Anadolu Eğitim Liderliği ve Öğretim Dergisi *dergipark.gov.tr/ajeli*
[Anatolian Journal of Educational Leadership and Instruction] *e-ISSN:2148-2667*
2023 – 11(1), 48-66

Okul Yönetiminde Dijital Veri Güvenliği: Tehditler ve Önlemler

Mehmet ÖZDOĞRU ve Muhammet ASLANLI

Özet

Dijital verilerin kullanımının gün geçtikçe arttığı okullarda dijital veri güvenliğine yönelik olası tehditlerin önceden bilinmesi dijital verilerin güvenliğini sağlamaya yönelik atılacak adımların başarıya ulaşmasında etkili olacaktır. Bu doğrultuda araştırmanın amacı okul yönetiminde dijital veri güvenliğine yönelik tehditleri ve önlemleri okul yöneticilerinin görüşleri doğrultusunda incelemektir. Araştırma nitel araştırma yöntemine uygun olarak gerçekleştirilmiştir. Araştırma durum çalışması desenine göre yürütülmüştür. Araştırmanın katılımcılarını Kütahya ilinde görev yapan 13 okul yöneticisi oluşturmaktadır. Katılımcıların belirlenmesinde "maksimum çeşitlilik örnekleme yöntemi" kullanılmıştır. Araştırma verilerinin toplanmasında "yarı yapılandırılmış görüşme formu" kullanılmıştır. Araştırmanın verileri 2022-2023 eğitim-öğretim yılı güz döneminde toplanmıştır. Verilerin toplanması sürecinde Kütahya il merkezinde devlet okullarında görevli 13 okul yöneticisiyle görüşmeler yapılmıştır. Araştırmada görüşmeler sonucu ulaşılan verilerin analizinde içerik analizi tekniğinden yararlanılmıştır. Araştırmada okul yönetiminde dijital veri güvenliğine yönelik tehditler teması altında 5 alt temaya ulaşılmıştır. Buna göre kullanıcılardan kaynaklı durumlar, şifre kullanımıyla ilgili sorunlar, teknolojik araç-gereçlerin yanlış kullanımı, internet kaynaklı tehditler ve depolama alanlarının güvenliğiyle ilgili sorunlar okul yönetiminde dijital veri güvenliğini tehdit eden unsurlardır. Ayrıca araştırmada okul yönetiminde dijital veri güvenliğine yönelik alınan önlemler teması altında 2 alt temaya ulaşılmıştır. Buna göre okullarda dijital verilerin güvenliği için kullanıcılara yönelik önlemler ile donanımsal ve yazılımsal önlemler olmak üzere birtakım tedbirlerin alındığı görülmüştür. Araştırma bulguları genel olarak değerlendirildiğinde okulun yönetsel işlerinde kullanılan dijital verilerin güvenliğine yönelik birçok tehdit unsurunun olduğu bununla birlikte okul yöneticileri tarafından bu tehditlere yönelik bazı önlemlerin alındığı sonucu ortaya çıkmıştır. Araştırma sonuçlarına dayanarak okullarda dijital veri güvenliğini sağlamaya yönelik yasal düzenlemelerin yanı sıra sürekli değişen tehditlere karşı okul çalışanlarının bilgilendirilmesine gereksinim olduğu söylenebilir.

Anahtar Kelimeler: Okul, dijital veri güvenliği, bilgi güvenliği, okul yöneticisi

Digital Data Security in School Management: Threats and Precautions

Abstract

In schools where the use of digital data is increasing day by day, knowing the possible threats to digital data security in advance will be effective in achieving success in the steps to be taken to ensure the security of digital data. Accordingly, the aim of this study is to examine the threats and measures for digital data security in school administration in line with the views of school administrators. The research was conducted in accordance with the qualitative research method. The research was conducted according to the case study design. The participants of the study consisted of 13 school administrators working in Kütahya. "Maximum diversity sampling method" was used to determine the participants. A "semi-structured interview form" was used to collect the research data. The data were collected in the fall semester of the 2022-2023 academic year. During the data collection process, interviews were conducted with 13 school administrators working in public schools in Kütahya city center. Content analysis technique was used to analyze the data obtained from the interviews. In the research, 5 sub-

Article/Makalenin; Submission Date / Gönderilme Tarihi: 17 March/Mart 2023
Revised Date / Hakem Atama: 01 May/Mayıs 2023
Accepted Date/ Kabul Tarihi: 10 June/Haziran 2023

themes were reached under the theme of threats to digital data security in school administration. Accordingly, situations arising from users, problems related to the use of passwords, misuse of technological tools, internet-based threats and problems related to the security of storage areas are the factors that threaten digital data security in school administration. In addition, 2 sub-themes were found under the theme of measures taken for digital data security in school administration. Accordingly, it was seen that some measures were taken for the security of digital data in schools, including user-oriented measures and hardware and software measures. When the findings of the research are evaluated in general, it is concluded that there are many threats to the security of digital data used in the administrative work of the school, but some measures are taken by school administrators against these threats. Based on the results of the research, it can be said that there is a need to inform school employees about the ever-changing threats as well as legal regulations to ensure digital data security in schools.

Keywords: School, digital data security, information security, school administrator

Extended Abstract

Introduction

The rapid development and progress in information technologies in recent years has closely affected the life of society. It is seen that these developments in technology have facilitated human life in many areas such as access to information, storage, reproduction and transportation of information. One of these facilitations is the ability to store and process information, which was previously stored in written form, in digital media with the development of technology. Information that can be transferred to digital media with the help of various technological tools can be converted into digital data and can be used, transported and reproduced whenever needed. In this way, significant gains are achieved in both time and labor.

Schools are one of the leading educational institutions where digital data are used intensively. In recent years, school administrations have been storing and processing data on students, teachers and many administrative activities in digital environments. In particular, data belonging to millions of students and teachers are stored in systems such as "MEBBİS (Ministry of National Education Information Systems), TEFBİS (Financing of Education in Turkey and Education Expenditures Information Management System), KBS (Public Accounts Information System) and e-School Management Information System". School administrators are primarily responsible for the use and security of these systems in schools. For this reason, school administrators' awareness of digital data security is important in terms of minimizing the impact of threats and attacks that may be encountered in the process.

Identifying threats to the security of digital data used in school administration and revealing the current measures taken against these threats are important for the development of effective policies on digital data security in educational institutions. School administrators, who are primarily responsible for the management of schools, are the people who produce solutions to the problems that occur in schools. In this direction, the opinions of school administrators can be considered as an important data source in the decisions to be taken regarding digital data security in school administration. There may be many problems in educational institutions regarding the security of digital data. Determining the problems encountered in school administration regarding digital data security in line with the opinions of administrators may contribute to reducing the impact of possible threats. Therefore, the aim of the study is to examine the threats and measures for digital data security in school administration in line with the views of school administrators.

Method

In this study, which aims to examine the threats and measures for digital data security encountered in school administration according to the views of school administrators, qualitative research method was used. The research was conducted according to the case study design. The aim of case studies is to examine the determined subject in depth and to reveal the results of the situation (Yıldırım & Şimşek, 2018).

The participants of this study consisted of 13 school administrators working in Kütahya. "Maximum diversity sampling method" was used to determine the participants. The purpose of this method is to create a small sample group that includes individuals who may be a party to the problem under investigation by ensuring maximum diversity (Yıldırım & Şimşek, 2018). In order to ensure this diversity in the study, attention was paid to ensure that the participants consisted of administrators who differed in terms of "educational status, seniority in administration, gender, age, and school level".

In the study, a semi-structured interview form was used to examine the threats and measures for digital data security encountered in school administration according to the views of school administrators. The data of the study were collected in the fall semester of the 2022-2023 academic year. During the data collection process, interviews were conducted with 13 school administrators working in public schools in Kütahya city center.

