T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ İLE ŞİRKET ÇALIŞANLARININ OLUŞTURDUĞU SİBER RİSK MATRİSİ VE AKSİYONLARIN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Esma SIĞIRTMAÇ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

ŞUBAT 2024

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

MAKİNE ÖĞRENMESİ İLE ŞİRKET ÇALIŞANLARININ OLUŞTURDUĞU SİBER RİSK MATRİSİ VE AKSİYONLARIN BELİRLENMESİ

YÜKSEK LİSANS TEZİ

Esma SIĞIRTMAÇ

Bilgisayar Mühendisliği Anabilim Dalı

Siber Güvenlik Bilim Dalı

Tez Danışmanı: Dr. Öğr. Üyesi Musa BALTA

ŞUBAT 2024

Esma SIĞIRTMAÇ tarafından hazırlanan "MAKİNE ÖĞRENMESİ İLE ŞİRKET ÇALIŞANLARININ OLUŞTURDUĞU SİBER RİSK MATRİSİ VE AKSİYONLARIN BELİRLENMESİ" adlı tez çalışması 14.02.2024 tarihinde aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı Siber Güvenlik Bilim Dalı'nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı :	**Dr. Öğr. Üyesi Murat İSKEFİYELİ** Sakarya Üniversitesi	**…….**
Jüri Üyesi :	**Dr. Öğr. Üyesi Musa BALTA** (Danışman) Sakarya Üniversitesi	**……...**
Jüri Üyesi :	**Doç. Dr. Süleyman EKEN** Kocaeli Üniversitesi	**……**

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum "MAKİNE ÖĞRENMESİ İLE ŞİRKET ÇALIŞANLARININ OLUŞTURDUĞU SİBER RİSK MATRİSİ VE AKSİYONLARIN BELİRLENMESİ" başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, etik kurul onay belgesi aldığımı, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(……/……/2024).

(imza)

Esma SIĞIRTMAÇ

TEŞEKKÜR

Yüksek lisans eğitimim ve bu tez çalışmasının yürütülmesi sırasında bilgi birikimini ve desteklerini esirgemeyen çok değerli danışman hocam sayın Dr. Öğr. Üyesi Musa BALTA'ya, teşekkürlerimi sunarım.

Tezimi yazarken hep yanımda olan beni yalnız hissettirmeyen ve her konuda yardımıma koşan Ferhat ACAR'a teşekkürlerimi sunarım.

Ayrıca, bu zorlu süreçte beni her zaman cesaretlendiren, destekleyen ve anlayışla yaklaşan sevgili anneme ve aileme de minnettarlığımı ifade etmek istiyorum.

Esma SIĞIRTMAÇ

İÇİNDEKİLER

Sayfa

KISALTMALAR

BT : Bilgi Teknolojileri

CAPTCHA : Completely Automated Public Turing Test To Tell Computers And Humans Apart

CIA : Central Intelligence Agency

CSAIL : Computer Science & Artificial Intelligence Laboratory

ENISA : The European Union Agency for Cybersecurity

FBI : Federal Bureau of Investigation

HTTPS : Hypertext Transfer Protocol Secure

KVKK : Kişisel Verileri Koruma Kanunu

QR : Quick-Response Code

SEO : Search Engine Optimization

SMS : Short Message/Messaging Service

SVM : Support Vector Machine

URL : Uniform Resource Locator

WCSS : Within-Cluster Sum of Square

2FA : Two-Factor Authentication

TABLO LİSTESİ

Sayfa

ŞEKİL LİSTESİ

Sayfa

MAKİNE ÖĞRENMESİ İLE ŞİRKET ÇALIŞANLARININ OLUŞTURDUĞU SİBER RİSK MATRİSİ VE AKSİYONLARIN BELİRLENMESİ

ÖZET

Günümüzde birçok alan, internet ve teknoloji ile harmanlanmış durumdadır. İnsanlar küçük büyük demeden internet üzerinden iş, banka, eğlence hatta temel ihtiyaçlarını bile karşılayabilir duruma gelmiştir. Tabi ki bu durum siber suçlular için birçok alanda zarar verilebilecek yeni kapılar demektir. Konu böyle olunca herkesin internet ortamında dikkatli hareket etmesi başta kendisi sonra çevresi için önemlidir.

Bu durum göz önüne alındığında, dijitalleşen şirketleri bekleyen tehlikeler nedir? Bu tehlikelere karşı nasıl önlem almak gereklidir? Özellikle büyük şirketler siber suçlular tarafından birçok saldırıya uğramaktadır. Saldırganlar, şirkete direkt zarar verebilir; sistemleri bozup şirket güvenilirliğini sarsabilirler. Ayrıca saldırganlar, şirket veya müşteri bilgilerini çalıp satabilirler veya şirketlere direkt maddi saldırılarda bulunabilirler. Bundan dolayı bu şirketler her işlemlerinde siber güvenliği bir adım önde tutarak ilerlemelidirler.

Siber güvenlik şirketler için büyük önem arz etmektedir. Şirket içinde çalışan yazılımcılara güvenli yazılım konusunda eğitim verilmektedir; aynı zamanda, çalışanlara atanmış yetkiler ve roller aracılığıyla erişebilecekleri alanlar kısıtlanmaktadır. Şirket içindeki veri merkezleri ve veri tabanları için gerekli güvenlik önlemleri alınmaktadır. Ağ sürekli olarak izlenerek gereksiz portlar kapatılmakta veya trafik yönlendirilmektedir. Bu gibi bir dizi önlem, teknik açıdan güvenliği sağlamak amacıyla kullanılmaktadır.

Teknik önlemlerin yeterli seviyede alınmasına rağmen, şirketler siber saldırılara maruz kalıp bu saldırılardan maddi ve manevi zarar görebilmektedirler. Bu durumun sebebi yeterli olmayan teknik önlemler değil, aksine siber alanda bilgisi olmayan şirket çalışanları, hatta belki de doğrudan şirket sahipleri olabilmektedir. Şirket çalışanları, istemeden de olsa siber saldırganlar için bir zafiyet oluşturabilirler.

Yapılan araştırmalar ve raporlar, günümüzdeki siber saldırıların en büyük zafiyetinin insan faktörü olduğunu ortaya koymaktadır. Çalışanların bilinçsizce gerçekleştirdiği her aksiyon, kişisel veya şirket bilgilerinin sızdırılmasına neden olabilir; bu da saldırganların büyük felaketlere yol açmasına neden olmaktadır.

Bu çalışmada hedeflenen, bu tür güvenlik zafiyetlerine neden olabilecek profilleri belirleyerek, uygun aksiyonlarla, şirketin siber güvenlik alanındaki savunma düzeyini artırmaktır. Risk oluşturan kişilerin profillerine göre gruplandırılması, teknik açıdan önlem alan şirketlerin insan faktörünü de güçlendirerek siber riskini minimuma indirmek için önlemler almasını sağlayabilir.

Bunu yapabilmek için doğru sonuçların elde edilmesinde ve veri yorumlanmasında en çok kullanılan yöntemlerden olan; makine öğrenmesinden yararlanılmaktadır. Makine öğrenmesi ile kişileri gruplamak, belirli profillerdeki insanlarda gözlemlenen belirli davranışlara dayanarak çıkarımlar yapmak ve bu doğrultuda bir risk matrisi

oluşturmak bu çalışmanın amacıdır. Çalışan profilleri üzerinden oluşturulan risk matrisine göre aksiyon maddeleri belirlenip yeni gelen veya var olan çalışanlar için siber risk matrisindeki aksiyonlar uygulanabilir.

Yapılan araştırmalar doğrultusunda makine öğrenmesinde gruplama (clustering) algoritmalarının kullanılması gerektiği sonucuna ulaşılmıştır. Birçok gruplama algoritması bulunduğundan, en çok kullanılan algoritmalar belirli testlere tabi tutulmuştur. Yapılan testler ve araştırma sonuçları birleştirerek, ihtiyacı karşılayacak en uygun iki algoritmanın K-means ve Mean Shift olduğuna karar verilip, bu algoritmalarla hesaplamalar yapılmıştır.

Birçok parametre kullanılıp, sonuçlar birbirleri ile kıyaslanarak tecrübe yıllarına ve yaşlarına göre gruplara ayrılan kişilerin, grup içlerinde benzer sorunlar ve davranışlar olduğu tespit edilmiştir. Bu doğrultuda, yine bu parametreler ile siber risk matrisi oluşturularak, belirli siber başlıklar altında grupların risk durumları belirlenmiştir. Bu risk durumlarına göre, nasıl aksiyonlar alınmalı, ne gibi önlemler alınabilir ve çalışanlar ne gibi riskler oluşturabilir sorularına cevaplar hazırlanmıştır. Bu kapsamda, şirket çalışanlarına veya yeni katılanlara yönelik, siber risk matrisi temelinde alınması gereken önlemlerin gözlemlenebileceği bir yapı oluşturulmuştur.

DETERMINING THE CYBER RISK MATRIX AND ACTIONS CREATED BY COMPANY EMPLOYEES USING MACHINE LEARNING

SUMMARY

Today, many fields are blended with the internet and technology. People, no matter how young or old, have become able to meet their business, banking, entertainment and even basic needs over the internet. Of course, this means new doors for cybercriminals to cause damage in many areas. When this is the case, it is important for everyone to act carefully on the internet, first for themselves and then for those around them.

Considering this situation, what are the dangers awaiting digitalizing companies? What precautions should be taken against these dangers? Especially large companies are subject to many attacks by cybercriminals. Attackers can cause direct damage to the company; They can disrupt systems and undermine company credibility. In addition, attackers can steal and sell company or customer information or make direct financial attacks on companies. Therefore, these companies must move forward by keeping cyber security one step ahead in every transaction.

Cyber security is of great importance for companies. Software developers working within the company are given training on secure software; At the same time, the areas that employees can access through assigned authorities and roles are restricted. Necessary security measures are taken for data centers and databases within the company. The network is constantly monitored and unnecessary ports are closed or traffic is redirected. A number of such measures are used to ensure technical security.

Despite adequate technical precautions, companies may be exposed to cyber attacks and suffer material and moral damage from these attacks. The reason for this situation is not inadequate technical measures, but on the contrary, it may be company employees who are not knowledgeable in the cyber field, and perhaps even direct company owners. Company employees may unintentionally create a vulnerability for cyber attackers.

Research and reports reveal that the biggest vulnerability in today's cyber attacks is the human factor. Every action taken by employees unconsciously may cause personal or company information to be leaked; This causes attackers to cause major disasters.

The aim of this study is to increase the company's defense level in the field of cyber security by identifying profiles that may cause such security vulnerabilities and taking appropriate actions. Grouping people who pose risks according to their profiles can enable companies that take technical precautions to take precautions to minimize cyber risk by strengthening the human factor.

In order to do this, one of the most used methods in obtaining accurate results and interpreting data; machine learning is used. The aim of this study is to group people with machine learning, make inferences based on certain behaviors observed in people with certain profiles, and create a risk matrix accordingly. Action items can be

determined according to the risk matrix created through employee profiles, and the actions in the cyber risk matrix can be implemented for new or existing employees.

In line with the research, it has been concluded that clustering algorithms should be used in machine learning. Since there are many grouping algorithms, the most used algorithms have been subjected to certain tests. By combining the tests and research results, the two most appropriate algorithms (K-means and Mean Shift) to meet the need were found and calculations were made based on them.

By using many parameters and comparing the results with each other, it was determined that people were divided into groups according to their years of experience and age and had similar problems and behaviors within the group. In this regard, a cyber risk matrix was created with these parameters and the risk status of groups under certain cyber headings was determined. According to these risk situations, answers to the questions of what actions should be taken, what precautions can be taken and what risks employees may pose are prepared. In this context, a structure has been created where the precautions to be taken based on the cyber risk matrix can be observed for company employees or new members.

A conclusion was reached by using many parameters and comparing the results with each other. It has been determined that people who are divided into groups according to their years of experience and age have similar problems and behaviors within the group. In this regard, a cyber risk matrix was created with these parameters and the risk situations of the groups were stated under certain cyber headings. According to these risk situations, answers to the questions of what actions should be taken, what precautions can be taken and what risks employees may pose are prepared. In this context, a structure has been created where the measures to be taken based on this matrix can be observed for company employees or new joiners.

In addition to employee profiles, another critical aspect of cybersecurity for digitalizing companies involves staying abreast of evolving cyber threats. Cybercriminals are constantly adapting their tactics, techniques, and procedures to bypass security measures. Therefore, companies must regularly update their cybersecurity protocols and tools to ensure resilience against emerging threats. Continuous monitoring of the cybersecurity landscape, participating in information-sharing networks, and engaging in threat intelligence activities become integral components of a proactive cybersecurity strategy.

Employee awareness and training programs are paramount in mitigating human-related vulnerabilities. Regular cybersecurity training sessions should be conducted to educate employees about the latest cyber threats, phishing techniques, and social engineering tactics. Employees should be trained to recognize suspicious activities and report them promptly. Simulated phishing exercises can also be employed to assess the organization's overall susceptibility to phishing attacks and enhance employee preparedness.

Beyond the technical aspects, fostering a culture of cybersecurity within the organization is crucial. Companies should promote a sense of responsibility among employees regarding the protection of sensitive information. Encouraging a cybersecurity mindset can help in creating a collective defense mechanism against potential cyber threats. Leadership plays a pivotal role in setting the tone for a cybersecurity-conscious workplace, emphasizing the importance of security measures and adherence to policies.

Collaboration with external cybersecurity experts and participation in industry-specific cybersecurity forums can provide valuable insights and best practices. Companies can leverage external expertise to conduct regular cybersecurity audits, penetration testing, and vulnerability assessments. These activities help identify and address potential weaknesses in the organization's systems and processes, ensuring a robust cybersecurity posture.

In the era of remote work, securing endpoints becomes a critical focus. With employees accessing company networks from various locations and devices, endpoint security solutions must be implemented. This involves deploying antivirus software, firewalls, and encryption tools on all devices connected to the corporate network. Additionally, companies should enforce the use of virtual private networks (VPNs) to secure communication channels and protect data during transit.

Data encryption is fundamental in safeguarding sensitive information. Companies should implement robust encryption protocols for both data at rest and in transit. This ensures that even if unauthorized access occurs, the intercepted data remains indecipherable and unusable. Regular data backups and secure storage practices further enhance the organization's ability to recover from potential cyber incidents, such as ransomware attacks or data breaches.

Incident response plans should be well-defined and regularly tested to ensure an effective and timely response to cyber incidents. Companies should establish a dedicated incident response team, outline escalation procedures, and conduct drills to simulate various cyber-attack scenarios. This proactive approach helps in minimizing the impact of potential breaches and facilitates a swift recovery process.

Legal and regulatory compliance is a critical aspect of cybersecurity, especially for companies dealing with sensitive customer information. Adhering to data protection laws and industry-specific regulations helps in avoiding legal ramifications and maintaining the trust of customers. Companies should regularly review and update their privacy policies, ensuring alignment with the latest legal requirements.

As technology evolves, so do the threats associated with it. Companies should invest in research and development to stay ahead of potential cyber threats. Innovations in cybersecurity technologies, such as artificial intelligence and machine learning, can be leveraged to enhance threat detection and response capabilities. Embracing emerging technologies allows companies to build adaptive and resilient cybersecurity infrastructures.

In conclusion, achieving a comprehensive cybersecurity strategy involves a multi-faceted approach that combines technical measures, employee training, cultural reinforcement, external collaboration, endpoint security, data encryption, incident response planning, legal compliance, and technological innovation. By addressing these aspects collectively, digitalizing companies can fortify their defenses against the ever-evolving landscape of cyber threats and create a secure environment for their operations.

1. GİRİŞ

1.1. Motivasyon ve Problemin Tanımlanması

İnsanlık, özellikle Covid-19 sonrası birçok işlem için interneti kullanmaya yönelmiştir. Yeni uygulamalar, yeni sistemler yapılıp, birçok işlem sanal ortama taşınmıştır. ENISA'nın (The European Union Agency for Cybersecurity, Avrupa Birliği Siber Güvenlik Ajansı) 20 Ekim 2020'de yayınladığı rapora göre siber saldırılarda ve çeşitlerinde artma gözlemlendiğinden bahsedilmiştir [1]. Covid-19 sonrasında yaşanan kapanmalar ve ekonomik dalgalanmalar, para odaklı suçluların internet kullanımındaki artışı fırsat bilerek birçok tüzel ve kurumsal alanı hedef almasına neden olmuştur. Siber alanda savaş veren ve dünyanın güçlü kurumlarından olan FBI'ın (Federal Bureau of Investigation, Federal Soruşturma Bürosu) Siber Bölüm Müdür Yardımcısı Tonya Ugoretz, 2020'de yaptığı açıklamaya göre, Covid-19 öncesi her gün 1000 siber saldırı şikayeti aldıklarını, ancak Covid-19 sonrasında bu rakamın 3000 ile 4000 arasında bir sıçrama yaşayarak arttığını belirtmiştir [2].

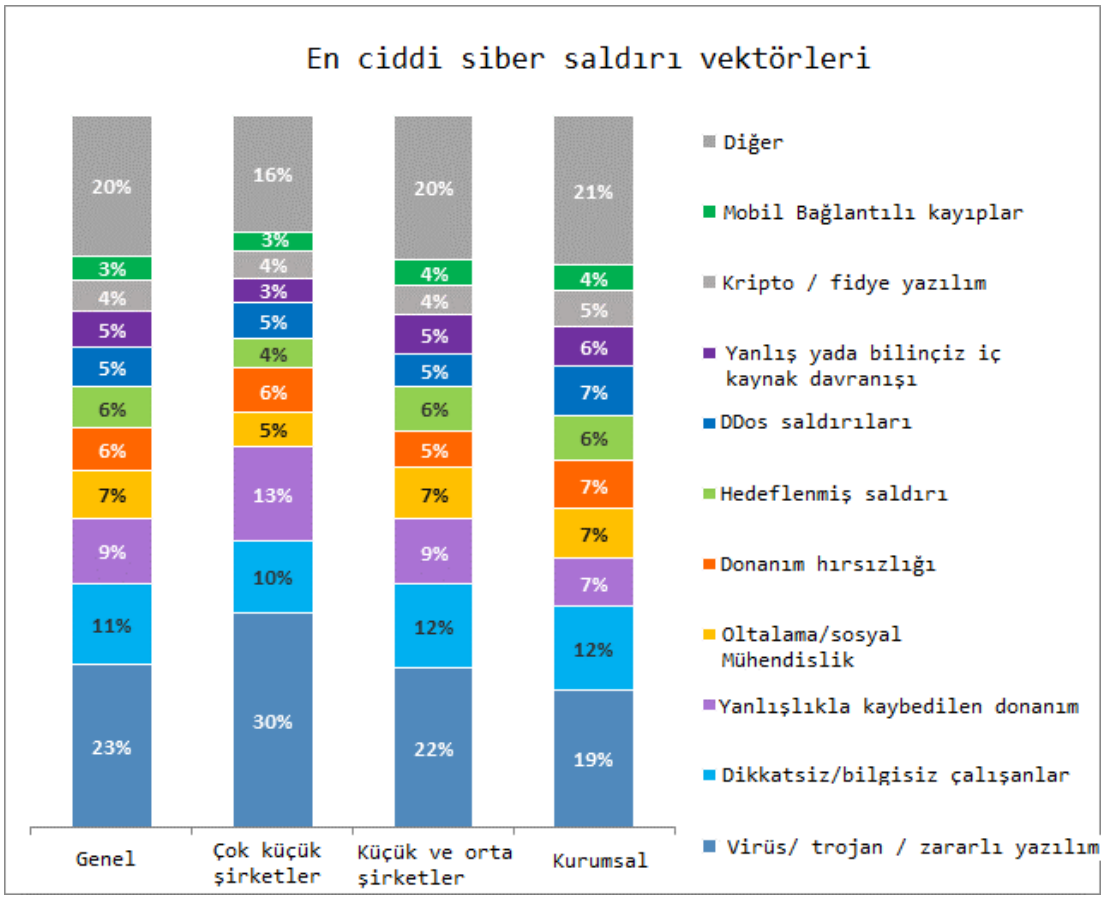
Yapılan araştırmalar doğrultusunda, siber saldırıların ve siber saldırı çeşitliliğin arttığı gözlemlenmiştir. Şirketlerin siber saldırılardan korunmak için ekstra güvenlik önemleri alınması gerektiği sonucuna ulaşılmıştır. Fakat ENISA'nın yaptığı açıklamalar doğrultusunda saldırı yöntemleri değiştiği için var olan önlemlerin de yeterli olmadığı belirtilmektedir [1].

Teknik olarak ne kadar önlem alınsa da işin içinde insan olunca hata yapma oranı artmaktadır. Mancuso, Strang, Funke ve Finomore adlı dört araştırmacı, 2014'te yayınladığı bildiriye göre siber saldırganların tercih ettiği yöntemlerin artık teknik açıklık değil, insanı hedef almaya başladığı sonucuna ulaşmışlardır [3]. Saldırganlar, daha çok psikoloji tabanlı yöntemler ile insanların bilinçsiz davranışlarını kullanarak, saldırılar yapmaya başlamıştır [3]. ENISA'nın yayınladığı raporlara göre, Covid-19 döneminde en çok kullanılan saldırı yöntemleri şu şekildedir: oltalama, sosyal mühendislik, kötü amaçlı yazılım, uyumsuzluk, kötü politikalar ve teknolojinin neden olduğu güvenlik açıkları [1]. Bu sıralama, en çok kullanılanından küçüğe doğru yapılmıştır.

Tarihsel olarak CIA (Central Intelligence Agency, Merkezi İstihbarat Teşkilatı), genellikle son kullanıcıların bilişsel süreçlerini, ihtiyaçlarını ve motivasyonlarını çok az dikkate alan ve sorunlara teknoloji merkezli bir bakış açısıyla yaklaşan bir kuruluş olmuştur [4]. Kuruluşlar potansiyel siber tehditlerle mücadele etmek için teknolojik çözümlere büyük önem vermelidirler. Siber güvenlik alanında yapılan son araştırmalar, siber saldırılara karşı koymak için tek başına teknik çözümlerin aksine bütünsel bir yaklaşımın gerekli olduğu konusunda büyük ölçüde hem fikirdirler. Bu durum özellikle eğitim ve sağlık gibi iyi hedeflenmiş sektörlerin yanı sıra, otonom araçlar gibi yeni ve gelişmekte olan alanlarda da fark edilmektedir. Kullanıcıların davranış ve tutumları, teknolojik ilerlemeleri baltalayabilmektedir.

Bu gelişmeler ve her geçen gün artan internet kullanımı dolayısıyla, her yaştan insanın internette olması özellikle şirketler için çok fazla tehlike doğurmaya başlamıştır. Bu kapsamda, şirketler her ne kadar teknik önlem almaya önem gösterseler ve yatırım yapsalar da şirket içinde çalışan bir kişinin dikkatsizliği sonucu birçok istenmeyen durum ortaya çıkabilmektedir. Ne kadar güvenlik önlemi alınırsa alınsın ne kadar çok para harcanırsa harcansın en önemli yatırım, insanların bilinçlendirilmesi, doğru güvenlik çözümlerinin ve stratejilerinin doğru yerde ve doğru zamanda kullanılmasıdır [5].

Büyük bir antivirüs yazılım şirketi olan Kaspersky'ın 2017'de yaptığı araştırmalara göre, işletmelerin 57%'si, artık BT (Bilgi Teknolojileri) güvenliklerinin tehlikeye gireceğini varsaydığı karmaşık ve büyüyen bir siber tehdit manzarasıyla karşı karşıyadırlar [6]. İşletmeler siber saldırılara karşı, bünyelerindeki en büyük çatlaklardan birinin kendi çalışanları olduğu gerçeğinin de farkındadırlar. Aslında işletmelerin 52%'si, çalışanların BT güvenliğindeki en büyük zayıflıkları olduğunu ve dikkatsiz eylemlerinin işletmenin BT güvenliği stratejisini riske attığını kabul etmiştir [6]. Şirket çalışanları, dikkatsizlik ve bilinçsizce yaptıkları hatalar nedeniyle şirketlerinin verilerini veya sistemlerini riske atabilecek durumlara sebep olabilmektedir. Bu durum, çalışanların nasıl uygun davranacaklarını ve işlerini nasıl koruyacaklarını öğretecek gerekli eğitime sahip olmamalarından kaynaklanmaktadır. Şekil 1.1.'de Kaspersky'ın yayınladığı en tehlikeli siber saldırı yöntemleri gösterilmiştir.



Şekil 1.1. Kaspersky 2017 global siber güvenlik araştırması [6].

Elde edilen veriler sonucunda, siber güvenlikte artık teknik boyuttan daha önemli bir konu olan insan faktörü ortaya çıktığı net olarak görülmektedir. Bu proje kapsamında, siber güvenlik alanında var olan insan risk faktörünü, minimum risk seviyesine indirmek hedeflenmektedir. İş hayatı, kişisel yaşam, eğitim vb. internetin kullanılabileceği her alanda incelemeler yapılmıştır. İnsan faktörünün minimuma indirilmesi amacıyla belirli yöntemler ve araştırmaların sonuçları ortak bir noktada birleştirilerek insan odaklı bir çalışma gerçekleştirilmiştir.

1.2. Çalışmanın Amacı ve Geliştirilen Çözüm Yöntemi

Değişen yeni siber saldırı yöntemleri ve tehditler sonucu insanların bilinçlendirilmesi gerekmektedir. Özel ihtiyaçlara uygun olarak, kişilere eğitici, öğretici ve kaçınmaları gereken aksiyonlar doğrultusunda eğitim verilmesi gerekmektedir. Yapılan araştırmalar ve gözlemler sonucunda teknik güvenlik önemlerin yeterli olmadığı tespit edilmiştir.

Bu tez çalışmasında, yapılan anket sonuçları üzerinden gidilerek, kişileri grup bazında genel geçer bir profilde toplamak hedeflenmiştir. Kullanılan teknolojiler ile birçok parametre ve veriler üzerinde testler yapılarak benzer sonuçlara ulaşılmıştır.

Sonuçlar incelediğinde belirli tecrübe yılı aralığındaki insanların aynı tarz yaklaşımlarda bulunduğu keşfedilmiştir. Bu doğrultuda belirli tecrübe yılı aralığındaki insanların, yapılan hatalar ve eksiklikler açısından benzerlik gösterdiği gözlemlenmiştir. Siber risk matrisi oluşturarak, bu kişilerin hangi durumlar için hangi risk kategorisine denk geldiği belirlenip bu kişiler için gerekli önlem ve alınması gereken aksiyonlar ve çeşitli eğitimler önerilmiştir.

Bilginin kıymetli olması bilgiyi ele geçirmeye yönelik tehditlerin ve kullanılan yöntemlerin çeşitliliği, bilgi güvenliğini sağlamak amacıyla aynı oranda önlem almayı gerektirmektedir. En hızlı ve etkili yöntemlerden biri eğitim programları vasıtasıyla bilgi güvenliğini sağlamak konusunda farkındalık yaratmak [7] ve gençleri bilinçlendirmektir [8].

