bir kişi tarafından da yapılabilir. Kurum bilgi sistemine zarar vermeyecek bile olsalar, bu tür kullanımlara izin verilmemelidir. İleride zararlara neden olabilir.

Saygınlık, bir kurum için çok önemlidir. Özellikle toplumda saygın konumu olan üniversiteler, bankalar ve kamu kuruluşlarının birinde olabilecek bir güvenlik açığı, bu kuruluşa olan güveni çok sarsar. Örneğin, İnternet bankacılığındaki bir güvenlik açığının toplum tarafından öğrenilmesi, müşterilerin o bankadaki hesaplarını kapatmasına neden olabilir. Ya da İstanbul Teknik Üniversitesi gibi saygınlığı ön planda tutan ve tutması da gereken bir okulun sistemindeki bir güvenlik açığının kullanılıp veri çalınması, okulun itibarını yerle bir edecek ve okula duyulan güveni de sarsacaktır.

Kurumsal bilgi sistemlerinde, güvenliği bozacak etkiler dışarıdan ve içeriden olabilmektedir. Değişik kaynaklarda açıklandığı kadarı ile içeriden yapılan saldırıların zarar etkisi dışarıdan yapılan saldırılara oranla daha yüksek olmaktadır. Dışarıdan ve içeriden yapılan saldırı türleri ve örnekleri 1. Bölümde anlatılmıştı. Dış ve iç saldırıları önlemek üzere, günümüzde özel donanımlar ve yazılımlar

üretilmektedir. Bunlar, saldırıları önemli ölçüde önleyebilmektedir. Ancak, zaman içinde saldırıların türü ve niteliği değişmektedir. Bu nedenle, koruyucu donanım ve yazılımların sürekli olarak güncellenmesi gerekmektedir. Saldırganlar, bu koruyucuların özelliklerini bilmekte ve zayıf noktalarını yakalamaya çalışmaktadırlar. Mevcut koruyucu donanım ve yazılımları kullanarak sağlanan güvenlik durağan bir çözümdür. Bu tür durağan çözümlere ek olarak, kurumsal bilgi sistemini sürekli izleyen ve aykırı davranışları ortaya çıkaran ve buna karşı önlem üreten yöntemlerin kullanılması daha doğru olur.

Kurum dışından yapılan saldırıları önlemek üzere, kurumun İnternet bağlantısı üzerine *güvenlik duvarı* ve sızmaları algılayacak *sızma algılayıcı* donanım ve yazılımlar yerleştirilir. Şekil 2.1'de Güvenlik Duvarı kullanımına dair örnek bir sistem gösterilmiştir.



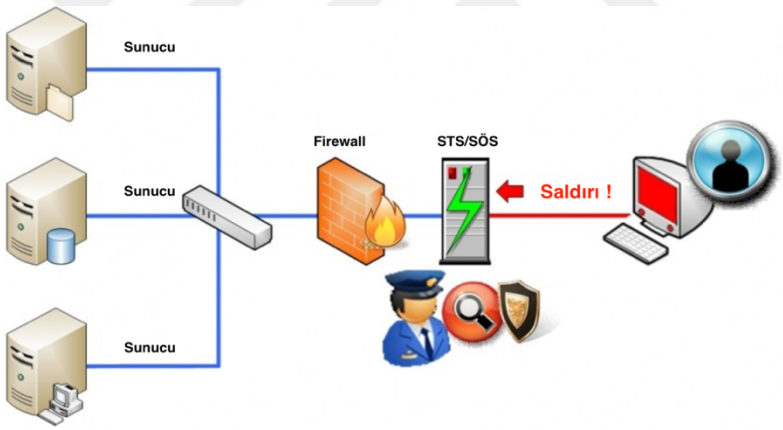
Şekil 2.1 : Güvenlik Duvarı Örneği [22]

Güvenlik duvarı, genel anlamıyla dışarıdan gelen ve içeriden çıkan veri trafiğini inceleyerek zararlı veya gereksiz veri paketlerinin içeriye geçmesine ve dışarı çıkması istenmeyen veri paketlerinin dışarı çıkmasını engelleyen donanım ve yazılımlar olarak tanımlanır. Bu görevi yapabilmeleri için, güvenlik duvarı kuruluşun bilgisayar ağı ile internet arasına yerleştirilir. Büyük ölçekli kuruluşlarda, bölüm

ağları arasına da yerleştirilir. Böylece bir bölümün diğer bir bölümdeki çalışmaları görmesi engellenir [22].

Temel veri paketi süzme işlevi gelen paketlerin geldiği ve gitmek istediği adresleri öğrenir. Bu adres bilgilerine bakarak paketin geçişine izin verir ya da vermez. Kapsamlı süzme işlevi, kural tabanlı ya da sezgisel yöntemlere göre çalışır. Daha önce geçişine izin verilmiş paket türlerine izin verirken, tanımadığı paketleri incelenmek üzere veri tabanına atar. Bu paketler de güvenlik duvarı yöneticisi tarafından incelenerek geçişleri üzerine karar verir [22].

Saldırı Tespit Sistemleri (STS), ağdaki paketleri inceler ve saldırıyı tespit edip, raporlama amaçlı kullanılırlar. STS'ler sadece analiz ve tespit amaçlı kullanılmaktadırlar ve saldırıyı engelleme özellikleri bulunmamaktadır. Engelleme için *Saldırı Önleme Sistemleri (SÖS)* kullanılır. Bu sistemlerin kullanımlarına dair Şekil 2.2'de örnek bir sistem gösterilmiştir.



Şekil 2.2 : Güvenlik Duvarı, STS ve SÖS Sistemlerinin Simülasyonu [21]

Kurum içinden saldırılar için de benzer donanım ve yazılımlar kullanılmaktadır. Ancak, kurum içinden yapılan eylemlerin biçimi farklı olmaktadır. Bu tür eylemlerde bulunanların belli bir kısmı, doğal olarak bilgi sistemine erişim hakkı olan kullanıcılardır ya da bunların kullanıcı haklarını elde etmiş kişilerdir. Bu nedenle, içeriden yapılan eylemler daha tehlikeli olmaktadır. İçeriden yapılabilecek eylemleri algılamak ve çözümlemek için *izleme yöntemleri* kullanılmaktadır.

2.1 Kurumsal Güvenliğin Geliştirilmesi

Bir kurumun bilgi sisteminin güvenliğini sağlamak üzere, önce *güvenlik politikası*nın belirlenmesi; ardından bağlayıcı ölçünlerin gözden geçirilmesi; daha sonra güvenlik ilkelerinin belirlenmesi ve son olarak da yönergelerin belirlenmesi gerekir.

Güvenlik Politikası: Her kurumun güvenliği değerlendirmesi farklı olabilir. Örneğin; bir banka veya kamu kurumu için güvenlik olmazsa olmaz bir koşuldur. Güvenlikte yaşanacak bir sorun ya da açık kurumun tüm saygınlığını yitirmesine neden olabilir. Sadece danışma hizmeti veren bir kuruluş için güvenlik konusu daha az önemli olabilir. Kurumun güvenlik politikasını kurumun üst düzey yöneticileri ile bilgi sistemlerinin teknik elemanları birlikte oluşturmalıdır. Üst düzey yöneticiler, beklentilerini ortaya koyarken, teknik elemanlar, mevcut teknolojiler ile istenen güvenliğin sağlanıp sağlanamayacağını ve nasıl sağlanacağını anlatırlar [22].

Ölçünler : Kurumsal bilgi sistemlerinin sağlaması ve uyması gereken ölçünler, yetkili kuruluşlar tarafından belirlenmekte ve yayınlanmaktadır. Bazı kurumlar bu tür ölçünlere zorunlu olmasalar da uymak isterler. Böylece kurumlarının güvenlik politikalarını belirlerler. Banka gibi kuruluşlar ise, bu tür ölçünlere zorunlu olarak uymak zorundadırlar. Uymadıkları saptandığında, bankacılık çalışmaları durdurulabilir. İTÜ gibi kurumlar ise öğrenci kayıtlarını, otomasyon sistemlerinde herhangi bir veriyi ve özellikle de toplumun gözündeki saygınlıklarını kaybetmek istemezler. Herhangi birinin kaybında saygınlıklarını kaybedecek olmanın bilinciyle güvenlik politikalarını belirlemek ve uygulamak zorundadılarlar [22].

İlkeler : Kurum için oluşturulan bilgi güvenliği ilkeleridir. Bu ilkeler kurum tarafından belirlendiği için, kurum güvenlik politikası için öneriler olarak değerlendirilebilir [22].

Yönergeler : Güvenlik konusunda izlenecek adımların tanımlandığı belge olarak düşünülebilir. Kurumda çalışanların, bilgi güvenliği konusunda alması gereken önlemler, güvenlik bozucu bir olayla karşılaştığında yapması gerekenleri anlatan *yönerge* olarak değerlendirilebilir [22].

Güvenlik politikası, uyulacak ölçünler, ilkeler ve süreçler yazılı biçimde hazırlanmalı ve gerekli kişilere dağıtılmalıdır. Bir kurum bu çalışmaları yaptıktan sonra ömür boyu güvende olacağını düşünmemelidir. Zaman içinde, güvenlik politikasını ve buna bağlı adımları gözden geçirmeli ve gerekli güncellemeleri yapmalıdır. Güvenlik

konusunda olabilecek olayları algılayabilmek ve gereken önlemleri alabilmek üzere, kurum içinde bir bilgi güvenliği biriminin oluşturulması gerekir. Bu birim, kurumsal bilgi sistemini sürekli olarak izlemeli; sorunları ortaya çıkarmalı ve gerekli önlemleri almalıdır. Bilgi güvenliği biriminin çalışmaları şu dört aşamadan oluşur:

- İnceleme ve Öneriler
- Uygulama
- İzleme
- Değerlendirme

İlk aşamada, kurum güvenlik politikasına uygun olarak planlama yapılır. Güvenliğin nasıl sağlanacağına, ne tür donanım ve yazılımların gerekeceğine karar verilir. İkinci aşama, kurum bilgi sistemini, güvenli çalışacak biçimde kurmaktır. Bu aşamadan sonra, bilgi sistemindeki hareketler izlenmeye başlar. İzleme sırasında ortaya çıkan aykırılıklar saptanır ve bunlar değerlendirilir. Değerlendirmelerin sonunda, gerekli iyileştirmeler yapılır [22].

3. İNCELEME VE ÖNERİLER

Bilgi güvenliği araştırması yapılacak olan kurumda, daha önce kurulmuş olan bir bilgi sisteminin var olduğu varsayıldığından, hedeflenen bilgi güvenliği seviyesini sağlayabilmek için, ilk aşamada mevcut durumu incelemek gerekir. Bu inceleme sırasında, her zaman şüpheci olmakta yarar vardır. Çünkü bilgi güvenliği eksiksiz sağlanmış bir yapının var olduğunu düşünmek yanlıştır.

Mevcut durumdaki gözlem sonuçları aşağıdaki gibidir:

1. İTÜ'deki öğrenci otomasyon sistemi kullanıcıların sisteme erişimi için Tek İmza (Tİ) kullanmaktadır. Tek imza yönteminde, hedef, kullanıcının tek kullanıcı adı ve parolası ile erişim yetkisi olduğu tüm sistemlere giriş yapabilmesini sağlamaktadır. Bu hedefe ulaşabilmek için orta bir kimlik denetim birimi bulunmaktadır. Aslında bu birim parolaları şifrelenmiş ve güvenli biçimde saklamak amacıyla tasarlanmış bir donanımdır.

   Kullanıcı adı ve parolası donanım tarafından doğrulanan kullanıcıya yarım saat süreyle geçerli olmak üzere bir yetkilendirme bileti atanmaktadır. Bu bilet sayesinde kullanıcı diğer sistemlere de giriş yapabilir ve bilet, yarım saat sonunda kullanıcının sistemde aktif ya da pasif olması durumuna bakmaksızın kullanıcıyı sistemden atmaktadır.
2. Öğrenci otomasyon sisteminin veri tabanı yönetimi, sistem ile ilgili hiçbir sorumluluğu olmayan başka bir departmana ait bir çalışandır. Dolayısıyla herhangi bir problem durumunda da hiçbir sorumluluğu bulunmayacaktır.
3. Not değişikliğini yapan kullanıcılar tamamiyle anonimdirler. Sistemde bir işlem yapıldığında bunu net olarak kimin yaptığı bilinememektedir. Aynı yetkiye sahip olan kullanıcılara aynı kimlik değerleri verilmiştir.
4. Uzaktan erişim de aynı şekilde anonimdir.
5. Parola değiştirme ve üretme konusunda bir politika ve uygulama bulunmamaktadır. Tüm sistemin temel politikası insana güven üzerine kuruludur.

İncelemeye, ilk olarak kurum içi bilgi sisteminin yapısını tanımayla başlanmalıdır. Kurum içi bilgi sistemlerine zaman içinde sürekli eklemeler yapıldığı için, donanımların görev ve işlevleri unutulabilmektedir. Bu nedenle, sistem içindeki tüm donanımların ve yazılımların konumları ve işlevleri ortaya konmalıdır. Bu öğrenme aşamasının ardından, bilgi güvenliğini artıracak birimler konusunda çalışmalar yapılmalıdır. Bu bağlamda, İTÜ Otomasyon Sistemi için incelemeler yapılmış ve bu incelemeler sonucunda, muhtemel güvenlik açıklıklarının olabileceği yerler saptanmaya çalışılmış, ileride güvenlik sorunu yaşanmaması için alınması gereken önlemler yöneticiye bildirilmiştir. Bu önlemler ve standartların belirlenmesi aşamasında ISO 27001 politikalarından ve 27002 yönergelerinden yararlanılmıştır. Bu politikaların üniversite için bir zorunluluğu yoktur, ancak bu politikalar üniversiteye uyarlandığında daha güvenli bir sistem elde edilecektir. Bu bölümde sorulan sorular ve öneriler açıklanacak ancak verilen cevaplar kötüye kullanımı engellemek için yazılmayacaktır.

Sistemi daha iyi anlayabilmek için sorulan sorular ve öneriler ISO 27001 politikaları ve 27002 yönergeleri temel alınarak sınıflandırılmıştır.

3.1 Kullanıcı Güvenliği

1. Oturum açma yetkilendirme biletinin güvenliği var mı?
   Sistemde oturum açılmak istendiğinde kullanıcı 3. parti bir oturum açma mekanizmasına yönlendiriliyor. Kullanıcı adı ve parolanız bu mekanizma tarafından onaylandıktan sonra, sisteme kendi yetkilendirmenizle erişiyorsunuz. Sıradan bir kullanıcı olarak gördüğümüz bu kadar ancak sistemi kötüye kullanmak isteyen birisi öncelikle trafiği kontrol edip verilerin şifreli mi şifresiz mi gittiğiniz kontrol edecektir; ya da bir hesapta oturum açıldıktan sonra aynı URL'yi başka bir web tarayıcısında açmak isterse, oturum açma mekanizmasını atlatıp atlatamayacağını kontrol edecektir. Eğer bilet her kullanıcı için bir değer kullanıyorsa ve bu değeri değiştirip başka bir kullanıcının yetkileri ile sisteme giriş yapabiliyor mu bunu kontrol edecektir.
2. Öğretim üyesi, öğrencisinin yokluğunda danışmanı olduğu öğrencinin ders kaydında değişiklik yapabilir mi?
   Lisans üstü öğrencileri ders alma işlemini, danışman hocasının ve öğrencinin kendisinin kullanıcı adı ve parola girdiği bir sistem üzerinden

gerçekleştirmektedir. Yani eğer hocanın ya da öğrencinin bilgileri eksik olursa ders alınamıyor olması gerekmektedir. Eğer bu sistem bir şekilde atlanabiliyorsa yani eğer öğretim üyesi öğrencisinin yokluğunda ders kaydı üzerinde değişiklik yapabiliyorsa; öğretim üyesi öğrencinin yokluğunda öğrencinin hakları ile oynayabilir.