In the research, content analysis technique was used to analyze the data obtained through interviews. In content analysis, the data obtained in the research are analyzed in detail. In order to understand the data, codes are given, and then similar codes are brought together to form themes (Yıldırım & Şimşek, 2018). Some measures were taken to ensure the validity and reliability of this qualitative research. These measures were handled within the framework of the concepts of "internal validity (credibility), external validity (transferability), internal reliability (consistency) and external reliability (confirmability)" put forward by Lincoln & Guba (1985).

Findings

In the study, 5 sub-themes were found under the theme of threats to digital data security in school administration. These sub-themes are situations arising from users, problems related to the use of passwords, misuse of technological tools, internet-based threats and storage area security problems. Situations arising from users regarding digital data security in school administration were identified as low technology literacy, low awareness of data security, sharing of personal data and frequent staff turnover. As problems related to the use of passwords, the opinions of not using secure passwords, filling forms automatically, sharing passwords with unauthorized people, sharing passwords on social networks, keeping them in visible environments and using passwords in insecure environments emerged. Threats to the misuse of technological equipment are shared use of computers, leaving computers on all the time, uncontrolled usb, external memory connection, use of pirated software, taking computers out of the institution for repair and not using anti-virus programs. Internet-based threats to digital data security in school administration are cyber-attacks, e-mails of unknown origin and network connection problems. Threats to the security of storage areas where digital data are stored are sudden voltage spikes, not using power supply and fire, flood, theft, etc.

In the study, 2 sub-themes were found under the theme of measures taken for digital data security in school administration. These sub-themes are measures for users and hardware and software measures. As measures for users, the opinions of disseminating the use of secure passwords, defining sub-users, informing the staff, sharing meetings, obtaining information from the internet and in-service training

activities emerged. Hardware and software measures taken to ensure digital data security in school management include data backup, secure internet usage, anti-virus software and licensed software.

Conclusion, Discussion And Recommendations

In this study, threats and precautions against digital data security in school administration were examined in line with the views of school administrators. First of all, threats to digital data security in school administration were revealed in the light of the data obtained from school administrators. In the research, 5 sub-themes were reached: threats to digital data security in school administration, situations arising from users, problems related to password use, misuse of technological tools, internet-based threats and threats to the security of storage areas. Accordingly, it is seen that there are many threats to the security of digital data that are used intensively in the administrative activities of schools. Praveena & Smys (2017) state that the increasing number of data used on digital platforms has led to the emergence of many issues and problems regarding the security of these data. Similarly, Yılmaz, Şahin & Akbulut (2016) state that there are many threats to digital data security today.

One of the main findings of the study is that a significant portion of the threats to digital data security in school administration are threats originating from users. These threats were identified as low technology literacy of users, low awareness of data security, sharing of personal data, and frequent staff turnover. According to Taha & Dahabiyeh (2020), low user awareness of digital data security is one of the main threats. Tekerek (2008) states in his study that situations arising from users are an important threat to data security. Wagner & Brooke (2007) state that human-related factors have an important share in negative situations that may occur in information security. Gökçearslan, Günbatar & Sarıtepeci (2021) state that individuals do not consciously perform behaviors that violate the security of information about their institutions and themselves.

Within the scope of the current study, the measures taken for digital data security in school administration were also identified. In this direction, it is seen that the opinions of school administrators about the measures taken to ensure digital data security in schools are grouped under two sub-themes: user-oriented measures and hardware measures. As measures for users, the measures include disseminating the use of secure passwords, defining sub-users, informing the staff, sharing meetings, obtaining information from the internet and organizing in-service training activities. Tekerek (2008) states that unconscious users constitute a significant part of the source of threats to the security of digital data. According to Gündüzalp (2021), technical measures taken in the security of digital data in organizations are insufficient, and measures aimed at users and individuals should be put into practice. In order to ensure the security of digital data and minimize threats, it is necessary to increase the awareness of individuals and users (Yılmaz, Şahin & Akbulut, 2016). In today's world where information technologies are rapidly changing and developing, individuals using these technologies need to renew and update themselves at the same speed (Yüksel & Adıgüzel, 2011). In this direction, it is important for users who process digital data to improve themselves at the point of ensuring the security of data.

When the research findings are evaluated in general, it is concluded that there are multiple threats to digital data security in school administration. The fact that digital data security has many subcomponents causes the threats that can be encountered to be very diverse. It is especially noteworthy that situations arising from users are an important factor in the security of digital data. Hardware and software measures taken for the security of digital data will not be sufficient if the level of awareness and consciousness of users is not high. This situation will make digital data vulnerable to threats. In the research, it was concluded that problems related to the use of passwords, misuse of technological tools, internet-based

threats and situations related to the security of storage areas also pose a threat to digital data security in school administration. In addition, the study concluded that some measures are taken to ensure the security of digital data in schools. These measures stand out as user-oriented measures and hardware measures. This result indicates that school administrators have a certain level of awareness about digital data security. These results can be an important source of data on digital data security in school administration.

Based on the findings of the research, some suggestions can be made to practitioners and researchers.

Periodic maintenance of the platforms where digital data are hosted should be carried out, and infrastructures should be better equipped in terms of cyber security against possible threats.

Newly recruited personnel in schools should be informed about digital data security and awareness should be raised.

The digital data security awareness of candidates for selection and appointment as school administrators should be determined, and pre-service training activities should be organized before they take office.

Giriş

Son yıllarda bilişim teknolojilerinde yaşanan hızlı gelişim ve ilerleme toplum hayatını yakından etkilemektedir. Teknolojide yaşanılan bu gelişmelerin bilgiye erişim, bilginin saklanması, çoğaltılması ve taşınabilmesi gibi daha birçok alanda insan hayatını kolaylaştırdığı görülmektedir. Önceleri yazılı olarak muhafaza edilen bilginin teknolojinin gelişimiyle birlikte dijital ortamlarda saklanması ve işlenebilmesi bu kolaylıklardan biridir. Çeşitli teknolojik araç gereçler yardımıyla dijital ortamlara aktarılabilen bilgiler dijital veri haline getirilerek ihtiyaç anında kullanılabilmekte, taşınabilmekte ve çoğaltılabilmektedir. Bu sayede hem zamandan hem iş gücünden önemli kazanımlar elde edilmektedir.

Bilgi ve iletişim teknolojilerindeki yaşanılan hızlı değişim beraberinde dijital verilerin güvenliğiyle ilgili sorunları da getirmiştir (Aldridge, Medina & Ralphs, 2010). Yapılan bir araştırmaya göre dijital verilerin yasadışı bir şekilde ele geçirildiği olayların sayısı 2020 yılında %20 artarak dikkat çekici bir seviyeye gelmiştir (Simplilearn, 2021). Teknoloji kullanımının giderek artmasıyla birlikte dijital verilere yönelik tehditlerde de önemli artışlar yaşanmaktadır. Dünya üzerinde dijital verilere yönelik tehditlerde 2021 yılında %25 oranında artış yaşanırken 2022 yılına gelindiğinde ise bu oran %62'ye çıkmıştır (ThinkTech, 2023).

Teknolojinin kullanımının insan hayatını kolaylaştırması beraberinde birtakım riskleri ortaya çıkarmıştır. Bu risklerden birisi de dijital verilerin güvenliğidir. Canbek & Sağıroğlu'na (2006) göre dijital veri güvenliği "elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında verilerin gizlilik ve bütünlüğünün korunması, yetkisiz kişilerce erişiminin önlenebilmesi için güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür.". Dijital veri güvenliği günümüzde bilişim teknolojileri kullanılarak gerçekleştirilen faaliyetlerde karşılaşılan en önemli sorunlardan biridir (Solichin & Ramadhan, 2017).

Dijital veri güvenliğiyle ilgili olarak gerek bireyler gerekse kurumlar genelde sorunla karşılaştıkları zaman önlem almaktadır. Ancak dijital verilerin güvenliği, sorunla karşılaşılmadan önce, sürecin başından itibaren önem verilmesi gereken bir konudur (Kruger & Kearney, 2006). Bu nedenle kurum ve kuruluşlar faaliyet alanları içerisinde kullandıkları dijital verilerin güvenliğine yönelik gereken tedbirleri önceden almakla sorumludur.