Siber risk matrisi kullanılarak, var olan çalışanlar veya yeni gelecek çalışanlar için matriste denk geldiği noktaya göre aksiyonlar alınır. Siber risk matrisi aracılığıyla, çalışanların siber açıdan eksik yönleri giderilir. Bu yolla siber tehditlerde insan faktörünü minimuma indirmek hedeflenmektedir.

2. TEMEL BİLGİLER VE LİTERATÜR ARAŞTIRMASI

2.1. Makine Öğrenmesi

Makine öğrenimi, genel olarak bir makinenin akıllı insan davranışını taklit etme yeteneği olarak tanımlanan yapay zekanın bir alt alanıdır. Yapay zeka sistemleri, karmaşık görevleri, insanların sorunları çözme biçimine benzer şekilde gerçekleştirmek için kullanılır [9].

CSAIL'deki (Computer Science & Artificial Intelligence Laboratory, Bilgisayar Bilimi ve Yapay Zeka Laboratuvarı) InfoLab Grubu başkanı ve baş araştırma bilimcisi Boris Katz'a göre yapay zekanın amacı, insanlar gibi "akıllı davranışlar" sergileyen bilgisayar modelleri yaratmaktır. Bu, görsel bir sahneyi tanıyabilen, doğal dilde yazılmış bir metni anlayabilen veya fiziksel dünyada bir eylem gerçekleştirebilen makineler anlamına gelir [10].

Makine öğrenimi yapay zekayı kullanmanın bir yoludur. 1950'lerde yapay zeka öncüsü Arthur Samuel tarafından "bilgisayarlara açıkça programlanmadan öğrenme yeteneği veren çalışma alanı" olarak tanımlanır [10].

Makine öğrenmesi alanında birçok algoritma mevcuttur. Bu çalışmada, makine öğrenmesi algoritmaları kullanılarak; yapılacak gruplama ve kişiler arasında davranış ağını çözebilmek için seçilmesi gereken en uygun algoritmayı tespit etmek amaçlanmıştır. Tez çalışmasında algoritmalar, iki ana başlık altında incelenmiştir.

2.1.1. Denetimli algoritma

Denetimli öğrenme, etiketli verilerden öğrenen bir tür makine öğrenme algoritmasıdır. Etiketli veriler, doğru bir cevap veya sınıflandırma ile etiketlenmiş verilerdir [11].

Araştırmacı Sarker, I.H., Kayes, A.S.M., Badsha 2020 yılında yayınladıkları makalede bu tür algoritmalara değinmişlerdir [12]. Araştırmacı Sarker, I.H., Kayes, A.S.M., Badsha makalelerinde; hizmet reddi saldırısını tahmin etmek (evet, hayır) veya tarama ve yanıltma gibi farklı ağ saldırı sınıflarını belirlemek için siber güvenlik alanında sınıflandırma tekniklerinin kullanılabileceği belirtmişlerdir [12]. Araştırmacı Sarker, I.H., Kayes, A.S.M., Badsha'nın makalesine göre ZeroR, OneR, Navies Bayes, Karar

Ağacı, K-means, destek vektör makineleri, uyarlamalı güçlendirme ve lojistik regresyon iyi bilinen sınıflandırma teknikleridir [12].

Denetimli öğrenme, adından da anlaşılacağı gibi, öğretmen olarak bir denetçinin varlığına sahiptir. Denetimli öğrenme, makineyi iyi etiketlenmiş verileri kullanarak öğrettiğimiz veya eğittiğimiz modeldir. Bu, bazı verilerin zaten doğru yanıtla etiketlendiği anlamına gelir. Bundan sonra makineye yeni bir örnek seti (veri) sağlanır, böylece denetimli öğrenme algoritması eğitim verilerini (eğitim örnekleri seti) analiz eder ve etiketli verilerden doğru bir sonuç üretir [11].

Örneğin, Fil, Deve ve İnek görsellerinden oluşan etiketli bir veri kümesinde her görselin "Fil", "Deve" veya "İnek" ile etiketlenmesi gerekir.

Denetimli öğrenme, modellere istenen çıktıyı verecek şekilde öğretmek için bir eğitim seti kullanır. Bu eğitim veri kümesi, modelin zaman içinde öğrenmesine olanak tanıyan girdileri ve doğru çıktıları içerir. Algoritma doğruluğunu, hata en aza indirilene kadar ayarlayarak kayıp fonksiyonu aracılığıyla ölçer [13].

Denetimli öğrenme, veri madenciliği sırasında sınıflandırma ve regresyon olmak üzere iki türe ayrılır:

- Sınıflandırma, test verilerini belirli kategorilere doğru şekilde atamak için bir algoritma kullanır. Veri kümesi içindeki belirli varlıkları tanır ve bu varlıkların nasıl etiketlenmesi veya tanımlanması gerektiği konusunda bazı sonuçlar çıkarmaya çalışır. Yaygın sınıflandırma algoritmaları, aşağıda daha ayrıntılı olarak açıklanan doğrusal sınıflandırıcılar, SVM (Support vector machine, destek vektör makineleri), karar ağaçları, K-means yakın komşu ve rastgele ormandır.
- Regresyon, bağımlı ve bağımsız değişkenler arasındaki ilişkiyi anlamak için kullanılır. Belirli bir işletmenin satış geliri gibi tahminlerde bulunmak için yaygın olarak kullanılır. Doğrusal regresyon, lojistik regresyon ve polinom regresyon popüler regresyon algoritmalarıdır.

2.1.2. Denetimsiz algoritma

Denetimsiz öğrenme, etiketlenmemiş verilerden öğrenen bir tür makine öğrenimidir. Bu, verilerin önceden var olan herhangi bir etikete veya kategoriye sahip olmadığı anlamına gelir. Denetimsiz öğrenmenin amacı, herhangi bir açık rehberlik olmaksızın verilerdeki kalıpları ve ilişkileri keşfetmektir [11].

Bu sebepten dolayı, Araştırmacı Sarker, I.H., Kayes, A.S.M., Badsha siber güvenlik alanında, kötü amaçlı yazılım gibi siber saldırıların bazı şekillerde gizli kalabildiğini; kötü amaçlı yazılımların tespit edilmekten kaçınmak için davranışlarını dinamik ve özerk bir şekilde değiştirebildiğinden bahsederler [12]. Denetimsiz öğrenmenin bir türü olan kümeleme teknikleri, veri kümelerindeki gizli kalıpları ve yapıları ortaya çıkarmaya ve bu tür karmaşık saldırıların göstergelerini tanımlamaya yardımcı olabilir. Benzer şekilde anormalliklerin, politika ihlallerinin belirlenmesinde, verilerdeki gürültülü örneklerin tespit edilmesi ve ortadan kaldırılmasında kümeleme teknikleri yararlı olabileceğine değinirler.

Denetimli öğrenmenin aksine, hiçbir öğretmen sağlanmaz, bu da makineye herhangi bir eğitim verilmeyeceği anlamına gelir. Bu nedenle makinenin etiketlenmemiş verilerdeki gizli yapıyı kendi başına bulması sınırlıdır [11].

Toplanan hayvan verilerini incelemek ve hayvanların özelliklerine ve eylemlerine göre çeşitli gruplar arasında ayrım yapmak için denetimsiz öğrenmeyi kullanabilirsiniz. Bu gruplamalar çeşitli hayvan türlerine karşılık gelebilir, bu da canlıları zaten var olan etiketlere bağlı kalmadan kategorilere ayırmanızı sağlar [11].

Kümeleme, etiketlenmemiş verileri benzerliklerine veya farklılıklarına göre gruplandıran bir veri madenciliği tekniğidir. Kümeleme algoritmaları ham, sınıflandırılmamış veri nesnelerini bilgideki yapılar veya kalıplarla temsil edilen gruplar halinde işlemek için kullanılır. Kümeleme algoritmaları, özellikle dışlayıcı, örtüşen, hiyerarşik ve olasılıksal olmak üzere birkaç türe ayrılabilir [13].

Özel kümeleme, bir veri noktasının yalnızca bir kümede bulunabileceğini öngören bir gruplama biçimidir. Buna “sert” kümeleme de denilebilir. K-means kümeleme algoritması özel kümelemeye bir örnektir.

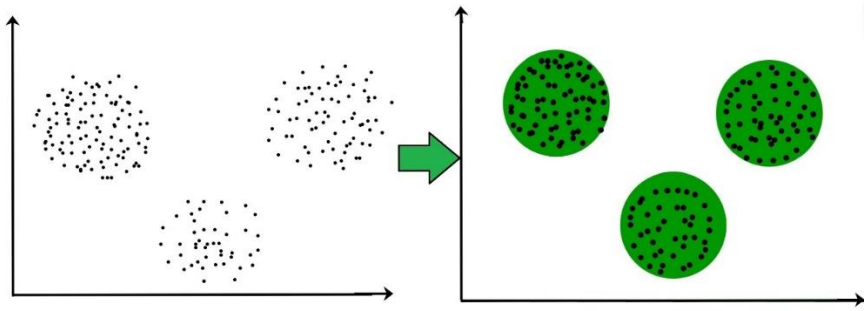
- K-means kümeleme, veri noktalarının K gruplarına atandığı özel kümeleme yönteminin yaygın bir örneğidir; burada K, her grubun ağırlık merkezinden uzaklığa bağlı olarak küme sayısını temsil eder. Belirli bir merkeze en yakın veri noktaları aynı kategori altında toplanacaktır. Daha büyük bir K değeri, daha fazla ayrıntı düzeyine sahip daha küçük gruplamaların göstergesi olacaktır; daha küçük bir K değeri ise daha büyük gruplandırmalara ve daha az ayrıntı düzeyine sahip olacaktır. K-means kümelemesi yaygın olarak pazar bölümlendirmede, belge kümelemede, görüntü bölümlendirmede ve görüntü sıkıştırmada kullanılır.

Örtüşen kümeler, veri noktalarının farklı üyelik derecelerine sahip birden fazla kümeye ait olmasına izin vermesi bakımından özel kümelemeden farklıdır. "Yumuşak" veya bulanık k-means kümelemesi örtüşen kümelemeye bir örnektir.

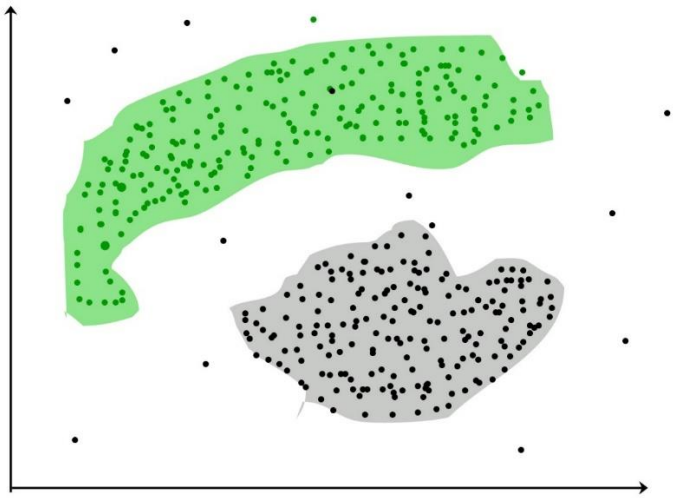
2.1.3. Makine öğrenmesi kümeleme

Temel olarak bir tür denetimsiz öğrenme yöntemidir. Denetimsiz öğrenme yöntemi, etiketli yanıtlar olmadan giriş verilerinden oluşan veri kümelerinden referanslar aldığımız bir yöntemdir. Genel olarak anlamlı yapıyı, açıklayıcı temel süreçleri, üretken özellikleri ve bir dizi örnekte var olan gruplandırmaları bulma süreci olarak kullanılır [14].

Kümeleme, popülasyonu veya veri noktalarını, aynı gruplardaki veri noktalarının aynı gruptaki diğer veri noktalarına daha fazla benzeyeceği ve diğer gruplardaki veri noktalarına benzemeyeceği şekilde bir dizi gruba bölme görevidir. Şekil 2.1.'de bulunan grafik örneği dairesel noktaların gruplanmasına örnek verilebilir. Şekil 2.2.' de bulunan grafik örneği ise dağınık noktaların gruplanmasına örnek verilebilir.



Şekil 2.1. Dairesel gruplama [14].



Şekil 2.2. Düzensiz şekilli gruplama [14].

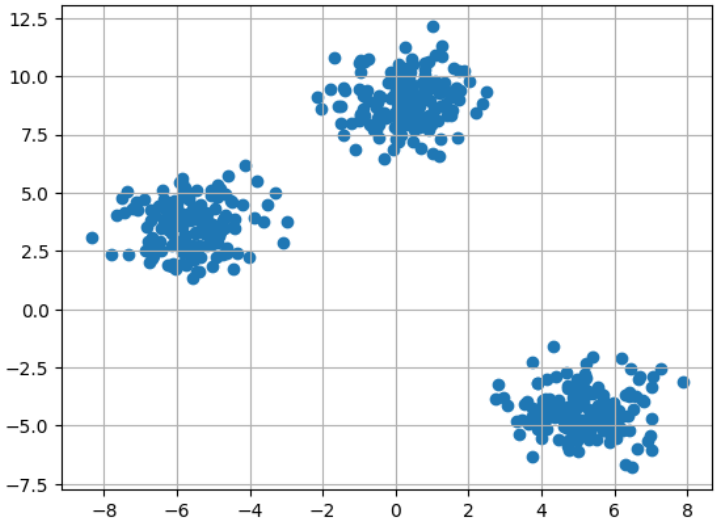
Kümeleme, mevcut etiketlenmemiş veriler arasındaki asıl gruplamayı belirlediği için çok önemlidir. İyi kümelenmenin hiçbir kriteri yoktur. Bu, kullanıcıya ve ihtiyaçlarını karşılamak için hangi kriterleri kullanabileceğine bağlıdır. Örneğin, homojen gruplar için temsilciler bulma (veri azaltma), "doğal kümeler" bulma ve bunların bilinmeyen özelliklerini tanımlama ("doğal" veri türleri), yararlı ve uygun gruplamalar bulma ("yararlı" veri sınıfları) veya olağandışı veri nesnelerinin bulunmasında (aykırı değer tespiti) kullanılır. Bu algoritma, noktaların benzerliğini oluşturan bazı varsayımlarda bulunmalı ve her varsayım farklı ve eşit derecede geçerli kümeler oluşturmalıdır. Kümeleme benzerlik ve farklılıklara dayalı olarak nesnelerin bir koleksiyonudur [14].

Tennessee Teknik Üniversitesi'nden iki araştırmacı Vitaly Ford ve Ambareen Sira'nın yayınladığı çalışmada siber güvenlik için kullanılabilecek en iyi yöntemlerden birinin desteksiz gruplama algoritmaları olduğunu vurgular. Yaptıkları çalışmada ağ sızıntısı, oltalama tespiti ve CAPTCHA (Completely Automated Public Turing Test To Tell Computers And Humans Apart, Bilgisayarları ve İnsanları Ayırmak İçin Tamamen Otomatik Herkese Açık Turing Testi) kaçak kontrolünde bu algoritmaları kullanmışlardır [15]. Veriler doğrultusunda algoritmanın doğruluk oranı 94.91% olarak paylaşılmıştır [15].

2.2. K-Means Algoritması

Denetimsiz Makine Öğrenimi, bir bilgisayara etiketlenmemiş, sınıflandırılmamış verileri kullanmayı öğretme ve algoritmanın bu veriler üzerinde denetim olmadan çalışmasını sağlama sürecidir. Makinenin görevi, önceden herhangi bir veri eğitimi olmadan sıralanmamış verileri, kalıplara ve varyasyonlara göre düzenlemektir.

Kümelemenin amacı, popülasyonu veya veri noktaları kümesini birkaç gruba bölerek her gruptaki veri noktalarının birbiriyle daha karşılaştırılabilir olmasını ve diğer gruplardaki veri noktalarından farklı olmasını sağlamaktır. Esasen, birbirine ne kadar benzer ve farklı olduklarına dayanan noktalar grubudur. Şekil 2.3.'te bulunan grafik incelendiğinde birbiri ile benzer ve farklı davranan noktalar kullanılarak üç adet grup oluşturulmuştur.



Şekil 2.3. Örnek K-means grafiği [14].

Bize belirli özelliklere sahip öğelerden oluşan bir veri seti ve bu özellikler için değerler veriliyor. Görev, bu öğeleri gruplara ayırmaktır. Bunun başarılması için K-means algoritması denetimsiz öğretim algoritması olarak kullanılacaktır. Algoritma adındaki 'K', öğelerimizi sınıflandırmak istediğimiz grup/küme sayısını temsil eder.

Algoritma, öğeleri k grup veya benzerlik kümesi halinde kategorilere ayıracaktır. Bu benzerliği hesaplamak için ölçüm olarak Öklid uzaklığı kullanılır.

Algoritma şu şekilde çalışır:

- İlk olarak, ortalamalar veya küme merkezleri adı verilen k noktayı rastgele başlatılır.
- Her öğe, en yakın ortalamaya göre kategorilere ayırılır ve o kümede o ana kadar kategorize edilen öğelerin ortalamaları olan ortalamanın koordinatları güncellenir.
- İşlem belirli sayıda yineleme için tekrarlanır ve sonunda kümeler elde edilir.

2.2.1. Elbow metodu

Kümeleme, denetimsiz bir makine öğrenme tekniğidir. Veri setinin, aynı gruptaki üyelerin özellik bakımından benzerliklere sahip olduğu gruplara bölünmesi işlemidir. Yaygın olarak kullanılan kümeleme teknikleri K-means kümeleme, Hiyerarşik kümeleme, Yoğunluk tabanlı kümeleme, model tabanlı kümelemedir. Bu algoritmalar büyük veri kümelerini bile işleyebilir. Python'daki, scikit-learn kütüphanesi kullanılarak, K-Means kümeleme makine öğrenmesi algoritması dirsek yönteminde uygulanılabilir.

Dirsek yöntemi, K-means kümelemede optimal K'yi bulmanın grafiksel bir temsilidir. WCSS'yi (Within-Cluster Sum of Square, Küme İçi Kareler Toplamı), bir kümedeki noktalar ile küme ağırlık merkezi arasındaki mesafenin karesinin toplamını bularak çalışır.

Daha iyi bir anlayış için K-means kümelemesinde yer alan adımlar aşağıdaki gibidir:

- Veri kümesi için küme sayısı seçilir (K).
- Veri kümesinden K sayısı rastgele seçilir.
- Noktaların, en yakın merkeze olan mesafesini hesaplamak ve noktaları en yakın küme merkezine atayarak K kümeleri oluşturmak için metrik olarak Öklid mesafesini veya Manhattan mesafesi kullanılır.
- Bu şekilde oluşan kümelerin yeni ağırlık merkezi bulunur.
- Tüm veri noktaları bu yeni ağırlık merkezine göre yeniden atanır, ardından 4. adım tekrarlanır. Bu işlem, ağırlık merkezinin konumu değişmeyene, artık yakınsama kalmayana kadar belirli sayıda yineleme için sürdürülür.

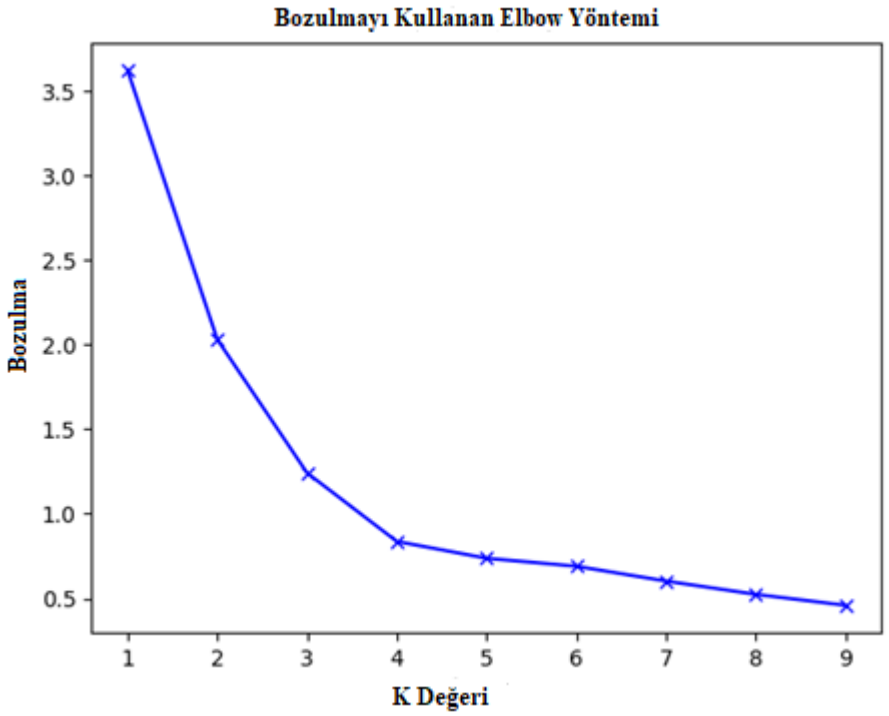
Bozulma: Formül 2.1, ilgili kümelerin küme merkezlerinden her bir veri noktasına olan uzaklıkların karesinin ortalaması olarak hesaplanır. Tipik olarak Öklid uzaklığı metriği kullanılır.

Atalet: Formül 2.2, örneklerin en yakın küme merkezlerine olan uzaklıklarının karelerinin toplamını ifade etmektedir.

$$\text{Bozulma} = \frac{1}{\text{n}} * \sum (Uzaklık(nokta, ağırlık\ merkezi)^2) \tag{2.1}$$

$$Atalet = \sum (Uzaklık(nokta, ağırlık\ merkezi)\text{^}2) \tag{2.2}$$

K değerini, 1'den n'ye kadar yinelenip her k değeri için distorsiyon değerleri hesaplanır. Verilen aralıktaki her k değeri için distorsiyon ve eylemsizliği hesaplanır. İşlemler çalıştırıldığında Şekil 2.4.'te bulunan grafik oluşmaktadır.



Şekil 2.4. Elbow grafiği [16].

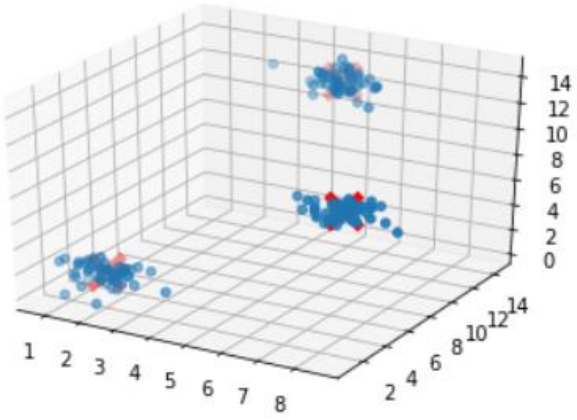
Tez çalışması için K-means kullanılan alanlarda uygun olan grup adedi bulunmaktadır. Bunun için elbow metodundan yararlanılmıştır. Araştırmalar sonucunda bu formüller dışında daha basit bir yöntem olduğu keşfedilmiştir. Yapılan algoritma aynı bırakılıp sırasıyla bir adet gruptan başlayarak dokuz adet olana kadar sırayla bakıldığı zaman çıkan grafikte yaşanan kırılma aslında tam olarak bize kullanılması gereken grup adedini vermektedir. Bu durumda Şekil 2.4.' te verilen grafiğe göre sıfır olmayan fakat sıfıra en yakın kırılma 4'te gerçekleşiyor. Bu durumda algoritmada grup adedi olarak 4 kullanılmıştır.

2.3. Mean Shift Algoritması

K-means algoritması iki parametre ile çalışır. Bazı karmaşık durumlarda K-means yeterlidir. Fakat daha sorunlu ve karmaşık durumlarda yeterli sonuç elde edilmemektedir. Bunun için aynı çalışma yöntemi ve aynı gruplama sistemi ile üç parametre alan yeni bir yapı kullanılması gereklidir. İhtiyaca göre K-means veya Mean Shift arasında geçişler yapılarak veriler analiz edilir.

Ortalama kaydırmalı kümeleme, bir veri kümesi içindeki kümeleri tanımlamak için kullanılan denetimsiz bir makine öğrenme algoritmasıdır. Yüksek yoğunluklu bölgeleri bulmaya ve veri noktalarını yinelemeli olarak en yüksek nokta yoğunluğuna

doğru kaydırmaya odaklanan, yoğunluğa dayalı bir kümeleme yöntemidir. Dolayısıyla bu algoritmaya "ortalama kayma" adı verilir. Algoritma, verilerde mevcut olan kümelerin sayısı hakkında herhangi bir ön bilgiye ihtiyaç duymaz, bu da onu özellikle keşif amaçlı veri analizi için faydalı kılar [17]. Mean Shift nokta yoğunluk grafiği Şekil 2.5.'te gösterildiği gibi üç boyutlu oluşmaktadır.



Şekil 2.5. Mean Shift örnek grafiği [27].

Şekil 2.5.'te bulunan grafikte görüldüğü gibi Mean Shift kullanıldığı zaman oluşan grafikte üç boyutlu görüntü oluşmaktadır. Bunun sonucunda daha karmaşık veri setleri kullanıldığında daha doğru sonuç alınabilir. Anket soruları analiz edilirken cevaplar ikiyi geçmiyorsa K-means; geçiyorsa Mean Shift kullanılarak verimli bir sonuç alınır. Örneklemek gerekirse, bize d boyutlu uzayda daha büyük bir popülasyondan örneklenen noktalardan oluşan bir veri seti {ui} verildiğini ve h bant genişliği parametresine sahip bir K çekirdeği seçtiğimizi varsayalım. Bu veriler ve çekirdek işlevi birlikte, tam popülasyonun yoğunluk işlevi için formül 2.3 çekirdek yoğunluğu tahmincisini döndürür [16].

$$\boldsymbol{f(x) = \frac{1}{nh^d} \sum_{i=1}^{n} K\left(\frac{u - u_i}{h}\right)} \tag{2.3}$$

Buradaki çekirdek fonksiyonunun, formül 2.4 ve 2.5 koşullarını sağlaması gerekmektedir:

$$\boldsymbol{\int K(u)du = 1} \tag{2.4}$$

$$\boldsymbol{K(u) = K(|u|)} \tag{2.5}$$

Bu koşulları karşılayan iki popüler çekirdek işlevi, formül 2.6 ve 2.7'de gösterilmektedir:

$$\textbf{Flat/Uniform } \boldsymbol{K(u)} = \frac{1}{2}\begin{cases} \mathbf{1} & \mathbf{-1 \leq |u| \leq 1} \\ \mathbf{0} & \mathbf{else} \end{cases} \tag{2.6}$$

$$\textbf{Gaussian } \boldsymbol{K(u)} = \frac{\mathbf{1}}{\mathbf{(2\pi)^{\frac{d}{2}}}} \mathbf{e}^{-\frac{1}{2}\,|u|^2} \tag{2.7}$$

Bu algoritmada K-means gibi grup adedini belirtmemize gerek yoktur. Fakat burada hesaplama için bir parametrenin ayarlanması gereklidir. Bunlar kaç adet örneklem kullanıldığı ve gruplama hassasiyetidir. Kullanılan yazılım içerisinde ve ayrıca yukarıda verilen formüller aracılığı ile verilerin karmaşıklığına göre bu iki parametreyi deneme ve yanılma yoluyla en optimal verilere ulaştırmak gereklidir. Eğer verilerimiz çok karmaşık ise daha fazla örneklem aldırarak daha iyi sonuçlar ve fazla gruplama elde edebiliriz. Eğer veri karmaşık değilse gruplama hassasiyetini ve örneklemi azaltarak gruplama konusunda güzel sonuçlar çıkarabiliriz.