3. Yetkililerin parola değiştirme politikaları var mı? Varsa nedir?

   Bir parola ne kadar uzun süre kullanılıyorsa, bilinmelidir ki saldırganca bulunma olasılığı da bu kadar fazladır. İyi bir parolanın nasıl olacağını anlatmak için, önce bir parolanın nasıl başka ellere geçebileceğini açıklamak gerekiyor ve buna sebep olabilecek çeşitli durumlar bulunmaktadır: Birincisi saldırgan hedef kullanıcıyı tanıyan ya da onunla ilgili bilgi toplamış birisi olabilir. Bu sayede elektronik postasının parolasını tahmin edebilir ve hesabına ulaşmak için "parolamı unuttum" seçeneğini kullanabilir. İkinci durumda ise hedef kullanıcı deneme yanılma saldırısına kurban gidebilir. Saldırgan bir grup kullanıcının parolalarının bulunmasına ya da sadece hedef bir kullanıcınınkini bulmaya odaklandıysa, deneme yanılma saldırıları ile tüm muhtemel parola kombinasyonlarını deneyerek hedef kullanıcının parolasına ulaşabilecektir. Daha iyisi eğer hedefteki kullanıcı ile ilgili elinde yeterli bilgi varsa tüm kombinasyonları denemesine gerek kalmadan, belli bir küme için çalışarak parolaya erişecektir. Son olarak da Heart-bleed gibi bir açıklık çıkmış ve bu açıklık kurumun sistemini de etkiliyorsa, sistemdeki tüm kullanıcılar bu açıklığı kullanan saldırganların parolalarını elde etmelerinden etkileneceklerdir. Tüm bu nedenlerden dolayı parola periyodik olarak değiştirilmelidirler ve bu periyod parola sahibinin bilgi erişiminin önem seviyesine göre kısa ya da uzun olmalıdır. Parolanın değiştirilmesi gerektiğinde mutlaka kullanıcıların kendileri tarafından ve kendi makineleri üzerinden değiştirilmelidir. En yetkili kullanıcı (*super user*) parolasının kesinlikle kimseyle paylaşılmaması ve belli sıklıklarla değiştirilmesi gerekmektedir. Ancak son parola kapalı bir zarf içerisinde daire başkanlığına teslim edilmelidir ve bu güvenli bir şekilde kasada saklanmalıdır. Veri tabanı yöneticisi kesinlikle parolasını kimseyle paylaşmamalı ve belli sıklıkta değiştirmelidir. Son parolası da kapalı bir zarf içerisinde daire başkanlığına teslim edilmelidir. Yetkililer kesinlikle parolasını kimseyle paylaşmamalı ve

belli sıklıkta değiştirmelidir. Son parolası da kapalı bir zarf içerisinde daire başkanlığına teslim edilmelidir.

4. Aynı parola 1 yıl içinde birden fazla kez kullanılabiliyor mu?

   Parolanın periyodik olarak değişiminin gereği beraberinde fayda getirdiği kadar zarar da getirmiştir. Bu zararlardan birisi de kullanıcıların 1 yıl içerisinde daha önce kullandıkları eski parolalarını ya da daha kolay hatırlamak amacıyla zayıf parola kullanmalarıdır. Zayıf parola kullanımı saldırganın işini kolaylaştıracağı için zararlıdır. Bilinen en iyi kriptografi ve güvenlik uzmanlarından biri olan *Bruce Schneier*'a göre; "hatırlanabilen parola kırılabilirdir", bu mantıktan yola çıkarak eğer 1 yıl içerisinde kullandığımız eski parolalarımızdan birisini kullanabiliyorsak, o parolanın kırılma olasılığının da oldukça yüksek olduğunu bilmemiz gerekiyor. Çünkü kullanıcı bu parolayı başka her hangi bir sistemde kullanmamış ya da parola tüm iyi parola şartlarını taşıyor bile olsa, o dönemde kullandığı sistemin parola bilgilerinin sızmadığından emin olamaz. Bu yüzden eğer mümkünse, sistem desteği ile 1 yıl içerisinde kullanılan bir parolanın bir daha kullanılmaması değilse de, kullanıcının kendisinin bunu yapması gerekmektedir.

5. Kullanıcı adı ve parola deneme sınırlaması var mı? Öğrenci, öğretim üyesi ve yetkililer için bu sınırlama aynı şekilde mi çalışıyor?

   Kullanıcı adı ve parola sisteme girişte tüm kullanıcıların giriş için kullandıkları kimlikleridir. Bu kimlik kullanıcının sistemdeki yetkisini belirtmektedir. Bu yüzden de özellikle yüksek yetkiye sahip olan kullanıcıların kullanıcı adı ve parola bilgileri hem kullanıcının kendisi hem de sistem tarafından mümkün olan en yüksek koruma yöntemiyle korunmalıdır. Sistemin bu noktada yapabileceği şeylerin başında da kullanıcı adı ve parola deneme için bir sınır belirlemesi geliyor. Özellikle bu sınırın sistemin yüksek yetkilendirme derecesine sahip olanlar (örn; yazılım geliştiricileri, bilgi işlem çalışanları vs.) için koyulmadığı düşünülürse, saldırganın çeşitli giriş sistemi kırma yöntemleri (deneme-yanılma, güncellenmemiş veri tabanındaki açıklık vs...) ile o kullanıcıların hesaplarını ele geçirebilmesi kaçınılmazdır.

6. Veri tabanının bulunduğu sunucu ile alakalı bir güvenlik politikası var mı varsa nedir? Veri tabanı yöneticisi sayısı kaçtır?

   Sistem Yöneticisi, Denetim, Ağ, Güvenlik Enstitüsü'ne (SDAGE) göre veri tabanının bulunduğu sunucunun güvensiz ve güvenlik açıklıklarına sahip olması saldırganların giriş noktası olmasına sebep olacaktır. Bu yüzden sunucunun güvenliğinin sağlanması için bir güvenlik politikası olmalıdır. Bir sistemin ne kadar çok güvenliğe ihtiyacı varsa, o sisteme erişen kullanıcı sayısı o kadar az olmalıdır. Bu bakış açısıyla bakıldığında veri tabanı yöneticisi sayısı da olabildiğince sınırlı sayıda tutulmalıdır.

7. Yetkililer parolalarını başkaları ile paylaşıyorlar mı?

   Bir sistemde her kullanıcının kendisine özel parolası ve bu kullanıcıya uygun düzeyde yetkilendirmesi olmalıdır. Bu yüzden de sistemi kullanan yetkililer parolalarını birbirleri ile paylaştıklarında hem parola güvenliği politikasına uymamış; hem de sistemin güvenliğini tehlikeye atmış olurlar. Başka bir yetkilinin parolasına sahip olan birden çok çalışan varsa kurumda, birisinin sistemde bir suç işlemesi durumunda bu işlemi yapan yetkili belirlenemeyecektir.

8. Veri tabanının bulunduğu sunucu ile alakalı bir güvenlik politikası var mı varsa nedir? Veri tabanı yöneticisi sayısı kaçtır?

   Sistem Yöneticisi, Denetim, Ağ, Güvenlik Enstitüsü'ne (SDAGE) göre veri tabanının bulunduğu sunucunun güvensiz ve güvenlik açıklıklarına sahip olması saldırganların giriş noktası olmasına sebep olacaktır. Bu yüzden sunucunun güvenliğinin sağlanması için bir güvenlik politikası olmalıdır. Bir sistemin ne kadar çok güvenliğe ihtiyacı varsa, o sisteme erişen kullanıcı sayısı o kadar az olmalıdır. Bu bakış açısıyla bakıldığında veri tabanı yöneticisi sayısı da olabildiğince sınırlı sayıda tutulmalıdır.

9. Yetkililer parolalarını başkaları ile paylaşıyorlar mı?

   Bir sistemde her kullanıcının kendisine özel parolası ve bu kullanıcıya uygun düzeyde yetkilendirmesi olmalıdır. Bu yüzden de sistemi kullanan yetkililer parolalarını birbirleri ile paylaştıklarında hem parola güvenliği politikasına uymamış; hem de sistemin güvenliğini tehlikeye atmış olurlar. Başka bir yetkilinin parolasına sahip olan birden çok çalışan varsa kurumda, birisinin

sistemde bir suç işlemesi durumunda bu işlemi yapan yetkili belirlenemeyecektir.

10. Yetkili makine başından ayrıldıktan beli bir süre sonra program kendiliğinden kapanıyor mu?

    Günümüzde en az yetki düzeyine sahip çalışandan en üst düzey yetki düzeyine sahip çalışana kadar tüm çalışanlar gözlemlendiğinde makinesinin başından kalktıklarında programı kapatan ya da makinesini başka kullanıcıların erişemeyeceği durumda bırakıp giden çok az çalışan bulunduğunu görebiliriz. Bunun için önerilen çeşitli yöntemlerden bir tanesi de çalışanın makinenin başından ayrıldıktan belli bir süre sonra makinenin ya da programın kendiliğinden kapanmasıdır. Aksi bir durumda eğer makine de program da aynı şekilde açık kalmaya devam ederse, dışarıdan gelecek bir saldırganın o programa sanki yetkiliymiş gibi erişebileceği ve kötü işlemler yapabileceği bilinmelidir. Günümüzde en etkili saldırı yöntemlerden birisi sosyal mühendislik saldırı yöntemleri olduğu için, saldırgana karşı sistemsel olduğu kadar fiziksel olarak da önlem alınmalıdır.

11. Yetkililerin uzaktan erişim hakkı var mı?

    Yetkililer kurum içerisinde çalışırken kendi bilgisayarları üzerinden eriştikleri program üzerinden çalışmaktadırlar. Bu programa dışarıdan erişimin olması güvenlik sorunlarını da beraberinde getirebilir. Örneğin; zararlı üçüncü parti yazılımlar kritik uygulamalara erişim sağlayabilirler ve ya bağlantıyı sağlayan yazılımın ve ağ protokolünün zayıflıklarından yararlanarak hassas veriye erişim sağlayabilirler. Yanlış ayarlanmış bağlantı yazılımları yetkilendirilmemiş kullanıcının erişimine olduğu kadar kurumun bilgi kaynağında değişimlere de sebep olabilirler. Ya da uygun güvenliğe sahip olmayan sunucu sistemleri uzaktan erişim sağlayacak bir saldırgan sistemdeki açıklıklardan faydalanabilir [3].

12. Yetkililerin makineleri sahibi dışında başkaları tarafından da kullanılıyor mu?

    Özellikle Üniversite gibi ortamlarda zaman zaman çalışanlar çocuklarını ya da bir tanıdıklarını ofis ortamlarında misafir edebiliyorlar. Bu süreçte kullansın diye makineler sahipleri dışında her ne kadar çocuk da olsa bir yabancının eline emanet ediliyor. Bunun sonucunda da çoğu zaman bu durum kötü şekilde sonuçlanıyor. Özellikle çocuk durumunda oyunlar aracılığıyla

bir çok kötü niyetli yazılım kolay bir şekilde kullanıcı anlamadan bilgisayarına yerleşiyor. Bu yüzden yetkililerin makineleri sahibi dışında bir başkası ya da başkaları tarafından kesinlikle kullanılmamalıdır.

13. Yetkililerin makinelerinde öğrenci otomasyon sistemi dışında hangi yazılımlar bulunuyor? Makinelerindeki yetki dereceleri nedir?

    Yetkililerin çoğunlukla güvenlik farkındalığı olmayan çalışanlardan oluştuğu bir ortamda ve hatta farkındalığı olan kişiler olsalar bile, makinelerindeki yetki dereceleri mümkün olan en düşük düzeyde tutulmalı. Hiçbir şartta en üst düzey kullanıcı yetkilendirmesine sahip olmamalılar. Ayrıca, yetkililerin makinelerindeki yazılımlar da mutlaka kontrol edilmeli ve sistemin güvenliği için öğrenci otomasyon sistemi dışında keyfi hiçbir programın kurulmasına izin verilmemelidir. Eğer izin verilirse her yetkili bir bombaya dönüşür ve eninde sonunda günümüzde kurumların yeni belası fidye yazılımları ile baş etmek zorunda kalınabilir.

14. Not değişikliği bilgisini alan yetkili ve notları giren yetkili aynı kişiler mi?

    Notlar girildikten sonra, zaman zaman not değişikliği gerekli olduğu için öğrenci işleri bölümüne notları değiştirilecek öğrenci bilgisi ve girilecek yeni not gönderilmektedir. Bu değişiklik bilgisini alan ve notları giren yetkili aynı kişiler ise yetkilinin notu yanlış girmesi, listeye bir kişi eklemesi ve ya listeden bir kişi silmesi gibi durumlar gözden kaçacaktır. Bu yüzden bu iki iş görevler ayrılığı ilkesi temel alınarak iki ayrı kişi tarafından gerçekleştirilmelidir ki, yanlışlıklara sebebiyet vermesin ve iki kişi birbirini kontrol edebilsin. Bu noktada oluşabilecek problemler için daha farklı ve en doğru çözüm yöntemi de bu sürecin otomatize edilmesidir. Böylece yaşanabilecek herhangi bir problem durumunda kolayca çözüm üretilecektir.

    Önerilen sisteme göre öğretim üyesi not girişini bir web uygulaması üzerinden değil, masa üstü uygulaması üzerinden internete bağlı olmaksızın gerçekleştirecek. Sonrasında uygulama bunu EVA ya da XML formatına sayısal imzalı olarak çevirip, önce fakülte veri tabanına gönderecek, buradan da fakülte ve öğrenci işleri arasında şifreli bir bağlantı kurulacak ve not belgesi şifreli olarak öğrenci işlerine gönderilecektir. Öğrenci işlerinde şifresinden çözülen belge öğrenci işleri veri tabanına kaydedilecek, böylece hem fakültede hem de öğrenci işlerinde bir kopyası bulunan belgede herhangi bir değişiklik yapılırsa kontrol edilip anlaşılabilecektir. Mevcut kullanılan

sistemde yetki bileti alındıktan sonra, yetki biletinin kopyasını elde eden birisinin öğretim üyesi gibi davranması olasılığı vardır. Önerdiğimiz yapıda ise ilk olarak, notlar çevrim içi girilmediği için bu sorun ortadan kalkmış olacaktır. İkinci olaraksa, öğretim üyesinin girmiş olduğu notların bir kopyası kendisinde ve fakültesinde tutulacak olması, bu belgelerin sayısal imza ile imzalanmış olması, ileride ortaya çıkabilecek bir problemde yapılacak araştırmalarda kaynak niteliği taşıyabilir. Özellikle mezuniyet durumuna gelmiş bir öğrencinin gerçekten mezuniyet durumuna gelip gelmediği net bir şekilde ortaya çıkarılacak bu karşılaştırmalar da bilgisayar üzerinde yapılacağı için kısa sürede sonuç alınacağı açıktır. İleride bir yetkilinin öğrenci notlarını değiştirerek öğrenci için haksız bir işlem yapmasının da önü kesilmiş olacaktır.

Başka bir sistem de not düzeltme ya da mezuniyet durumu olan öğrencinin notlarını sorgulama için tasarlanmıştır. Bir öğrencinin notunun değiştirilmesi gerektiğinde bu işlem bir karar yazışması ile birlikte gerçekleştirilir. Bu yüzden not düzeltme işlemini gerçekleştiren öğretim üyesi not belgesini EVA ya da XML formatında, sayısal imzalı olarak fakülteye gönderir. Fakülte önce not değişimi için gelen yazışmayı kendi yazışma veri tabanına kaydeder, not belgesini de not için oluşturulmuş olan veri tabanına kaydedip, sonrasında not belgesini ve yazışmayı şifreleyerek öğrenci işleri ile arasında kurulan güvenli bağlantı aracılığıyla öğrenci işlerine gönderecektir. Öğrenci işlerinde yazışma delil olması için yazışma veri tabanına, not belgesi de öğrenci veri tabanına kaydedilecektir. Öğrencinin mezuniyet durumunda ise, hem fakülte veri tabanındaki hem de öğrenci veri tabanındaki notlar karşılaştırılır ve eğer ikisi birbirinin aynısı ise, "öğrenci mezun olabilir" bilgisi verilir. Bu noktada verinin güvenirliğini ve inkar edilemezliğini sağlayan mekanizma sayısal imza ile sağlanmıştır. Eğer farklılıklara rastlanırsa, "öğrenci mezun olamaz" bilgisi döner ve bu aşamada farklılık sorgulaması işlemleri başlatılır. Not düzeltme yazıları da elektronik belge haline getirileceği için yapılan tüm not değişikliklerinin de bir resmi tutanağı üretilmiş olacaktır. Bu tutanak hem fakültede hem de öğrenci otomasyon sisteminde tutulacağı için de bir araştırma sırasında karşılaştırma olanağına sahip olunacaktır. Böylece not girişi ve not düzeltme aşamaları güvenli hale getirilmiş olacaktır.