Dijital verilerin güvenliğine yönelik alınan tedbirlere bakıldığında sistemsel ve donanımsal önlemlerin öne çıktığı görülmektedir. Konuyla ilgili araştırmalarda ise insan unsuruna yeterince önem verilmeyen sistemsel ve donanımsal önlemlerin dijital verilere yönelik riskleri ve tehditleri azaltmada yetersiz olduğu sonuçları ortaya çıkmıştır (Avcı & Arslan, 2019; Şahinaslan vd., 2009; Yılmaz vd, 2015). Dijital verilerin güvenliğiyle ilgili tehditlerin önemli bir kısmı kullanıcıların dijital veri güvenliği farkındalıklarının düşük olmasına dayanmaktadır (Taha & Dahabiyeh, 2020).

Bilişim teknolojilerinin kullanımı bireyler arasında artmakla birlikte kurumlar arasında da kullanım alanarının hızla yaygınlaştığı görülmektedir. Kurumlar teknolojiyi faaliyetlerine entegre ederek birçok hizmeti dijital ortamlarda sunmaktadır. Günümüzde bilişim teknolojilerinin yoğun olarak kullanıldığı kurumlardan biri de eğitim kurumlarıdır. Eğitim kurumları faaliyet alanlarına giren öğrenme süreçleri, yönetim faaliyetleri ve iletişim gibi daha birçok alanda teknolojiyi kullanarak çalışmalarını gerçekleştirmektedir. Bu sayede gerek zaman gerek insan kaynağının etkili kullanımı açısından önemli faydalar elde edilmektedir. Ancak teknolojinin eğitim-öğretim süreçlerine tüm bu katkılarının yanı sıra meydana gelebilecek riskleri ve olumsuzlukları gözden kaçırmamak gerekir. Eğitim kurumları açısından bakıldığında bu risklerin başında dijital verilerin güvenliği gelmektedir (Keser & Yayla, 2021).

Okullar dijital verilerin yoğun bir şekilde kullanıldığı eğitim kurumlarının başında gelmektedir. Son yıllarda okul yönetimleri tarafından başta öğrencilere, öğretmenlere ve birçok yönetimsel faaliyete ait veriler dijital ortamlarda saklanmakta ve işlenmektedir. Özellikle milyonlarca öğrenci ve öğretmene ait veriler "MEBBİS (Millî Eğitim Bakanlığı Bilişim Sistemleri), TEFBİS (Türkiye'de Eğitimin Finansmanı ve Eğitim Harcamaları Bilgi Yönetim Sistemi), KBS (Kamu Hesapları Bilgi Sistemi) ve e-Okul Yönetimi Bilgi Sistemi" gibi sistemlerde depolanmaktadır. Okullarda söz konusu sistemlerin kullanımından ve güvenliğinden öncelikle okul yönetimleri sorumludur. Bu nedenle okul yöneticilerinin dijital veri güvenliğine yönelik farkındalıkları süreçte karşılaşılabilecek tehditlerin ve saldırıların etkisinin en aza indirilmesi bakımından önemlidir.

Alan yazında eğitim kurumlarında dijital veri güvenliği konusunda yapılan araştırmalar incelendiğinde; öğretmenlere yönelik dijital veri güvenliği farkındalık ölçeği geliştirilmesi (Çetinkaya, Güldüren & Keser, 2017; Yılmaz, Şahin & Akbulut, 2015), öğretmenlerin ve öğrencilerin dijital veri güvenliği farkındalık düzeylerinin belirlenmesi (Avcı & Oruç, 2020; Göldağ, 2021; Keser & Yayla, 2021; Öztürk & Çakır, 2022; Talan & Aktürk, 2021; Yılmaz, Şahin & Akbulut, 2016), üniversite çalışanlarının dijital veri güvenliği farkındalıklarının belirlenmesi (Aslay, Handan & Üstün, 2019; Gündüzalp, 2021) gibi konuların incelendiği görülmektedir. Söz konusu akademik çalışmalar genel olarak değerlendirildiğinde yapılan çalışmaların öğretmen ve öğrenciler üzerinde yoğunlaştığı görülmektedir. Bununla birlikte teknolojinin gelişmesiyle dijital verilerin okul yönetiminde kullanımı hızla artmaktadır. Ancak okullarda söz konusu dijital verilerin kullanımından ve güvenliğinden öncelikle sorumlu olan okul yöneticileriyle yapılmış herhangi bir araştırmaya rastlanmamıştır. Bu çalışmayla dijital verilerin yoğun bir şekilde kullanıldığı okulların yönetim faaliyetlerinde olası tehditleri ve alınan önlemleri okulların yönetiminden birinci derecede sorumlu okul yöneticilerinin perspektifinden incelemek amaçlanmaktadır. Bu bağlamda araştırma sonuçlarının okul yönetiminde dijital veri güvenliği konusunda farkındalık oluşturacağı ve bu konuda yapılacak çalışmalara katkı sağlayacağı düşünülmektedir.

Okul yönetiminde kullanılan dijital verilerin güvenliğine yönelik tehditlerin tespit edilmesi ve bu tehditlere karşı alınan mevcut önlemlerin ortaya çıkarılması eğitim kurumlarında dijital veri güvenliği konusunda etkili politikaların geliştirilmesi açısından önem arz etmektedir. Okulların yönetiminden birinci derecede sorumlu olan okul yöneticileri okullarda meydana gelen sorunlara çözüm üreten kişilerdir. Bu doğrultuda okul yönetiminde dijital veri güvenliğine yönelik alınacak kararlarda okul yöneticilerinin görüşleri önemli bir veri kaynağı olarak değerlendirilebilir. Dijital verilerin güvenliğiyle

ilgili eğitim kurumlarında birçok sorun olabilir. Kullanıcılardan kaynaklı sorunlar (Wagner & Brooke ,2007), şifre kullanımıyla ilgili sorunlar (Kruger, Drevin & Steyn, 2010), korsan yazılımlar (Ünver, Canbay & Mirzaoğlu, 2009), spam e-postaları ve bilgisayar virüsleri (Yılmaz, Şahin & Akbulut, 2016) bu sorunlardan bazılarıdır. Araştırmayla dijital veri güvenliği konusunda okul yönetiminde karşılaşılan sorunların yöneticilerin görüşleri doğrultusunda belirlenmesi, olası tehditlerin etkisinin azaltılmasına katkı yapabilir. Bu nedenle araştırmanın amacı okul yönetiminde dijital veri güvenliğine yönelik tehditleri ve önlemleri okul yöneticilerinin görüşleri doğrultusunda incelemektir. Bu amaca ulaşmak için şu sorulara cevap aranmıştır:

1. Okullarda dijital veri güvenliğine yönelik tehditler nelerdir?
2. Okul yönetiminde dijital veri güvenliğini sağlamaya yönelik neler yapılmaktadır?

Yöntem

Araştırma Deseni

Okul yönetiminde karşılaşılan dijital veri güvenliğine yönelik tehditleri ve önlemleri okul yöneticilerinin görüşlerine göre incelemeyi amaçlayan bu çalışmada nitel araştırma yöntemine başvurulmuştur. Araştırma durum çalışması desenine göre yürütülmüştür. Durum çalışmalarının amacı belirlenen konunun derinlemesine ele alınması ve duruma ilişkin sonuçların ortaya çıkarılmasıdır (Yıldırım ve Şimşek, 2018). Durum çalışmalarında araştırılan durum gerçek yaşamın içerisinde olmalı, güncel bağlamından koparılmadan araştırılmalıdır (Creswell, 2016). Bu bağlamda araştırmada okul yönetiminde dijital veri güvenliğine yönelik tehditlerin neler olduğu incelenmiş ve bu tehditlere yönelik alınan önlemler durum olarak araştırılmıştır.