2.4. Siber Güvenlik Farkındalığının Önemi

Siber güvenlik farkındalığı, bireylerin, kurumların ve toplumun dijital dünyadaki riskleri anlaması, bu risklere karşı nasıl korunacağını öğrenmesi ve bu konuda bilinçli hareket etmesidir.

Siber farkındalık, bireylerin ve kurumların kişisel ve kurumsal verilerini korumasına yardımcı olur. Siber güvenlik bilinci, kişilerin ve kurumların finansal zararlara uğramasını önler. Bilinçli kullanıcılar, dolandırıcılık ve kimlik avı gibi saldırıları tanıyabilir ve önleyebilirler. Kullanıcılar, kişisel ve kurumsal verilerini daha iyi koruyabilir, bu da veri ihlallerinin azalmasına yardımcı olur.

Siber güvenlik farkındalığı, kritik altyapı ve hizmetlerin korunmasına da yardımcı olur. Bilinçli kullanıcılar, bu tür hizmetlerin siber saldırılara karşı daha dirençli olmasını sağlarlar. Siber güvenlik farkındalığı, toplumun genel olarak dijital ortamda güvende hissetmesine yardımcı olur. Bu da dijital ekonomi ve iletişimde sağlıklı bir ortamın oluşmasını sağlar. Sonuç olarak, siber güvenlik farkındalığı, bireylerin ve

kurumların dijital ortamda daha güvenli ve bilinçli hareket etmelerini sağlar, bu da çeşitli olumlu sonuçlar doğurur ve dijital dünyadaki riskleri azaltır.

Siber güvenlik farkındalığı ile ilgili çalışmalar şunları içerebilir:

1. Eğitim ve Seminerler: Siber güvenlik uzmanları tarafından düzenlenen eğitimler ve seminerler, bireyleri ve kurumları dijital tehditler konusunda bilinçlendirir ve korunma yöntemleri hakkında bilgi verir.
2. Kampanyalar ve Bilgilendirme Materyalleri: Siber güvenlik farkındalığı artırmak amacıyla kampanyalar düzenlenir ve bilgilendirme materyalleri hazırlanır. Bu materyaller, sosyal medya, web siteleri, broşürler ve afişler gibi çeşitli kanallar aracılığıyla yayılır.
3. Simülasyon ve Egzersizler: Kurumlar, çalışanların siber saldırıları nasıl tanıyacaklarını ve nasıl tepki vereceklerini öğrenmeleri için simülasyonlar ve egzersizler düzenleyebilir.
4. Güvenlik Politikaları ve Prosedürler: Kurumlar, güvenlik politikaları ve prosedürler geliştirerek çalışanlarına nasıl güvenli bir şekilde davranacaklarını öğretebilir ve uygulamalarını sağlayabilir.
5. Literatürde siber güvenlik farkındalığı ve bilincini arttırmaya yönelik çalışmalar mevcuttur. Tablo 2.1.'de bu çalışmalar ve içeriklerinden bahsedilmiştir.

Tablo 2.1. Literatürde siber güvenlik farkındalığı ile ilgili çalışmalar [18-20].

Başlık	Yayın Yılı	Özet
Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi	2020	Bu makalede üniversite öğrencilerinin bilgi güvenliği farkındalıkları ile çeşitli demografik değişkenlere göre siber güvenlik davranışları ve bilgi güvenliği farkındalıkları arasındaki ilişki incelenmiştir. Öğrencilerin farkındalıklarının artırılması amacıyla konuyla ilgili derslerin öğretim programlarına yerleştirilmesi, küçük yaşlardan itibaren öğrencilerin bu konularda bilgilendirilmesi, siber güvenliği sağlamanın öneminin farkında olmaları gerektiği gibi çözüm önerileri, sunulmuştur.
Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diğer Değişkenlere Göre İncelenmesi	2019	Bu makalede üniversite öğrencilerinin siber güvenlik davranışları kişilik özellikleri ve cinsiyet, sınıf düzeyi, bölüm, bilişim güvenliği eğitimi alma durumu ve haftalık internet kullanım süresi değişkenlerine göre incelenmiştir. Çalışma sonunda, ulaşılan bulgular ışığında siber güvenlik eğitimlerine ağırlık verilmesi ve öğrencilerin kişilik özelliklerinin bu eğitimlerde dikkate alınması önerilmiştir.
User preference of cyber security awareness delivery methods	2014	Bu makalede insan kaynaklı zafiyetlerden kaynaklanan bilgi güvenliği risklerini azaltmak için bilgi güvenliği farkındalığı büyük öneminden bahsetmektedir. Makalede son kullanıcıların bilgi güvenliği farkındalığını ve davranışlarını iyileştirmede kullanılan çeşitli bilgi güvenliği farkındalığı sağlama yöntemlerinin etkileri tartışılmakta ve değerlendirilmektedir.

Tablo 2.1. (Devamı) Literatürde siber güvenlik farkındalığı ile ilgili çalışmalar [21-23].

Başlık	Yayın Yılı	Özet
Karabük Üniversitesi Çalışanlarına Yönelik Kişisel Siber Güvenlik Üzerine Araştırma	2020	Bu makalede, Karabük Üniversitesinde görev yapan akademik ve idari personelin kişisel siber güvenlik algılarını ölçülmüş. Anket yöntemiyle toplanan veriler Cronbach Alpha, tek örneklem t testi, bağımsız örneklem t testi ve ANOVA testi ile analiz edilmiştir. Çalışanların kişisel siber güvenliğe dair algılarında parametrelere göre farklılıklarının olduğuna değilmiş ve çeşitli eğitim önerileri verilmiştir.
Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi	2022	Bu makalede siber farkındalık ile son kullanıcı tarafında kişisel siber güvenlik bilincinin arttırılabileceğine değinilmiştir. Makalede çevrimiçi bireysel kimlik verilerinin güvenliğinin sağlanması kapsamında güvenli parola oluşturulması için son kullanıcılara yönelik yeni yaklaşımlar önermektedir.
Öğrencilerin Siber Güvenlik Farkındalık Düzeylerinin Makine Öğrenmesi Yöntemleri ile Belirlenmesi	2023	Bu makalede siber tehditlerle ilgili, öğrencilerin siber güvenlik farkındalık düzeylerini makine öğrenme yöntemleri ile tespit edilmiştir. Anket yöntemiyle veri toplanılmıştır. Öğrencilerin okudukları bölüm, cinsiyet gibi faktörlerin öğrencilerin siber güvenlik farkındalıklarına etkisinin üzerinde durulmuştur.

Tablo 2.1. (Devamı) Literatürde siber güvenlik farkındalığı ile ilgili çalışmalar [24, 25].

Başlık	Yayın Yılı	Özet
Üniversite Öğrencilerinin Siber Güvenlik Davranışlarının İncelenmesi	2017	Bu makalede, bilişim teknolojileri ile ilgili bir bölümde öğrenim gören üniversite öğrencilerinin siber güvenlik davranışları farklı değişkenler açısından incelenmiştir. İnternet-bilgisayar güvenlik eğitimi alan veya bu konuda iş deneyimi olan öğrencilerin siber güvenlik davranışları daha olumludur. Öğretim programlarına siber güvenlik derslerinin eklenmesi, internet ve internet teknolojileri ile ilgili derslerin arttırılması önerilmiştir.
Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçümlenmesi	2019	Bu makalede; Gümüşhane Üniversitesi'ndeki öğrenci, çalışan ve akademisyenlerin İnternet kullanım düzeyleri ve kişisel bilişim güvenliği tutumları incelenmiştir. Verilerin analizi için açımlayıcı faktör analizi, tanımlayıcı istatistiksel analizler ve iki yönlü varyans analizi kullanılmıştır. Araştırma sonuçları, yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin artırılmasına ilişkin çalışmaların yapılması gerektiği vurgulanmıştır.

3. DENEYSEL ÇALIŞMALAR VE UYGULAMALAR

3.1. Algoritma Belirlenmesi

Proje için birçok soru ve cevap mevcuttur. Bununla beraber kişilerin nasıl davranacağı belirsizdir. Makine öğrenmesi kullanımı kişilerin gruplanması için önemlidir fakat insan davranışı söz konusu olduğunda net olarak bir sonuç elde edilemez. Bundan dolayı, herhangi bir şekilde denetimli makine öğrenmesi algoritmasını kullanmak gibi bir durum söz konusu değildir.

Çalışmanın ilk başlarında denetimli regresyon algoritmaları ile gruplamak istenmiştir. Kişilerin aldığı önlemler ve bu önlemlerin sonucunda daha önce siber saldırıya uğrayıp uğramadı bilgisi baz alınmıştır. Bu bilgiler ışığında davranış analizi yapılmıştır. Fakat anket sonucunda, daha önce hiç siber saldırıya uğramadığını veya bunu bilmediğini iddia edenlerin sayısının çok fazla olduğu gözlemlenmiştir. Bu açıdan, kişiler için siber saldırıya uğramış veya uğramamış gibi net bir sonuca ulaşılamamıştır. Ayrıca daha önce siber saldırıya uğramış bir kişinin, bu olaydan ders çıkarmış olma ve tekrar bu saldırıya uğramama olasılığı da yüksektir.

Yapılan gözlemler ve incelemeler sonucunda, denetimli çalışmaların sonuç vermeyeceği kararına varılmıştır. İnsan davranışlarında, net bir sonuç elde edilemeyeceği için bu kişiler üzerinde çalışma yaparken desteksiz bir algoritma kullanmak daha doğru olacaktır.

Desteksiz algoritmalar incelediğinde birçok çeşit olduğu görülmüştür. İncelemeler sonucunda, desteksiz algoritmalar kategorisindeki gruplama algoritmalarının istenen sonucu verdiği gözlemlenmiştir.

Gruplama, girilen parametrelere göre veriyi benzerliklerine göre gruplara ayıracak algoritmaları içermektedir. Bu algoritmalarda, çalışma mantığı değişmektedir. Merkeze uzaklık, komşuya uzaklık vb. farklılıklar mevcuttur. Fakat hepsinin ortak bir noktası mevcuttur. Bu ortak nokta benzer verilerin gruplandırılmasıdır.

Kodun çalışırlığı ve kurulan sistemin testi için ilk olarak K-means ile testlere başlanmıştır. K-means kodu yazılmış ve bu algoritma ile çalışma kararı alınmıştır.

Kodu yazmak ve grafiği çizdirmek için gerekli olan kütüphaneler indirilerek testlere başlanmıştır. Çalışmalar esnasında Mean Shift algoritmasını da karmaşık durumlarda kullanmak için gerekli kod ve hazırlığı tamamlanmıştır. Çünkü karmaşık verilerde K-means fazladan merkez çizmiştir ve anlamsız gruplama yapmıştır. Bunun için en doğru yolun Mean Shift algoritmasının kullanmak olduğu tespit edilmiştir.

3.2. Verilerin Toplanması ve Formatlanması

3.2.1. Anket nedir

Anket, belli bir konuda saptanmış hipotezlere ya da sorulara bağlı olarak bir evren ya da örneklemi oluşturan kaynak kişilere sorular yöneltmek suretiyle sistemli veri toplama tekniği olarak tanımlanabilir [28].

Bu metodoloji, genellikle yazılı olarak tasarlanmış sorular içeren bir form ya da belge aracılığıyla katılımcılara sunularak, onların yanıtları sistematik bir şekilde toplanır. Sorular, genellikle çoktan seçmeli, açık uçlu veya derecelendirme biçiminde yapılandırılır.

Anketler, çeşitli disiplinlerde, özellikle pazar araştırmaları, müşteri memnuniyeti analizleri, siyasi değerlendirmeler, eğitim araştırmaları, sağlık analizleri ve sosyal bilimlerde, araştırmacılar tarafından kullanılmaktadır. Ankete katılan bireyler, genellikle belirli bir popülasyonu temsil eder ve elde edilen veriler, istatistiksel analizlere tabi tutularak anlamlandırılır.

Anketler, katılımcıların düşünce yapısını, görüşlerini ve tutumlarını anlamak amacıyla kullanıldığından, soruların özenle ve bilinçli bir şekilde formülize edilmesi ve katılımcılara güven verilmesi, anketin güvenilirliği açısından kritik bir önem arz etmektedir.

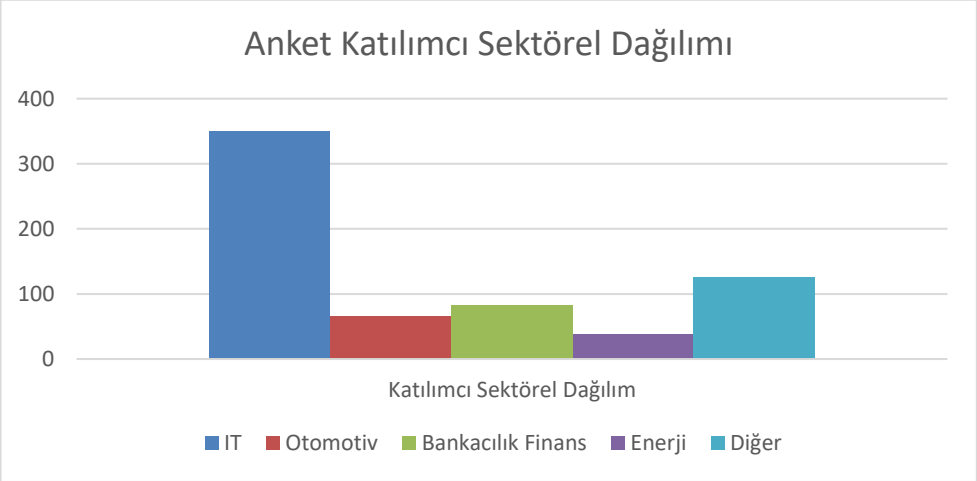
Anketlerin soru sayısının belirlenmesi, araştırmanın kapsamına, metodolojisine, hedef kitlenin özelliklerine ve araştırmanın amaçlarına bağlı olarak değişiklik gösterir. Anketler genellikle katılımcıların dikkatini sürdürmek ve anketi tamamlamalarını teşvik etmek amacıyla belirli bir süre içinde gerçekleştirilir. Bu bağlamda, anketlerin soru sayısının makul ve etkili bir düzeyde tutulması önerilir.

Soru sayısının genellikle 10 ila 30 arasında olduğu görülmekle birlikte, konunun karmaşıklığı, hedef kitlenin özellikleri ve araştırma alanının spesifik gereksinimleri, bu sayının artmasına veya azalmasına neden olabilir.

Tez çalışmam için; kullanıcıların siber farkındalık seviyesini içeren veri seti gereklidir. Çalışanların siber farkındalığını ölçen bir çalışma veya veri seti halihazırda bulunmamaktadır.

Bu çalışmada Google Forms aracılığıyla şirket çalışanları için Siber Farkındalık Formu adlı anket oluşturulmuştur. Katılımcılar, internet üzerinden Siber Farkındalık Formu anketine erişip, anketi anonim olarak doldurmaktadır. Anket ve anket içeriğindeki tüm sorular ekler bölümünde bulunmaktadır.

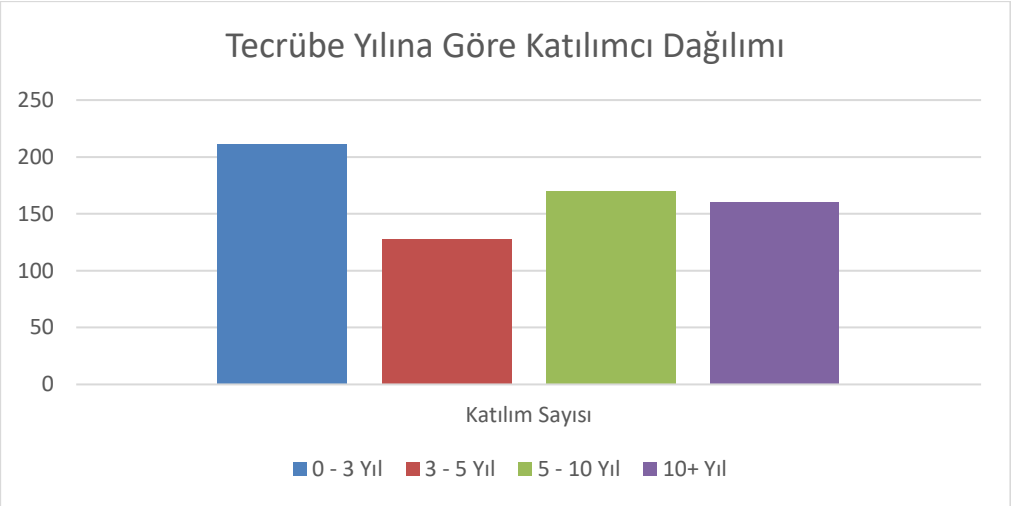
Siber Farkındalık Formu anketi 22 sorudan oluşmaktadır. Bu sorular ile şirket çalışanlarının siber farkındalık oranını ölçmek amaçlamaktadır. Siber Farkındalık Formu anketi, çoğunluğu bilişim, bankacılık, finans, otomotiv vb. sektörlerin çalışanları tarafından doldurulmuştur. Siber farkındalık formu isimli ankete toplam 659 kişi cevap vermiştir. Kişilerin sektörel bazda dağılımı Şekil 3.1.'de görülmektedir.



Şekil 3.1. Anket katılımcı sektörel dağılımı

Siber güvenlik farkındalığı, 'internet kullanıcılarını çeşitli siber tehditlere karşı duyarlı olmaları ve bilgisayarların ile verilerin bu tehditlere karşı savunmasızlığı konusunda eğitmek için bir metodoloji' olarak tanımlanmaktadır [29].

Siber farkındalık, bireylerin ve organizasyonların dijital dünyada karşılaşabilecekleri tehditleri kavrama yeteneğiyle, çevrimiçi güvenliklerini artırma ve savunma stratejilerini geliştirme kapasitesi arasındaki dengeyi sağlar. Anket katılımcılarının tecrübe yılına göre dağılımı Şekil 3.2.'de görülmektedir.



Şekil 3.2. Tecrübe yılına göre katılımcı dağılımı

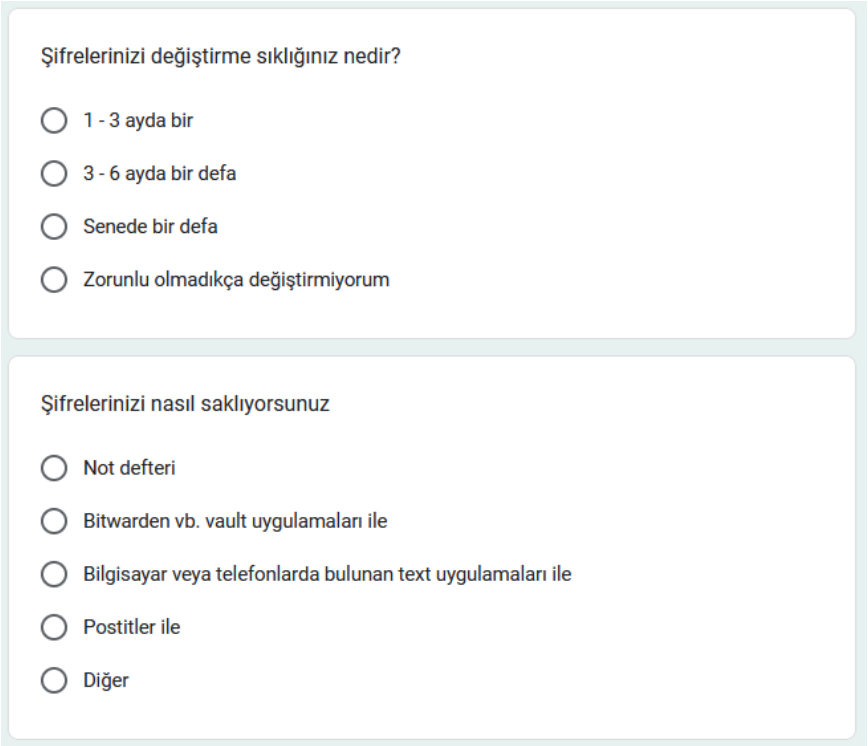
3.2.2. Anket içeriği ve sorular

Makine öğrenmesi ile şirket çalışanlarının oluşturduğu siber güvenlik riskini ölçen ve çalışanlar için gerekli aksiyonun belirlenmesi sağlayan anketimiz aşağıdaki siber farkındalık konu başlıklarından oluşmaktadır.

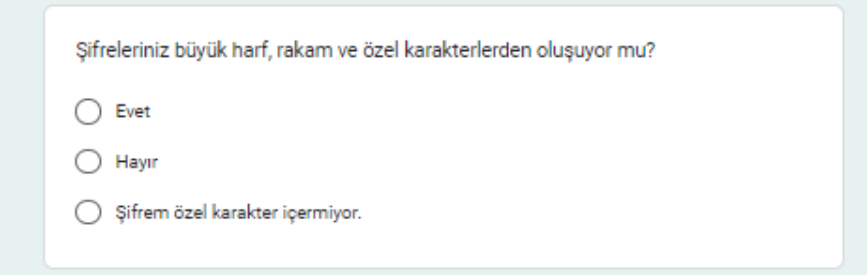
Genel farkındalık soruları ile kişinin siber güvenlik temel terimleri ve kavramlarına olan hakimiyetinin ölçülmesi amaçlanmaktadır. Kullanıcının daha önce siber güvenlik farkındalık eğitimi alıp almadığı ve KVKK (Kişisel Verilerin Korunması Kanunu) hakkında bilgisinin olup olmadığı ölçülmek istenmiştir. Anket, hesap ve parola güvenliğini ölçen sorular içermektedir. Günümüzde oldukça yaygın kullanılan iki faktörlü kimlik doğrulamayla hesap güvenliğimiz artmaktadır.

Şifre güvenliği, dijital hesaplara erişim sağlamak için kullanılan şifrelerin güvenliğini arttırmak amacıyla alınan tedbirleri ifade eder. Parola, genellikle kullanıcı adıyla birlikte kullanılan ve hesap güvenliğini sağlamak için gizli tutulan bir kimlik doğrulama bilgisidir. Temel hedef, bu şifrelerin yetkisiz erişimlere karşı korunmasını sağlayarak kullanıcı hesaplarını güvende tutmaktır.

Anket şifre güvenliği sorularını da içermektedir. Uzun, karmaşık ve rastgele karakterlerden oluşan şifrelerin tercih edilmesi gerekmektedir. Şekil 3.1 ve Şekil 3.2'deki sorularla, şifrelerin ne tür karakterleri içerdiği, şifre değiştirme sıklığı ve kullanıcıların şifrelerini nasıl sakladığı sorularıyla kullanıcının parola güvenliği bilgisini ölçmek amaçlanmıştır.



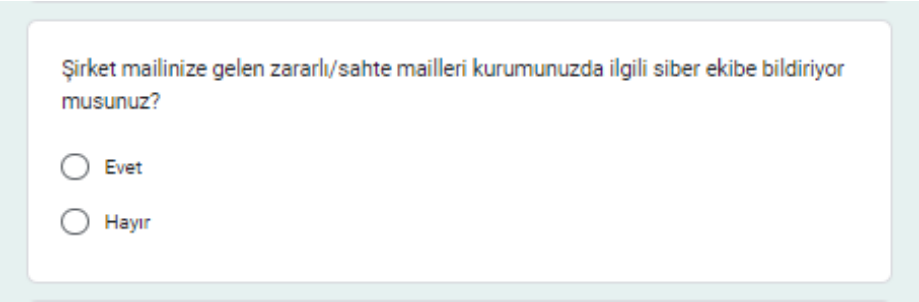
Şekil 3.3. Anket soruları.



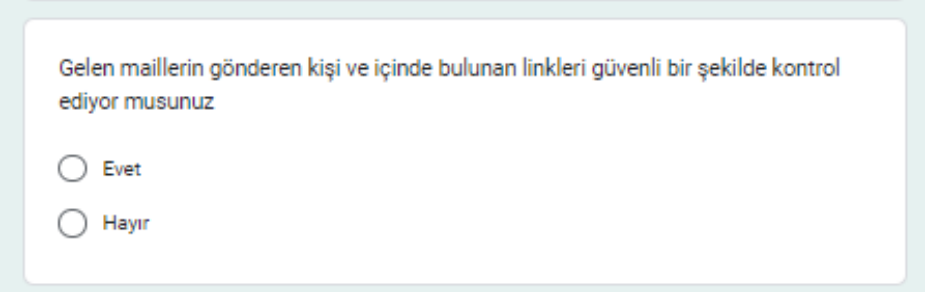
Şekil 3.4. Anket soruları.

E-posta güvenliği, elektronik posta iletişiminin çeşitli tehditlere karşı korunmasını sağlayan önlemleri ifade eder. Bu önlemler, e-posta hizmetleri üzerinden gönderilen ve alınan iletilerin gizliliğini, bütünlüğünü ve güvenliğini artırmayı amaçlar. E-posta güvenliği, bireylerin, işletmelerin ve kuruluşların hassas bilgilerini koruma, siber saldırılara karşı direnç gösterme ve güvenilir iletişim kanalları oluşturma konularında kritik bir rol oynar.

E-posta güvenliği, elektronik posta iletişimini korumak ve yetkisiz erişim, veri sızıntısı, kimlik avı (phishing), kötü amaçlı yazılımlar gibi tehditlere karşı önlemler almayı sağlar. Çalışan, kendisine gelen maillerdeki linkleri dikkatle kontrol etmelidir. Şirket mailine gelen zararlı/sahte mailleri ilgili ekibe bildirmesi şirket için önem teşkil eder. Şekil 3.5. ve Şekil 3.6. mail güvenliği ile ilgili sorular içermektedir.



Şekil 3.5. Anket soruları.



Şekil 3.6. Anket soruları.

3.2.3. Veri formatlanması

Anket verileri, verilen soru ve soruların cevapları incelediğinde çoğunun karakter ve metinlerden oluştuğu görülebilir. Veri seti sayısal veriden oluşmamaktadır. Veri setini kod içinde kullanabilmek için metinsel veriler sayısal bir formata çevirmek gereklidir.