3.2 Veri tabanı ve Sistem Güvenliği

1. Kullanılan veri tabanının güvenlik derecesi nedir?

   Nato tarafından da kullanılan çok seviyeli erişim denetim modelinde güvenlik A,B,C,D olarak ana seviyelere ayrılmıştır. Ayrıca bu seviyelerin alt sınıfları da vardır. Buna göre, D seviyesi en düşük güvenliğe sahiptir; bu seviyenin alt sınıfı yoktur. C seviyesi; zararlı yazılım kullanmayan kullanıcılara karşı alınması gereken güvenlik engellerini tanımlar. Temel ilkesi, gerektiği kadar bilmeye dayanır. B seviyesinde; C sınıfında isteğe bağlı olan tüm kurallar zorunlu kılınmıştır. Erişimler, erişim denetim cetveline uygun olarak yapılır. A seviyesi ise her türlü saldırıya karşı koruma sağlayacak cinstendir.

   Amerika Savunma Birimi'nin (ASB) belirlediği bu standartlara göre Üniversite gibi bir kurumda en az B seviyesinde güvenlik olan veri tabanı kullanılması beklenmektedir.

2. Sisteme girişte robot denetimi var mı? Varsa robot denetimi yeterli mi? Optik Karakter Tarama (OKT) araçları ile deneme yapıldı mı?

   Bazı Sisteme giriş noktalarında kullanıcının bir robot mu yoksa insan mı olduğunu anlamak önemlidir. Aksi takdirde robotla parola denenmesinden Dağıtık Hizmet Dışı Bırakma Saldırısı (DHDBS) sebebiyle sayfanın kullanılamamasına kadar bir çok problem yaşanabilir. Daha önceki yıllarda öğrencilerin otomatik robotlarla ders seçim döneminde sisteme giriş yaptırmaya çalıştıkları bilinmektedir. Öğrencinin yaptığı şey aslında oldukça masum gibi görünse de bir saldırganın da bu sistemi kendi lehine kullanabileceğini düşünecek olursak, oldukça tehlikeli de bir açıklık olabilir. Bu yüzden mutlaka robot denetimi yapılmalıdır, denetim *captcha* aracılığıyla yapılıyorsa, OKT araçları ile captcha'nın güvenliği test edilmeli ya da güvenli olduğu bilinen captcha yazılımları kullanılmalıdır.

3. Oturum zaman aşımı kavramı sistemde nasıl çalışıyor? Son aktif kullanım zamanından itibaren zaman ölçümlemesi mi yapılıyor yoksa oturumun başladığı andan itibaren belli bir süre mi tanınıyor?

   Oturum zaman aşımı güvenliği sağlamak için önemli özelliklerden biridir. Sisteme giriş yapıldığında kullanıcıya bir oturum bileti verilir ve oturum zaman süresi bitene kadar bu biletle sistem içerisinde kullanıcı hareket

edebilir. Her kullanıcının bileti kendisine özeldir, o kullanıcıyı tanımaya yönelik bilgi ve kullanıcının oturumunu ne zaman başlattığı vs. gibi bilgiler içermektedir. Oturum zaman aşımının sistemde 2 farklı şekilde çalışma şansı bulunmaktadır. Bunlardan ilki kullanıcının sistemdeki aktif hareketine bakmaksızın belli bir oturum süresi belirleyip o süre dolduktan sonra oturumu sonlandırmak, diğeri de kullanıcının son aktif olduğu zamandan itibaren bir süre belirleyip o süre bitene kadar kullanıcı sistemde tekrar aktif olmazsa oturumu sonlandırmak şeklindedir. Günümüzde en çok kullanılan yöntem 2.sidir, yani kullanıcının sistemdeki son aktivite zamanından itibaren bir oturum süresi belirlenmesidir. Her iki durumda da oturum zamanı sona erdikten sonra kullanıcı tekrar kullanıcı adı ve parolası ile sisteme giriş yapmaya zorlanmalıdır.

4. Sistem yöneticisinin güvenlikle alakalı bir politikası var mı?

   Sistem yöneticisinin güvenlikle alakalı hem fiziksel hem de sistemsel politikaları olmalıdır, bu politikaların varlığı sistemde güvenliği mümkün kılacaktır. Politikanın olmaması bir güvenlik ihlali durumunda sisteme etkisini ve büyüklüğünü anlayamayacak, güvenlik risklerinin farkında olamayacak, gerekli önlemleri alamayacak ve hatta belki de güvenlik ihlalini fark edemeyecektir. Bu yüzden sistem yöneticisinin güvenlikle alakalı bir politikasının olması önemlidir.

5. Makinelere düzenli olarak virüs sınaması yapılıyor mu?
   Makinelerin güncel bir virüs programına sahip olması ve düzenli olarak virüs testinden geçirilmesi sistemin güvenliğinin devamlılığını sağlamak için gereklidir. Aksi bir durumda sistemdeki bir virüsün verileri değiştirmesi, yok etmesi vb. durumlarla karşılaşılabilir.
6. Sistemin yedekleri düzenli olarak alınıyor mu ve bu yedekler nerede tutuluyor?

   Sistemin yedeklerinin düzenli olarak alınması ve bu yedeklerin başka bir ortamda tutulması sistem kullanılmaz hale geldiğinde yedekten devam edilmesi açısından oldukça önemlidir. Kuruluşa ilişkin tüm bilgilerin saklandığı veri tabanlarının yedeklerinin alınması gerekir. Yedek bilgiler, bilgisayar odasında tutulmalı; olabildiğince uzak bir yerde saklanmalıdır.
7. Yıkımdan geri kazanım merkezi var mı?

Bilgisayar odasının başına gelebilecek büyük çaplı saldırı ya da afet sonucunda, bilgi sistemi çalışamaz duruma gelecektir. Böyle bir felaket durumunda, hizmetlerin sürdürülebilmesi için bir yıkımdan geri kazanım merkezinin kurulması gerekir. Yıkımdan geri kazanım merkezinin, ana bilgisayar odasından çok uzaklarda olması gerekir. Farklı bir kentte olması daha uygun olur. Her kuruluşun kendine özgü bir yıkımdan geri kazanım merkezi kurması ve bunu sürekli çalışır halde tutması çok maliyetlidir. Bu nedenle, birden çok kuruluşun birlikte kullanabilecekleri yıkımdan geri kazanım merkezinin kurulması yeğlenmelidir.

İTÜ gibi saygın ve toplumda yüksek bir kurumun ise öğrenci otomasyon sisteminin bir felaket durumunda çalışamaz duruma gelmesi kabul edilemez. Bu yüzden mutlaka yıkımdan geri kaznım merkezi kurulmalıdır.

8. Terminalden ana sisteme giderken aradaki bağlantıda şifreleme var mı?

   Bir sistemden diğer bir sisteme gönderilmesi gereken gizli bilgilerin güvenli bir şifreleme algoritması ile şifrelenmemesi gibi bir durumda saldırganın aradaki adam saldırısı yaparak verilere erişmesi mümkün olacaktır. Bu yüzden bağlantının mutlaka şifreli gerçekleştirilmesi gerekmektedir.

3.3 Uygulama Güvenliği

1. Yeni uygulamalar işletmeye alınmadan önce test ediliyor mu?

   Yeni uygulamalar işletmeye alınmadan önce test edilmesi programcının gözden kaçırdığı güvenlik açıklıklarının belirlenmesi ve kapatılması ile sonuçlanır. Böylece işletmedeyken oluşabilecek hatalar önlenmiş, saldırı giriş noktaları kapatılmış olur.

2. Mevcut uygulamaya bakım, destek ve güncelleme için kurum dışından kişilerin dışarıdan erişim, sistemi açıp kamapa hakları var mı?

   Kurum dışından kişilerin bakım, destek güncelleme için dışarıdan uygulamaya erişimine belli zamanlarda ve belli bir süre için izin verilmeli ve hemen ertesinde şifreler değiştirilmeli. Bağlandığı süre boyunca yapılan eylemlerle alakalı eylem tutanağı tutulmalı ve sonrasında yaptığı eylemler incelenmelidir. Dünyada görülen örneklerde dışarıdan alınan yazılım ve desteklerin her zaman tehlikeli olduğu ve kötü sonuçlar doğurduğu

bilinmektedir. Güncelleme yapan kişilerin sistem içerisine bir bomba koyabileceği ve ya belli verileri değiştirebileceği bilinmektedir.

3. Otomasyon sisteminin kullandığı ders ekleme-silme vs işlemlerinin gerçekleştirildiği program web tarayıcısı üzerinden mi çalışıyor?

   Masa üstü üzerinden çalışan programlar için bakılması gereken güvenlik açıklıkları başka, web tarayıcı üzerinde olduğunda başkadır. Bu yüzden bir uygulama üzerinde güvenlik kontrolü geliştirmek istendiğinde bu bilgiye de sahip olmak gereklidir.

4. UYGULAMA

İçerideki ve dışarıdaki kullanıcılardan kaynaklanan güvenlik açıklıklarını tespit etmek için kural tabanlı bir yazılım geliştirildi. Bu yazılım ile, Çizelge 4.1 ve Çizelge 4.2'deki kurallara göre kontrol gerçekleştirilip aykırılıkların varlığının ortaya çıkarılması amaçlanmıştır.

Çizelge 4.1 : Sistemi kullanan kullanıcıların örüntü diyagramı

Öğretim Üyesi	Bir öğretim üyesinin not değiştirme miktarının ortalamanın üzerinde olması Çok az not değişikliği yapan bir öğretim üyesinin çok not değiştirmesi durumu Bir dersin notlarının sınav döneminde çok sayıda değiştirilmesi Öğretim üyesinin not girişi işlemlerini kendisine tanınmış zamanın dışında yapıyor olması Öğretim üyesinin not girişlerini kendisine tanınmış zamanın dışında öğrenci işlerinde yapıyor olması
Öğrenci	Bir öğrencinin notlarında bir dönem içinde çok not değişikliği gerçekleşmesi Bir öğrencinin notlarında her dönem değişiklik gerçekleşmesi Bir öğrencinin notlarının not değiştirme miktarı az olan bir öğretim üyesinin dersinde de değişmesi Bir öğrencinin toplam eğitim hayatındaki not değişiklik miktarının ortalamanın üzerinde olması Öğrencinin her dönem gereğinden fazla ders alıp bırakıyor olması Öğrencinin ders bırakma işlemini sistemin seyrek kullanım zamanlarında yapıyor olması Öğrencinin ders kayıt işlemlerinin kendisine tanınmış zamanın dışında yapıyor olması
Yetkili	Bir yetkilinin bir öğrenci için ortalamanın üzerinde not değişikliği yapıyor olması Bir yetkilinin not veya ders değişimi için, farklı Internet Protocol (IP)'lerden giriş yapıyor olması Bir yetkilinin mesai saatleri dışında sistemde işlem yapıyor olması Bir yetkilinin ders kayıt işlemlerini kendisine tanınmış zamanın dışında yapıyor olması Bir yetkilinin ders bırakma işlemlerini kendisine tanınmış zamanın dışında yapıyor olması

Çizelge 4.2 : Sistemdeki derslerin örüntü diyagramı

Başarı ortalamasının genel ortalamaya uygunluğu
Başarı ortalamasının genel ortalamanın üzerinde olması
Başarı ortalamasının genel ortalamanın altında olması

Otomasyon sisteminden metin halinde eylem tutanağı alındı ve sqlite veritabanına aktarıldı. Buradaki aykırılıkları bulmak için Python dili ile bir karar destek yazılımı geliştirildi. Öncelikle normal davranış örüntüsü çıkarıldı, daha sonrasında aykırı davranışların tespiti yapılması amaçlandı. Ancak otomasyon tarafından sağlanan veri setindeki bazı veri tiplerinin anonim, bazı veri tiplerinin ise özel sonuçlara ulaştıracak tipte olmaması sebebiyle bazı aykırı davranış tespitleri yapılamamıştır.

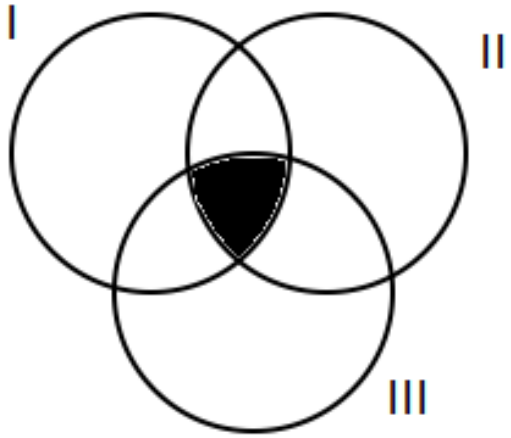
Karar destek yazılımının tasarımı 2 aşamadan oluşmaktadır:

1. Sistemi kullananların tamamının kullanım örüntüsünün çıkarılması:
   Çizelge 4.1'de görüldüğü gibi sistemdeki kullanıcılar için 4 adet grup belirlendi ve işlemler bu gruplara göre gerçekleştirildi. Ancak, "Bir yetkilinin ders bırakma işlemini kendisine tanınmış zaman dışında yapıyor olması", "Sistem ve veri tabanı yetkilisinin yetkilendirme değişikliği yapıyor olması", "Bir yetkilinin not veya ders değişimi için, farklı Internet Protocol (IP)'lerden giriş yapıyor olması" vs. gibi örüntüler otomasyon tarafından sağlanan veriler ile elde edilememiştir. Ayrıca sağlanan bazı sonuçlar gizlilik gereğince tez kitabı içerisine dahil edilmemiştir.
2. Derslerin örüntüsünün çıkarılması:
   Çizelge 4.2'de görülen örüntülerin çıkarılması amaçlanmasına rağmen otomasyon tarafından sağlanan veri setinde derslerin özelinde bir örüntü çıkartmaya yarayacak içerik bulunmamaktadır.

4.1 Olası Ders Satışlarının Tespiti

Bazı öğrencilerde bilinçli olarak fazla sayıda ders alıp menfaat ve ya dostluk karşılığında başka öğrencilere devrettiği şüphesi bulunmaktadır. Bu şüpheyi anlamak için Şekil 4.1'de görselleştirilmiş şekilde bulunan, şöyle bir algoritma teklif ediyoruz:

1. Öğrenci olduğu her dönemde hep fazla ders almış ve bırakmış öğrencileri bulunuyor.
2. En fazla 3 dakika arayla başkasına devredilmesi durumunda şüpheli görülen öğrenciler bulunuyor.
3. Hep aynı kişilere mi devredilmiş kontrolü yapılıyor.
4. Ayrıca bunlara ek olarak elimizde 5 dönemlik bilgi bulunduğu için bazı öğrencilerin mezun olup gitmelerine karşın bulunan şüpheli listesi kaç dönem öğrenci olduklarına göre de sıralanmıştır.



Şekil 4.1 : Muhtemel ders satışlarının tespiti

Yukarıda bahsi geçen algoritmanın akış diyagramı birbirini takip eden 5 ayrı fonksiyondan oluşmaktadır. Bu fonksiyonlar Şekil 4.3, Şekil 4.4, Şekil 4.5, Şekil 4.6 ve Şekil 4.7'de sırasıyla gösterilmiştir. İlk fonksiyon 5 dönem boyunca kayıt dönemleri içerisinde ders bırakan öğrencileri bulmaktadır. Sonrasında, bulunan öğrencilerin eldeki 5 döneme göre kaç dönem boyunca öğrenci oldukları bulunmuştur. Böylece sonuçta verilere göre öğrenci oldukları dönemler içerisinde ders bırakma işlemi gerçekleştirmiş öğrenciler elde edilmiştir. Bunu yapmaktaki sebep; mezun olup gitmiş, ama o dönemler içerisinde ders satışı da yapmış olması olası öğrenciyi de gözden kaçırmamaktır. Sonrasında, bu dönem değerlerine göre, öğrenci olarak bulunduğu her dönem mutlaka en az 1 ders bırakmış öğrenciler tespit edilmiştir. Son olarak da elde edilen listedeki öğrenciler dersi bıraktıktan en fazla 3 dakika sonrasında ders almış öğrenciler bulunmuştur. Böylece para karşılığı ders alışverişi yapmış olası öğrencilerin listesi çıkarılmıştır. Bu listeye göre 5 dönemde

23222 öğrenci içerisinden 1195 öğrencinin olası ders satışı yapmış öğrenciler olduğu ve 4390 öğrencinin de olası ders satın alan öğrenciler olduğu tespit edilmiştir.