Çalışma grubu

Bu araştırmanın katılımcılarını Kütahya ilinde görev yapan 13 okul yöneticisi oluşturmaktadır. Katılımcıların belirlenmesinde "maksimum çeşitlilik örnekleme yöntemi" kullanılmıştır. Bu yöntemdeki amaç incelenen probleme taraf olabilecek bireylerin maksimum düzeyde çeşitliliğinin sağlanarak yer aldığı küçük bir örneklem grubu oluşturmaktır (Yıldırım ve Şimşek, 2018). Çalışmada bu çeşitliliğin sağlanması için katılımcıların "eğitim durumu, yöneticilik kıdemi, cinsiyet, yaş, görev yapılan okul kademesi" açısından farklılaşan yöneticilerden oluşmasına dikkat edilmiştir. Çalışma grubu toplam 13 okul yöneticisinden oluşmaktadır. Katılımcı okul yöneticilerinin 6'sı lisans, 7'si yüksek lisans mezunudur. Yöneticilik kıdemi olarak katılımcı okul yöneticilerinin 6'sı 8 ve üzeri yıl, 4'ü 3 ve üzeri yıl, 3'ü 11 ve üzeri yıl kıdeme sahiptir. Okul yöneticilerinin 10'u erkek, 3'ü kadındır. Katılımcıların 5'i ilkokulda, 4'ü ortaokulda, 4'ü lisede görev yapmaktadır.

Veri Toplama Aracı

Çalışmada okul yönetiminde karşılaşılan dijital veri güvenliğine yönelik tehditleri ve önlemleri okul yöneticilerinin görüşlerine göre incelemek için "yarı yapılandırılmış görüşme formu" kullanılmıştır. Görüşme formu geliştirilmeden önce ilk olarak ilgili alan yazın taranarak konuyla ilişkili çalışmalar (Çetinkaya, Güldüren & Keser, 2017; Gündüzalp, 2021; Öz, 2020; Simplilearn, 2021; Yılmaz, Şahin & Akbulut, 2016) incelenmiş ve taslak form hazırlanmıştır. Hazırlanan form iki alan uzman tarafından incelenmiştir. İncelemeyi yapan uzmanlar nitel araştırmalar konusunda deneyimi olan eğitim yönetimi alanında görev yapan akademisyenlerdir. Uzman görüşleri doğrultusunda taslak formda gerekli düzenlemeler yapılmıştır. Son olarak form araştırmanın çalışma grubu içerisinde yer almayan iki okul yöneticisine uygulanarak öneriler alınmıştır. Pilot uygulaması yapılan formun anlaşılır ve amaca uygun olduğu görülmüştür. Son halini alan form iki bölümden oluşmaktadır. Görüşme formunun birinci bölümünde katılımcıların demografik özelliklerini belirlemek için 6 soru yer almaktadır. Formun ikinci

bölümünde ise okul yönetiminde dijital veri güvenliğine yönelik tehditleri ve önlemleri belirlemeye yönelik 2 açık uçlu soru ve 4 sonda soru bulunmaktadır.

Verilerin Toplanması

Araştırmanın verileri 2022-2023 eğitim-öğretim yılı güz döneminde toplanmıştır. Verilerin toplanması sürecinde Kütahya il merkezinde devlet okullarında görevli 13 okul yöneticisiyle görüşmeler yapılmıştır. Araştırma öncesi katılımcılarla iletişime geçilerek araştırmanın içeriği açıklanmış, yapılacak görüşmenin zamanı ve yeri belirlenmiştir. Görüşmeler katılımcıların talepleri doğrultusunda görevli oldukları okullarda yapılmıştır. Görüşmelerden önce okul yöneticileri onam formuyla bilgilendirilmiştir. Ayrıca katılımcılara araştırma etiği ve gizlilik konularında açıklamalar yapılmış, katılımın gönüllük esaslı olduğu ifade edilmiş ve ses kaydı onayı alınmıştır. İki okul yöneticisi ses kaydına izin vermediğinden görüşme esnasında notlar tutularak görüşme kayıt altına alınmıştır. Katılımcılara demografik bilgilerinin yanı sıra araştırmanın amacı kapsamında okullarda dijital veri güvenliğine yönelik tehditler neler olduğu ve bu tehditlere yönelik okul yöneticilerinin neler yaptıkları sorulmuştur. Katılımcılarla yapılan görüşmelerin süresi 25-30 dakika aralığında olmuştur. Toplamda 365 dakikalık ses kaydı elde edilmiştir. Çalışmanın etik kurul izni; Kütahya Dumlupınar Üniversitesi Rektörlüğü Sosyal ve Beşeri Bilimler Bilimsel Araştırma ve Yayın Etiği Kurulu'ndan, 05.10.2022 tarih ve 2022/08 sayılı karar ile alınmıştır.

Verilerin Analizi

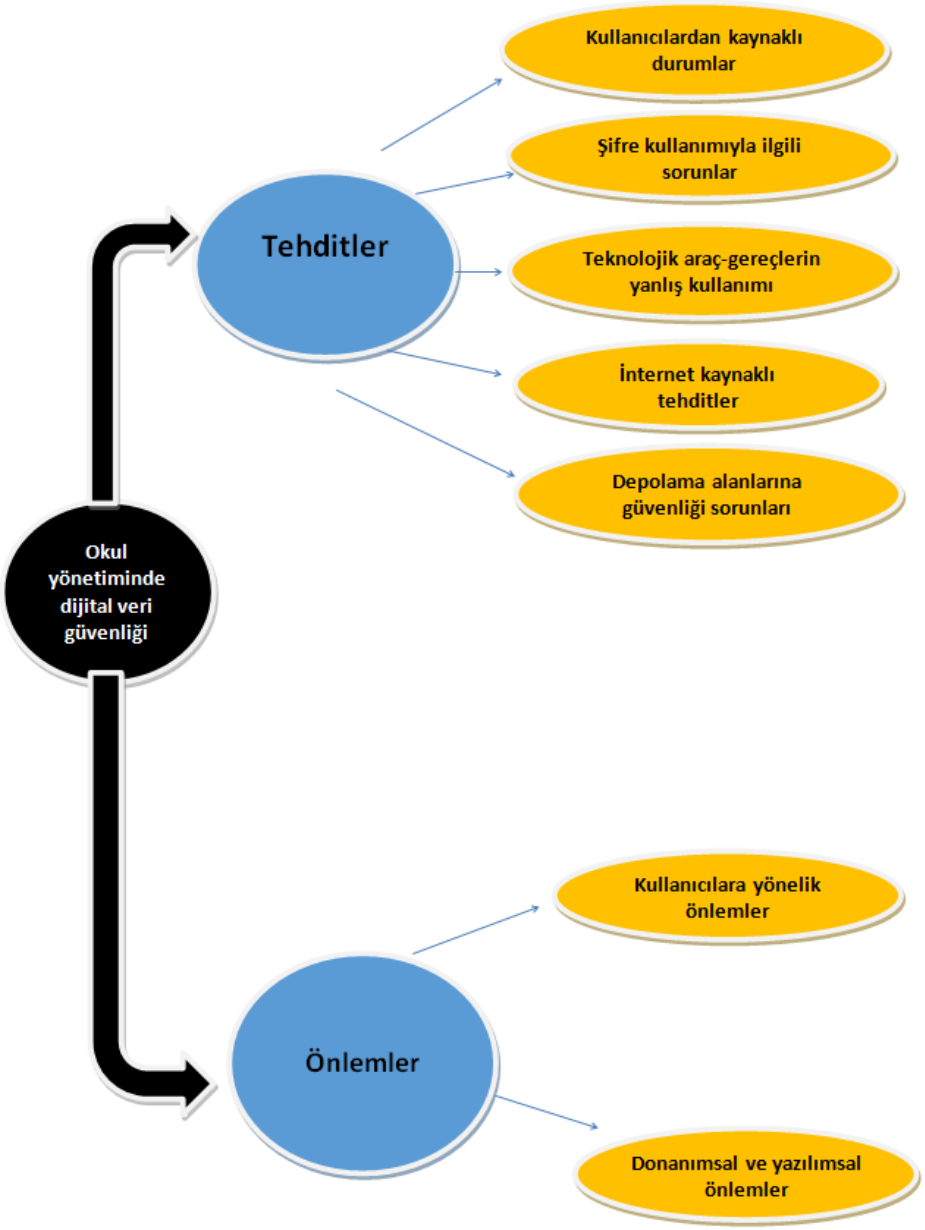
Araştırmada görüşmeler sonucu ulaşılan verilerin analizinde içerik analizi tekniğinden yararlanılmıştır. İçerik analizinde araştırmada ulaşılan veriler ayrıntılı olarak analiz edilmektedir. Verilerin anlaşılabilmesi için kodlar verilmekte, daha sonra benzer kodlar bir araya getirilerek temalar oluşturulmaktadır (Yıldırım ve Şimşek, 2018). Analize başlamadan önce ses kayıtları bilgisayara aktarılarak yazılı hale getirilmiştir. Yazılı hale getirilen veriler ses kayıtlarıyla karşılaştırılarak kayıp verinin önüne geçilmiştir. Daha sonra katılımcıların araştırma sorularına vermiş oldukları cevaplardaki ortak noktalar tespit edilerek kodlar verilmiştir. Birbiriyle ilişkili kodlar bir araya getirilerek temalar oluşturulmuştur. Kavramsal çerçeve göz önünde bulundurularak temaların kendi içinde anlamlı olmasına özen gösterilmiştir. Bulgular yorumlanırken katılımcı grubun özgün düşünce ve görüşlerini yansıtmak amacıyla doğrudan alıntılar da sunulmuştur. Ayrıca katılımcı gizliliğinin sağlanması amacıyla araştırmaya katılan okul yöneticilerine Yönetici 1 (Y1), Yönetici 2 (Y2),... şeklinde kısaltma yapılmış ve numara verilmiştir.