Ayrıca, kullanılan algoritmalar doğrultusunda verileri sayısal formata dönüştürmek gereklidir. Bu işlem, grafiksel veri veya kod içinde kullanılırken veri setinin optimizasyonda sorun oluşturmaması için önemlidir. Şekil 3.7.'de bulunan kod parçası bu dönüşüm için kullanılmıştır.

```
import csv
formLines = []

with open('Data/FormAnswers.csv', mode ='r', encoding='UTF8')as file:
    csvFile = csv.reader(file)
    for lines in csvFile:
            formLines.append(lines)


def FormatData():
    for item in formLines:
        if item[1] == "Çalışıyor":
            item[1] = 1
        elif item[1] == "Çalışmıyor":
            item[1] = 0
```

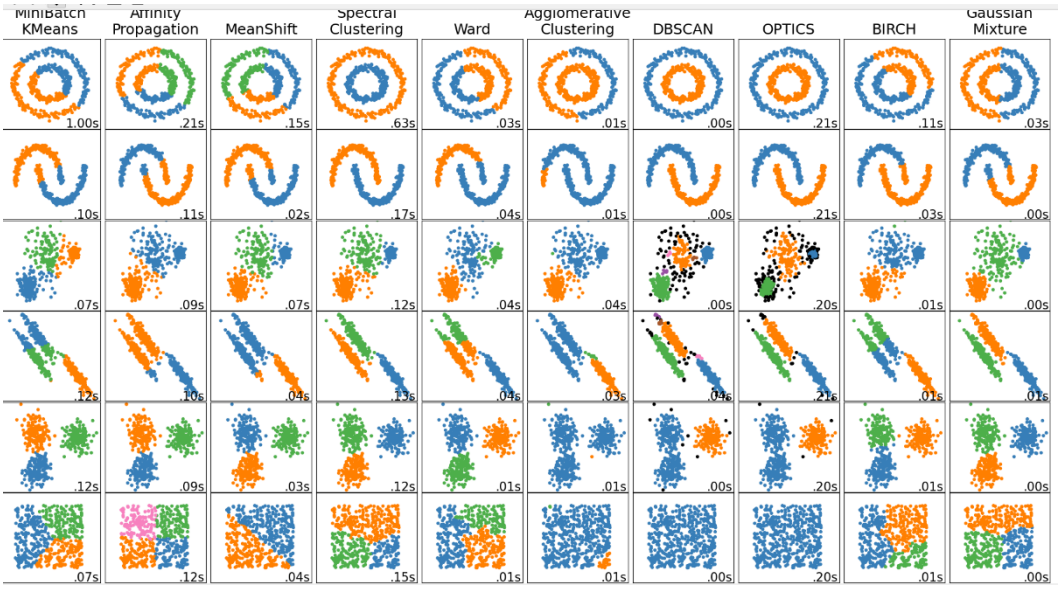
Şekil 3.7. Veri formatlama kodu.

Şekil 3.6. ve 3.5.'te görüldüğü gibi veriler "Evet", "Hayır"; Şekil 3.7.'de ise "Çalışıyor", "Çalışmıyor" gibi metinsel ifadeler barındırmaktadır. Verilerin çevirimi "evet = 1 hayır = 0", "Çalışıyor = 1 çalışmıyor = 0" olacak şekilde yapılır. Evet/hayır gibi ikili cevaplar dışında, birden fazla cevabı olan sorular için farklı bir yapı izlenmesi gerekmektedir.

İkili cevaplar dışındaki sorular için de parametresel bir yol izlenmesi gerekmektedir. Bu dönüşüm, 1 ve 0 dışında rakamlar kullanılarak yapılmıştır. Örneğin ankette bulunan, tecrübe yılı sorusunun dört adet cevabı vardır. 0-3, 3-5, 5-10, 10+ cevaplarına sırasıyla 1,2,3,4 sayıları verilmiştir ve bu veriler ile yeni bir doküman oluşturulmuştur. Formatlanmış doküman sayısal verilerden oluşmaktadır. Bu sayısal veriler algoritmalarda kullanılmıştır.

3.3. Test ve Performans Ölçümü

En doğru algoritmanın tespiti için belirli modellerde rastgele veriler oluşturulmuştur. Yapılan anket dışında, rastgele oluşturulan veriler ile birlikte en çok bilinen algoritmaların performansı ve verdiği çıktıları görmek için bir çalışma yapılması gereklidir. 10 adet algoritmanın bulunduğu ve bunların test edilebileceği bir yapı hazırlanmıştır. Oluşturulan rastgele veriler ile spiral, dairesel, halka, çizgisel ve rastgele vb. olmak üzere 6 çeşit veri tipi hazırlanmıştır. Hazırlanan veriler, sırayla algoritmalara sokularak Şekil 3.8.'de bulunan grafik elde edilmiştir.



Şekil 3.8. Algoritma karşılaştırma grafiği.

Şekil 3.8.'deki grafik incelendiğinde kullanımının uygun olacağı düşünülen birkaç algoritma belirlenmiştir. Algoritmalar üzerinde araştırmalar yapılarak, bu algoritmalar üzerinden ilerlenmek hedeflenmiştir. Belirlenen algoritmalardan ilki DBSCAN'dir. Bu algoritmanın en büyük avantajları şu şekildedir; grup sayısını önceden belirlenmesinin gerekmemesi, karmaşık ve değişik şekildeki verilerin kolayca gruplanabilmesi, gürültü kavramının bulunmasıdır [30]. DBSCAN algoritmasının belirtilen bu özelliklerinden dolayı, kullanımının uygun olduğu gözlemlenmiştir. Özellikle gürültü kavramı, gruplar dışında kalan istisna durumlar açısından yararlı olacaktır. Fakat zamanla bazı durumlarda, anket verileri ile yapılan tüm noktalar gürültü olarak algılanmıştır. DBSCAN algoritmasının, tüm anket cevaplarını gürültü olarak görülmesinden dolayı kullanımı uygun olmamıştır.

DBSCAN durumu öğrenildikten sonra buna benzer olan diğer algoritmalar kullanımdan çıkartılmıştır. Yapılan araştırmalar sonucunda, siber farkındalık anketimizin veri setleri için K-means algoritmasıyla devam etme kararı alınmıştır. Son olarak, K-means'a benzer çıktılar üreten Mean Shift algoritması araştırıldığında 3 parametre alabildiği fark edilmiştir. Bu durumda, algoritmaya sadece kişilerin tecrübe yılı ve X bir parametre eklemek yerine başka bir Y parametresi de ekleyerek üç boyutlu uzayda grafik çıkarılabileceği tespit edilmiştir.

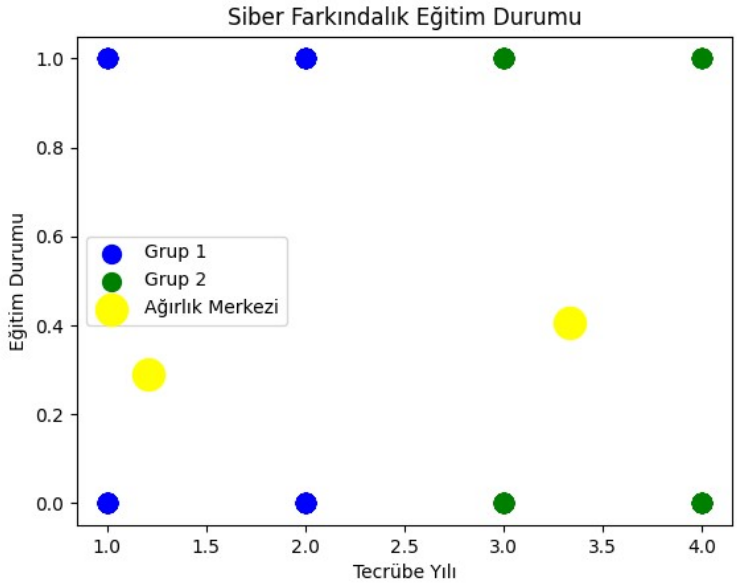
Örneğin, tecrübe yılı, oltalama saldırısına uğrayanlar ve mail URL (Uniform Resource Locator, Tekdüzen Kaynak Bulucu) kontrolü gibi 3 parametre ekleyerek kişilerin bilinç seviyesi hakkında bir çıkarımda bulunabiliriz. 3 parametre almasından dolayı Mean Shift algoritmasının kullanımı yapıyı kurmak için gerekli olacaktır. Ayrıca karmaşık veri setinde iyi sonuçlar elde edebilir.

Şekil 3.8.'de görüldüğü gibi incelenmesi gereken veriler, grafikte çıkan 3. veya 5. şekildekiler gibi düz bir düzlemde rastgele dağılmış gözükecektir. K-means, Mean Shift ve birkaç algoritma dışında gruplama dağılımı düzgün yapılamamıştır. Şekil 3.6. incelendiğinde, verilerin en az üç gruba ayrılması gerekirken bazıları iki gruba bazıları bir gruba ayrılmıştır. Ayrıca veri setini gürültü olarak algılayan algoritmaların olduğu gözlemlenmektedir. Anket verilerinin bu kadar karmaşıklık içermediğini varsayarsak, en az üç gruba ayırma yapmayan algoritmaların kullanımı uygun olmayacaktır.

Karar sonrası, artık test verileri veya rastgele veriler yerine; bu algoritmalar üzerinde anket verilerinin formatlanmış hali test edilecektir. Çalıştırılan veriler sonrasında

DBSCAN tüm verileri gürültü olarak algılanmıştır. DBSCAN, iki cevabı olan soruların tamamını gürültü olarak algılamıştır. Cevap sayısı ikiden fazla olan sorular için ise sadece tek bir veri grubu oluşturulmuştur. Bu tez çalışması kapsamında DBSCAN algoritmasının kullanılmasının doğru sonuç vermeyeceği görülmektedir.

K-means ile yapılan test sonrasında, iki cevabı olan sorular için uygun sonuç alınmıştır. Şekil 3.9.'da görüldüğü gibi evet veya hayır cevaplı bir soru için merkez noktaları çıkarılmıştır. Ayrıca gruplama işlemi de ihtiyaçlar doğrultusunda gerçekleşmiştir.



Şekil 3.9. Anket soruları ile test edilen K-means grafiği.

Algoritma doğruluğu için örnek bir parametre seçilmiştir ve bu parametre ile Şekil 3.9.'da oluşan grafiğin doğruluğu test edilmiştir. Grafikte anlatılana göre veri seti 2 gruba bölünmektedir. Bir grup mavi, 0-3 ve 3-5 yıl tecrübe aralığındaki çalışanları göstermektedir. Diğer grup ise yeşil, 5-10 ve 10+ yıl tecrübe aralığındakileri göstermektedir. Bir diğer parametre ise daha önce siber farkındalık eğitimi alınıp alınmadığının bilgisidir. Centroidlere (ağırlık merkezi), bakılırsa mavi grup için centroid 0,3 seviyesinde yer almaktadır. Yeşil grubun ağırlık merkezi ise 0,4 seviyesinde bulunmaktadır. Elde edilen verilere göre, tecrübe yılı az olan kişilerin çoğunlukla siber farkındalık eğitimi almadığı görülmektedir. Doldurulan anket verileri filtrelenip incelediğinde durumun bu şekilde çıkması olasıdır. Veri seti incelendiğinde, 0-5 yıl arasında tecrübeye sahip kişilerin eğitim düzeyinin, tecrübe yılı 5 yıldan fazla olan kişilerden düşük olduğu gözlemlenmektedir. Ayrıca 0-5 yıl tecrübeli

katılımcıların olduğu grupta, 0-3 yıl tecrübeli kişilerin sayısının; 3-5 yıl iş tecrübesine sahip gruptan fazla olduğu gözlemlenmiştir. Grafikteki mavi grubun merkezinin de sola kaydığını görülebilir. Çünkü ağırlık merkezi olarak 0-3 yıl arası tecrübeye sahip katılımcı sayısı daha fazladır. Bu test, birkaç veri ile daha test edilmiştir sonra aynı şekilde Mean Shift grafiklerinde de yapılan çalışmalarda güzel bir gruplama yaptıklarını ve algoritmaların doğru çalıştığı görülmüştür.

3.4. Gerçekleme ve Yorumlama

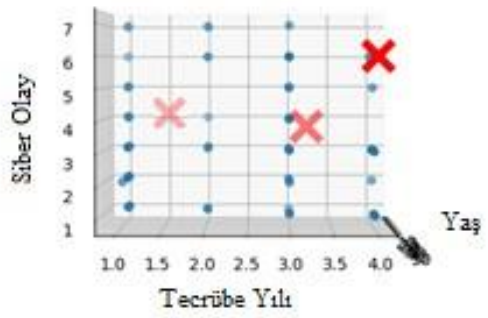
Grafiklerin doğruluğunu sağladıktan sonraki aşama, verilerin incelenmesi ve yorumlanmasıdır. Bu aşamada şu şekilde ilerleme yapılmıştır: Ana parametre olan tecrübe yılına göre diğer veriler çalıştırılmıştır ve durum not edilmiştir. İşlemler sırasında değişik tecrübe yıllarına göre cevaplar birbiri ile kıyas edilmiştir. Algoritmaya sokulan cevaplar, genel işlemler sonrasında bir de tecrübe yıllarına göre sınıflandırılmıştır. Örneğin, sadece 0-3 yıl tecrübeye sahip olan kişiler için algoritma çalıştırılarak detaylı veriler incelenmiştir. Ardından, sadece 3-5 yıl tecrübeye sahip olan kişiler için benzer bir analiz gerçekleştirilmiştir.

Şekil 3.9'da görüldüğü gibi mavi grubun merkezinde sola kayma gerçekleşmiştir. Bu, mavi grup üyelerinin içinde 0-3 yıl tecrübe yılına sahip kişilerin daha çok olduğu anlamına gelmektedir. Merkez noktasının bulunduğu konumu belirleyen 0-3 yıl tecrübe aralığındaki kişiler, 3-5 yıl arasında tecrübeye sahip kişilerin cevabını etkilemektedir. 0-5 yıl tecrübe aralığını oluşturan grupta 0-3 yıl tecrübe yılına sahip kişiler çoğunluğu oluşturmaktadır. Bu da bize yanlış sonuç üreteceğinden dolayı genel bazda, algoritma çalıştırıldıktan sonra bir de detay bazda, her bir tecrübe yılı grubu için çalıştırılıp incelemeler yapılmıştır.

Bundan sonraki işlemler için veri seti, değişik parametrelerle yorumlanarak matris oluşturulmuştur. Bunun için genelden özele giden bir yapı kurulmuştur. Bu yapıda, her tecrübe ve yaştan insanlar tek bir yapı altında incelenmiştir. İnceleme sonunda, yaş bazında yapılan çalışma ile kişilerin siber risk oluşturup oluşturmayacağı daha net anlaşılmaktadır. Bu durum kişilerin, hangi koşullarda risk oluşturacağı konusunda bir sonuç üretmektedir.

İlk incelenmiş veri, kişilerin daha önce siber saldırı olayı yaşayıp yaşamadıkları bilgisidir. Bu sorunun cevabı, ikiden fazla olduğu için en doğru sonucu alabilmek

adına Mean Shift algoritması kullanılmıştır. Algoritmaya, kişilerin yaşı, tecrübe yılı ve daha önce siber saldırı yaşayıp yaşamadıkları bilgisi olacak şekilde 3 parametre verilmiştir. Şekil 3.10. incelediğinde, grafiğin x eksenindeki sayılar tecrübe yılını göstermektedir. X ekseninde 1 rakamı 0-3 tecrübe yılı aralığını; 2 rakamı 3-5 yıl tecrübe aralığını; 3 rakamı 5-10 yıl tecrübe aralığını; son olarak 4 rakamı ise 10+ yıl tecrübeyi göstermektedir. Tüm grafiklerimiz için x eksenindeki anlamlandırma bu şekilde olacaktır.



Şekil 3.10. Daha önce yaşanan siber saldırı olay grafiği.

Şekil 3.10.'da bulunan grafikte, sağ tarafta z ekseninde sıkışık halde bulunan veriler, kişilerin yaş bilgisini göstermektedir. Y eksenindeki veriler, kişilerin bu soruya verdiği cevabı simgelemektedir. Soruya ait cevaplar ikiden fazla olduğu için verinin formatlanması gereklidir. Grafikte y ekseninde bulunan rakamlara göre cevaplar şu şekildedir; 1 = "bilmiyorum", 2 = "yaşamadım", 3 = "Mail yolu ile link yönlendirmesi sonucu bilgilerin ele geçirilmesi (Phishing, Oltalama)", 4 = "Zararlı sitelerde gezinme sonucu", 5 = "Farklı cihazlarda kullanılmış tanışabilir disk/CD vb. cihazların kullanımı", 6 = "İnternet üzerinden indirilen bir uygulama ile", 7 = "3. bir kişiden elde edilen zip/rar tarzı dosyalar üzerinden".

Şekil 3.10.'da bulunan grafiğin yorumlanması aşamasında, kırmızı çarpı olan merkezler ve mavi noktalar cevapların çoğunluğu oluşturur. Çoğunluğun olduğu noktalar incelenerek veriler kaydedilmektedir. Şekil 3.10 incelendiğinde, 0-3 ve 3-5 yıl tecrübe aralığındaki kişilerin daha çok dördüncü cevapta toplandığı görülebilir. Bu

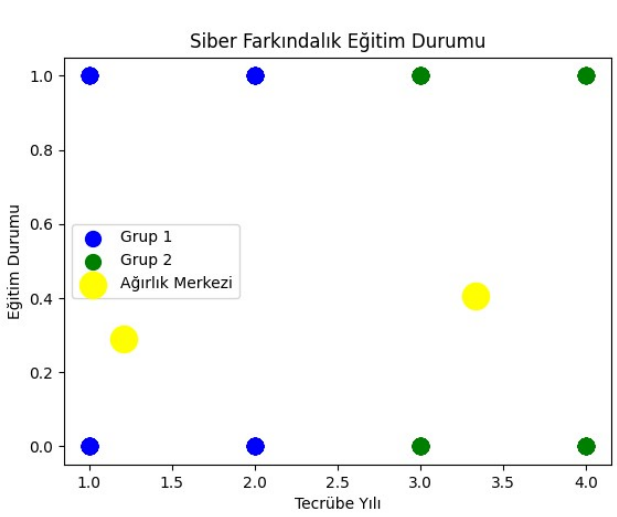
demektir ki, yeni çalışma hayatına girmiş olan, tecrübesi az kişiler genelde 4 numaraya denk gelen olay "Zararlı sitelerde gezinme sonucu" şıkkını seçmişlerdir. Tecrübesi 0-3 yıl arasında olan kişiler, girdikleri sitelerde HTTPS (Hypertext Transfer Protocol Secure, Köprü Metni Aktarım Protokolü Güvenli) kontrolü yapmamış olabilirler veya bilmedikleri herhangi bir sitede HTTPS bulunsa bile güvenilirliğini kontrol etmemiş olabilirler. Kişiler, bu sitelerde gezinirken, bir reklama tıklamış olabilirler veya bir uygulama, dosya vb. indirme işlemi gerçekleştirmiş olabilirler. Bundan dolayı bilgisayara zararlı bir yazılım yüklenmesine, cookie'lerinin (çerezlerinin) çalınmasına, kişisel bilgilerinin çaldırılmasına sebep olmuş olabilirler. Bu durumda, tecrübesi az olan insanlar internette yaptığı sörflerde dikkatli olmalılar sonucu çıkarılmaktadır. Bunun için şirketler, çalışanlarını bu konuda bilinçlendirmeliler. Kişilere güvenli internet gezintisi hakkında eğitim, seminer verilmelidir. Şirketler, tuzaklar hazırlayarak kişilerin, olayı tecrübe etmesi sağlayarak kişilerin öğrenmesi sağlanabilir. Tez çalışmamın son aşamasında, alınması gereken aksiyonlar içerisinde bu konulardan bahsedilmektedir.

Veriler detay bazda incelendiğinde tecrübesi az olan kişilerin, daha çok bilmiyorum seçeneğini işaretlediğini görülebilir. Bu da tecrübesi az olan kişilerin bilinçsiz davrandığının göstergesidir. Bu işlem ayrıca tecrübe yılı ve yaş bazlı yapılmaktadır. Detaylı gösterimlerde de inceleme mevcuttur.

Aynı durumun bir değişiği ise tecrübe yılı fazla olan kişilerde gözlemlenmektedir. İnternet sitelerinden indirilen uygulamalar (6 numara) aracılığı sonucu benzer siber olaylar yaşandığı görülebilir. Site güvenli olsa da indirme yapmamak gerekmektedir. İndirme işlemi sonrasında, bilgisayara aktif olmayan bir virüs girebilir ve açık kapı bırakıp ağa yayılabilir. Bundan dolayı, internette gezinirken dikkatli olma alışkanlığı elde edilmelidir. Şekil 3.10'daki sonuçlar 0-3, 3-5 ve 5-10 yıl tecrübe aralığı için 4 noktasında toplanmıştır. 10 yıldan fazla tecrübeli çalışanlar içinse 6 numaralı cevapta toplanma görülmektedir. Bu cevaplar genel gösterim tablosunda rakamsal olarak kullanılacaktır.

Bir sonraki yorum için parametreler değiştirilip, kişilerin siber güvenlik eğitimi alıp almadığının bilgisi analiz edilmiştir. Şekil 3.11.'de görüldüğü üzere, genel bazda bakıldığında eğitim görenlerin sayısının az olduğu gözlemlenmektedir. Özellikle tecrübesi az olan kişiler arasında, eğitim almış kişilerin sayısının az olduğu gözlemlenmiştir. Şekil 3.11.'deki grafik ve verileri incelenmiştir. Sorulan soru, daha

önce siber güvenlik eğitimi alıp alınmadığı sorusudur ve evet/hayır cevabından oluşmaktadır. Bu cevaplar koda dökülürse, karşılığı 1 ve 0 olduğundan, yeşil ve mavi grupların sadece 1 ve 0 da toplandığı fark edilmektedir.



Şekil 3.11. Siber eğitim grafiği.

Veri seti, karmaşık cevaplar içermediği için Mean Shift algoritmasının kullanılması uygun değildir. Veri seti K-means algoritması ile çalışıldığında ise doğru bir sonuç elde edilmektedir.

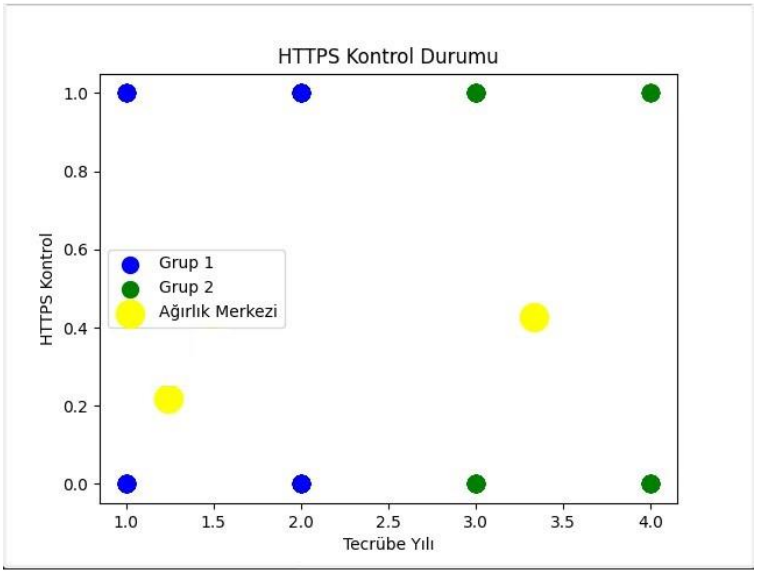
Şekil 3.11.'de görüldüğü gibi grup sayısı, algoritma tarafından 2 adet oluşturulmuştur. Oluşan gruplar, 0-5 yıl ve 5 yıldan fazla tecrübeye sahip kişiler olarak ikiye ayrılmaktadır. Genel bazda yorumlama yapıldıktan sonra detay bazda inceleme yapılarak, daha doğru bir sonuç elde edilebilir.

1 ve 2 numaralı kişiler, 0-3 yıl ve 3-5 yıl arasında tecrübeye sahip olan kişilerin sıfıra olan yakınlığı fazladır. Bu kişiler, şirket için risk oluşturmaktadır. Ayrıca, bu sonuç, Yaşanılan siber olayın 0-3 yıl tecrübe aralığındaki çalışanlar detay bazda incelenmesi sonucunda bu grubun ağırlık merkezi bilmiyorum cevabında toplamıştır. Bu bilgi ile siber güvenlik eğitimini almamaları birleştirilirse, şirketler yeni alınacak veya var olan çalışanların tecrübe yıllarına bakarak, siber güvenlik eğitimini baştan vermelidirler.

Grup 2 için incelenirse bu oranın neredeyse yarı yarıya olduğu gözlemlenmektedir. Tez çalışmasının ilerleyen aşamalarında detay bazda inceleme yapılacaktır. Fakat genel olarak tecrübe yılı fark etmeksizin her kişiye temel siber farkındalık eğitimi mutlaka verilmelidir. Tez çalışmasının ilerleyen aşamalarında, siber risk matrisi

oluşturulurken, siber farkındalık eğitim eksikliğinin büyük risk teşkil ettiğine değinilmektedir.

Bu çalışmada ankete cevap veren kişilerin girdiği sitelerde, HTTPS kullanılıp kullanılmadığını kontrol edilip edilmediği öğrenilmek istenmiştir. Şekil 3.10.'da 10 yıldan fazla iş tecrübesine sahip kişilerden, internet gezintilerinde saldırıya uğradıkları cevabı alınmıştır. Bu doğrultuda Şekil 3.12. incelendiğinde bu tip bir grafik görme olasılığı yüksektir.



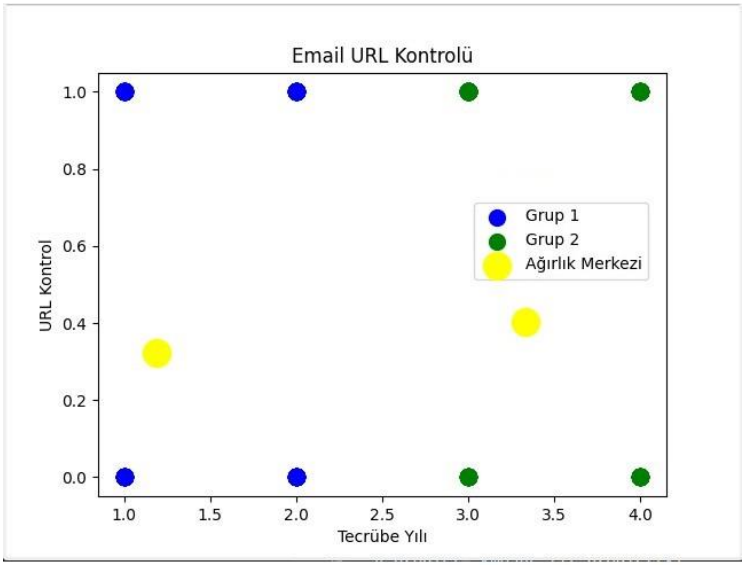
Şekil 3.12. HTTPS kontrol durumu grafiği.

Tecrübe fark etmeksizin, HTTPS kontrolünün çok az olduğu gözlemlenmektedir. Kişilerin verdiği cevaplar, 0 ise HTTPS kullanımını kontrol etmediği, 1 ise kontrol ettiği anlamına gelmektedir. Gözlemler sonucunda, merkez ağırlığının, yoğunluğun sıfıra daha yakın olduğu tespit edilmiştir. Anket katılımcılarının, HTTPS kontrolü açısından eksik olduğu görülmektedir. Bu durumda kişilerin, internet üzerindeki sahte sitelere girip bilgilerini çaldırma olasılığı yüksektir.