Aynı kişiler ile en fazla 3 dk içerisinde ders bırakıp, alma işlemini gerçekleştirmiş olan öğrencilerin sayısı toplamda 652 iken, bu rakamın 235'i ders bırakan öğrencileri, 467'si de bırakılan dersleri alan öğrencileri içermektedir. Yine aynı kişiler ile farklı dönemlerde de ders alışverişi yapmış olan öğrencilerin sayısı 74 olup, bunun 35'i ders bırakan sınıfında, 42'si dersi alan sınıfındadır.

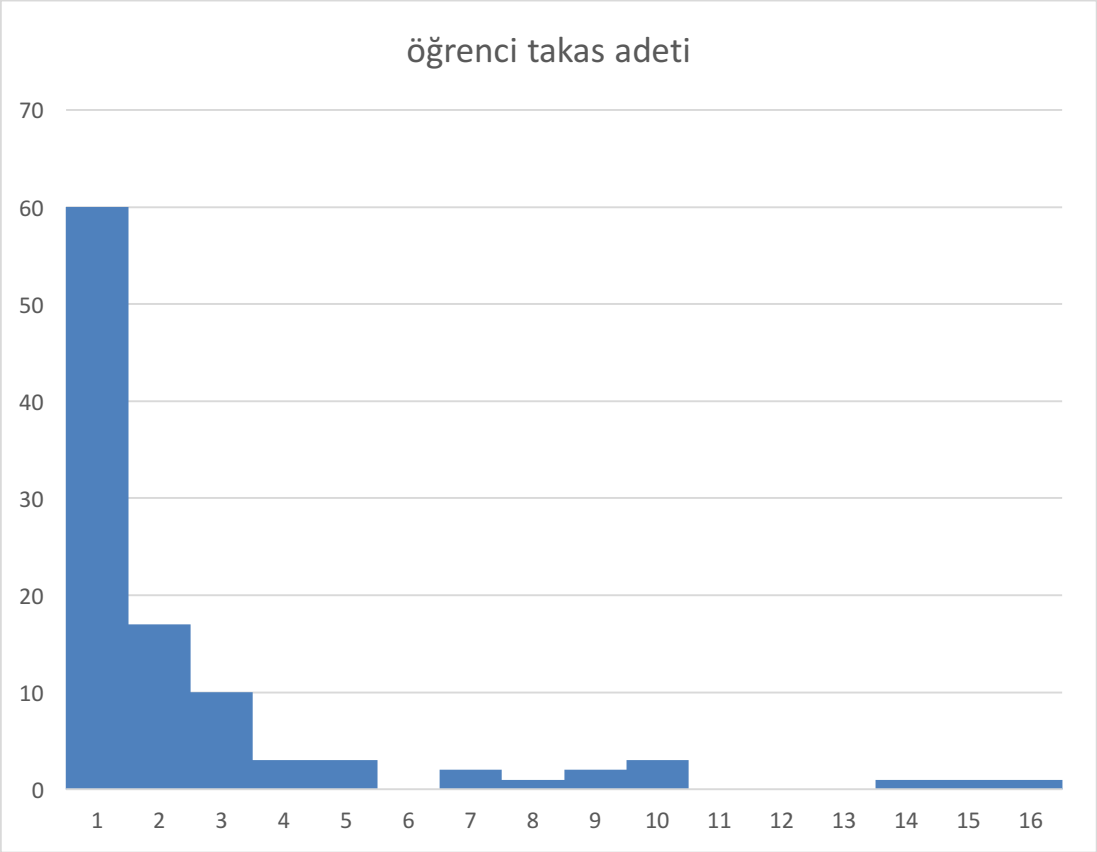
Bu olası liste bulunurken amaçlananlardan birisi de en çok hangi derste bu satış işleminin gerçekleştirildiğini bulmaktı. Ancak veri yapısı itibariyle ders bilgilerine erişim sağlanamadığı için ders bilgilerini temsil eden ve dönemlik olarak rastgele üretilen rakamlardan oluşan "crn" değeri kullanılmıştır. Bunun yanında bir diğer amaç en fazla hangi öğretim üyesinin dersinde ders satışı ve ders alımı olduğunu bulmak bulunuyordu. Ancak yine otomasyon tarafından sağlanan veri setinin yapısı içerisinde ders ve öğretim üyesi arasındaki bağlantı direk sağlanmadığı için dersin "crn"si ya da öğrenci bilgisi üzerinden dersi veren öğretim üyesi bilgisine ulaşılamamıştır.

Otomasyon tarafından sağlanan veri seti 5 dönemi içerdiği için o 5 dönem süresince hangi dönemlerde ne kadar olası ders satış işlemi gerçekleştiği bilgisi elde edilmiş ve Çizelge 4.3'te tablo olarak gösterilmiştir.

Çizelge 4.3 : Ders satma ve satın alma işlemleri yapmış olası öğrenci sayısının dönemlere göre dağılımı

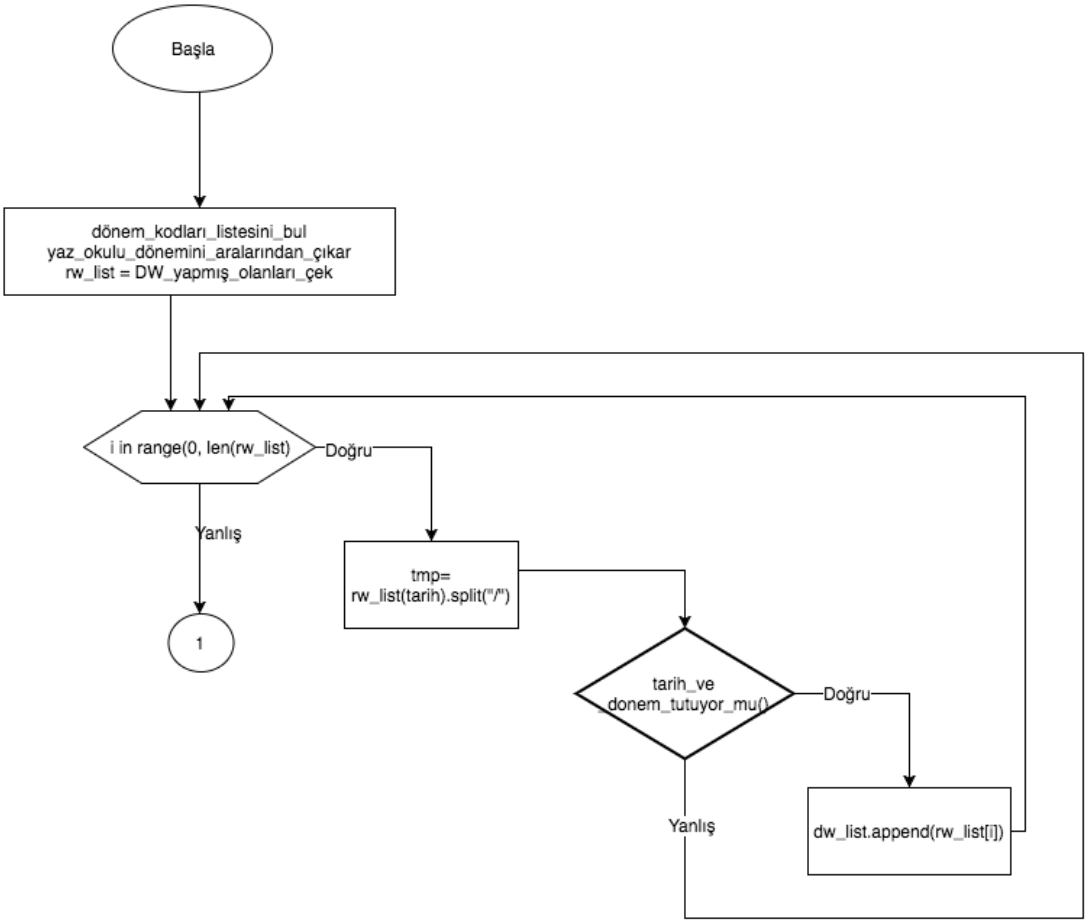
Dönem Kodu	Ders Satışı Yapması Muhtemel Öğrenci Sayısı	Ders Satın Almış Olması Muhtemel Öğrenci Sayısı
201510	597	1573
201520	646	1803
201530	36	75
201610	388	1055
201620	210	738

Çizelge 4.3'te gösterilen sonuçlara göre en çok olası ders alım satım işlemi 2015 yılının bahar döneminde; en az olası ders alım satım işlemi de 2015 yılının yaz okulu döneminde gerçekleşmiştir. Sonrasında bu işlemi takas yoluyla gerçekleştiren öğrenciler saptanmaya çalışılmıştır. Şekil 4.2'deki histogram değerlerine göre takas yoluyla ders alışverişi yapmış olası öğrenci sayısı ve takas grafiği gösterilmiştir.



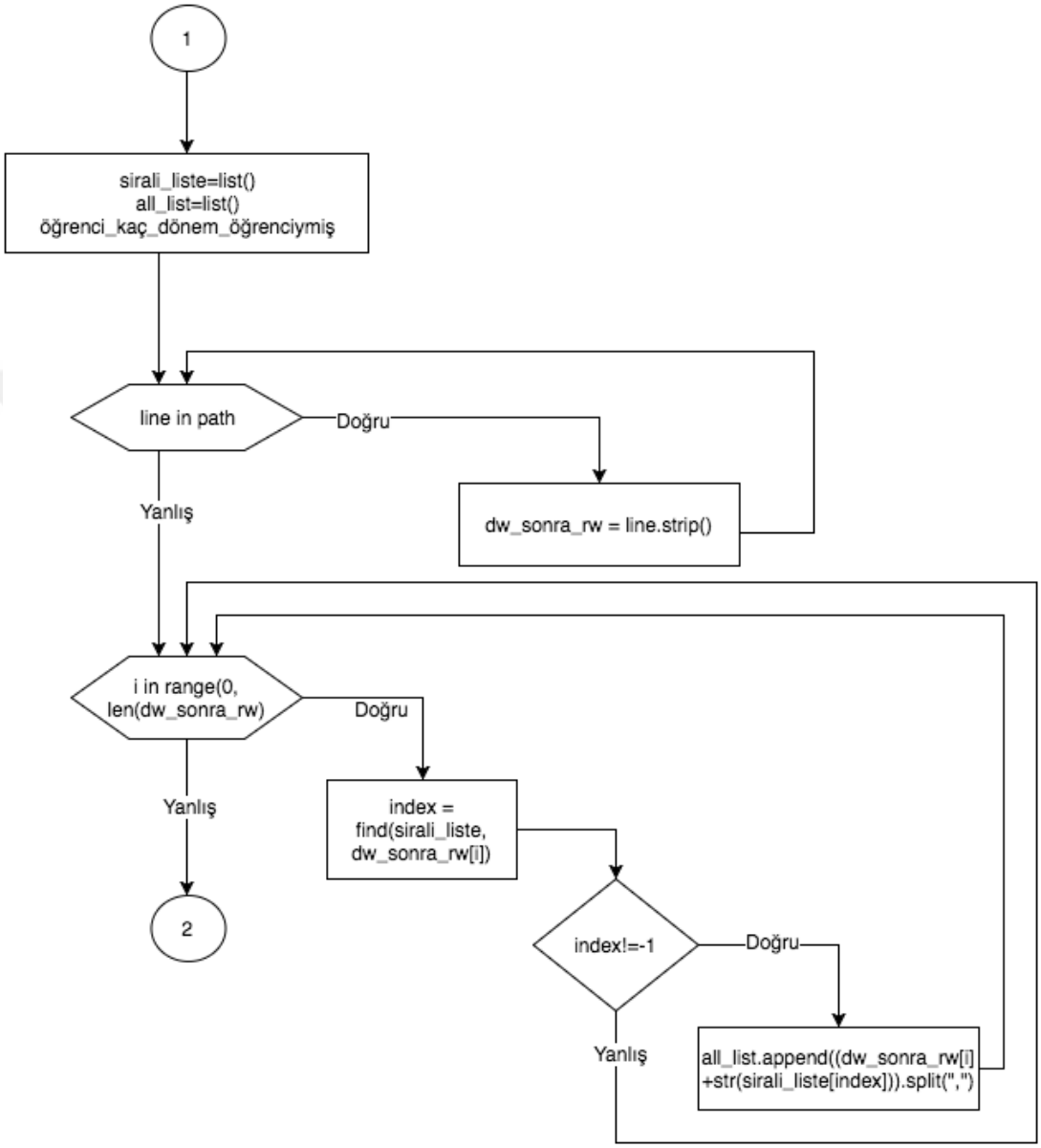
Şekil 4.2 : Takas yoluyla ders alışverişi yapmış olası öğrenci sayısı takas adeti grafiği

Bulunan olası liste üzerinden ders alış verişini takas yöntemi ile yapmış öğrencilere bakıldığında toplamda 104 öğrenci olası ders takası gerçekleştirmiş öğrenciler olarak bulunmuştur. Özellikle bazı öğrencilerin bu işlemi diğer öğrencilere oranla daha sık yaptıkları görülmüştür. Örneğin "MDMwMTEwMTE3" numaralı öğrenci 5 dönemde bu işlemi 16 kez gerçekleştirmişken, 60 adet öğrenci yalnızca 1 kez gerçekleştirmiş. Listede 1 kez gerçekleştirmiş olarak bulunmuş öğrenciler incelendiğinde, takas yaptıklarından şüphelenilen öğrencinin de yalnızca 1 kez eşleştiği öğrenci ile ders bırakıp alma işlemi yaptığı görüldüğü için liste daha da daraltılarak 2 defa olası ders takası yapmış öğrencilerden itibaren liste incelenebilir. Özellikle 16, 15, 14 gibi yüksek değerlerde olası ders takası yapmış olduğu tespit edilen öğrenciler ile alakalı olarak inceleme yapmak daha da süreci hızlandıracaktır.