Geçerlik ve Güvenirlik

Nitel yöntemle yürütülen bu araştırmanın geçerlik ve güvenirliğini sağlamak için bazı önlemler alınmıştır. Bu önlemler Lincoln & Guba (1985) tarafından ortaya koyulan "iç geçerlik (inandırıcılık), dış geçerlik (aktarılabilirlik), iç güvenirlik (tutarlılık) ve dış güvenirlik (teyit edilebilirlik)" kavramları çerçevesinde ele alınmıştır.

Araştırmada iç geçerliliğin sağlanması için görüşme sorularının hazırlanmasında alan yazın incelenmiş, uzman görüşlerinden yararlanılmıştır. Hazırlanan sorular katılımcı gruptan olmayan iki okul yöneticisine uygulanarak ön uygulama yapılmıştır. Görüşmelerin öncesinde katılımcılar araştırmanın amacı konusunda bilgilendirilmiş, gizlik ve araştırma etiği konusunda açıklamalar yapılmıştır. Görüşmelerde katılımcılarla yeteri kadar etkileşimde bulunulmuştur. Görüşmeler sonucu ulaşılan verilerin deşifresinden sonra katılımcılara gönderilmiştir. Katılımcılardan eksik veya hatalı ifadelerin tespit edilmesi istenerek katılımcı teyidi sağlanmıştır.

Dış geçerliğin (aktarılabilirlik) sağlanması için çalışmanın tüm aşamaları detaylı olarak okuyuculara sunulmuştur. İç güvenirliğin (tutarlılık) sağlanması için "kodlayıcılar arası görüş birliği" tekniğinden yararlanılmıştır (Cresswell, 2016). Buna göre kod ve temalar oluşturması için araştırmada ulaşılan verilerin ham hali eğitim bilimleri alanından, nitel araştırma konusunda deneyimi olan bir akademisyenle paylaşılmıştır. Akademisyenin oluşturduğu kod ve temalarla araştırmacının oluşturduğu kod ve temalar karşılaştırılmıştır. Karşılaştırma sonucunda kod ve temalar arasındaki uyumun %91,6 düzeyinde olduğu görülmüştür. Araştırmada dış güvenirliği (teyit edilebilirlik) sağlamak için araştırma süreci şeffaf bir şekilde raporlanmış, araştırmacının rolü açıklanmış, araştırma sonuçları alan uzmanına sunularak teyit alınmıştır. Araştırmada katılımcı görüşleri sonucu oluşturulan temaların görselleştirilmesi amacıyla bir model oluşturulmuştur. Oluşturulan model Şekil 1 de sunulmuştur.



Şekil 1. Okul yöneticilerinin görüşlerinin analizi sonucu oluşturulan model

BULGULAR

Bu bölümde okul yönetiminde dijital veri güvenliğine yönelik tehditler ve önlemlere yönelik okul yöneticilerinin görüşlerinin belirlenmesi amacıyla yapılan içerik analizi sonucunda elde edilen bulgulara yer verilmiştir.

Okul Yönetiminde Dijital Veri Güvenliğine Yönelik Tehditler

Okul yönetiminde dijital veri güvenliğine yönelik tehditlere ilişkin okul yöneticilerinin görüşleri Tablo 1'de sunulmuştur.

Tablo 1
Okul yönetiminde dijital veri güvenliğine yönelik tehditlere ilişkin bulgular

Tema	Alt tema	Kodlar
Okul yönetiminde dijital veri güvenliğine yönelik tehditler	Kullanıcılardan kaynaklı durumlar	Teknoloji okur-yazarlığının düşük olması
		Veri güvenliği bilincinin düşük olması
		Kişisel verilerin paylaşımı
		Personelin sık değişmesi
	Şifre kullanımıyla ilgili sorunlar	Güvenli şifre kullanmama
		Formları otomatik doldurma
		Yetkisiz kişilerle paylaşma
		Sosyal ağlarda paylaşma
		Görülebilir ortamlarda bulundurma,
		Güvensiz ortamlarda şifre kullanımı
	Teknolojik araç-gereçlerin yanlış kullanımı	Bilgisayarların ortak kullanımı
		Bilgisayarların sürekli açık bırakılması
		Kontrolsüz usb, harici bellek bağlanması
		Korsan yazılım kullanımı
		Bilgisayarları tamir amaçlı kurum dışına çıkarma
		Antivirüs programı kullanmama
	İnternet kaynaklı tehditler	Siber saldırılar
		Kaynağı bilinmeyen e-postalar
		Ağ bağlantısı sorunları
	Depolama alanlarının güvenliği sorunları	Ani voltaj yükselmeleri
		Güç kaynağı kullanmama
		Yangın, sel, hırsızlık vb. durumlar

Çalışmada okul yönetiminde dijital veri güvenliğine yönelik tehditler teması altında 5 alt temaya ulaşılmıştır. Bu alt temalar kullanıcılardan kaynaklı durumlar, şifre kullanımıyla ilgili sorunlar, teknolojik araç-gereçlerin yanlış kullanımı, internet kaynaklı tehditler ve depolama alanlarının güvenliği sorunlarıdır. Okul yönetiminde dijital veri güvenliğine yönelik kullanıcılardan kaynaklı durumlar teknoloji okur-yazarlığının düşük olması, veri güvenliği bilincinin düşük olması, kişisel verilerin paylaşımı ve personelin sık değişmesi olarak tespit edilmiştir. Şifre kullanımıyla ilgili sorunlar olarak güvenli şifre kullanmama, formları otomatik doldurma, şifreleri yetkisiz kişilerle paylaşma, sosyal ağlarda paylaşma, görülebilir ortamlarda bulundurma ve güvensiz ortamlarda şifre kullanımı görüşleri ortaya çıkmıştır. Teknolojik araç-gereçlerin yanlış kullanımına yönelik tehditler bilgisayarların ortak kullanımı, bilgisayarların sürekli açık bırakılması, kontrolsüz usb, harici bellek bağlanması, korsan

yazılım kullanımı, bilgisayarları tamir amaçlı kurum dışına çıkarma ve anti virüs programı kullanmamadır. Okul yönetiminde dijital veri güvenliğine yönelik internet kaynaklı tehditler siber saldırılar, kaynağı bilinmeyen e-postalar ve ağ bağlantısı sorunlarıdır. Dijital verilerin saklandığı depolama alanlarına güvenliğine yönelik tehditler ani voltaj yükselmeleri, güç kaynağı kullanmama ve yangın, sel, hırsızlık vb. durumlardır. Konuya ilişkin bazı okul yöneticilerinin görüşleri aşağıdadır:

> *Benim gördüğüm en çok yapılan hata verilerin olduğu modüle girerken kullanıcı adı ve şifreleri otomatik olarak algılatmaktır. Bu durum büyük bir güvenlik riski doğuruyor. Siz olmadığınız zaman yetkisiz bir kişi şifreyle girilebilen ve sizin sorumluluğunuzda olan bir modüle kolaylıkla girebilir, istediği her bilgiye ulaşabilir Y6.*
>
> *Son yıllarda e-maillerimize tanımadığımız kişi ve kurumlardan birçok mail geliyor. Bu maillerin hepsinin iyi niyetli olduğunu düşünmüyorum. Fakat okulumda çalışan bazı personelimin bu maillerin kaynağını kontrol etmeden açtığını gözlemliyorum. Bazen içlerinde virüs olabiliyor ve bu virüsler kurum bilgisayarlarımızın güvenliğini tehdit ediyor Y3.*
>
> *Okul yöneticilerinin çok yoğun iş yükleri olduğu herkes tarafından biliniyor. İdari işlerin aksamaması ve gecikmemesi için bize tanımlanan dijital verilerin olduğu sistemlere erişim şifremizi bazen başkalarına veriyoruz. Şifrenin sorumluluğu bizde olmasına rağmen başkalarıyla paylaşarak hem kendimizi hem de dijital verileri riske atıyoruz Y8.*
>
> *Okullarda biz en çok e-okul ve MEBBİS sistemlerinde verileri saklıyoruz. Bu sistemlerin donanımsal ve yazılımsal güvenliği tamamen bakanlığımız tarafından takip ediliyor. Ancak bu sistemleri kullananlardan kaynaklı bazı hatalar verilerin güvenliğini tehdit edebiliyor. Örneğin öğrenci ve öğretmenlere ait bilgilerin bazen herkes tarafından görülebilecek şekilde paylaşıldığına şahit oluyoruz. Bu sistemlere erişim yetkisi olan yönetici, öğretmen ve personelin bazılarının veri güvenliği bilincinin düşük olması bu duruma neden olabiliyor Y12.*

Okul Yönetiminde Dijital Veri Güvenliğini Sağlamaya Yönelik Alınan Önlemler

Okul yönetiminde dijital veri güvenliğini sağlamaya yönelik alınan önlemlere ilişkin okul yöneticilerinin görüşleri Tablo 2'de sunulmuştur.

Tablo 1
Okul yönetiminde dijital veri güvenliğini sağlamaya yönelik alınan önlemlere ilişkin bulgular

Tema	Alt tema	Kodlar
Okul yönetiminde dijital veri güvenliğini sağlamaya yönelik alınan önlemler	Kullanıcılara yönelik önlemler	Güvenli şifre kullanımını yaygınlaştırma
		Alt kullanıcı tanımlama
		Personeli bilgilendirme
		Paylaşım toplantıları
		İnternetten bilgi edinme
		Hizmet içi eğitim faaliyetleri
	Donanımsal ve yazılımsal önlemler	Veri yedekleme
		Güvenli internet kullanımı
		Anti-virüs programı kullanma
		Lisanslı yazılım kullanma

Çalışmada okul yönetiminde dijital veri güvenliğine yönelik alınan önlemler teması altında 2 alt temaya ulaşılmıştır. Bu alt temalar kullanıcılara yönelik önlemler ve donanımsal önlemlerdir. Kullanıcılara yönelik önlemler olarak güvenli şifre kullanımını yaygınlaştırma, alt kullanıcı tanımlama, personeli bilgilendirme, paylaşım toplantıları, internetten bilgi edinme ve hizmet içi eğitim faaliyetleri görüşleri ortaya çıkmıştır. Okul yönetiminde dijital veri güvenliğini sağlamaya yönelik alınan donanımsal ve yazılımsal önlemler ise veri yedekleme, güvenli internet kullanımı, anti-virüs programı ve lisanslı yazılım kullanmadır. Konuya ilişkin bazı okul yöneticilerinin görüşleri aşağıdadır:

> *Okulun yönetiminden sorumlu olduğum için birçok kişinin verilerine erişim yetkim var. Bu yetki beraberinde sorumlu davranmayı da getiriyor. Özellikle kişisel bilgilerin kötü niyetli birçok kişinin hedefinde olması okulları da risk altında bırakıyor. Ben de sorumluluk bilinciyle hareket ederek dijital dünyada meydana gelen gelişmeleri takip etmeye çalışıyorum. Siber saldırılar konusunda güncel olayları paylaşan internet sitelerinden öğrendiğim önlemleri okulumda uygulamaya çalışıyorum. Şifrelerin kullanımı, yetkisiz erişimin engellenmesi, dijital ortamdaki verilerin belli dönemlerde yedeklenmesi gibi çalışmaları okulumda yapmaya çalışıyorum Y13.*
>
> *Biz okulumuzda öncelikle idari personelimizde farkındalık oluşturuyoruz. Olabilecek riskler hakkında arkadaşlarımızı bilgilendiriyoruz. Güvenli şifre kullanmalarını ve şifreleri başkalarıyla paylaşmamaları konusunda gerekli uyarılarımızı yapıyoruz Y4.*
>
> *Okulumuzun bulunduğu bölgede sık sık elektriklerin kesiliyor. Bilgisayarlarımızın ve serverlarımızın zarar görmesinin önüne geçmek için okulumuza güç kaynakları aldık. Bu sayede ani voltaj yükselmeleri karşısında verilerimizi korumaya çalışıyoruz Y2.*
>
> *Okul idaresinde kullandığımız bilgisayarların tamamına lisanslı anti virüs programı kurduk. Biraz maliyetli olmasına rağmen siber saldırılar karşısında güvende olduğumuz hissetmek bizi rahatlatıyor Y5.*

Tartışma

Bu araştırmada okul yönetiminde dijital veri güvenliğine yönelik tehditler ve önlemler okul yöneticilerinin görüşleri doğrultusunda incelenmiştir. Araştırmada ilk olarak okul yöneticilerinden elde edilen veriler ışığında okul yönetiminde dijital veri güvenliğine yönelik tehditler ortaya çıkarılmıştır. Araştırmada okul yönetiminde dijital veri güvenliğine yönelik tehditler kullanıcılardan kaynaklı durumlar, şifre kullanımıyla ilgili sorunlar, teknolojik araç-gereçlerin yanlış kullanımı, internet kaynaklı tehditler ve depolama alanlarına güvenliğine yönelik tehditler olmak üzere 5 alt temaya ulaşılmıştır Buna göre okulların yönetimsel faaliyetlerinde yoğun bir şekilde kullanılan dijital verilerin güvenliğine yönelik birçok tehdit unsurunun olduğu görülmektedir. Praveena & Smys (2017) dijital platformlarda kullanılan veri sayısının giderek artmasının bu verilerin güvenliğine yönelik çok sayıda sorunun ve problemin ortaya çıkmasına neden olduğunu ifade etmektedir. Benzer şekilde Yılmaz, Şahin & Akbulut (2016) çalışmalarında günümüzde dijital veri güvenliğine yönelik çok sayıda tehdidin olduğunu belirtmektedir.