Son zamanlarda, kurulan tuzaklara yakalanan insanların sayısının fazla olması da bu grafiği doğrular niteliktedir. Milli Gazete haber sitesinde 2023'te yayınlanan bir haberde, çok kullanılan bir alışveriş zincirine ait sahte bir site ve uygulama yapıldığı duyurulmuştur [31]. Bu alışveriş zincirinin web sitesi tamamen kopyalanmıştır. Arama motorlarında en üstte çıkabilmesi için reklamlar ve SEO (Search Engine Optimization, Arama Motoru Optimizasyonu) ayarlaması yapılmıştır. İnternette bu alışveriş zincirini

araştırdığınızda karşınıza bu sahte site çıkmaktadır. Eğer link ve HTTPS kontrolü yapılmazsa bu tuzağa yakalanma olasılığı yüksektir.

Diğer bir kontrol Şekil 3.13.'te kullanılan ve dikkat edilmesi gereken konulardan bir tanesidir. Kimlik avı saldırısı, gizlenmiş e-postayı silah olarak kullanan bir siber saldırı türüdür [32]. Kimlik avının çeşitlerinde kısa mesajlar, sesli posta veya QR (Quick-Response Code, Hızlı Cevap Kodu) kodları kullanılır. Bu saldırılar, e-posta alıcısını mesajın istediği veya ihtiyaç duyduğu bir şey olduğuna (örneğin bankadan gelen bir istek) inandırmak için sosyal mühendislik tekniklerini kullanır.



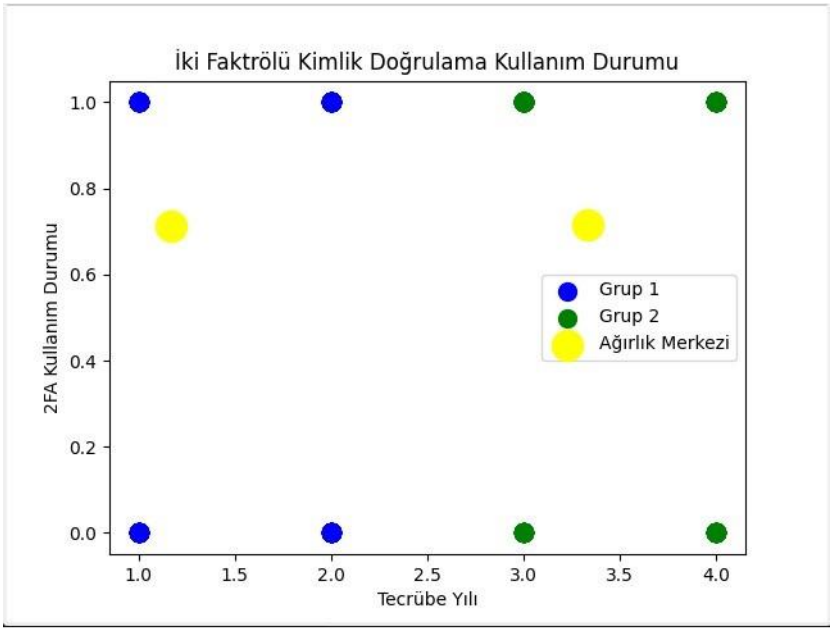
Şekil 3.13. E-mailde bulunan link kontrolü grafiği.

Josh, F.'nin CSO adlı web sitesinde yayınladığı blog yazısından yola çıkarak, özellikle şirkette önemli bir rol oynayan kişilerin gelen maillerde bulunan uzantılar ve linklerin kontrol etmesi gerektiğine değinilmiştir [32]. Oltalama saldırısına uğrayıp bilgilerini çaldıran çok fazla insan mevcuttur. Oltalama saldırısı, şirketlerin dikkat ettiği ve çalışanlarını uyardığı bir konudur. Bu konuda dikkatli olmak ve kontrol sağlamak, kişilerden beklenen bir aksiyondur. Ayrıca, bilgisayar kullanıcılarının dikkatsizliği nedeniyle kimlik avı saldırıları çok karmaşık ve hatta daha başarılı hale gelmiştir. Başarılı kimlik avlarının özellikle çalışan nüfus üzerinde güçlü etkileri vardır ve ulusal güvenliğini de tehdit etme potansiyeline sahiptir [33].

Gelen linkler, örneğin google.com değil de g00gle.com gibi değişik domainler gelmiş olabilir. Çok farklı bir link üzerinden de yönlendirme yapılabilir. İki grup için de genel

olarak 0,3 ve 0,4 seviyesinde bir sonuç alınmıştır. Tam güvenlik için bu oranın 0.8 ve 0.9 seviyesine kadar yükseltirilmesi gerekmektedir.

İki faktörlü kimlik doğrulama kullanımı konusunda oluşan grafik Şekil 3.14.'te verilmiştir. Tecrübe yılı fark etmeksizin kişiler, çoğunlukla aktif olarak İki faktörlü kimlik doğrulama kullanmaktadırlar. Bu açıdan kişilerin bilgileri çalınsa bile kişisel cihazlarından veya uygulamalarından yetki vermedikçe saldırganlar erişimi ele geçiremeyeceklerdir.



Şekil 3.14. İkili kimlik doğrulama kullanım grafiği.

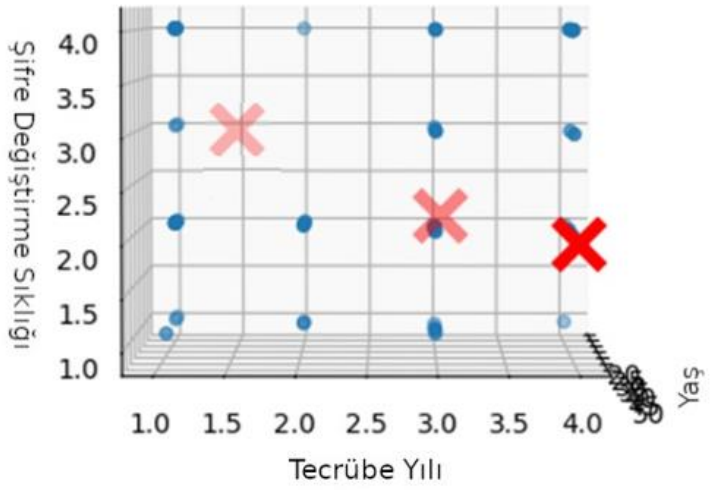
2FA (Two-factor authentication, İki faktörlü kimlik doğrulama), kullanıcıların şifrelerini girene kadar hesaplarına erişmelerine izin verilmemesini ve ayrıca farklı kimlik kanıtları sağlamalarını (örneğin, parmak izlerini doğrulamaları veya sahip olduklarını kanıtlamaları gerekebilir) gerektiren bir kimlik doğrulama tekniğidir. İki adımlı kimlik doğrulama kullanılarak hesapların güvenliği artırılır ve parolaların çalınma olasılığını düşürür. Kişilerin hesaplarına, saldırganların yetkisiz erişim durumlarını azaltır. 2FA, kuruluşların uğradığı kimlik avı saldırılarını veya insan hatası sonucu oluşan açıklıklara karşı kendilerini daha etkili bir şekilde korumalarına olanak tanır [34].

Sosyal mühendislik, oltalama saldırıları vb. yollarla çalınan bilgileri kullanmak isteyen saldırganların işlem yapmalarını engelleyen ek bir yöntem olarak 2FA'dan

bahsedilebilir. Bu açıdan 2FA kullanımı oldukça önemlidir. Uygulamada, e-posta girişlerinde, hesaplarda vb. yerlerde kullanmanın faydası vardır.

Uygulamaların, insanları 2FA kullanması konusunda zorlamasından dolayı yüksek bir kullanım oranı gözlemlenmektedir. Telefon, SMS (Short Message /Messaging Service, Kısa Mesaj/Mesajlaşma Servisi), MicrosoftAuthenticator vb. uygulamalar kullanılırsa veriler saldırganlar tarafından ele geçirilse bile, kullanıcılar telefondan kod veya onay vermedikçe saldırganlar, kullanıcılara ait sistemlere giremeyecektir. 2FA'nin kullanım oranının yüksek olması oldukça önemlidir.

Bir sonraki kontrol, şifrenizi ne sıklıkla değiştiriyorsunuz sorusu üzerine, Şekil 3.15.'te gösterilmiştir. Bu sorunun ikiden fazla cevabı mevcuttur. Cevap sayısı ikiden fazla olduğu durumda, Mean Shift kullanılarak gösterim yapılması gerekmektedir. Parametre olarak yaş ve tecrübe yılı girildikten sonra ölçülmek istenen diğer veri olan, şifre değişiklik aralığı bilgisi kullanılmıştır.



Şekil 3.15. Şifre değiştirme sıklığı grafiği.

Şekil 3.15.'te bulunan grafikte, X düzlemi tecrübe yıllarını, Z düzlemi yaş ve Y düzleminde bulunan rakamlar ise kişilerin cevaplarını belirtmektedir. Cevaplar 1 = "1-3 ayda bir", 2 = "3- 6 ayda bir defa", 3 = "Senede bir defa", 4 = "Zorunlu olmadıkça değiştirmiyorum" olacak şekilde sıralanmıştır.

Şekil 3.15.'te bulunan grafik incelendiğinde, tecrübesi 5 yıldan az olan kişilerin üçüncü seçenekte yoğunlaştığı görülmektedir. Bu da kişilerin çoğunlukla şifrelerini senede bir defa değiştirdiği anlamına gelmektedir. 5 yıldan fazla tecrübesi olan

kişilerin, 3-6 ayda bir şifre değiştirdiği görülmektedir. Bu durum tecrübesi 5 yıldan az olan kişilere kıyasla daha iyi bir durumdur. Yapılan araştırmalara göre, kullanıcıların 1-3 ayda bir şifre değişikliği yapmasının uygun olduğu görülmüştür. Fakat tecrübe yılı 5 yıldan az olan kişilerin, senede bir defa şifre değiştirmeleri şirketler açısından risk teşkil eder.

Kişiler, hesaplarının tümü için aynı şifreyi kullanıyorlarsa ve eğer kişilerin hesaplardan biri saldırıya uğrarsa diğer hesaplarının da saldırıya uğrama olasılığı yüksektir. Her hesabın benzersiz bir şifresi olmalıdır. Örneğin; Facebook şifresi, iş şifresi olarak veya mobil bankacılık şifresi olarak kullanmamalıdır [35]. Şifrelerin sık sık değiştirilmesinin faydaları şu şekildedir:

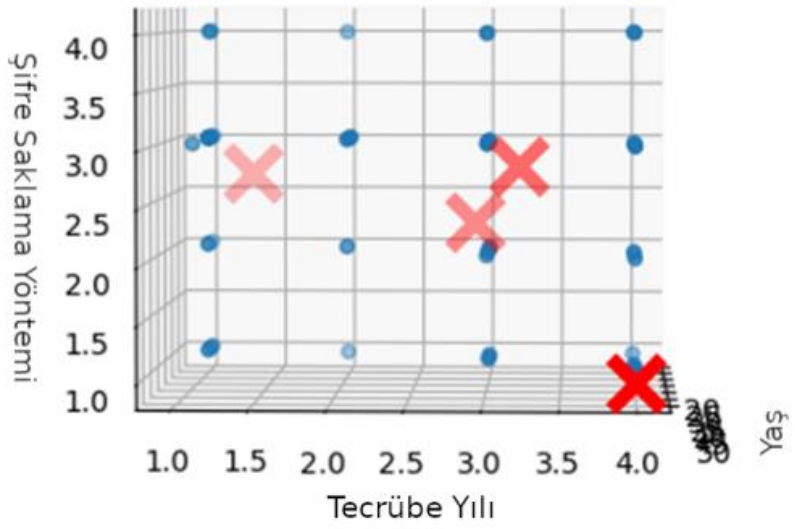
- Sürekli erişimi engeller: Bir bilgisayar korsanı, belirli bir süre içinde hesabınıza birden fazla kez erişmeye çalışabilir. Şifrenizi sıklıkla değiştirmeniz, saldırganın erişime sahip olma riskini azaltır [35].
- Kayıtlı şifrelerin kullanılmasını engeller: Bilgisayarlarınızı kaybederseniz veya değiştirirseniz, başka birinin şifrelerinize erişmesi mümkündür. Şifrelerinizi düzenli olarak güncellemek, saldırgan eski veya kayıtlı bir şifre bulsa bile şifrenin artık kullanışlı olmayacağı ve verilerinizin güvende olacağı anlamına gelir [35].
- Tuş vuruşu kaydediciler tarafından elde edilen erişimi engellemek: tuş vuruşu kaydedici tuş vuruşlarını kaydetmek için kullanılan gözetim teknolojisidir. Genellikle kredi kartı bilgilerinin yanı sıra oturum açma kimlik bilgilerini çalmak için kullanılır. Şifrenizi düzenli olarak değiştirmek, bu şekilde elde edilen şifrelerin herhangi bir süre boyunca yararlı olma olasılığını azaltır [35].

Bruteforce saldırıları yöntemi hedef sistemdeki parolayı deneme saldırılarıyla kırmak mantığıyla çalışmaktadır. Bu amaçla oluşturulan harfler ve özel karakterler içeren bir liste hazırlanır [36]. Bruteforce saldırısının başarı süresi hedef sistemdeki parolanın karmaşıklığına ve saldırıda kullanılan sistemimin donanım gücüne göre değişiklik göstermektedir [36].

Bruteforce yöntemi ile şifre çözmeye çalışan saldırganlar, kullanıcı bilgileri internet ortamına sızdığında mevcut şifreleri üzerinden kullanıcı sistemlerine kolayca erişebilmektedirler. Şifreleri sık sık değiştirmeyen kişilerin, şifrelerini çaldırma olasılıkları yüksektir. Bu durum, kullanıcı ve kurum için güvenlik açısından ciddi bir

tehdit oluşturmaktadır. Ayrıca genel olarak uzun ve karmaşık şifreler, özellikle kullanıcıların yüksek riskli olarak algıladığı uygulamalar için, çok sık değiştirilmesi gereken şifrelerden daha kabul edilebilir görünmektedir [37].

Şekil 3.16.'daki grafik kişilerin, şifrenizi nasıl saklarsınız sorusuna verdikleri cevaplar incelenmiştir. Bu soruya ait cevaplar iki cevaptan fazla olduğundan dolayı, cevaplar 1 = "Not Defteri", 2 = "Vault Uygulamaları", 3 = "Bilgisayar, telefonda bulunan text uygulamaları", 4 = "Postitler" olacak şekilde formatlanmıştır ve Mean Shift algoritmasına sokulmuştur.



Şekil 3.16. Şifre saklama yöntemi.

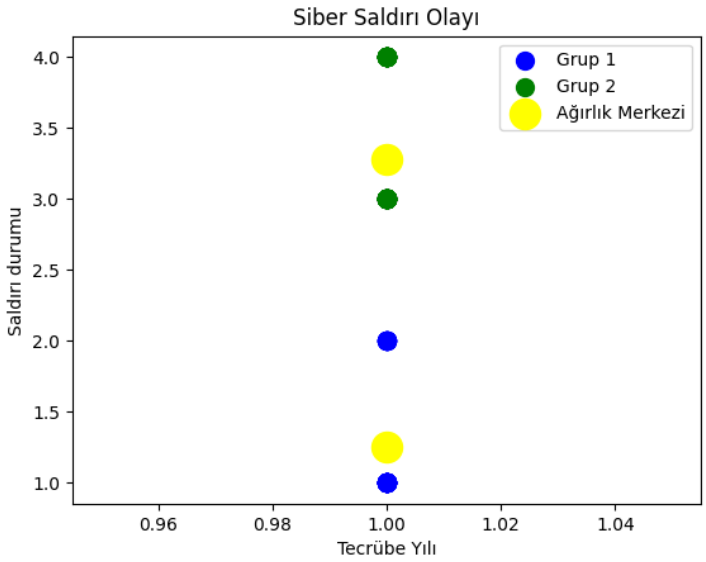
İncelemeler sonucunda, tecrübe yılı fazla olan insanlardan teknolojiden yoksun bir sonuç elde edilmiştir. 10 yıldan fazla iş tecrübesi olan kişiler, birinci seçenekte ağırlıklı olarak toplanmıştır. Bu demektir ki 10 yıldan fazla tecrübesi olan kişiler, şifrelerini not defterlerinde düz yazı olarak saklamaktadırlar. Bu, kişiler için risk teşkil eden bir durumdur. Herhangi bir kişi şifreyi görebilir, not defterini çalabilir. Bu durum şifrenin açıkta olduğu anlamına gelmektedir. Bu profilde bulunan insanlar için şirketler, belirledikleri şifre saklama yöntemlerini öğretilmeli ve gösterilmelidir. Doğru şifre seçimi kullanıcılar için çok önemlidir. Eğer kullanıcı güçlü bir parolaya sahip değilse, saldırganlar hizmetlerin güvenliği ne olursa olsun kullanıcı parolasını kolaylıkla tahmin edebilir [38].

5-10 yıl ve 0-3 yıl tecrübeye sahip kişiler arasında, şifrelerini not defterinde tutmak yerine daha iyi bir yöntem olan bilgisayar ve telefonlarda bulunan metin

uygulamalarını kullanma eğilimi gözlemlenmiştir. Bu yöntem ideal olmayabilir, ancak bilgisayar ve telefona şifre ile erişildiği için çalınması daha zorludur.

Şekil 3.16.'da bulunan 3 – 5 yıl tecrübeye sahip kişiler, 2'ye, vault uygulamalarına daha yakındır. En doğru şifre depolama yöntemi, şifre saklama uygulamalarını kullanmaktır. Risk matrisinde ve detay çalışmalarda bu kısımlar belirtilecektir. Kısacası herkese şifre depolama ve yöntemi konusunda mutlaka anlatım yapılmalıdır.

Bölümün başında bahsedildiği gibi tüm bu veriler ve grafikler şu ana kadar genel bazda incelenmiştir. Bu kısma kadar incelenen tüm grafikler, her tecrübe ve yaştan insanların ortak değerlendirilmesini içermektedir. Kullanılan veriler gerçekliği gösterse de detay bazda birbirini etkileyebilmektedir. Örneğin Şekil 3.9.'a bakılırsa mavi grubun ağırlık merkezinin sola kaydığı görülebilir. Bu durumda, grafikte oluşan kaymanın nedeni, 1. Grup içinde 0-3 yıl arasında tecrübeye sahip insanların fazla olmasından kaynaklanmaktadır. Buradan çıkarılması gereken durum, 3-5 yıl tecrübeye sahip insanların, ayrıca incelenmesi gerektiğidir. Şekil 3.17.'de bulunan grafik detay bazda, sadece 0-3 yıl tecrübesi olan kişiler için gerçekleştirilmiştir. Şekil 3.17. ve 3.9. karşılaştırıldığında 0-3 ve 3-5 yıl tecrübeye sahip kişiler arasındaki fark görülmektedir.



Şekil 3.17. Siber saldırı olay (0-3 yıl tecrübe) detay grafiği.

Bu işlemi gerçekleştirebilmek için oluşturulan veri formatlama koduna Şekil 3.18.'de bulunan kod bloğu eklenmiştir. Ekleme işlemi şu şekilde yapılmaktadır. Gelen veriler içinde 4 indeksli kolonda olan veri, 0-3 yıl tecrübeye sahip kişilerse yeni formatlı

dosyaya 1 olarak yazdırılır. İşlem sona erdiğinde, algoritmaya sokulacak formatlı dosya, sadece 0-3 yıl arası tecrübesi bulunan insanlardan oluşmaktadır.

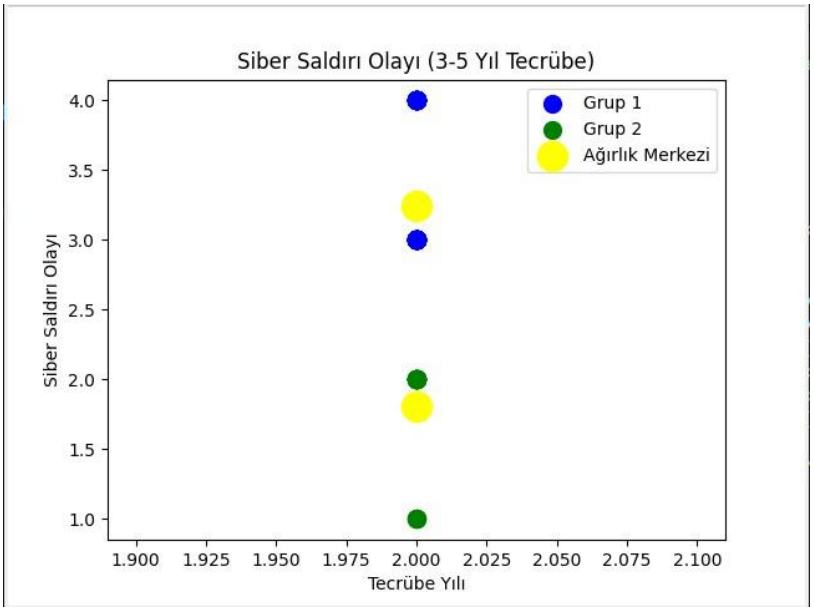
```
with open('Data/FormettedData.csv', 'w', encoding='UTF8') as f:
    counter = 0
    writer = csv.writer(f, delimiter=',',lineterminator='\n',)
    for row in formLines:

        if counter > 0:
            if row[4] == 1:
                writer.writerow(row)
        counter = counter + 1
```

Şekil 3.18. Tecrübeye göre veri oluşturan kod parçası.

Bundan sonraki grafikler tecrübe bazında incelenecektir. Şekil 3.17.'de bulunan grafik sadece 0–3 yıl arasında tecrübesi olanlar için oluşturulmuştur. Önceki incelemeler için genel bir gösterim gerçekleştirilmiştir. Fakat detay bazda incelenirse daha spesifik sonuçlar elde edilebileceğinden dolayı tecrübe yılı bazında inceleme yapılmıştır.

Şekil 3.19.'da görüldüğü üzere grafik siber saldırı olayını baz almaktadır. Ankette bulunan, daha önce siber saldırı olayı yaşadınız mı? Yaşadıysanız, hangi yöntem ile hacklendiniz sorusu 3-5 tecrübe yılındaki kişiler için incelenmiştir. Genel incelemede bahsedildiği gibi ağırlık merkezleri iki yerde toplanmıştır. İlk olarak 2. Seçenek olan yaşamadım şıkkında toplanma olmuştur. Tecrübesi az olan insanların siber güvenlik eğitimi almamış olmaları ve dikkatsiz davranmaları sonucunda, 'yaşamadım' cevabı vermiş olmaları dikkat çekicidir.



Şekil 3.19. Siber saldırı olay (3-5 yıl tecrübe) detay grafiği.

Şekil 3.19.'a bakıldığında, diğer toplanma 3. noktada gerçekleşmiştir. Kişiler, oltalama saldırısına uğrayarak dikkatsizlik ve eğitimsizlik nedeniyle birçok bilgiyi maile gelen oltaya takılarak sızdırmışlardır. Genel bazda elde edilen veriler ile detay bazda elde edilen veriler bir tabloda tutulmuştur. Bu verilerle oluşturulacak matrise tezin ilerleyen aşamalarında değinilmiştir.

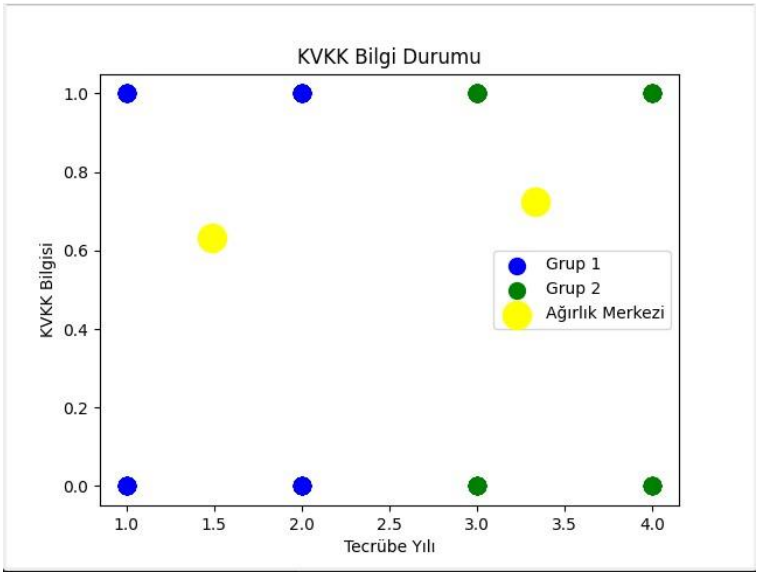
Şekil 3.17.'de olduğu gibi aynı konu ve algoritma kullanılarak bu sefer 3-5 yıl arasında tecrübe sahibi olan kişiler için çalışma gerçekleştirilmiştir. Genel bazlı grafik ve detay bazlı grafik arasındaki ilk fark burada görülmektedir.

Şekil 3.10. tekrar incelendiğinde, 0-3 ve 3-5 yıl tecrübeye sahip kişiler için ortak bir grup oluşturulup bunlar için sonuç 4'te toplanmıştır. Bu sonuç "Zararlı sitelerde gezinme sonucu yaşanan siber olay" demektir. Burada iki grup için ortak veri verdiğinden dolayı daha isabetli sonuçlar için detay kırılım mutlaka şarttır.

Ortak verilen grafikte sonuç 4 iken, Şekilde 3.17.'deki grafik, 0-3 yıl arası tecrübeli kişiler için incelendiğinde yoğunluğun iki yerde topladığı gözlemlenmiştir. Bu merkezler ortalama olarak, bilmiyorum ve mail yolu ile link yönlendirmesi sonucu bilgilerin ele geçirilmesi şıkları olan, 1 ve 3 noktalarında toplanmıştır. Şekil 3.19.'daki grafik, 3-5 yıl tecrübesi olan insanlar için incelenir ise sonuç ortalama olarak 2 ve 3'e yakın çıkmaktadır. Bu da yaşamadım ve mail yolu ile link yönlendirmesi sonucu bilgilerin ele geçirilmesi anlamına gelmektedir.

Sonuç olarak, genelden detaya gidildiği taktirde, grafikler arasında farklılıklar olduğu gözlemlenebilir. Bu farklılığı ve cevapları yorumlamak gerekirse çıkarmamız gereken sonuç: Tecrübesi az olan kişiler, internette gezinirken dikkatsiz davranmaktadırlar. Kişiler, bilinmeyen sitelerde gezerken veya korsan yayın yapan siteler aracılığı ile zarar görebilmektedirler. Bunlara ek olarak kişilerin, çoğunlukla yaşamadım veya bilmiyorum şıklarını seçmesi de kişilerin bilgi seviyesinin düşük olduğunun göstergesidir. Teknoloji, bireylerin ve işletmelerin kişisel finansal, hukuki ve itibari verilerini çeşitli araçlarla paylaşmalarına ve yaymalarına olanak tanır. Bu tür bir kullanım, kişisel veriler üzerindeki kontrolün kaybedilmesine neden olabilir. Kişisel verilerin korunması şirketlerin vazgeçilmez bir yükümlülüğüdür [39].