Şekil 4.3 : Kayıt dönemi dersi bırakan öğrencilerin listesi

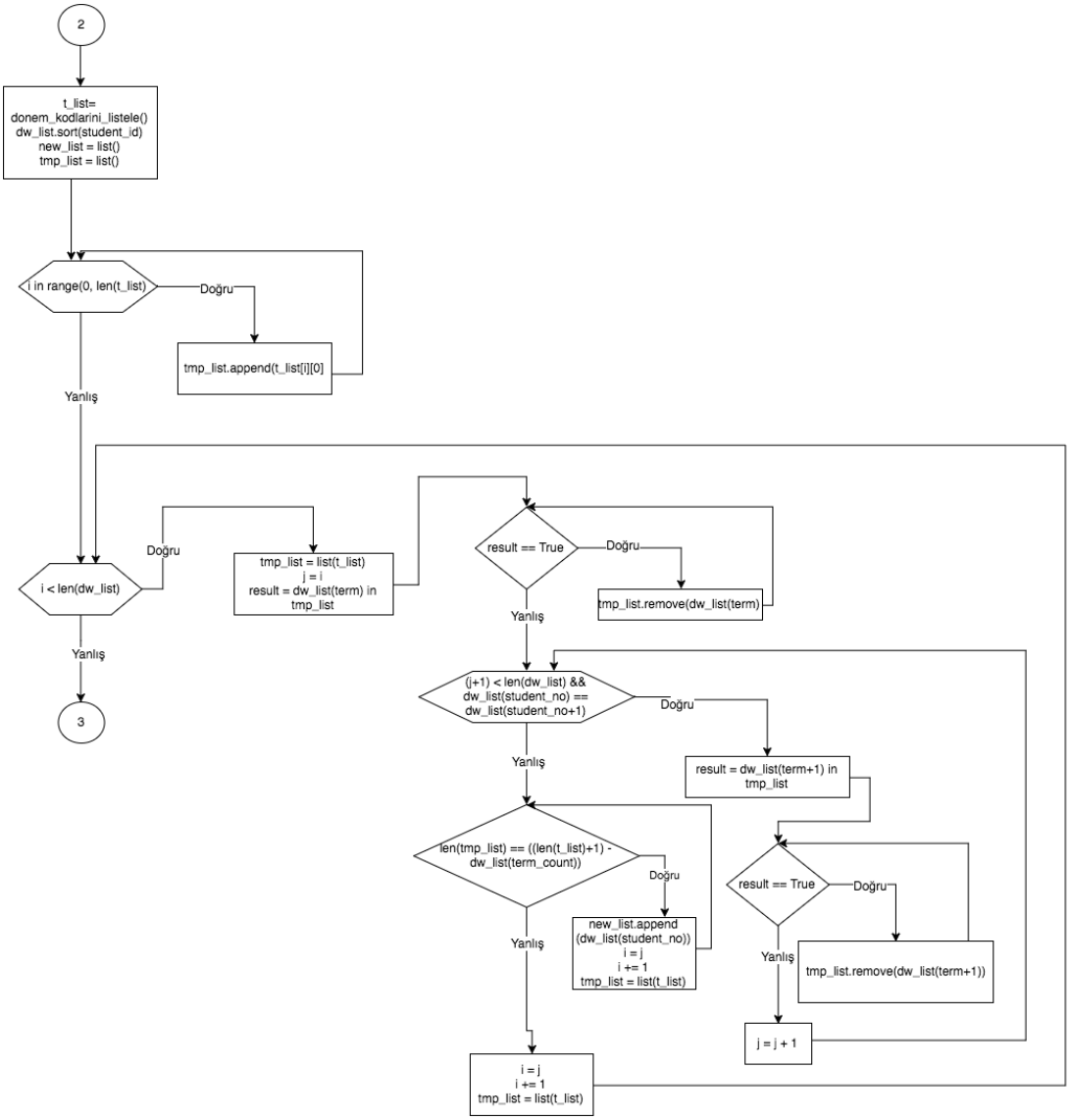
Şekil 4.3'de gösterilen algoritmaya göre kayıt dönemi içerisinde ders bırakan öğrencilerin listesi bulunmuştur. Bu liste ile 5 dönemlik veri setindeki kayıt dönemleri süresince en az 1 ders bırakmış tüm öğrenciler tespit edilmiştir. Ders satışının tespiti için başlangıçta ders bırakmış her öğrenci ilk şüpheli gurup olarak belirlenmiştir.



Şekil 4.4 : Öğrencilerin kaç dönem öğrenci oldukları listesi

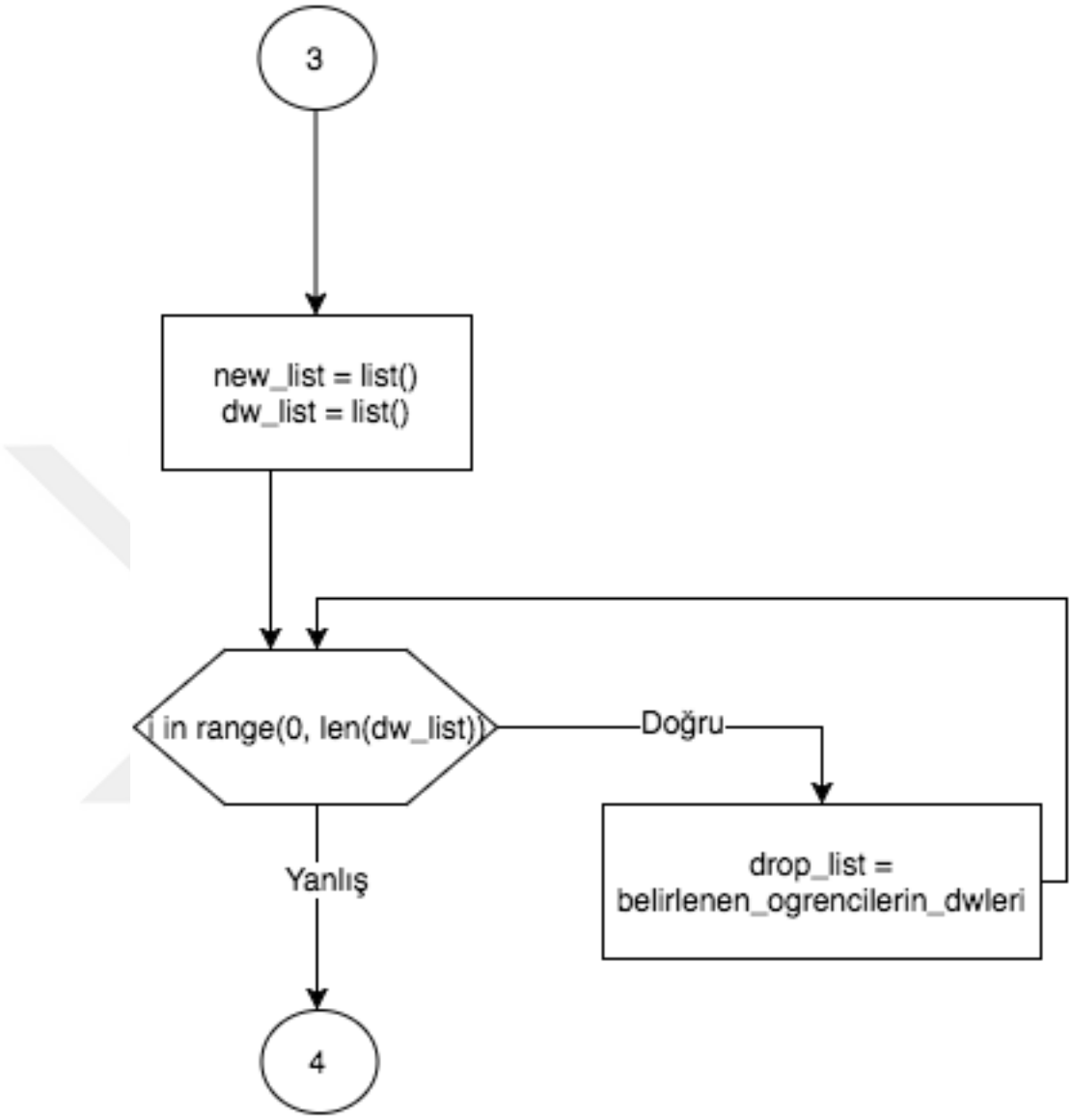
Şekil 4.4'te gösterilen algoritmanın akış diyagramına göre, en az 1 ders bırakanlardan oluşan öğrencilerin elimizdeki 5 dönemlik veri setinde ne kadar süre öğrenci oldukları bulunmuştur. Bunu yapmaktaki amaç, bu 5 dönem içerisinde mezun olmuş olmasına rağmen ders satış işlemi yapmış öğrencileri bulmaktır. Böylece olası ders satışı yapmış öğrencilerin listesi sadece veri setindeki 5 dönem

boyunca öğrenci olanlar değil, ayrıca bu süre boyunca 4, 3, 2 ya da 1 dönem boyunca öğrenci olmuş öğrencileri de kapsamaktadır.



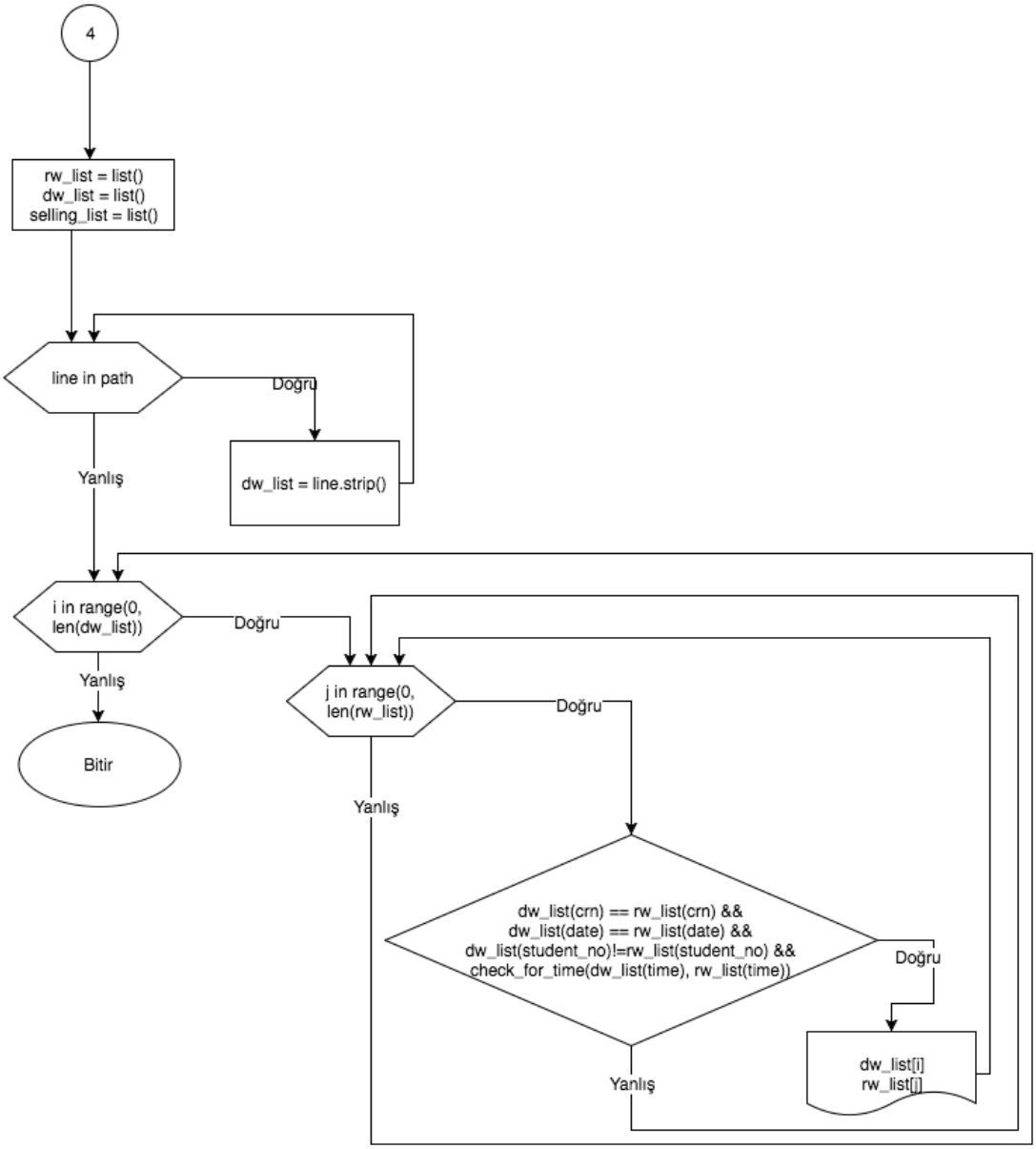
Şekil 4.5 : Öğrenci oldukları her dönem ders bırakmış öğrenciler

Şekil 4.5'te gösterilen algoritmaya göre bir önceki listeden gelen ders bırakmış ve 5 dönemlik veri listesinde kaç dönemdir öğrenci oldukları belli olan öğrenciler içerisinden, öğrenci oldukları sürece her dönem en az 1 ders bırakmış öğrenciler bulunmuştur. Bunu yapmaktaki amaç, kümeyi olabildiğince en olası ders satışı yapmış öğrenciler kümesine daraltmaktır. Böylece, kontrol edilmesi gereken daha az sayıda ama daha yüksek olasılıkla ders satmış öğrencilerin listesi elde edilmiştir.



Şekil 4.6 : Her kayıt döneminde ders bırakmış olan öğrenciler

Son olarak, Şekil 4.6'te gösterilen algoritma ile her kayıt döneminde mutlaka en az 1 ders bırakmış öğrenciler elde edilmiştir. Bu yolla, liste daraltılarak elde edilen verinin güvenirliği artırılmıştır. Bu algoritma sonunda elde edilmiş listede her kayıt döneminde mutlaka ders bırakmış, ders bırakma işlemini sistem üzerinden gerçekleştirmiş; ders satışı yapmış olması daha yüksek olasılıklı öğrenciler kalmıştır.



Şekil 4.7 : Ders bırakan öğrencilerin hemen arkasından ders alan öğrencileri listeleyen algoritmanın akış diyagramı

Son olarak Şekil 4.7'da gösterilen algoritmanın akış diyagramına göre, Şekil 4.6'da gösterilen algoritma üzerinden elde edilen listedeki öğrencilerin her biri eldeki ilk liste ile karşılaştırılmıştır. Karşılaştırma, Şekil 4.6'teki algoritma üzerinden elde edilen ders bırakmış öğrencilerin en fazla 3 dakika arkasından ders almış öğrencileri kontrol ederek, tüm bu öğrencileri listelemektir. Böylece, elde edilen son listede ders satışı yapmış olma olasılığı en yüksek olan öğrenciler bulunmaktadır.

4.2 Beklenenin Üzerinde Not Değişikliği Yapılan Dersler

Beklenenin üzerinde not değişikliği yapılmış olan dersler ya dersi veren öğretim elemanının dikkatsiz bir şekilde notlandırma yaptığı ya da Otomasyonun notları bilinçli ya da bilinçsizce değiştirerek girdiği anlamına gelebilir.

Bu çalışma ile bulunması amaçlanan derslerin bulunması ve bu işlemleri gerçekleştirenlerin kimliklerinin elde edilmesiydi. Ancak otomasyon tarafından sağlanan 4 dönemlik veri setine göre, sistem üzerinde aynı yetki düzeyine sahip yetkililerin ve öğretim üyelerinin aynı değer ile temsil edilmeleri nedeniye bu bilgiler elde edilememiştir. Toplamda 12041 ders içerisinden 1005 derste beklenenin üzerinde not değişikliği yapıldığı görülmüştür. Daha derin bir analiz için, Çizelge 4.4'te beklenilenin üzerinde not değişikliğinin değişiklik başlığına göre dağılımı gösterilmiştir:

Çizelge 4.4 : Beklenenin üzerinde not değişikliğinin değişiklik başlığına göre dağılımı

Değişiklik Sayısı	Başlık
9858	Eksik Not Girişi
1820	Fakülte Yönetim Kurulu Kararı(YKK)
1380	Otomasyon Düzeltmesi
224	Gelmeyen Eksik Not
91	Fen Bilimleri Enstitüsü YKK
32	Sosyal Bilimler Enstitüsü YKK
26	Bütünleme Sınavı
23	Mazeret Sınavı
17	Üniversite Kurulu Kararı
9	Enerji Enstitüsü YKK
7	Deprem Enstitüsü YKK

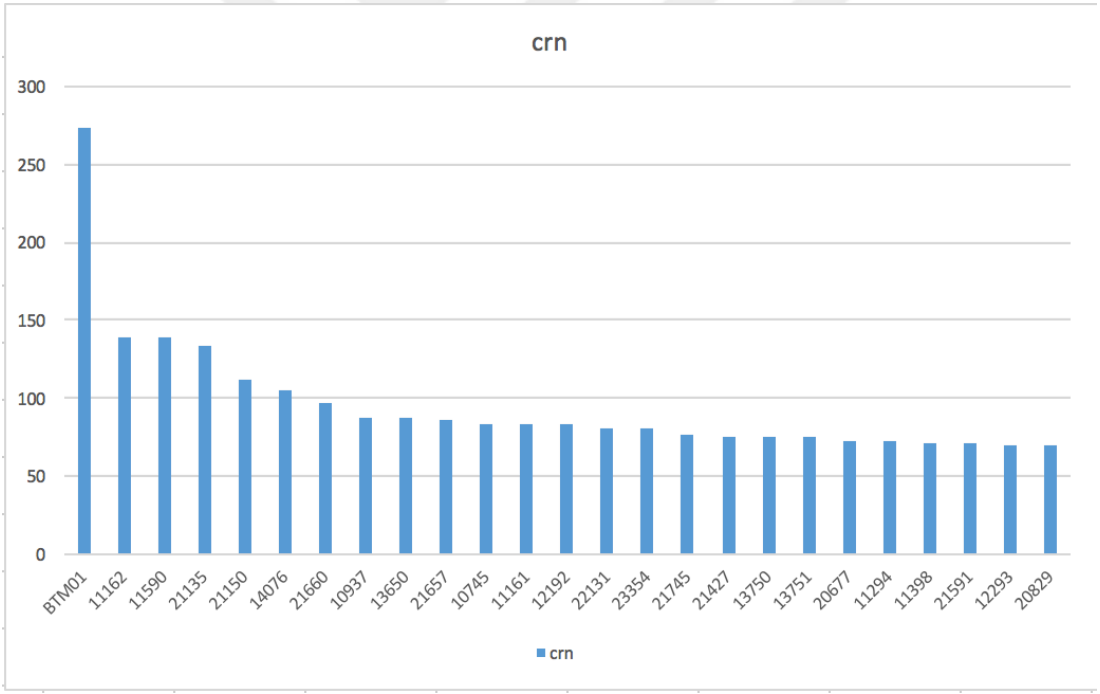
Çizelge 4.4'e göre beklenenin üzerinde not değişikliği gerçekleşen derslerin notlarının değişme sebepleri bulunmuştur. Buna göre, en fazla not değişikliği sebep "Eksik Not Girişi"dir. Bu sebepten anlaşılan şudur ki, öğretim üyelerinin bir kısmı notlarını zamanında girmeyerek, sonrasında işlemi Otomasyon'a giderek hallediyorlardır. Bir sonraki en yüksek değişiklik sebeplerinden biri olan "Otomasyon Düzeltmesi" de ayrıca dikkat çekmektedir. Çünkü, Otomasyon'un notlar üzerinde bir düzeltme yapması çok nadir gerçekleşmesi gereken bir durumken, yukarıda görülen tabloya göre oldukça sık gerçekleşmektedir. Bunun yanında hangi dönemde en yüksek, hangi dönemde en düşük değişikliklerin gerçekleştiği de araştırılmış ve Çizelge 4.5'te değişim miktarlarının dönemlere göre dağılımı gösterilmiştir.