Araştırmanın başlıca bulgularından birisi okul yönetiminde dijital veri güvenliğine yönelik tehditlerin önemli bir kısmını kullanıcılardan kaynaklı tehditlerin oluşturmasıdır. Araştırmada bu tehditler kullanıcıların teknoloji okur-yazarlığının düşük olması, veri güvenliği bilincinin düşük olması, kişisel verilerin paylaşımı ve personelin sık değişmesi olarak tespit edilmiştir. Taha & Dahabiyeh'e (2020) göre dijital veri güvenliği konusunda kullanıcı farkındalığının düşük olması başlıca tehditlerdendir. Tekerek (2008) çalışmasında kullanıcılardan kaynaklı durumların veri güvenliğine yönelik önemli bir tehdit unsuru olduğunu belirtmektedir. Wagner & Brooke (2007) bilgi güvenliğinde meydana gelebilecek olumsuz durumlarda insanla ilgili faktörlerin önemli payının olduğunu ifade etmektedir. Gökçearslan, Günbatar & Sarıtepeci (2021) ise bireylerin kurumları ve kendileriyle ilgili bilgilerin güvenliğini ihlal edecek davranışları bilinçli olarak gerçekleştirmediklerini ifade etmektedir.

Araştırmada şifre kullanımından kaynaklı durumların okul yönetiminde dijital veri güvenliğine yönelik tehdit oluşturduğu bulgusuna ulaşılmıştır. Buna göre güvenli şifre kullanmama, formları otomatik doldurma, şifreleri yetkisiz kişilerle paylaşma, sosyal ağlarda paylaşma, görülebilir ortamlarda bulundurma ve güvensiz ortamlarda şifre kullanımı okul yönetiminde dijital veri güvenliğine yönelik tehditlerdir. Dijital veri güvenliği konusunda yapılan başka bir araştırmada da katılımcıların önemli bir kısmının güvenli şifre ve parola kullanma noktasında yetersiz oldukları sonucuna ulaşılmıştır (Kruger, Drevin & Steyn, 2010).Öğretmenlerle gerçekleştirilen Yılmaz, Şahin & Akbulut (2016) tarafından yapılan çalışmada ise güvenli parola oluşturma konusunda öğretmenlerin farkındalıklarının yüksek olduğu ortaya çıkmıştır.

Araştırma bulgularına göre teknolojik araç-gereçlerin yanlış kullanımı okul yönetiminde dijital veri güvenliği için önemli bir tehdittir. Buna göre bilgisayarların ortak kullanımı, bilgisayarların sürekli açık bırakılması, kontrolsüz usb, harici bellek bağlanması, korsan yazılım kullanımı, bilgisayarları tamir amaçlı kurum dışına çıkarılması ve anti virüs programı kullanılmaması teknolojik araç-gereçlerin yanlış kullanımıyla ilgili tehditlerdir. Okullarda yapılan başka bir araştırmada öğretmenlerin güvenlik duvarı yazılımları konusundaki farkındalıkları düşük çıkmıştır (Yılmaz, Şahin & Akbulut, 2016). Ünver, Canbay & Mirzaoğlu, (2009) çalışmalarında korsan yazılımların sisteme izinsiz girilmesini sağlayarak dijital verilerin güvenliğini tehdit ettiğini belirtmektedir. Dijital dünyada ortaya çıkan tehditlerin büyük kısmı bilişimle ilgili sistemlerin ve araç gereçlerin kullanımındaki açıklıklardan ve zafiyetlerden ortaya çıkmaktadır (Derin & Gençoğlu, 2020).

Araştırmada okul yönetiminde dijital veri güvenliğini tehdit eden bir diğer unsur internet kaynaklı tehditlerdir. Siber saldırılar, kaynağı bilinmeyen e-postalar ve ağ bağlantısı sorunları okullarda dijital veri güvenliğini tehdit etmektedir. Siber saldırılar kişilerin ve kurumların bilişim alt yapısına ve sistemlerine yönelik yapılan planlı saldırılardır (Alkan, 2019). Bu sayede istenilen verilere izinsiz erişim sağlanmaya çalışılır. İnternet alt yapısı kullanılarak yapılan siber saldırılar ülkeler ve özellikle kurumlar için önemli bir tehdit oluşturmaktadır (Aytekin, 2015). Solichin & Ramadhan, (2017) internet ağlarından

yapılan dijital veri paylaşımın hızla artması beraberinde internet kaynaklı tehditleri getirdiğini ifade etmektedir.

Katılımcı okul yöneticileri depolama alanlarının güvenliğiyle ilgili sorunların okul yönetiminde dijital verilerin güvenliğinde tehdit oluşturabileceğini ifade etmiştir. Buna göre ani voltaj yükselmeleri, güç kaynağı kullanmama, yangın, sel ve hırsızlık gibi durumlar dijital verilerin saklandığı depolama alanlarının güvenliğini tehdit etmektedir. Vural & Sağıroğlu (2008) doğal afetlerin enerji ve güç kaynakları ile donanımsal ve yazılımsal alt yapılar için önemli tehditler olduğunu ifade etmektedir. Bu nedenle okullarda dijital veri güvenliğinin sürdürülebilirliği noktasında fiziki alt yapının iyileştirilmesi üzerinde önemle durulması gereken bir konudur. Dijital verilerin barındırıldığı platformların güvenliğinin sağlanması verilerin güvenliği açısından önemli bir tedbirdir (Canbek & Sağıroğlu, 2006). Mevcut çalışma kapsamında okul yönetiminde dijital veri güvenliğine yönelik alınan önlemler de tespit edilmiştir. Bu doğrultuda okul yöneticilerinin okullarda dijital veri güvenliğini sağlamaya yönelik alınan önlemlerle ilgili görüşlerinin kullanıcılara yönelik önlemler ve donanımsal ve yazılımsal önlemler olmak üzere iki alt temada toplandığı görülmektedir. Kullanıcılara yönelik önlemler olarak güvenli şifre kullanımını yaygınlaştırma, alt kullanıcı tanımlama, personeli bilgilendirme, paylaşım toplantıları, internetten bilgi edinme ve hizmet içi eğitim faaliyetleri düzenlemedir. Tekerek (2008) dijital verilerin güvenliğiyle ilgili tehditlerin kaynağının önemli bir kısmını bilinçsiz kullanıcıların oluşturduğunu belirtmektedir. Gündüzalp'e (2021) göre kurumlarda dijital verilerin güvenliği noktasında alınan teknik önlemler yetersiz kalmakta, kullanıcılara ve bireylere yönelik önlemler işe koşulmalıdır. Dijital verilerin güvenliğini sağlamak ve tehditleri minimuma düşürmek için bireylerin ve kullanıcıların farkındalıklarını arttırmak gerekir (Yılmaz, Şahin & Akbulut, 2016). Bilişim teknolojilerinin hızla değiştiği ve geliştiği günümüzde bu teknolojileri kullanan bireylerinde aynı hızda kendilerini yenilemeleri ve güncellemeleri gerekmektedir (Yüksel & Adıgüzel, 2011). Bu doğrultuda dijital verileri işleyen kullanıcıların verilerin güvenliğini sağlama noktasında kendilerini geliştirmeleri önem arz etmektedir.

Araştırmada okul yöneticileri dijital veri güvenliğini sağlamaya yönelik okullarda birtakım donanımsal ve yazılımsal önlemler aldıklarını ifade etmişlerdir. Veri yedekleme, güvenli internet kullanımı, anti-virüs programı ve lisanslı yazılım kullanma dijital veri güvenliğini sağlamada alınan donanımsal önlemlerdir. Dijital dünyada güvenlik hem donanımsal hem de yazılımsal olarak çözüm üretilmesi gereken bir konudur (Avcı vd., 2022). Acarer, (2020) son yıllarda siber saldırıların donanımsal ekipmanlara yönelik olduğunu belirtmektedir. Ayrıca bu saldırıların yazılımsal hasarların yanı sıra donanımsal hasara da neden olmaktadır. Güven & Aktel, (2020) dijital verilerin saklandığı donanımların periyodik olarak saldırılara karşı güvenlik kontrollerinin yapılması gerektiğinin altını çizmektedir. Öğün & Kaya (2013) çalışmalarında kurumların dijital veri güvenliğini sağlamak için dijital alt yapı ve donanımlarını son sistemlerle donatması gerektiğini belirtmektedir.