Şekil 3.20.'deki genel bazda KVKK bilgisinin ölçüldüğü grafik incelendiğinde çalışanların kmeans algoritmasıyla 0-5 yıl tecrübeliler ve 5-10 yıl üstü tecrübeliler olarak 2 gruba ayrıldığı görülmektedir. Bu inceleme sonucu verilecek çözüm önerilerini matriste hukuki bilgiler başlığı altına yerleştireceğiz. Girdiğimiz günlük internet sitelerinden tutun alışveriş, banka, formlar vb. her alanda KVKK bilgisi ile karşılaşıyoruz. Rızamızın istendiği ve KVKK bilgilendirmesi bu kadar sık yapıldığı için çalışanların KVVK farkındalığının 2 grup için de 0.5'ten yüksek olduğu görülmektedir. KVKK'nın siber güvenlikle ilişkisi, kişisel verilerin korunmasını ve güvenliğini sağlamak için önemlidir. Bu çerçevede, kuruluşlar hem KVKK uyumluluğunu hem de siber güvenlik önlemlerini dikkate almalıdır.



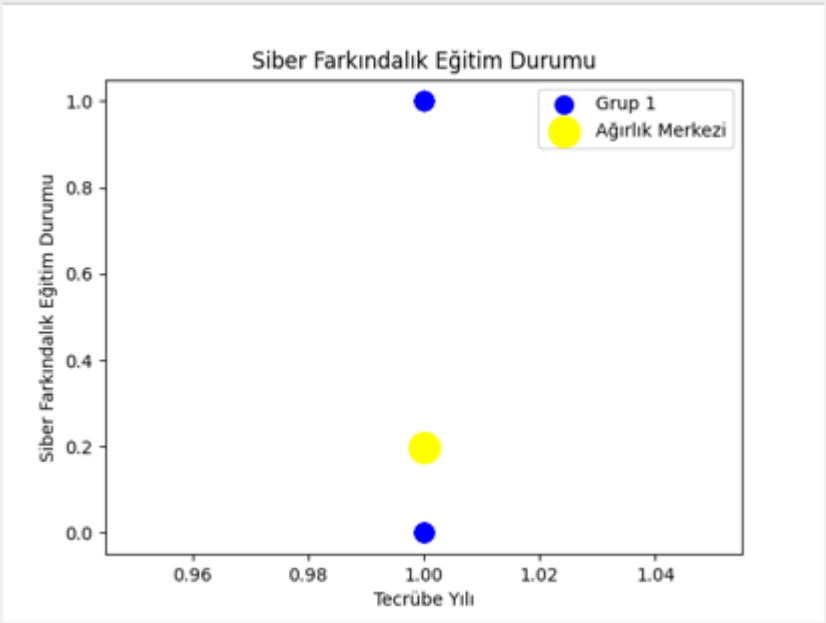
Şekil 3.20. KVKK bilgisi grafiği.

Sonuç olarak tüm veriler ve parametreler incelenmiştir. Bu incelemeler ayrı bir tabloda genel bazda ve detay bazda tutulmuştur. Çok fazla deneme ve tespit yapılmıştır. Bu grafiklerden çıkan veriler, birbiri ile kıyaslanıp bağlantı kurularak bir sonraki adım olan risk matrisi oluşturulması için çıktılar hazırlanmıştır. Bu tablolar ve çıktılardan bir sonraki başlıkta detaylı olarak bahsedilecektir.

3.5. Detay Bazda Grafiklerin İncelenmesi

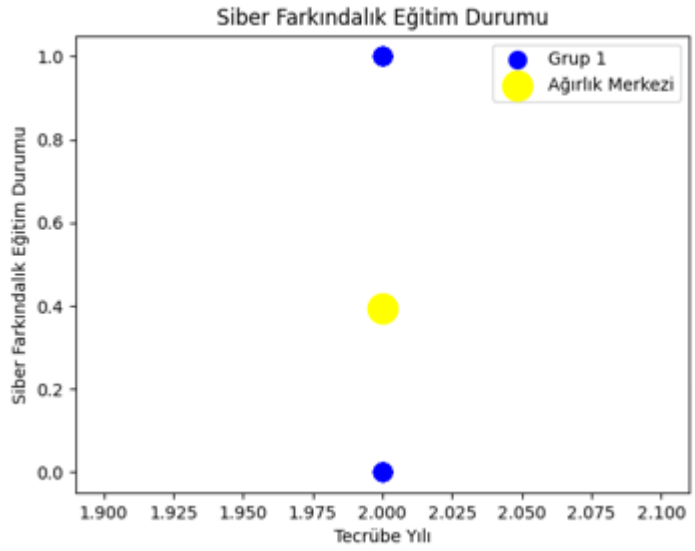
Aşağıdaki grafikler her bir tecrübe aralığı için detay bazda sonuçları içermektedir. Detay bazda grafiklerin oluşturulması için K-Means algoritması kullanılarak bu grafiklerin ağırlık merkezleri belirlenmiştir. Çıkan sonuçlar genel ve detay algoritma sonuçları tablosunda verilmiştir.

Şekil 3.21'de siber farkındalık eğitim durumu 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



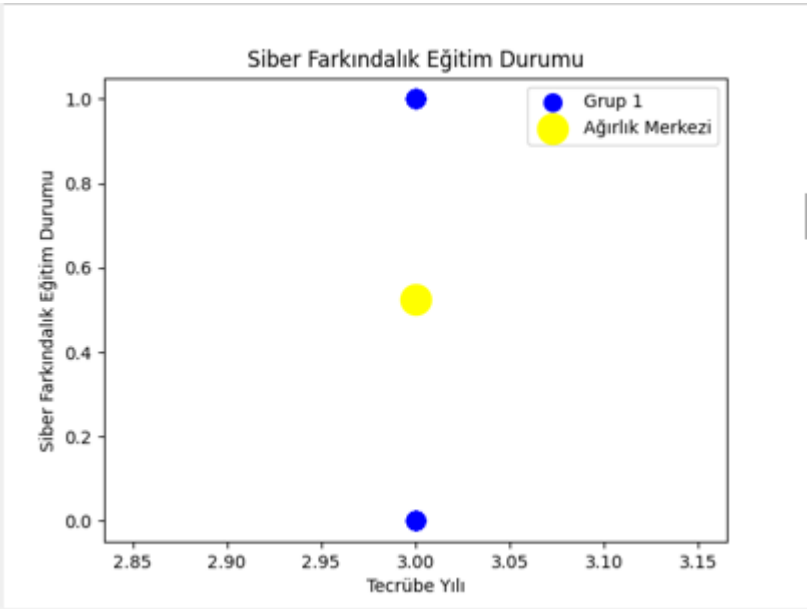
Şekil 3.21. Siber farkındalık eğitim durumu (0-3 yıl tecrübe)

Şekil 3.22'de siber farkındalık eğitim durumu 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.4 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



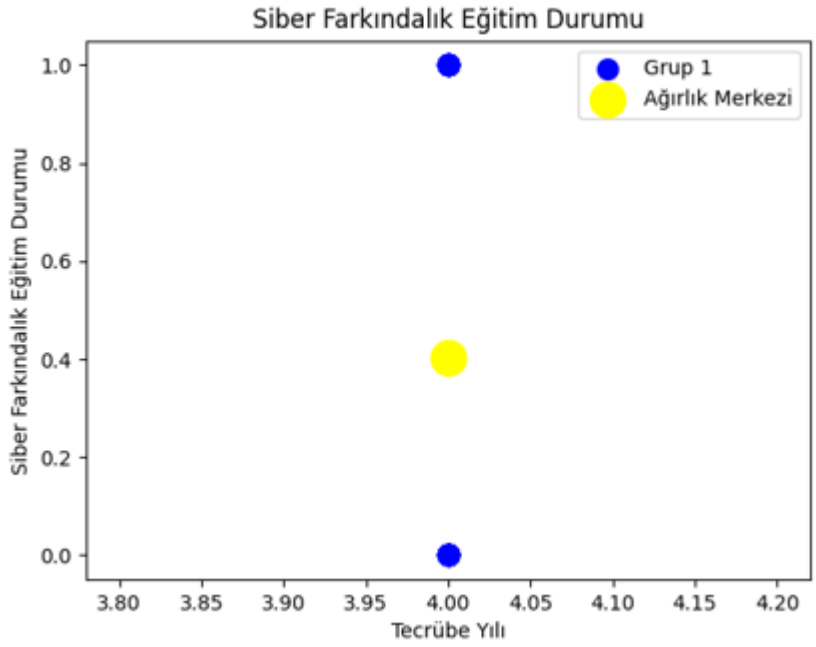
Şekil 3.22. Siber farkındalık eğitim durumu (3-5 yıl tecrübe)

Şekil 3.23'te siber farkındalık eğitim durumu 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.5 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



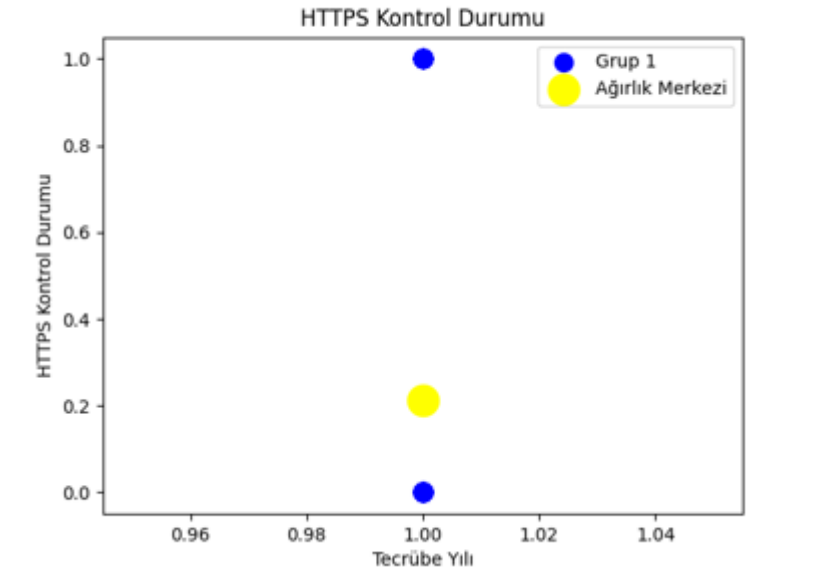
Şekil 3.23. Siber farkındalık eğitim durumu (5-10 yıl tecrübe).

Şekil 3.24'te siber farkındalık eğitim durumu 10+ yıl tecrübesinde detay bazda ölçülmüştür. Sonuç 0.4 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



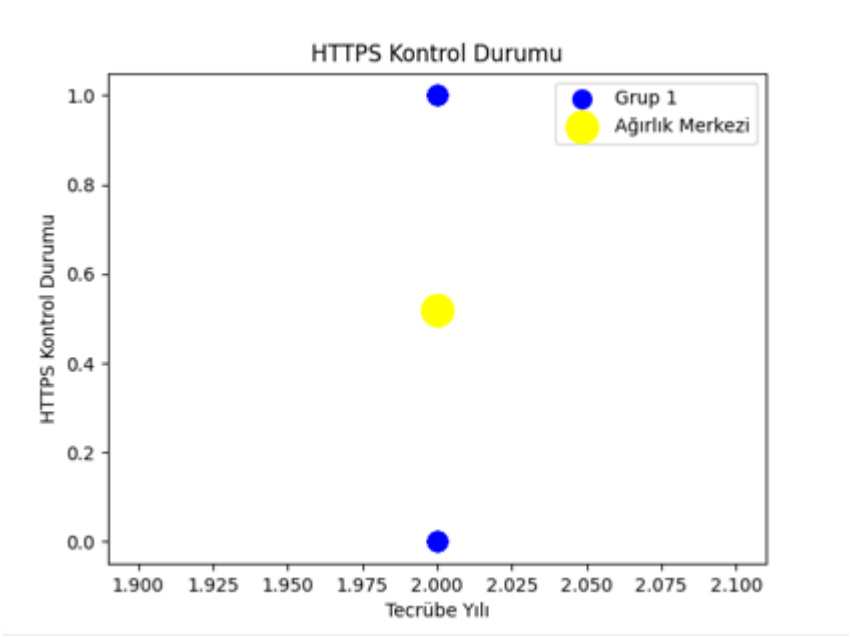
Şekil 3.24. Siber farkındalık eğitim durumu (10+ yıl tecrübe)

Şekil 3.25'te https kontrol durumu 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



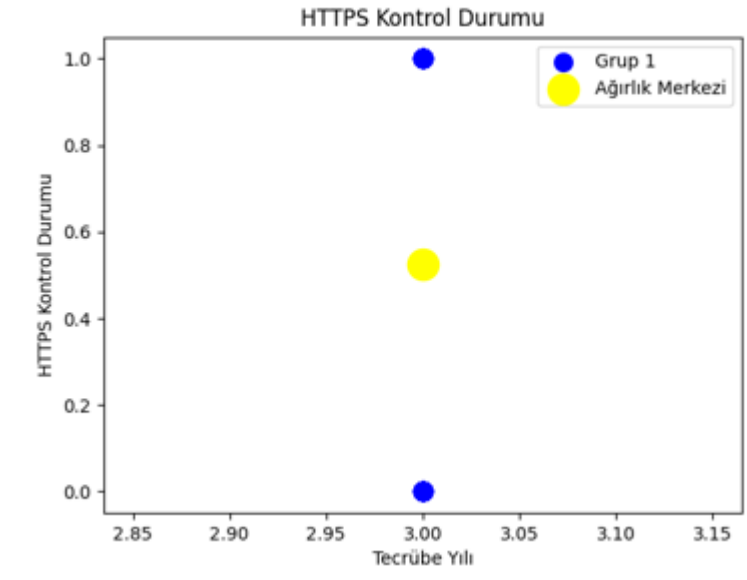
Şekil 3.25. HTTPS kontrol durumu (0-3 yıl tecrübe)

Şekil 3.26'da https kontrol durumu 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.5 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



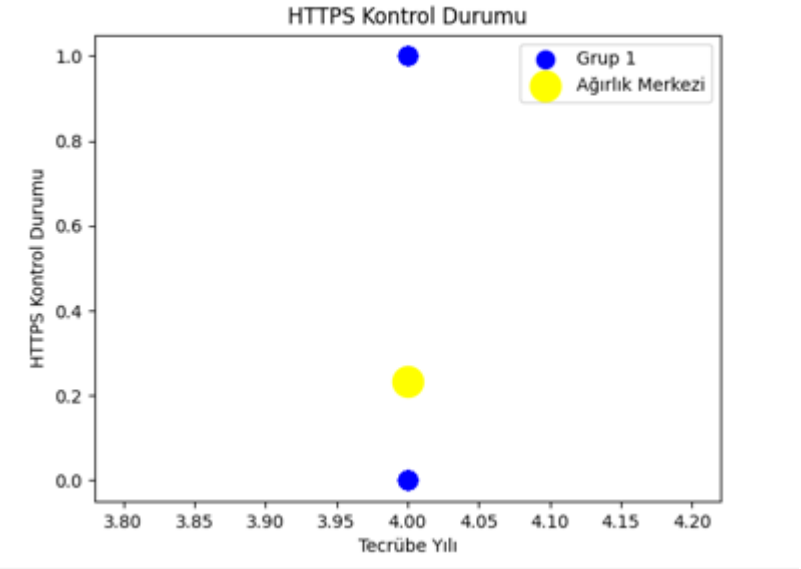
Şekil 3.26. HTTPS kontrol durumu (3-5 yıl tecrübe)

Şekil 3.27'de https kontrol durumu 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.5 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



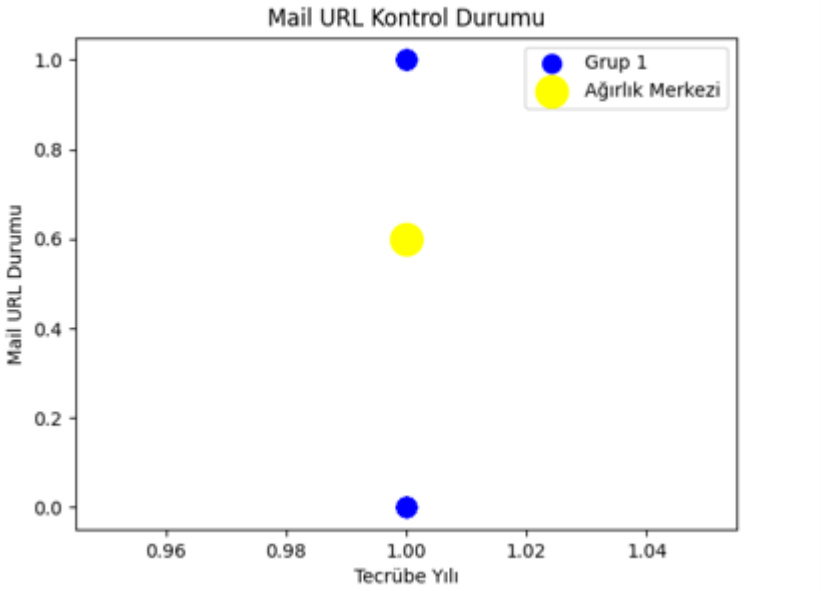
Şekil 3.27. HTTPS kontrol durumu (5-10 yıl tecrübe)

Şekil 3.28'de https kontrol durumu 10+ yıl tecrübesinde detay bazda ölçülmüştür. Sonuç 0.2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



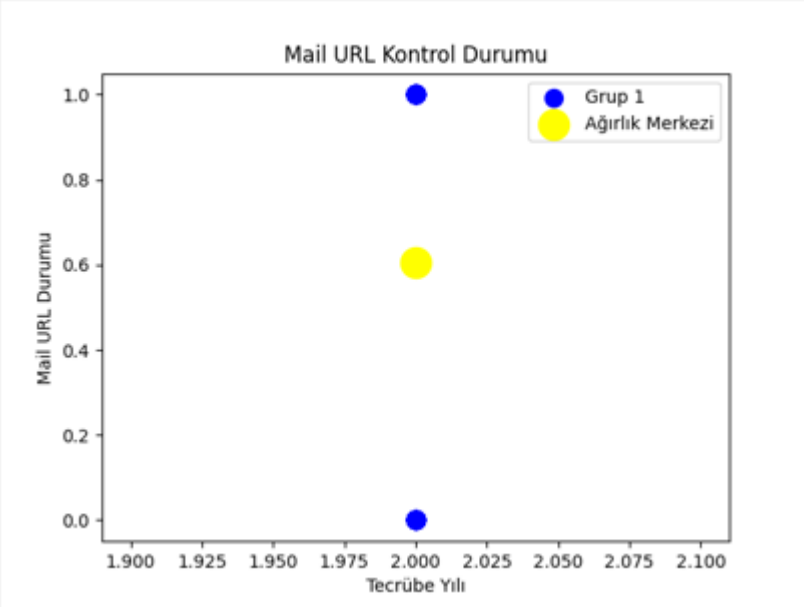
Şekil 3.28. HTTPS kontrol durumu (10+ yıl tecrübe)

Şekil 3.29'da mail URL kontrol durumu 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



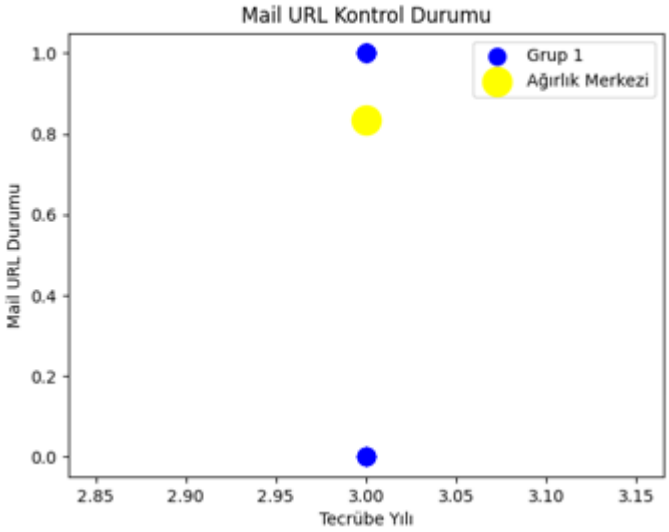
Şekil 3.29. Mail URL kontrol durumu (0-3 yıl tecrübe)

Şekil 3.30'da mail URL kontrol durumu 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



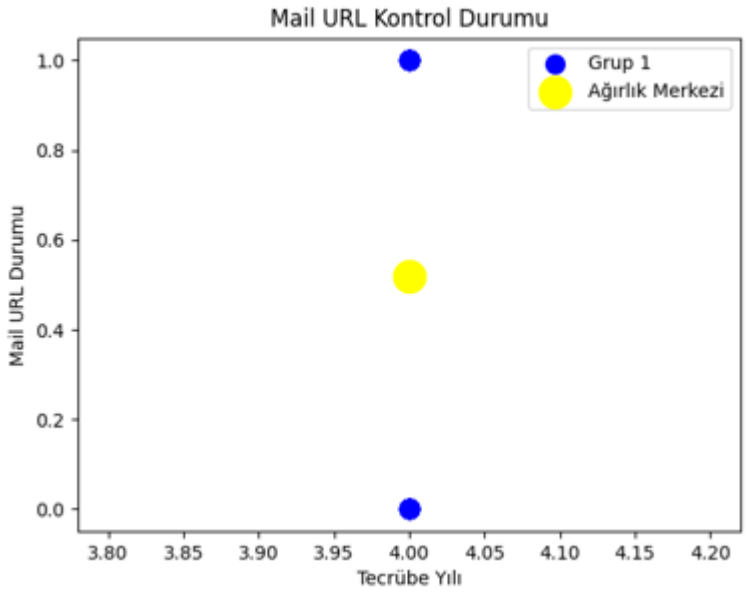
Şekil 3.30. Mail URL kontrol durumu (3-5 yıl tecrübe)

Şekil 3.31'de mail URL kontrol durumu 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



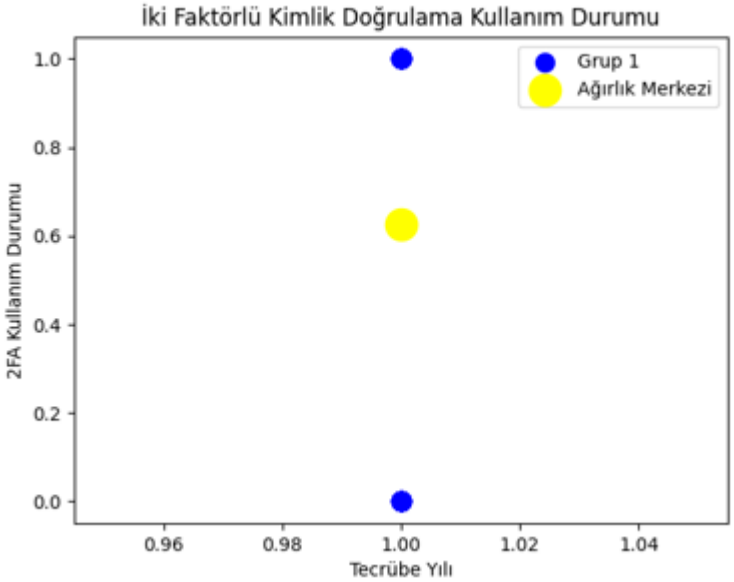
Şekil 3.31. Mail URL kontrol durumu (5-10 yıl tecrübe)

Şekil 3.32.'de mail URL kontrol durumu 10+ yıl tecrübesinde detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



Şekil 3.32. Mail URL kontrol durumu (10+ yıl tecrübe)

Şekil 3.33'te iki faktörlü kimlik doğrulama durumu 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.

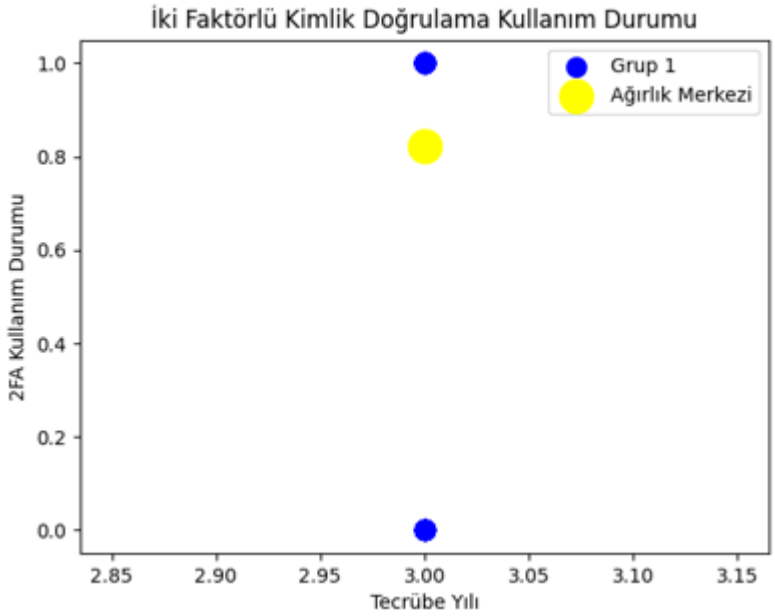


Şekil 3.33. 2FA kullanım durumu (0-3 yıl tecrübe)

Şekil 3.34'te iki faktörlü kimlik doğrulama durumu 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.