Çizelge 4.5 : Beklenenin üzerinde gerçekleşen not değişikliklerinin yıl ve dönemlere göre dağılımı

Dönem Kodu	Değişiklik Sayısı
201510	4858
201520	5609
201530	682
201610	2431

Ayrıca dönem dönem yapılmış olan beklenenin üzerinde yapılmış değişikliklerin miktarı Çizelge 4.5'te gösterilmiştir. Buna göre en fazla beklentinin üzerinde değişikliğin gerçekleştiği dönem 2015'in bahar dönemidir. Bu değişikliklerin nedenlerinden birinin öğrencilerin mezun olması için notlarında değişiklik yapılması ihtimali olması, bu dönemi incelenebilir kılan etmenlerden biridir.

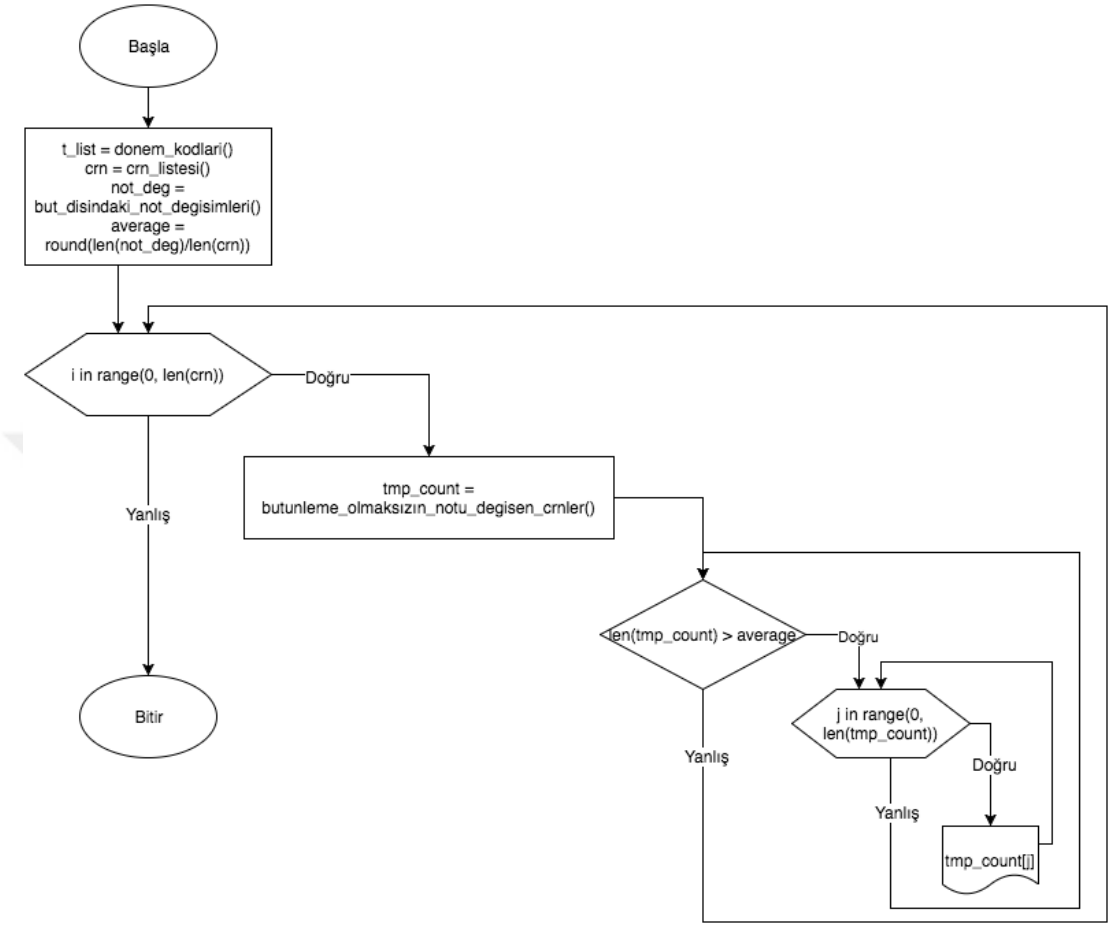
Ayrıca derslerin dağılımına da tek tek bakılmış ve beklenenin üzerinde not değişimi içeren ilk 25 ders Şekil 4.8'de gösterilmiştir.



Şekil 4.8 : Beklenenin üzerinde not değişimi içeren ilk 25 dersin dağılımı

Şekil 4.8'de beklentinin üzerinde not değişikliği gerçekleşmiş "crn" kodlarının ilk 25'i en yüksekten en düşüğe doğru sıralanmıştır. "Crn" kodları dersleri temsilen dönemlik olarak atanan rastgele sırada sayılardan oluşmaktadır. Bu aşamada amaç ders bilgilerini ve dersi yürütmüş öğretim üyesini de elde ederek, onlar üzerinde beklenenin üzerinde yapılan değişiklikleri ve sebeplerini de araştırmaktı. Ancak otomasyon tarafından elde edilen veri setinde derslerin "crn" kodları üzerinden

öğretim üyesine ve ders kodlarına erişmek mümkün değildir. Bu yüzden dersi yürütmüş öğretim üyesi ve dersin kodu ile ilgili yapılacak olan araştırmalar gerçekleştirilememiştir.



Şekil 4.9 : Beklenenin üzerinde not değişikliği yapılan dersler

Şekilde 4.9'de gösterilen algoritmanın akış diyagramına göre beklenenin üzerinde not değişikliği yapılan dersler, "crn" bazında bulunmuştur. "crn" ile "ders kodları" eşleştirmesi otomasyon tarafından sağlanan veri setinin yapısı gereği yapılamamıştır.

4.3 Beklenenin Üzerinde Derslerinde Not Değişimi Gerçekleşmiş Öğrenciler

Beklenenin üzerinde derslerinde not değişimi gerçekleşmiş öğrencileri bulmanın amaçlanmasının sebebi haksız yere notları değişen öğrenci bulunup bulunmadığını tespit edebilmektir. Bulunan listedeki öğrenciler için kesin olarak not değişimi aşamasında bir sahtecilik yaşanmış olduğu söylenemeyeceğine rağmen, küme daraltılarak incelemeye değecek bir öğrenci listesi elde edilmiştir. Öğrenci listesini veren algoritmanın akış diyagramı Şekil 4.11'de gösterilmiştir.

Toplamda incelemeye değer 868 öğrenci bulunmuştur. Bu öğrencilerde toplamda 4 dönemde yapılan not değişiklikleri gözlemelenmiş ve bazılarının özellikle her dönem notlarının değiştiği gözlemlenmiştir. Bu 868 öğrenciye ilişkin oluşturulan histogram Şekil 4.9'da gösterilmiştir:

Şekil 4.10 : Not Değişim miktarı beklenenin üzerinde olan öğrencilerin not değişim miktarı grafiği

Beklenenin üzerinde derslerinde not değişimi gerçekleşmiş öğrencilerin Şekil 4.9'da görülen histogramına bakıldığında, 4 dönem boyunca 9 defa notlarında değişiklik gerçekleşmiş tek 1 öğrenci bulunduğu, 8 defa not değişikliği gerçekleşen 19 öğrenci bulunduğu görülmüştür.

Her ne kadar beklenenin üzerinde notlarında değişiklik olan öğrencilerin sayısı az görünse de bu kadar çok notları değişmiş bu öğrencilerin not değişim sebeplerini incelemek doğru olacaktır. En fazla notunda değişiklik gerçekleşmiş olan öğrencinin notunu değiştiren kullanıcının kimliği araştırılmıştır. Ancak eldeki veri setinde aynı yetki düzeyine sahip olan kullanıcıların kimlikleri aynı değerle gösterildiği için kimlik tespit etme konusunda daha ileri gidilememiştir. Ancak not değiştirilme sebebi olarak "Eksik Not Girişi", "Fen Bilimleri Enstitüsü Yönetim Kurulu Kararı" ya da "Gelmeyen Eksik Not" notu düşüldüğü görülmüştür. Notlarına bakıldığında ise hemen her biri farklı dersler için gerçekleşmiş olan not değişimlerinde notlar "BA", "BB" ya da "AA" gibi yüksek harf notlarına güncellenmiştir. Listede kalan

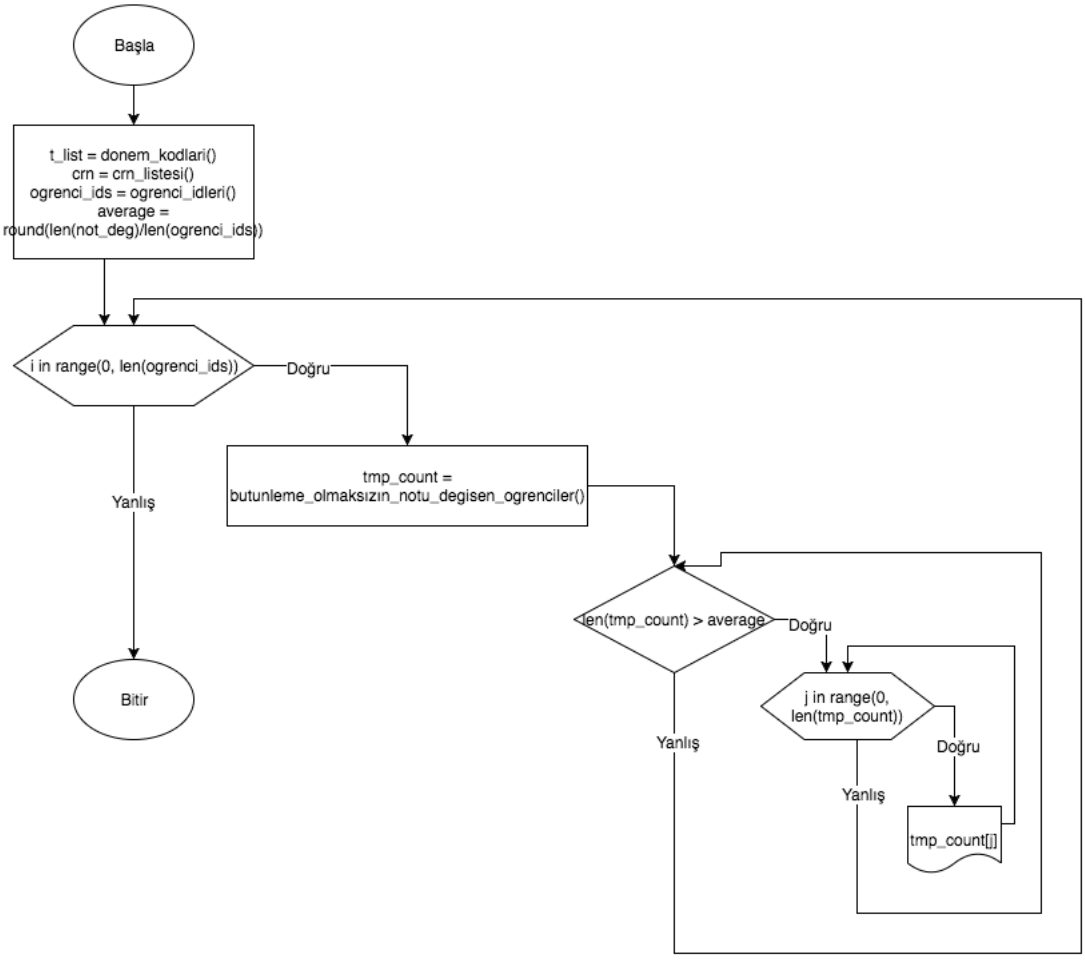
diğer öğrenciler de tek tek kontrol edildiğinde görülmüştür ki özellikle bazı öğrencilerin notları 9 değişim gerçekleşen öğrencininki gibi hep benzer nedenler başlığı altında, yüksek harf notlarına yükseltilmiştir. Bu da listedeki tüm öğrencilerin not değişimlerini kontrol etmeye değer kılmıştır.

Not değişimi gerçekleştiren yetkili kullanıcıları bulmak amacıyla not değişimi ve kullanıcıların dağılımını gösteren Çizelge 4.6 hazırlanmıştır:

Çizelge 4.6 : Not değişim işlemini yapan kullanıcı ve değişim adedi

İşlem Yapan ID	Not Değişimi Sayısı
WWW2_USER_CUS	2395
167	242
165	224
214	210
210	95
169	29
235	12
230	11
301	2
212	2
159	1
190	1
330	1
336	1
339	1

Çizelge 4.6'ya göre beklenenin üzerinde derslerinde not değişimi gerçekleşmiş öğrenciler için bu değişimi gerçekleştiren yetkililer bulunmuştur. Yetkililerin her birini tek tek kontrol edip bu değişimlerin en çok hangi yetkililer tarafından, hangi zaman dilimleri içerisinde gerçekleştirildiğini bulmak amaçlanmış; ancak otomasyon tarafından sağlanan veri setinin yapısı gereği yetkililerin özelleşmiş kimlik değerlerine ulaşılamamıştır. Veri setinde, sistemde aynı yetki düzeyine sahip yetkililer aynı kimlik değeri ile ifade edilmiştir.

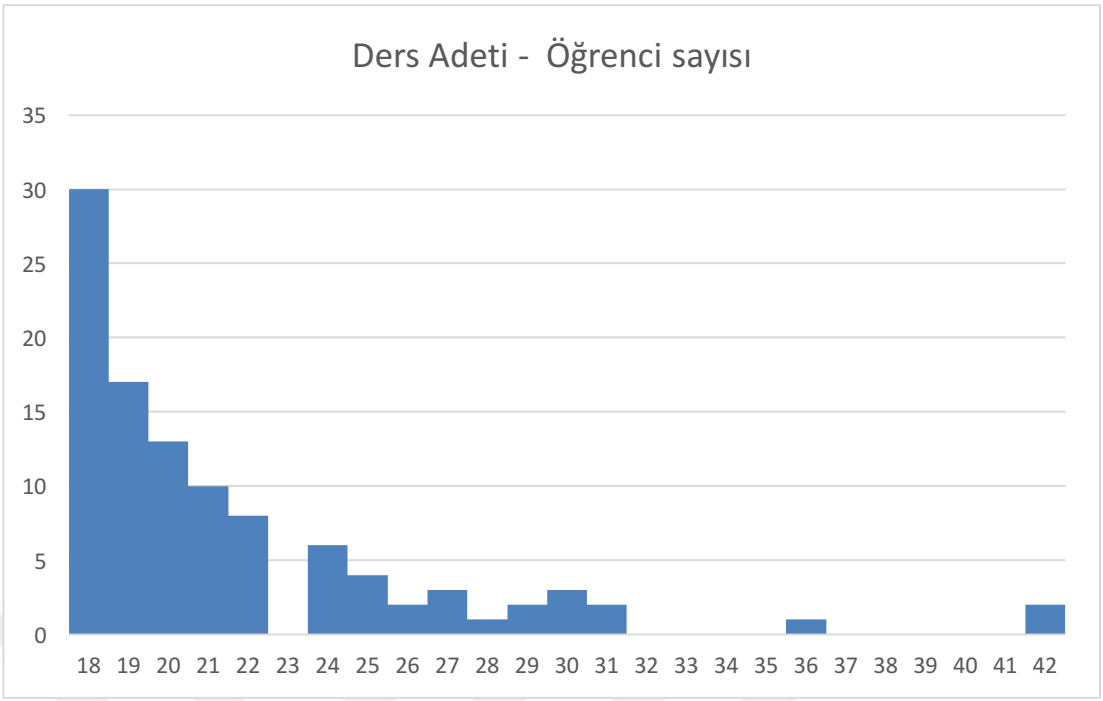


Şekil 4.11 : Not Ortalaması Beklenenin Uzerinde Olan Oğrencilerin Listesini Veren Algoritmanın Akış Diyagramı

Şekil 4.11'da gösterilen algoritmanın akış diyagramına göre beklenenin üzerinde derslerinde not değişikliği gerçekleşmiş öğrencilerin listesi elde edilmiştir. Listeye göre, veri setinin el verdiği ölçülerde çeşitli analizler gerçekleştirilmiştir. Şüpheli görülen durumlar rapor edilmiştir.

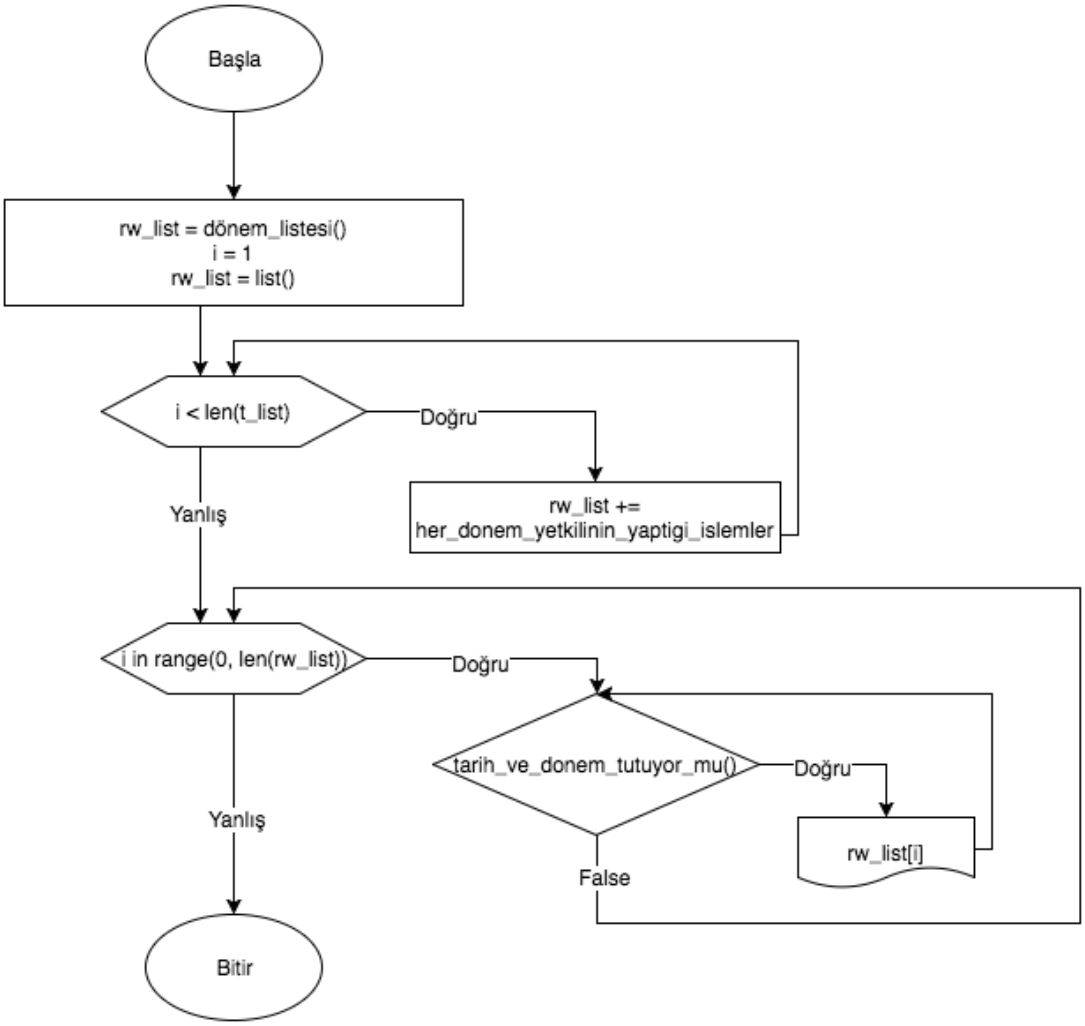
4.4 Yetkililerin Kayıt Tarihleri Dışında Gerçekleştirdiği Ders İşlemleri

Otomasyon içerisinde çalışan yetkililerin içerisinde öğrenciler de bulunduğu için kayıt tarihleri dışında gerçekleştirilen işlemler üzerinde incelemeye yapmaya değerdir. 5 dönem boyunca hakkında kayıt zamanı dışında işlem yapılan 14371 öğrenci Şekil 4.13'te akış diyagramı gösterilen algoritma ile bulunmuştur. Ayrıca, yetkililerin, kayıt tarihleri dışında öğrenciler için gerçekleştirdiği işlemlerin sayısal incelemesi de Şekil 4.12'de gösterilmiştir.



Şekil 4.12 : Yetkililerin kayıt tarihleri dışında gerçekleştirdiği işlem sayısı

Şekil 4.12'teki grafiğe göre yetkililer kayıt tarihleri dışında da oldukça fazla sayıda derse kayıt ve dersten silme işlemleri gerçekleştirmişlerdir. Grafiğe göre 2 öğrenci için 42 işlem gerçekleştirilmiştir. Bu öğrencilerden biri olan "MDEwMTQwOTM3" kimlik değeri ile gösterilen öğrencinin işlemlerinin çoğu 2015'in güz dönemi içerisinde gerçekleştirilmiş olup, sürekli olarak yetkililer tarafından farklı derslere kayıt edilip, o dersten silinmiştir. Daha sonrasında da en son aldığı ders için notu yine yetkililerce AA olarak güncellenmiştir. Bir sonraki öğrenci olan "ODIwMTQwMTA5" için de 2016 güz döneminde bir önceki öğrenci ile benzer işlemler gerçekleştirilmiştir. Son olarak da 36 işlem gerçekleştirilmiş olan "ODIwMTMwMjA3" numaralı öğrenci için 2016 güz dönemi içerisinde 8 ayrı ders için sık sık kayıt edilip dersten silme işlemi gerçekleştirilmiştir. Ancak bu işlemlerin kayıt dönemleri dışında gerçekleştirilmiş olması verileri incelemeye değer kılmaktadır.



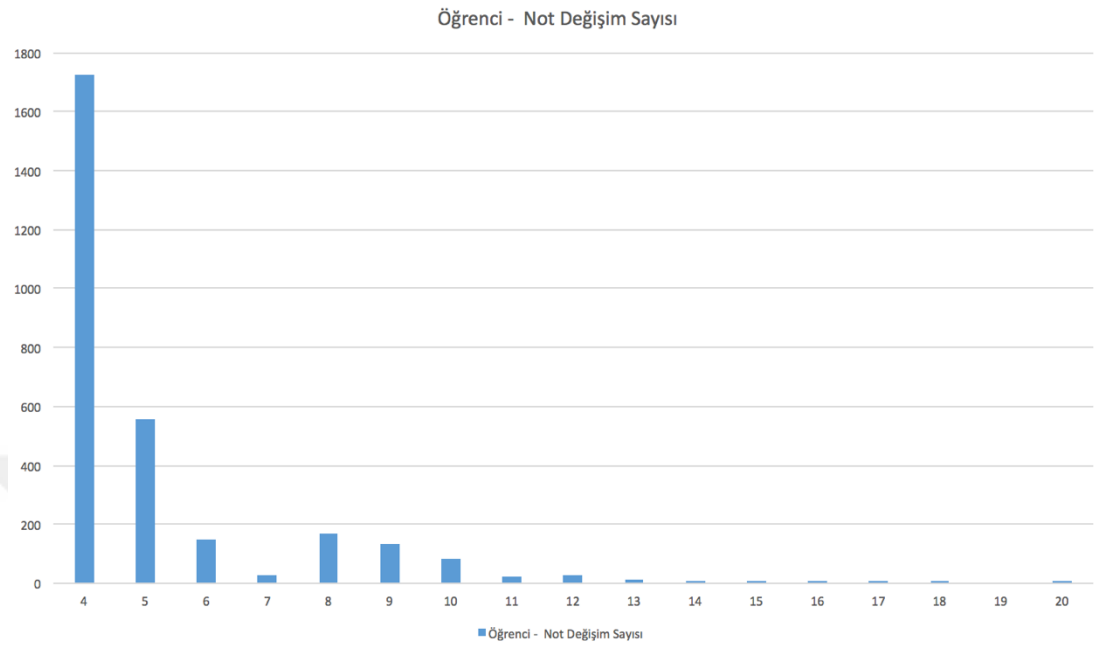
Şekil 4.13 : Yetkilinin, Kayıt Zamanı Dışında Gerçekleştirilen Ders Kayıtları ve Dersten Çekilmeler

Şekil 4.13'te gösterilen algoritmanın akış diyagramına göre yetkililerin, kayıt zamanı dışında gerçekleştirilen ders kayıt ve dersten çekilme işlemleri listelenmiştir. Dikkat çekici bazı şüpheli sonuçlar raporlanmıştır.

4.5 Yetkililer Tarafından Yapılan Beklenenin Üzerinde Not Değişikliği

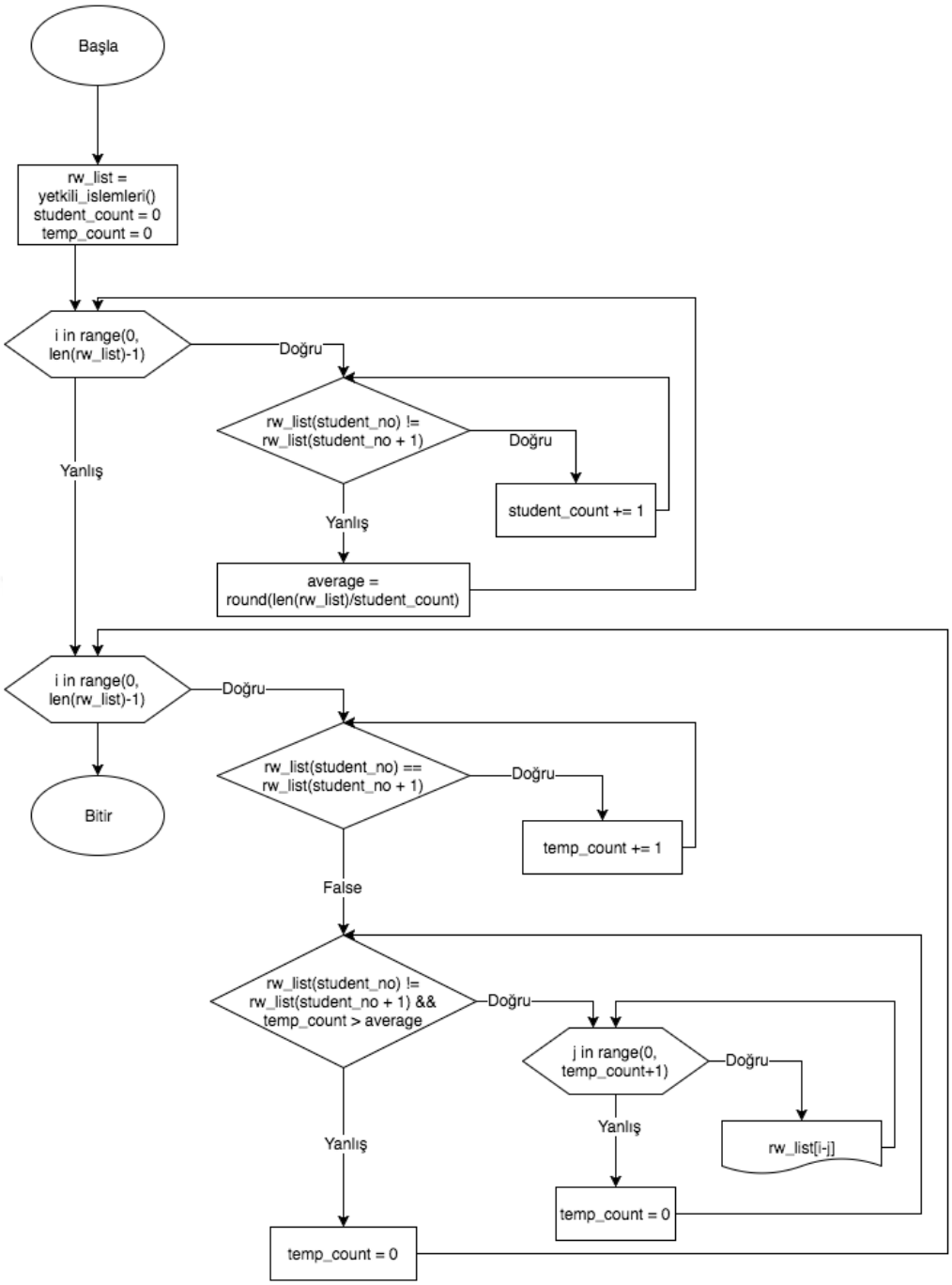
Not değişikliği işlemleri bir yazışma karşılığında yapılıyor. Ancak yazışmayı teslim alan ve notları giren kişiler aynı kişiler olduğu için ve notlar dijital ortamda değil fiziksel bir ortamda saklandığı için beklenenin üzerinde not değişikliği yapılmış öğrencilerin listesi de incelenmiştir. Listenin oluşturulması için Şekil 4.15'te akış diyagramı ile gösterilen algoritma kullanılmıştır. Bu çalışmanın yapılmasının en büyük sebeplerinden birisi sistemde, yetkili notları girdikten sonra, başka bir kişinin girilen notların yazışmada belirlenen kişiler olup olmadığına dair kontrolün

yapılmıyor olmasıdır. Buna dayanarak belirlenen liste üzerinden öğrenci not değişim grafi oluşturulmuş ve Şekil 4.14'te gösterilmiştir.



Şekil 4.14 : Beklenenin üzerinde notlarında değişiklik yapılmış öğrenci – not değişim grafiği

4 dönem boyunca 2917 öğrenci için beklenenin üzerinde not değişikliği yapılmıştır. 15099 adet beklenenin üzerinde değişiklik tespit edilmiş ve bu değişikliklerin 13917 adeti bütünleme sınavı sebebiyle yapılmıştır. Özellikle Şekil 4.14'ye göre toplamda 20 değişiklik yapılan 1 öğrenci bulunmaktadır; "MjcxMDYwNDY5" numaralı bu öğrencinin tüm not değişimlerinin bütünleme sebebiyle gerçekleştiğini ve tüm bu işlemlerin 2015 bahar ve güz dönemlerinde gerçekleştirildiği görüldü. Bu bilgiden daha derine gidilmesi amaçlanmış olmasına rağmen veri setinin içerdiği bilgilerin ayrıntı içermemesi sebebiyle amaçlanana ulaşılamamıştır. Yetkililer tarafından yapılmış beklenenin üzerinde not değişikliği işlemi gerçekleştirildiğinde, elde edilen listeden yüksek not değişikliği işlemleri gerçekleştirmiş yetkililerin listesine de ulaşmak amaçlanmıştı. Ancak, otomasyon tarafından sağlanan veri seti içerisinde aynı yetki düzeyine sahip kullanıcıların aynı kimlik değerine sahip olması nedeniyle, yetkililerin kimlik değerlerine ulaşılamadı.