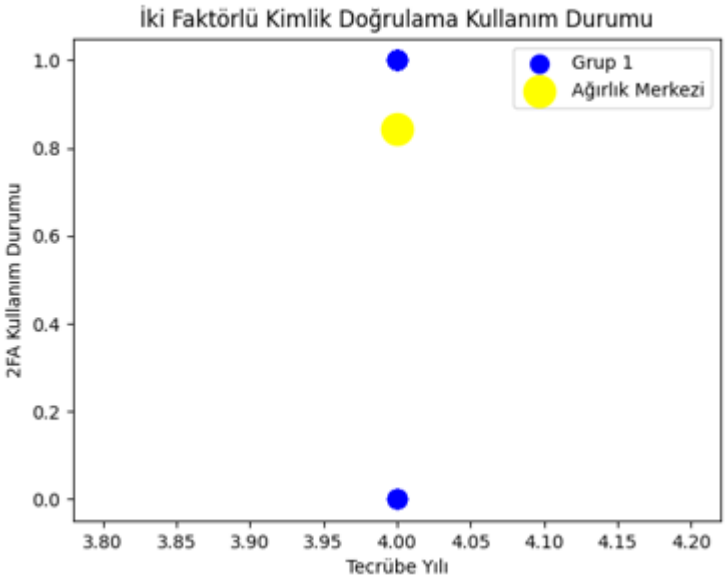
Şekil 3.34. 2FA kullanım durumu (3-5 yıl tecrübe)

Şekil 3.35'te iki faktörlü kimlik doğrulama durumu 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



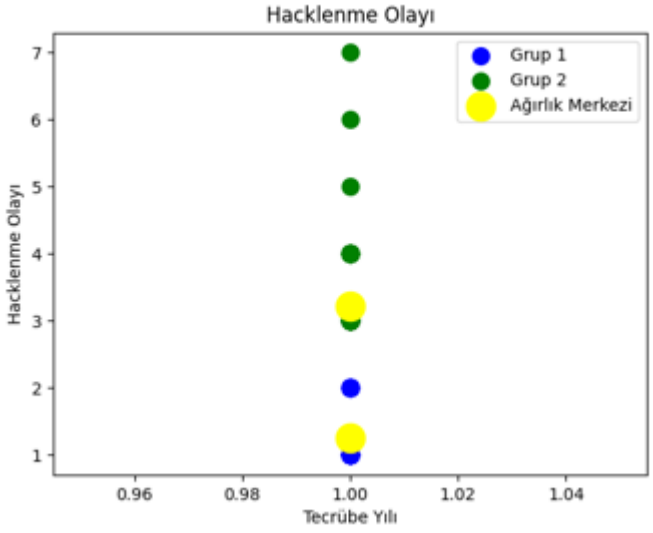
Şekil 3.35. 2FA kullanım durumu (5-10 yıl tecrübe)

Şekil 3.36'da iki faktörlü kimlik doğrulama 10+ yıl tecrübesinde detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



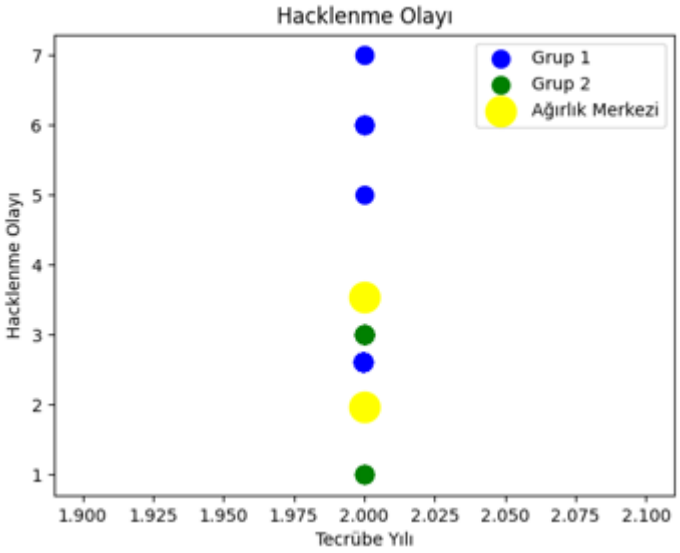
Şekil 3.36. 2FA kullanım durumu (10+ yıl tecrübe)

Şekil 3.37'de hacklenme olayı 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,2 ve 3,1 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



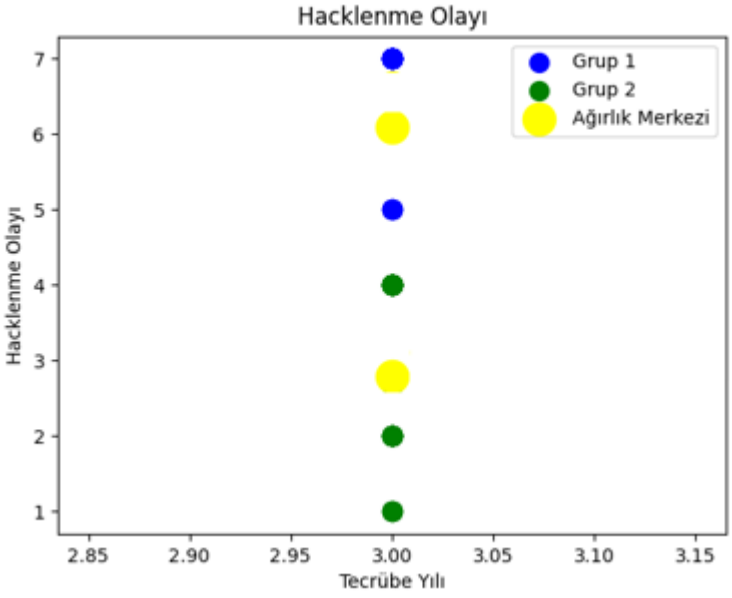
Şekil 3.37. Hacklenme olayı (0-3 yıl tecrübe)

Şekil 3.38'de hacklenme olayı 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,9 ve 3,3 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



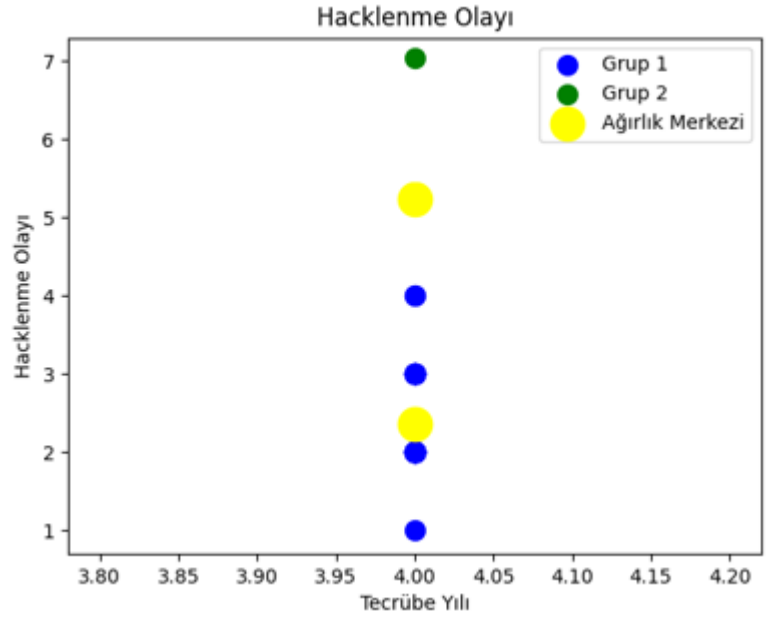
Şekil 3.38. Hacklenme olayı (3-5 yıl tecrübe)

Şekil 3.39'da hacklenme olayı 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 2,5 ve 6,0 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



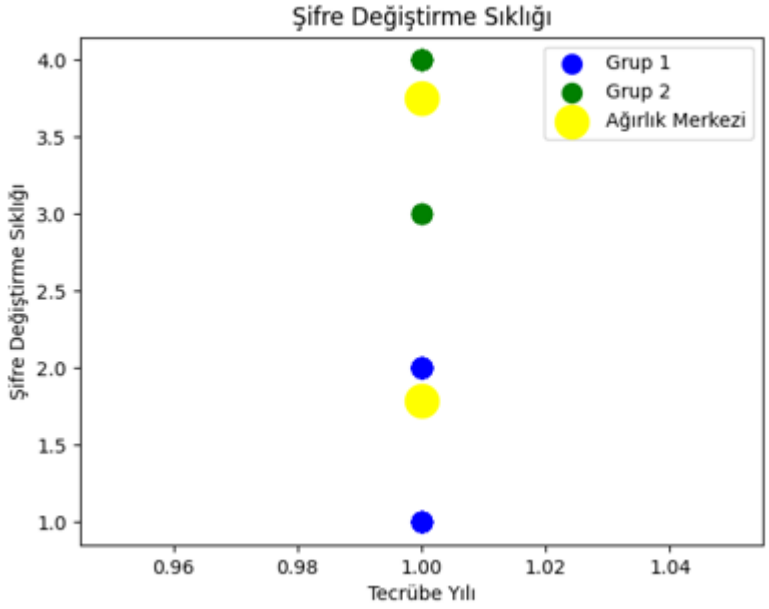
Şekil 3.39. Hacklenme olayı (5-10 yıl tecrübe)

Şekil 3.40'ta hacklenme olayı 10+ yıl tecrübesinde detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 2,2 ve 5,1 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



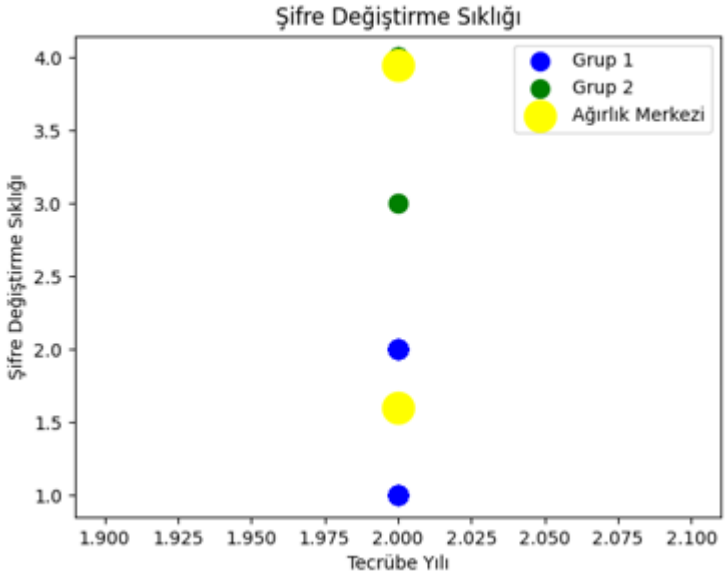
Şekil 3.40. Hacklenme olayı (10+ yıl tecrübe)

Şekil 3.41'de şifre değiştirme sıklığı 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,7 ve 3,8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



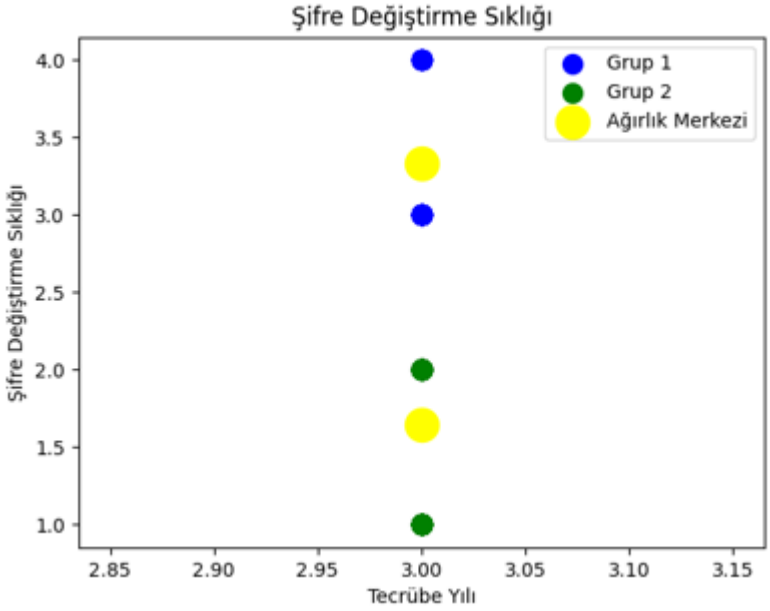
Şekil 3.41. Şifre değiştirme sıklığı (0-3 yıl tecrübe)

Şekil 3.42'de şifre değiştirme sıklığı 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,5 ve 4,0 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



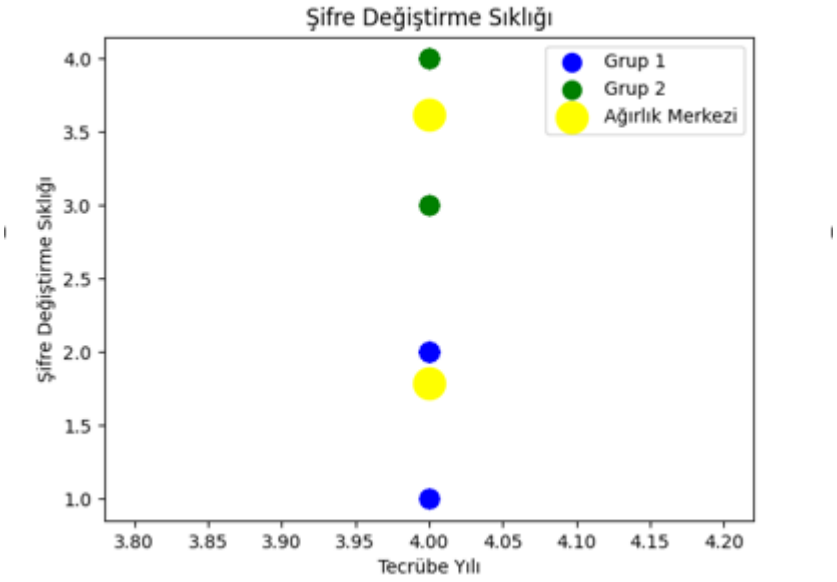
Şekil 3.42. Şifre değiştirme sıklığı (3-5 yıl tecrübe)

Şekil 3.43'te şifre değiştirme sıklığı 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,6 ve 3,3 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



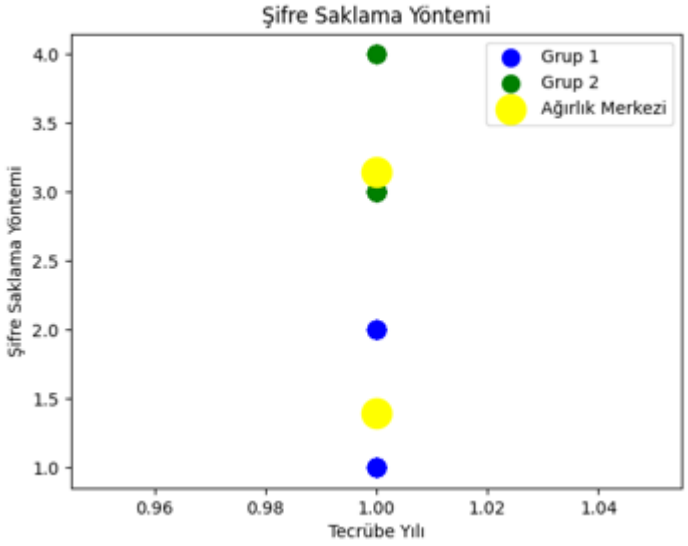
Şekil 3.43. Şifre değiştirme sıklığı (5-10 yıl tecrübe)

Şekil 3.44'te şifre değiştirme sıklığı 10+ yıl tecrübesinde detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,7 ve 3,6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



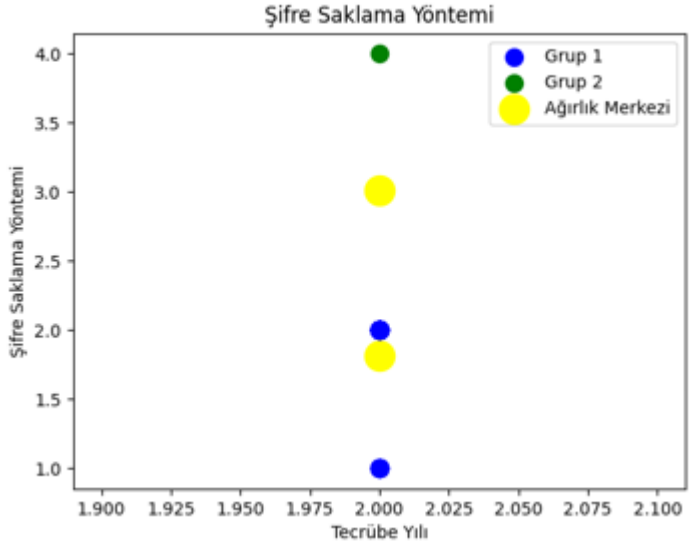
Şekil 3.44. Şifre değiştirme sıklığı (10+ yıl tecrübe)

Şekil 3.45'te şifre saklama yöntemi 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,3 ve 3,2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



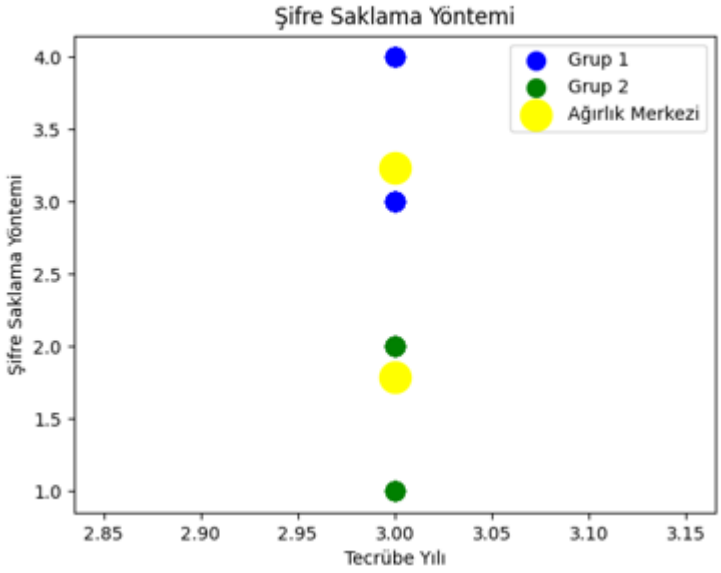
Şekil 3.45. Şifre saklama yöntemi (0-3 yıl tecrübe)

Şekil 3.46'da şifre saklama yöntemi 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,8 ve 3,0 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



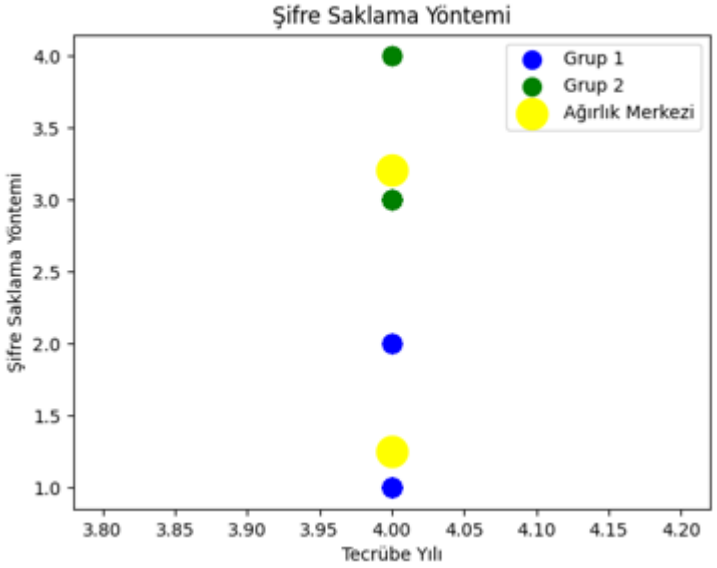
Şekil 3.46. Şifre saklama yöntemi (3-5 yıl tecrübe)

Şekil 3.47'de şifre saklama yöntemi 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,8 ve 3,2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



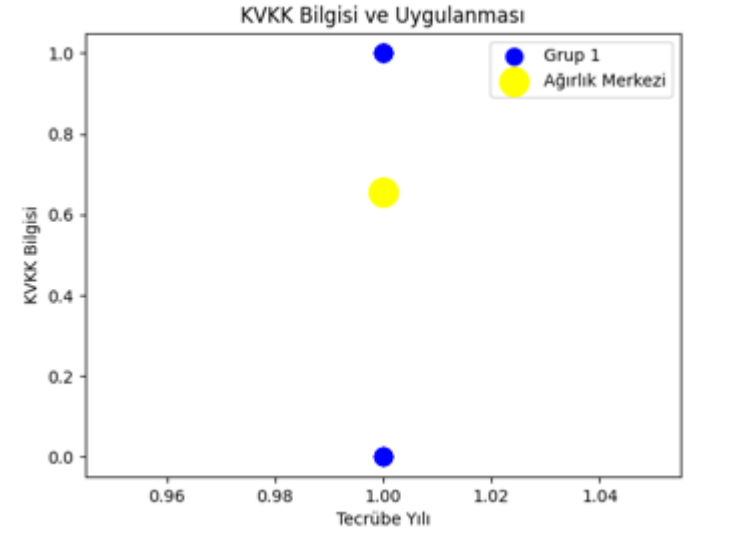
Şekil 3.47. Şifre saklama yöntemi (5-10 yıl tecrübe)

Şekil 3.48'de şifre saklama yöntemi 10+ yıl tecrübesinde detay bazda ölçülmüştür. 2 merkeze bakıldığında sonuç 1,2 ve 3,2 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



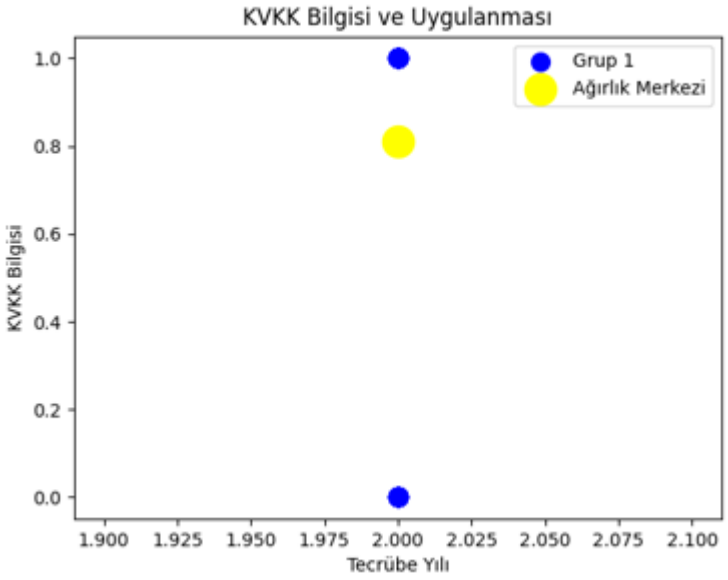
Şekil 3.48. Şifre saklama yöntemi (10+ yıl tecrübe)

Şekil 3.49'da KVKK bilgisi ve uygulanması 0-3 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.6 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



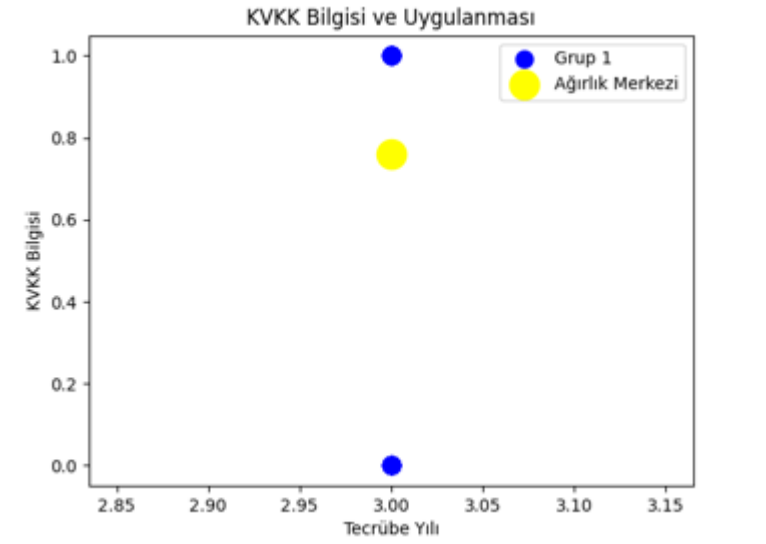
Şekil 3.49. KVKK bilgisi ve uygulaması (0-3 yıl tecrübe)

Şekil 3.50'de KVKK bilgisi ve uygulanması 3-5 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



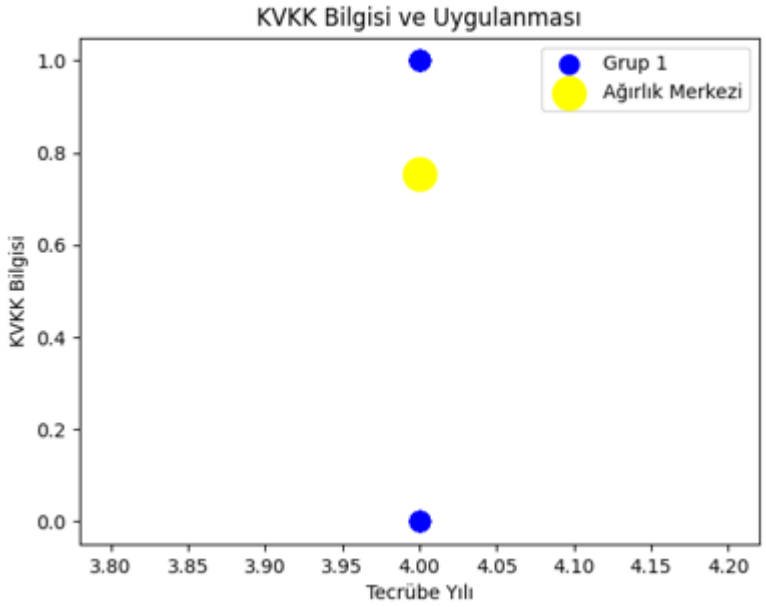
Şekil 3.50. KVKK bilgisi ve uygulaması (3-5 yıl tecrübe)

Şekil 3.51'de KVKK bilgisi ve uygulanması 5-10 tecrübe yılı aralığında detay bazda ölçülmüştür. Sonuç 0.8 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



Şekil 3.51. KVKK bilgisi ve uygulaması (5-10 yıl tecrübe)

Şekil 3.52'de KVKK bilgisi ve uygulanması durumu 10+ yıl tecrübesinde detay bazda ölçülmüştür. Sonuç 0.7 olup genel ve detay algoritma sonuç tablolarında kullanılacaktır.



Şekil 3.52. KVKK bilgisi ve uygulaması (10+ yıl tecrübe)

3.6. Risk Matrisinin ve Aksiyonların Oluşturulması

Anket verilerinden oluşan veri seti, formatlandıktan sonra gerçek veriler ile test yapılmıştır. İncelemelerin ve yorumların bir kısmı önceki başlıkta açıklanmıştır. Genel ve detay bazda algoritmalar çalıştırılıp çıkan sonuçlar, Tablo 3.1. ve Tablo 3.2.'de rakamsal olarak saklanmıştır.

Tablo 3.1. Genel algoritma sonuçları.

	Genel			
Alan/ Yıl	**0-3**	**3-5**	**5-10**	**10+**
1	0,3	0,3	0,4	0,4
2	0,2	0,2	0,4	0,4
3	0,3	0,3	0,4	0,4
4	0,7	0,7	0,7	0,7
5	0,6	0,6	0,7	0,7
6	4,0	4,0	4,0	6,0
7	2,5	2,5	2,0	1,5
8	2,5	2,0	2,5	1,0

Tablo 3.2. Detay algoritma sonuçları.

	Detay							
Alan/ Yıl	**0-3**		**3-5**		**5-10**		**10+**	
1	0,2		0,4		0,5		0,4	
2	0,2		0,5		0,5		0,2	
3	0,6		0,6		0,8		0,5	
4	0,6		0,6		0,8		0,8	
5	0,6		0,8		0,8		0,7	
6	1,2	3,1	1,9	3,3	2,5	6,0	2,2	5,1
7	1,7	3,8	1,5	4,0	1,6	3,3	1,7	3,6
8	1,3	3,2	1,8	3,0	1,8	3,2	1,2	3,2

Tablo 3.1. ve Tablo 3.2.'de bulunan alanlar ve bunların anlamı aşağıdaki gibidir.

1. Siber farkındalık eğitimi.
2. HTTPS kontrolü.
3. Mail URL kontrolü.
4. İkili doğrulama kullanımı.
5. KVKK Bilgisi
6. Siber olay.
7. Şifre değiştirme sıklığı.
8. Şifre saklama yöntemi.