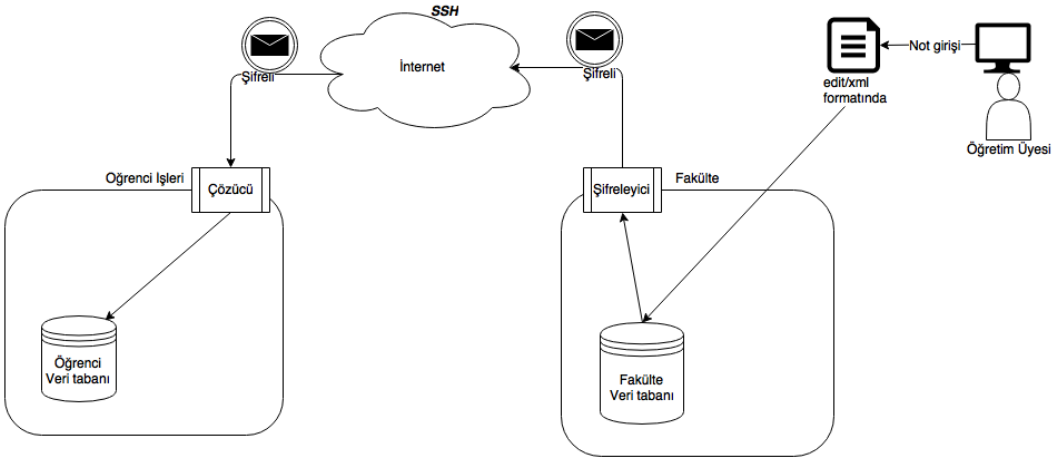


Şekil 4.15 : Yetkililer Tarafından Yapılan Beklenenin Üzerinde Not Değişikliği Yapılmış Öğrenciler

Şekilde 4.15'te bulunan algoritmaya göre yetkililer tarafından gerçekleştirilen beklenenin üzerinde yapılmış not değişiklikleri listesi öğrenci bazında bulunmuş ve incelenmiştir. Şüpheli görülen durumlar raporlanmıştır.

5. SONUÇ VE ÖNERİLER

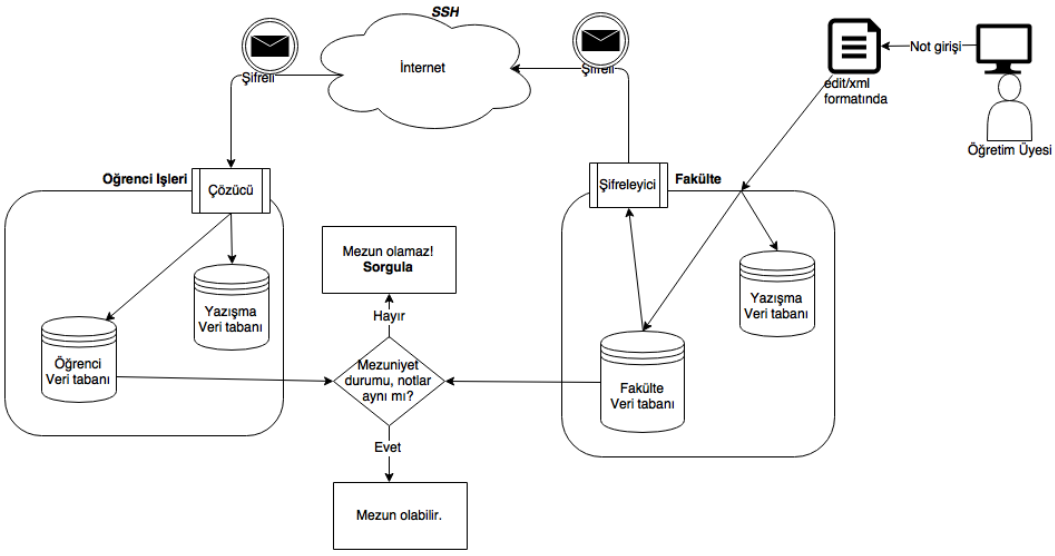
Güvenlik açıkları araştırılması kısmında belirlenen açıklar ve bunların nasıl giderilebileceği anlatılmıştır. Ayrıca bundan sonraki olası güvenlik açıklarını ortaya çıkarmak için de kural tabanlı bir yazılım hazırlanmış ve kullanım için sunulmuştur. Bunun yanı sıra ileride bir güvenlik problemi yaşanmaması açısından not girişi, not düzeltimi ve özellikle de mezuniyet aşamasındaki not kontrolünü daha güvenli hale getirmek için Şekil 6.1 ve Şekil 6.2'deki tasarımlar önerilmiştir:



Şekil 6.1 : Not girişi işlemi için geliştirilen sistem

Yukarıda önerilen sisteme göre öğretim üyesi not girişini bir web uygulaması üzerinden değil, masa üstü uygulaması üzerinden internete bağlı olmaksızın gerçekleştirecek. Sonrasında uygulama bunu EVA ya da XML formatında sayısal imzalı bir şekilde önce fakülte veri tabanına gönderecek. Buradan da fakülte ve öğrenci işleri arasında şifreli bir bağlantı kurulacak ve not belgesi sayısal imza ile imzalanmış ve şifreli bir halde öğrenci işlerine gönderilecek. Öğrenci işlerinde şifresinden çözülen belge öğrenci işleri veri tabanına kaydedilecek.

Böylece hem fakültede hem de öğrenci işlerinde bir kopyası bulunan belgede herhangi bir değişiklik yapılırsa kontrol edilip anlaşılabilecek. Sayısal imza göndericinin kimliğinin teyidini, oluşturulan elektronik dökümanın da orjinalliğini ve güvenirliğini mümkün kılacaktır. Mevcut kullanılan sistemde yetki bileti alındıktan sonra, yetki biletinin kopyasını elde eden birisinin öğretim üyesi gibi davranması olasılığı vardır. Önerilen yapıda ise ilk olarak notlar çevrim içi girilmediği için bu sorun ortadan kalkmış olacaktır. İkinci olaraksa, öğretim üyesinin girmiş olduğu notların bir kopyası kendisinde ve fakültesinde tutulacak olması, ileride ortaya çıkabilecek araştırmalarda kaynak niteliği taşıyabilir. Özellikle mezuniyet durumuna gelmiş bir öğrencinin gerçekten mezuniyet durumuna gelip gelmediği ortaya çıkarılacak bu karşılaştırmalar ile bilgisayar üzerinde yapılacağı için kısa sürede sonuç alınacağı açıktır. İleride bir yetkilinin öğrenci notlarını değiştirerek öğrenci için haksız bir işlem yapmasının da önü kesilmiş olacaktır.



Şekil 6.2 : Not düzeltme ve mezuniyet sorgusu için geliştirilen sistem

Şekil 6.1'de gösterilen sistem not girişi için tasarlanmıştı, Şekil 6.2'deki sistem de not düzeltme ya da mezuniyet durumu olan öğrencinin notlarını sorgulama için tasarlanmıştır. Bir öğrencinin notunun değiştirilmesi gerektiğinde bu işlem bir karar yazışması ile birlikte gerçekleştirilir. Bu yüzden not düzeltme işlemini gerçekleştiren öğretim üyesi not belgesini EVA ya da XML formatında yine sayısal imza ile imzalanmış şekilde fakülteye gönderir. Fakülte önce not değişimi için gelen yazışmayı kendi yazışma veri tabanına kaydeder, not belgesini de not için

oluşturulmuş olan veri tabanına kaydedip, sonrasında not belgesini ve yazışmayı sayısal imzalı olarak şifreleyerek öğrenci işleri ile arasında kurulan güvenli bağlantı aracılığıyla öğrenci işlerine gönderecektir. Öğrenci işlerinde yazışma delil olması için yazışma veri tabanına, not belgesi de öğrenci veri tabanına kaydedilecektir.

Öğrencinin mezuniyet durumunda ise, hem fakülte veri tabanındaki hem de öğrenci veri tabanında bulunan sayısal imzalı not belgeleri ve eğer notu değişmişse yazışma veritabanındaki not düzeltme yazıları karşılaştırılır ve eğer ikisi birbirinin aynısı ise, "öğrenci mezun olabilir" bilgisi verilir. Eğer farklılıklara rastlanırsa, "öğrenci mezun olamaz" bilgisi dönülür ve bu aşamada farklılık sorgulaması işlemleri başlatılır. Not düzeltme yazıları da elektronik belge haline getirileceği için yapılan tüm not değişikliklerinin de bir resmi tutanağı üretilmiş olacaktır. Bu tutanak hem fakültede hem de öğrenci otomasyon sisteminde tutulacağı için de bir araştırma sırasında karşılaştırma olanağına sahip olunacaktır.

Böylece not girişi ve not düzeltme aşamaları güvenli hale getirilmiştir. Sonrasında yetkili kullanıcıların davranışları ile ilgili aykırı davranışların saptanması ile alakalı çalışmalar yapılmış ve bunlar da 4. kısımda anlatılmıştır. Bundan sonraki dönemde yetkili kullanıcıların aykırı davranışlarını tespit edecek bir yazılım hazırlanıp teslim edilmiştir.

Temel güvenlik ilkesi gereği bizim çalışmamızla tüm güvenlik açıklarının bulunduğu söylenemez. Ayrıca yetkili kullanıcıların da davranışları ile ilgili olarak hiç eksiksiz bir yöntem geliştirdiğimizi iddia edemeyiz. Zaman içerisinde çıkabilecek yeni sorunları ortaya çıkartmak için temel olarak bizim çalışmamız kullanılarak yeni çalışmalar yapılabilir.

Tüm bunların dışında periyodik yedeklerin de alınması şart ancak bu yedeklerin bilgilerin sürekli olduğu bilgisayar ortamından uzakta bulunması lazım. Öneri olarak bilgi işlem daire başkanlığında değil öğrenci işleri otomasyon binasında tutulması gerekli. İTÜ gibi saygın ve toplumda yüksek bir kurumun öğrenci otomasyon sisteminin bir felaket durumunda çalışamaz duruma gelmesi kabul edilemez. Bu yüzden mutlaka bir Yıkımdan Geri Kazanım Merkezi kurulmalıdır.

KAYNAKLAR

[1] **Information Security.** Erişim: 20 ocak 2016, https://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/pdf/USCODE-2011-title44-chap35-subchapIII-sec3542.pdf

[2] **Burlu, K.** (2010). *Bilişimin Karanlık Yüzü*, Nirvana Yayınları

[3] *Information Assets*, Cobit 4.1 Chapter 4

[4] **Garfinkel, S.L., Beebe, N., Lishu, L., Maasberg, M.** (2013). Detecting threatening insiders with lightweight media forensics. *Technologies for Homeland Security (HST), 2013 IEEE International Conference on,* 86-92. doi: 10.1109/THS.2013.6698981

[5] **Parveen, P., Weger, Z.R., Thuraisingham, B., Hamlen, K., Khan, L.** (2011). Supervised Learning for Insider Threat Detection Using Stream Mining*, Tools with Artificial Intelligence (ICTAI), 2011 23rd IEEE International Conference*, 1032-1039. doi:10.1109/ICTA.2011.176

[6] **Ard, J. B., Bishop, M., Gates, C., Sun, M.,X.** (2013). Information Behaving Badly, *Proceedings of the 2013 workshop on New Security Paradigms Workshop,* 107-118. doi:10.1145/2535813.2535825

[7] **Kim, J., Grillo, J., M., Boxwala, A.,A., Jiang, X., Mandelbaum, R.B., …. Ohno-Machado, L.** (2011). Anomaly and Signature Filtering Improve Classifier Performance For Detection Of Suspicious Access To EHRs, *AMIA Annual Symposium Proc.*723-731.

[8] **Mardani, S., Shahriari, H., R.** (2013). A New Method For Occupational Fraud Detection in Process Aware Information Systems, *Information Security and Cryptology (ISCISC), 2013 10th Information ISC Conference*, 1-5. doi: 10.1109/ISCISC.2013.6767348

[9] **Hunker, J., Probst, C., W.** (2008). Insiders and Insider Threats An Overview of Definitions and Mitigation Techniques, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications,* 1(2), 4-27.

[10] **Bankacılık Düzenleme ve Denetleme Kurumu,** (2007). Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, *Resmi Gazete,* 26643

[11] **DoD Insider Threat Mitigation Final Report of the Insider Threat Integrated Process Team.** erişim:Mart 2011, https://acc.dau.mil/CommunityBrowser.aspx?id=37478

[12] **Anderson, R., H.** (1999). Research and development initiatives focused on preventing, detecting, and responding to insider misuse of critical defense information systems, *RAND Corporation, Tech. Rep. RAND CF-151- OSD*

[13] **Anderson, R., H., Bozek, T., Longstaff, T., Meitzler, W., Skroch, M., Wyk, K.,V.** (2000). Research on mitigating the insider threat to information systems#, *RAND Corporation, Tech. Rep. RAND CF-163-DARPA*

[14] **Brackney, R.,C., Anderson, R. H.** (2004). Understanding the insider threat, *RAND Corporation, Tech. Rep. RAND CF-196-DARPA*

[15]**Civil Fraud in Turkey.** erişim:27.01.2016, http://www.baspinar.av.tr/dosya/CivilFraudTurkey.pdf

[16] **Choosing Secure Passwords,** erişim: 06.02.2016,

https://www.schneier.com/blog/archives/2014/03/choosing_secure_1.html

[17] **Server Security Policy,** erişim: 06.02.2016,

https://www.sans.org/security-resources/policies/server-security/pdf/server-security-policy

[18] **University of Glasgow Guidelines for System and Network Administrators,** erişim: 09.02.2016,

http://www.gla.ac.uk/services/it/informationsecurity/policies/guidelinesforsystemandnetworkadministrators/

[19] **TS ISO/IEC 27001 Denetim Listesi**, erişim: 17.02.2016,

http://www.gla.ac.uk/services/it/informationsecurity/policies/guidelinesforsystemandnetworkadministrators/

[20] **ISO 27001:2013 Bilgi Güvenliği Sistemi Standardındaki Değişiklikler ve Yenilikler,** erişim: 17.02.2016, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/iso-27001-2013-bilgi-guvenligi-yonetim-sistemi-standardindaki-degisiklikler-ve-yenilikler.html

[21] **Introducing IDS and IPS,** erişim: 25.04.2016,

https://infosecprimer.wordpress.com/2013/07/09/introducing-ids-and-ips/

[22] **Adalı, E.** (2016). *Bilgisayar ve Bilgi Güvenliği Yönetimi*, İTÜ Ulusal Yazılım ve Sertifikasyon Merkezi

[23] **Tuğlular, T.** (2003). Üniversitelerde Bilgi Güvenliği Politikaları, *Ulaknet Sistem Yönetimi Konferansı*

ÖZGEÇMİŞ

Ad-Soyad : Ayşe Bilge İnce

Doğum Tarihi ve Yeri : 1990 / Ankara

E-posta : aysebilgegunduz@gmail.com

ÖĞRENİM DURUMU:

- **Lisans** : 2008, Sakarya Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği

YÜKSEK LİSANS TEZİNDEN TÜRETİLEN YAYINLAR, SUNUMLAR VE PATENTLER:

- İnce A.B., Adalı E., 2016. Üniversiteler İçin Kurumsal Güvenlik Çözüm Önerileri. ERPA International Congresses on Education 2016, 2-4 June.

DİĞER YAYINLAR, SUNUMLAR VE PATENTLER:

- Gündüz A.B., Çelebi S., Yurtay N., Bicil Y., 2013. A Mobile Product Recognition System for Visually Impaired People with IPhone 4. *3rd International Congress - AWERProcedia Information Technology & Computer Science*, March, 2013, Vol 03, 204-211.