Tez çalışmasının amacı, veri setinin yorumlanmasıdır. Yorumlara göre hangi durumlarda risk oluşturduğu ve hangi durumlar için ne gibi aksiyonlar alınması gerektiğinin tespit edilmesidir. Şirket ihtiyaçlarına göre, anket soruları ve aksiyonlar değişebilir. Değişmiş hali ile algoritmalar çalıştırılıp yeni aksiyonlar ve yeni matris belirlenebilir. Fakat belirlenen sorular, belirli araştırmalar sonucunda ve alanında uzman kişilerin onayı alınarak hazırlanmıştır. Bu sorular, değer yaratan ve genel geçer sorular olduğu için yeterlidir. Ayrıca anket katılımcıları, tek bir şirketten ve meslekten olmadıkları için sorular genel kullanıma uygundur. Kısacası gerçekleştirilen çalışma, genel bir çalışma olduğu için her şirket için etkili olacaktır.

Oluşturulan siber risk matrisi, sadece teknik bilgi içeren ve insan davranışlarını baz almayan risk matrislerinden farklıdır. Normalde siber risk matrisinde teknik açıdan inceleme gerçekleştirilir. Tez için oluşturulan matriste, tecrübe yılına göre kişilerin ne gibi açılardan siber risk oluşturabileceği gösterilmiştir. Örneğin; 10 yıldan fazla tecrübesi olan insanların, grafik incelendiğinde şifre saklama yöntemi olarak not defterini kullanmayı tercih ettikleri gözlemlenmiştir. Bu kişilerin, şifre saklama konusunda teşkil ettiği siber risk seviyesi yüksek olarak belirlenmektedir.

Tablo 3.1'de bulunan veriler, algoritma sonucu oluşan detay bazda ve genel bazda yapılan çalışmaların sonuçlarını içermektedir. Bu sorular ve cevaplar incelendiğinde, belirli gruplar içinde benzerlik gözlemlemek mümkündür. Bu gözlem sonrasında siber risk matrisi için genel başlıklar oluşturulmaya başlanmıştır. Bazı durumlarda, bir başlık iki soru ile ilişkili iken bazı durumlarda tek soru ile ilişkilidir.

Başlıklardan bahsetmek gerekirse 1. Başlık "Siber Eğitim" başlığıdır. Bu başlık kişilerin temel siber güvenlik eğitim durumu ile alakalıdır. 2. Başlık "Siber

Sorgulama" başlığıdır. Bu başlık kişilerin girdiği sitelerde yaptığı HTTPS kontrolü, maillerde bulunan eklerin ve linklerin kontrolünü içermektedir. Kişilerin siber sorgulama yeteneğinin olup olmadığı bu şekilde anlaşılmaktadır. 3. Başlık "Şifre Koruma" başlığıdır. Bu başlık kişilerin şifrelerini nasıl sakladığı ile ilgilidir. 4. Başlık "Şifre Değişikliği" başlığıdır. Bu başlık kişilerin şifre değiştirme sıklığını ve sık şifre değiştirmenin önem durumunu belirtir. 5. Başlık "Ek Önlemler" başlığıdır. Bu başlık, kişilerin internet ortamında korunmak için kullandığı ekstra uygulamalar, şifre oluşturma, koruma uygulamaları, ekstra eklentiler vb. konular ile ilgilidir. 6. Başlık "Hukuksal Hakimiyet" başlığıdır. Bu başlık ise kişilerin KVKK bilgisi, siber saldırı sonucu takip etmesi gereken prosedürler vb. genel olarak hukuksal prosedür bilgi durumunu içermektedir. Başlıklar ve etki alanları belirlendikten sonra matris oluşturulmuştur. Bu başlıklar altında kişiler, tecrübe yıllarına göre ayrılıp matrise eklenmiştir.

İki cevaplı sorular baz alınarak çalışanların risk durumu hesaplanırken, Tablo 3.1. ve Tablo 3.2.'de bulunan veriler tecrübe yılına göre detay ve genel bazda çıkan sonuçları toplanıp ikiye bölünür. Elde edilen ortalama 0,0 – 0,4 arasında ise yüksek riskli, 0,4 – 0,6 arasında ise orta riskli, 0,6 – 1,0 arasında ise düşük riskli olarak değerlendirilir.

Birden fazla cevabı olan sorular için kullanıcıların risk durumu ölçülürken ortalama alarak ilerlenmektedir. Birden fazla cevabı olan sorular için literatür taraması yapılarak soruların şıkları en doğru, orta doğrulukta ve yanlış olarak 3 bölüme ayrılmıştır. Çıkan ortalama bu şıklardan hangisine yakın ise risk durumu buna göre tayin edilmektedir. Bu yöntem ile elde edilmiş veriler incelenerek çalışanların risk durumlarını gösteren Tablo 3.3.'te bulunan yapı hazırlanmıştır.

Tablo 3.3. Siber risk matrisi.

Alan/ Tecrübe Yılı	0-3 Yıl	3-5 Yıl	5-10 Yıl	10+ Yıl
6	Düşük	Düşük	Düşük	Düşük
5	Düşük	Düşük	Düşük	Düşük
4	Orta	Orta	Düşük	Düşük
3	Orta	Orta	Düşük	Yüksek
2	Orta	Orta	Orta	Yüksek
1	Yüksek	Yüksek	Yüksek	Yüksek

Tablo 3.2.'ye göre belirlenen alanların numaralandırılması şu şekildedir:

1. Siber farkındalık eğitimi.
2. Siber sorgulama bilinci.
3. Şifre korunması.
4. Şifre değiştirme sıklığı.
5. Ek önlemler.
6. Hukuksal hakimiyet.

Tablo 3.2.'de bulunan siber risk matrisini incelemek gerekirse. 1. Başlık, siber güvenlik eğitim konusunu baz almaktadır. Tecrübe yılı fark etmeksizin kişilerin hepsinde riskin yüksek olduğu görülmektedir. Bundan dolayı 1. başlık olan siber farkındalık eğitimi için tecrübe yılı fark etmeksizin siber riskin yüksek olduğu gösterilmiştir. Bu durumda, şirkete giren herkes için tecrübe yılı fark etmeksizin mutlaka temel siber farkındalık eğitimi verilmelidir.

Tablo 3.2.'de bulunan siber risk matrisine tekrar bakıldığında bu sefer de 2. başlık olan siber sorgulama adına yorumlama yapılmıştır. Bu başlık için bakıldığında 10 yıldan fazla tecrübesi olan kişiler için siber risk çok fazladır. Şekil 3.14.'te bulunan grafik incelendiğinde özellikle 10 yıldan fazla tecrübeli kişiler için ağırlık merkezi, cevap birde toplanmıştır. Bu kişilerin şifrelerini, not defterinde sakladıkları gözlemlenmektedir. Bundan dolayı 10 yıldan fazla tecrübesi olan kişiler, şirket için risk oluşturacaktır. Diğer tecrübe yıllarına sahip kişilerde risk orta seviyededir.

Şirketlerin, şirkete yeni gelen veya 10 yıldan fazla iş tecrübesine sahip olan mevcut çalışanları için, alması gereken aksiyonları şunlardır: Bu kişilere şifre saklama uygulamaları önerilmelidir. Bu uygulamaların kullanımı öğretilebilir ve şifrelerinin saklanmasının öneminden bahsedilebilir. 10 yıldan fazla tecrübesi olan kişiler için bu konu riskli olacağından, bu çalışanlara öğretici ve yol gösterici olmak gerekmektedir. Orta risk seviyesinde olan kişiler için de aynı durum geçerlidir. Fakat yüksek öncelik, tecrübe yılı 10 yıldan fazla olan çalışana veya yeni gelen çalışana verilmelidir.

Çalışmamız kapsamında çalışanlara yönelik siber bilinç ve farkındalığı arttırmak için çeşitli aksiyon maddeleri önerilmiştir. Risk matrisinde bulunan başlıklar ve bu başlıklara ait alınması gereken önlemler Tablo 3.4.'te gösterilmiştir.

Tablo 3.4. Aksiyon maddeleri.

Alan No	Alan	Aksiyon
1	Siber farkındalık eğitimi	Genel siber farkındalık eğitimi verilmeli. Kişilere, siber saldırılar sonucu neler olabileceği, geçmişte yaşanan bireysel veya kurumsal siber olaylar vb. konularda bilgilendirilmeli ve önemi vurgulanmalıdır.
2	Siber sorgulama bilinci	Siber sorgulama alanında yapılan her aksiyonun, girilen bir site, gelen bir mail, internetten indirilen bir dosyanın, tıklanılan bir linkin nelere yol açabileceği konusunda örnekler ile ilgili kişilerde farkındalık yaratılmalıdır. Ayrıca bu konuda nasıl kontroller yapabilecekleri, nelere dikkat edecekleri konusunda bilgi verilmelidir.
3	Şifre korunması	Şifre koruma konusunda kişilere eğitimler verilmelidir. Kişilere, şifrelerini iyi saklayamadıkları durumda neler olabileceği konusunda bilgi verilmelidir. Şifre saklamak için dünyaca kullanılan kriptolu uygulamalardan bahsedilmeli ve bu uygulamaların kullanımı teşvik edilmelidir. Var olan şifreleri değiştirip bu uygulamalara geçilmesi konusunda tavsiye verilmelidir.

Tablo 3.4. (Devamı) Aksiyon maddeleri.

Alan No	Alan	Aksiyon
4	Şifre değiştirme sıklığı	Şifre değiştirme konusunda, kişilere şifre değiştirmez ise neler olabileceği açıklanmalıdır. Kişiler, şifrelerini değişmediği durumda saldırganların şifre elde etmek için izlediği yollardan bahsedilmelidir. Ayrıca şifre oluştururken kullanılabilecek uygulamalar gösterilmelidir ve kullanımı teşvik edilmelidir. Doğru şifre oluşturulması için dikkat edilmesi gereken noktalar gösterilmelidir. Şifreler en az 1 sayısal karakter, 1 özel karakter içermesi ve karmaşık şiflerin oluşturulup kullanılması konusunda çalışanlar bilgilendirilmelidir.
5	Ek önlemler	Ek önlemler olarak, kullanılan tarayıcılara reklam engelleyici, HTTPS zorlayıcı, güvenilir link kontrolü vb. işlemleri gerçekleştirecek eklentilerden ve uygulamalardan bahsedilmelidir. Şirket içinde bu uygulama ve eklentilerin kullanımı teşvik edilmelidir.
6	Hukuksal hakimiyet	Kişilere, hukuki yönden neler yapabilecekleri hakkında bilgilendirme yapılmalı. KVKK hakkında bilgiler verilmeli. Kişilerin hakları öğretilmeli. Şirket içinde ve dışında yaşanan siber suç karşısında bu olay kimlere bildirilmeli ne gibi prosedürler izlenmesi gerektiği öğretilmelidir.

4. TARTIŞMA VE SONUÇ

Bu tez çalışması, siber güvenlik alanında önemli bir zafiyet kaynağı olan insan faktörünü ele almıştır. Tez çalışması, şirket içindeki çalışanların davranışları üzerinden risk profilleri oluşturmayı ve buna dayalı olarak etkili önlemler geliştirmeyi amaçlamıştır. Makine öğrenmesi araçlarının kullanımıyla elde edilen bulgular, şirketlerin siber güvenlik stratejilerini güçlendirmek adına değerli bir kaynak sunmaktadır.

Çalışmanın ana odak noktası, K-means ve Mean Shift algoritmalarını kullanarak çalışanları belirli gruplara ayırmaktır. Bu gruplar içindeki benzer davranışların tespit edilip, ortak bir aksiyon belirlenmesidir. Elde edilen grupların, yaş ve tecrübe gibi parametrelerle birleştirilmesiyle ortaya çıkan risk matrisi, şirketlerin siber güvenlik risklerini daha iyi anlamalarını ve buna göre stratejiler geliştirmelerini sağlamaktadır.

Bu tez çalışması, siber güvenlik alanında önleyici önlemlerin teknik yönünün ötesine geçerek, insan faktörünü ele alan bir yaklaşım sunmaktadır. Çalışan profilleri üzerinden oluşturulan risk matrisi, şirketlere belirli departmanlarda veya yaş gruplarında potansiyel risklere dair net bir bakış açısı sunmakta ve bu doğrultuda özelleştirilmiş çözümler üretmelerine yardımcı olmaktadır.

Çalışma şirketler üzerinde, okullarda, devlet dairelerinde hatta bireysel hayatta uygulanabilir. Yapı gereğiyle aksiyonlar tüzel veya kurumlara göre değişikliğe açıktır. Anketler kurumlara göre tekrar doldurulabilir ve bu bilgilerle çalıştırılan algoritmalar sonucunda yeni sonuçlar elde edilebilir. Bu şekilde şirkete özel matris ve aksiyonlar çıkararak daha efektif bir kullanım sağlanabilir.

Sonuç olarak, bu çalışma, siber güvenliği sadece teknik önlemlerle sınırlamayan, aynı zamanda çalışan davranışlarını da merkeze alan bütüncül bir yaklaşım sunmaktadır. Şirketler, bu metodolojiyi benimseyerek, siber güvenlik stratejilerini daha etkili ve kapsamlı bir şekilde optimize edebilirler. Gelecekteki araştırmalarda, daha fazla veri kaynağının entegrasyonu ve yeni algoritmaların incelenmesi ile bu yaklaşımın daha da geliştirilmesi önerilmektedir.

KAYNAKLAR

[1] Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected. https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020 adresinden 4 Haziran 2023 tarihinde alınmıştır.

[2] FBI sees spike in cyber crime reports during coronavirus pandemic. https://thehill.com/policy/cybersecurity/493198-fbi-sees-spike-in-cyber-crime-reports-during-coronavirus-pandemic/ adresinden 13 Mart 2023 tarihinde alınmıştır.

[3] Mancuso, V. F., Strang, A. J., Funke, G. J., & Finomore, V. S. (2014). Human factors of cyber attacks: a framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting(Vol. 58, No. 1, pp. 437-441). Sage CA: Los Angeles, CA: SAGE Publications. https://doi.org/10.1177/1541931214581091

[4] Abawajy, J. (2014) User preference of cyber security awareness delivery methods, Behaviour & Information Technology, 33:3, 237-248. https://doi.org/10.1080/0144929X.2012.708787

[5] Eminağaoğlu, M. ve Gökşen, Y. (2009). Bilgi güvenliği nedir, ne değildir, Türkiye'de bilgi güvenliği sorunları ve çözüm önerileri. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 11(4), 1-15.

[6] Kaspersky dataset. The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within. Retrieved November 12, 2014, from https://www.kaspersky.com/blog/the-human-factor-in-it-security/ adresinden 20 Ocak 2023 tarihinde alınmıştır.

[7] Canbek, G. ve Sağıroğlu, Ş. (2007). Çocukların ve gençlerin bilgisayar ve internet güvenliği. Gazi Üniversitesi Politeknik Dergisi, 10(1), 33-39.

[8] Brady, C. (2010). Security awareness for children. Technical Report RHUL–MA–2010–05 (Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England.) 20 Haziran 2023 tarihinde https://www.ma.rhul.ac.uk/static/techrep/2010/RHUL-MA-2010-05.pdf adresinden alınmıştır.

[9] Machine Learning Explained. https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained adresinden 5 Temmuz 2023 tarihinde alınmıştır.

[10] Philip C. Jackson, On achieving human-level knowledge representation by developing a natural language of thought, Procedia Computer Science, Volume 190, 2021, Pages 388-407, ISSN 1877-0509. https://doi.org/10.1016/j.procs.2021.06.048

[11] Supervised & Unsupervised learning. https://www.geeksforgeeks. org/supervised- unsupervised-learning/ adresinden 10 Temmuz 2023 tarihinde alınmıştır.

[12] Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020). https://doi.org/10.1186/s40537-020-00318-5

[13] What is supervised learning. https://www.ibm.com/topics/supervised-learning. adresinden 15 Temmuz 2023 tarihinde alınmıştır.

[14] Clustering in machine learning. https://www.geeksforgeeks.org/clustering-in-machine-learning/ adresinden 25 Temmuz 2023 tarihinde alınmıştır.

[15] Ford, V., & Siraj, A. (2014, October). Applications of machine learning in cyber security. In Proceedings of the 27th international conference on computer applications in industry and engineering (Vol. 118). Kota Kinabalu, Malaysia: IEEE Xplore. https://doi.org/10.1016/j.cose.2023.103694

[16] Elbow Method for optimal value of k in KMeans https://www.geeksforgeeks.org/elbow-method-for-optimal-value-of-k-in-kmeans/ adresinden 22 Temmuz 2023 tarihinde alınmıştır.

[17] Mean-Shift Clustering: A Powerful Technique for Data Analysis with Python. https://medium.com/@shruti.dhumne/mean-shift-clustering-a-powerful-technique-for-data-analysis-with-python-f0c26bfb808a adresinden 2 Ağustos 2023 tarihinde alınmıştır.

[18] Üniversite Öğrencilerinin Kişisel Siber Güvenlik Davranışları ve Bilgi Güvenliği Farkındalıklarının İncelenmesi, İnönü Üniversitesi Eğitim Fakültesi Dergisi Cilt 21, Sayı 1, 2022

[19] Öğrencilerin Siber Güvenlik Davranışlarının Beş Faktör Kişilik Özellikleri ve Çeşitli Diğer Değişkenlere Göre İncelenmesi, "Mersin Üniversitesi Eğitim Fakültesi Dergisi, 2019; 15(1): 186-215"

[20] Abawajy, J. H. (2014). User preference of cyber security awareness delivery methods. http://dx.doi.org/10.1080/0144929X.2012.708787

[21] KARABÜK ÜNİVERSİTESİ ÇALIŞANLARINA YÖNELİK KİŞİSEL SİBER GÜVENLİK ÜZERİNE ARAŞTIRMA, Yıl 2020, Cilt: 10 Sayı: 2, 157 - 172, 30.12.2020, Kahramanmaraş Sütçü İmam Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi

[22] Kişisel Siber Güvenlik Yaklaşımlarının Değerlendirilmesi, Yıl 2022, Cilt: 13 Sayı: 3, 429 - 438, 30.09.2022, Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi.

[23] Albrechtsen, Eirik & Hovden, Jan. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security. 29. 432-445. 10.1016/j.cose.2009.12.005. https://doi.org/10.1016/j.cose.2009.12.005

[24] TOKMAK, M. (2023). Öğrencilerin Siber Güvenlik Farkındalık Düzeylerinin Makine Öğrenmesi Yöntemleri ile Belirlenmesi. Yüzüncü Yıl Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 28(2), 451-466. https://doi.org/10.53433/yyufbed.1181694

[25] KARACI, A., AKYÜZ, H. İ., & BİLGİCİ, G. (2017). Investigation of Cyber Security Behaviors of University Students. Kastamonu Eğitim Dergisi, 25(6), 2079-2094. https://doi.org/10.24106/kefdergi.351517

[26] Çam, H., Aslay, F., & Özen, Ü., (2019). Yükseköğretim Kurumlarında Bilgi Güvenliği Farkındalık Düzeylerinin Ölçümlenmesi. Yönetim Bilişim Sistemleri Dergisi , vol.5, no.2, 1-11.

[27] ML | Mean-Shift Clustering. https://www.geeksforgeeks.org/ml-mean-shift-clustering/ adresinden 4 Ağustos 2023 tarihinde alınmıştır.

[28] Anket Tekniği. https://www.bingol.edu.tr/media/226197/sayt-bolum13c-anket-teknigi.pdf adresinden 9 Şubat 2023 tarihinde alınmıştır.

[29] Quayyum, F., Cruzes, D. S., & Jaccheri, L. (2021). Cybersecurity awareness for children: A systematic literature review. International Journal of Child-Computer Interaction, 30, 100343. https://doi.org/10.1016/j.ijcci.2021.100343

[30] DBSCAN. https://en.wikipedia.org/wiki/DBSCAN adresinden 13 Eylül 2023 tarihinde alınmıştır.

[31] A101 dolandırıcılığı ortaya çıktı! Birebir aynısını yaptılar. https://www.milligazete.com.tr/haber/16761370/a101-dolandiriciligi-ortaya-cikti-birebir-aynisini-yaptilar adresinden 2 Ekim 2023 tarihinde alınmıştır.

[32] What is phishing? Examples, types, and techniques. https://www.csoonline.com/article/514515/what-is-phishing-examples-types-and-techniques.html adresinden 9 Kasım 2023 tarihinde alınmıştır.

[33] K. Coronges, R. Dodge, C. Mukina, Z. Radwick, J. Shevchik and E. Rovira, "The Influences of Social Networks on Phishing Vulnerability," 2012 45th Hawaii International Conference on System Sciences, Maui, HI, USA, 2012, pp. 2366-2373, https://doi.org/10.1109/HICSS.2012.657.

[34] Two-Factor Authentication Statistics By Users, Industry, Adoption Rate and Benefits https://www.enterpriseappstoday.com/stats/two-factor-authentication-statistics.html adresinden 18 Kasım 2023 tarihinde alınmıştır.

[35] Benefits of Changing Your Password Regularly https://www.proactive-info.com/blog/change-your-password adresinden 21 Kasım 2023 tarihinde alınmıştır.

[36] Kara, İ. (2019). “Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi.” Sakarya University Journal of Computer and Information Sciences, 2(2): 61-69.

[37] Bilgin, M., Sema, E., İdil, A., & Enes, Y. Kişisel Verileri Koruma Dergisi, 1(2): 1-2.

[38] T. KOCATEKİN, “Evolution and State of the Art in Password Storage”, ESTUDAM Bilişim, c. 4, sy. 3, ss. 37–44, 2023. https://doi.org/10.53608/estudambilisim.1318760

[39] Gebauer, J., Kline, D. M., & He, L. (2011). Password security risk versus effort: an exploratory study on user-perceived risk and the intention to use online applications. Journal of Information Systems Applied Research, 4(2), 52.

EKLER

EK A. Siber Farkındalık Formu

EK B. Etik Kurulu İzin Belgesi

EK A. Siber Farkındalık Formu

Tablo A.1. Anket Soruları

Soru	Cevaplar
1. Yaş	"Serbest format girilecektir"
2. Çalışma Durmu	Çalışıyor
	Çalışmıyor
3. Çalışılan Sektör	"Serbest format girilecektir"
4. Mesleğiniz	"Serbest format girilecektir"
5. Tecrübe Yılı	0-3
	3-5
	5-10
	10+
6. Daha önce siber farkındalık eğitimi aldınız mı?	Evet
	Hayır
7. Şirketiniz düzenli olarak siber farkındalık eğitimi yapıyor mu?	Evet
	Hayır
8. KVKK hakkında bilgi sahibi misiniz ve uygulamaya dikkat ediyor musunuz?	Evet
	Hayır
9. Şirket mailinize gelen zararlı/sahte mailleri kurumunuzda ilgili siber ekibe bildiriyor musunuz?	Evet
	Hayır

10. Girilen sitelerde HTTPS kullanım durumuna dikkat ediyor musunuz?	Evet Hayır
11. Gelen maillerin gönderen kişi ve içinde bulunan linkleri güvenli bir şekilde kontrol ediyor musunuz?	Evet Hayır
12. İki faktörlü kimlik doğrulama kullanıyor musunuz?	Evet Hayır
13. Bilgisayar başında olmadığınız zaman bilgisayarı kitliyor musunuz?	Evet Hayır
14. Bilmediğiniz sitelerden herhangi bir şekilde indirme işlemi gerçekleştiriyor musunuz?	Evet Hayır
15. Şifrelerinizi değiştirme sıklığınız nedir?	1-3 ayda bir 3-6 ayda bir defa Senede bir defa Zorunlu olmadıkça değiştirmiyorum
16. Şifrelerinizi nasıl saklıyorsunuz?	Not defteri Bitwarden vb. vault uygulamaları ile Bilgisayar veya telefonlarda bulunan text uygulamaları ile Postitler ile Diğer

17. Daha önce virüs/hack olayı yaşadınız mı? Yaşadıysanız hangi yöntem uygulandı?	Bilmiyorum Yaşamadım Mail yolu ile link yönlendirmesi sonucu bilgilerin ele geçirilmesi (Phishing) Zararlı sitelerde gezinme sonucu Farklı cihazlarda kullanılmış tanışabilir disk/CD vb. cihazların kullanımı İnternet üzerinden indirilen bir uygulama ile 3. bir kişiden elde edilen zip/rar tarzı dosyalar üzerinden
18. Kullandığınız teknolojik cihazların yazılımını ne sıklıkla güncelliyorsunuz?	Haftada bir Ayda bir Otomatik Güncelleme Etkin Yapmıyorum
19. Bilgisayarınızda Antivirüs yazılımı yüklü mü?	Evet Hayır Bilmiyorum
20. Bağlantılı veya belge içeren bir e-posta aldığınızda ne yaparsınız?	Beklenen bir e-posta değilse tıklamayacağım Bağlantıyı endişelenmeden kontrol ederdim.
21. Şifreleriniz büyük harf, rakam ve özel karakterlerden oluşuyor mu?	Evet Hayır Şifrem özel karakter içermiyor

EK B. Etik Kurulu İzin Belgesi

T.C.

SAKARYA ÜNİVERSİTESİ REKTÖRLÜĞÜ

Etik Kurulu

Sayı : E-61923333-050.99-318688 26.12.2023

Konu : 41/02 Esma SIĞIRTMAÇ

Sayın Esma SIĞIRTMAÇ

İlgi : 15.12.2023 tarihli ve E--000-0 sayılı yazınız.

Üniversitemiz Fen ve Mühendislik Bilimleri Etik Kurulunun 25.12.2023 tarihli ve 41 sayılı toplantısında alınan "02" nolu karar ile Esma SIĞIRTMAÇ'ın başvurusu **uygun** görülmüş ve karar örneği ekte sunulmuştur.

Bilgilerinizi rica ederim.

Prof. Dr. Şenol YILMAZ

Fen ve Mühendislik Bilimleri Etik Kurul Başkanı

2. Esma SIĞIRTMAÇ'ın " Siber Farkındalık Formu " başlıklı çalışması görüşmeye açıldı. Yapılan görüşmeler sonunda Esma SIĞIRTMAÇ'ın " Siber Farkındalık Formu " başlıklı çalışmasının Etik açıdan uygun olduğuna oy birliği ile karar verildi.

Bu belge, güvenli elektronik imza ile imzalanmıştır.

Doğrulama Kodu :BSDL3H9VNE Pin Kodu :06182 Belge Takip Adresi : https://turkiye.gov.tr/ebd?eK=5783&eD=BSDL3H9VNE&eS=318688 Adres:Esentepe Kampüsü 54187 Serdivan SAKARYA / KEP Adresi: Bilgi için: Hanife Babacan sakaryauniversitesi@hs01.kep.tr Unvanı: Birim Evrak Sorumlusu

Telefon No:0264 295 50 00 Faks No:0264 295 50 31

e-Posta:ozelkalem@sakarya.edu.tr Elektronik Ağ:www.sakarya.edu.tr

ÖZGEÇMİŞ

Ad-Soyad : Esma SIĞIRTMAÇ

ÖĞRENİM DURUMU:

- **Lisans :** 2021, Sakarya Üniversitesi, Bilgisayar ve Bilişim Bilimleri Fakültesi, Bilgisayar Mühendisliği Bölümü
- **Yüksek lisans :** Devam ediyor, Sakarya Üniversitesi, Bilgisayar ve Bilişim Mühendisliği Anabilim Dalı, Siber Güvenlik Programı

MESLEKİ DENEYİM:

- 2022 yılında özel bir bankada kimlik erişim ve yönetim uzmanı olarak çalışmaya başladı.