Sonuç

Dijital verilerin kullanımının gün geçtikçe arttığı okullarda dijital veri güvenliğine yönelik olası tehditlerin önceden bilinmesi dijital verilerin güvenliğini sağlamaya yönelik atılacak adımların başarıya ulaşmasında etkili olacaktır. Toplumun büyük bir kesimine hizmet veren okulların sahip olduğu dijital verilerin güvenliğinden öncelikle okul yöneticileri sorumludur. Bu doğrultuda araştırmada okul yönetiminde dijital veri güvenliğine yönelik tehditler ve önlemler okul yöneticilerinin görüşleri doğrultusunda incelenmiştir. Araştırma bulguları genel olarak değerlendirildiğinde okul yönetiminde dijital veri güvenliğine yönelik birden çok tehdit unsurunun olduğu sonucu ortaya çıkmıştır. Dijital veri güvenliği konusunun birçok alt bileşeninin olması karşılaşılabilecek tehditlerin de çok çeşitli olmasına neden olmaktadır. Özellikle kullanıcılardan kaynaklı durumların dijital verilerin güvenliğinde önemli bir etken olması dikkat çekicidir. Dijital verilerin güvenliğine yönelik alınan donanımsal ve yazılımsal önlemler kullanıcıların bilinç ve farkındalık düzeyi yüksek olmadığı takdirde yeterli olmayacaktır. Bu durum ise dijital verileri tehditlere açık bir hale getirecektir. Araştırmada şifre kullanımıyla ilgili sorunlar, teknolojik araç-gereçlerin yanlış kullanımı, internet kaynaklı tehditler ve depolama alanlarının güvenliğiyle ilgili durumların da okul yönetiminde dijital veri güvenliğine yönelik tehdit oluşturduğu sonucuna ulaşılmıştır. Bununla birlikte araştırmada okullarda dijital verilerin güvenliğini sağlamaya yönelik birtakım önlemlerin de alındığı sonucuna ulaşılmıştır. Bu önlemler kullanıcılara yönelik önlemler ve donanımsal önlemler olarak öne çıkmaktadır. Bu sonuç okul yöneticilerinin dijital veri güvenliği konusunda belli bir bilinç düzeyine sahip olduğunun göstergesidir. Araştırmada ulaşılan bu sonuçlar okul yönetiminde dijital veri güvenliği konusunda önemli bir veri kaynağı olabilir.

Öneriler

Araştırmada elde edilen bulgulardan yola çıkarak uygulayıcılara ve araştırmacılara bir takım önerilerde bulunulabilir.

Dijital verilerin barındırıldığı platformların periyodik bakımları yapılmalı, olası tehditlere karşı alt yapılar siber güvenlik açısından daha donanımlı hale getirilmelidir.

Okullarda göreve yeni başlayan personellere dijital veri güvenliği konusunda bilgilendirmeler yapılmalı, farkındalık oluşturulmalıdır.

Okul yöneticiliğine seçme ve atamada adayların dijital veri güvenliği farkındalıkları belirlenmeli, göreve başlamadan önce hizmet öncesi eğitim faaliyetleri düzenlenmelidir.

Dijital verilere yönelik tehditlerin her geçen gün artması ve değişmesi nedeniyle kullanıcılar anlık olarak bilinçlendirilmeli, çevrim içi eğitim faaliyetleri düzenlenmelidir.

Dijital verilerin güvenliğine yönelik tehditler hakkında önceden senaryolar hazırlanmalı, bu doğrultuda tedbirler alınmalıdır.

Kullanıcılara dijital veri güvenliği konusunda verilecek eğitimlerin sürekliliği sağlanmalı, eğitimlerin etkililiği arttırılmalıdır.

Yazar Katkı Beyanı

Bu çalışmaya her iki yazar tarafından eşit oranda katkı verilmiştir.

Çatışma Beyanı

Bu çalışmanın herhangi bir kurum, kuruluş, kişi ile mali çıkar çatışması yoktur ve yazarlar arasında çıkar çatışması bulunmamaktadır.

Kaynakça

Acarer, T. (2020). Ülke güvenliğimizde alınabilecek makro siber güvenlik önlemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 6*(2), 61-71.

Alkan, M. (2012). *Siber güvenlik ve siber savaşlar*, Bilgi Güvenliği Derneği TBMM İnternet Komisyonu Sunumu.

Aldridge, J., Medina, J., & Ralphs, R. (2010). The problem of proliferation: Guidelines for improving the security of qualitative data in a digital age. *Research Ethics, 6*(1), 3-9.

Aslay, F., Çam, H., & Özen, Ü. (2019). Yükseköğretim kurumlarında bilgi güvenliği farkındalık düzeylerinin ölçümlenmesi. *Yönetim Bilişim Sistemleri Dergisi, 5*(2), 1-11.

Avcı, İ., Özarpa, C., Özdemir, M., Kınacı, B. F. & Kara, S.A. (2022). Akıllı ulaşım sistemlerindeda siber güvenlik ve çok kaynaklı güvenlik önlemi. *Akıllı Ulaşım Sistemleri ve Uygulamaları Dergisi*, 5 (1), 22-35.

Avcı, Ü. & Arslan, E. (2019). Dijital veri güvenliği farkındalığı ve bilgi okuryazarlığı ile elde edilen hizmetçi eğitimin etkisi. *Ankara Üniversitesi Eğitim Bilimleri Fakültesi Dergisi (JFES), 52*(3), 891-914.

Avcı, Ü. & Oruç, O. (2020). Üniversite öğrencilerinin kişisel siber güvenlik davranışları ve bilgi güvenliği farkındalıklarının incelenmesi. *İnönü Üniversitesi Eğitim Fakültesi Dergisi, 21*(1), 284-303. doi: 10.17679/inuefd.526390.

Aytekin, A. (2015). T*ürkiye'nin siber güvenlik stratejisi ve eylem planının değerlendirilmesi.* [Yayımlanmamış Yüksek Lisans Tezi]. Bilişim Sistemleri Anabilim Dalı, Gazi Üniversitesi.

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

Creswell, J. W. (2016). *Nitel araştırma yöntemleri: Beş yaklaşıma göre nitel araştırma ve araştırma deseni* (Çev. Ed. M. Bütün ve S. B. Demir). Ankara: Siyasal.

Çetinkaya, L., Güldüren, C. & Keser, H. (2017). Öğretmenler için bilgi güvenliği farkındalık ölçeği (BGFÖ) geliştirme çalışması. *Milli Eğitim Dergisi, 46*(216), 33-52 .

Derin, M. A. & Gençoğlu, M. T. (2020). Ortaokul öğrencilerinin bilgi güvenliği farkındalığı. *Savunma Bilimleri Dergisi*, (38), 159-181.

Gökçearslan, Ş., Günbatar, M. S., & Sarıtepeci, M. (2021). Ortaöğretim öğrencilerinin bilgi güvenliği farkındalıklarının incelenmesi. *Yüzüncü Yıl Üniversitesi Eğitim Fakültesi Dergisi*, *18*(1), 354-373.

Göldağ, B. (2021). Üniversite öğrencilerinin dijital okuryazarlık düzeyleri ile dijital veri güvenliği farkındalık düzeyleri arasındaki ilişkinin incelenmesi. *E-Uluslararası Eğitim Araştırmaları Dergisi, 12*(3), 82-100. DOI: 10.19160/e-ijer.950635.

Gündüzalp, C. (2021). Üniversite çalışanlarının dijital veri ve kişisel siber güvenlik farkındalıkları (Bilgi işlem daire başkanlıkları örneği). *Journal of Computer and Education Research, 9*(18), 598-625.

Güven, F., & Aktel, M. (2020). ABD-Rusya ile ilişkilendirilen siber saldırılar ve türk kamu yönetimince alınması gereken önlemler. *Uluslararası İşletme, Ekonomi ve Yönetim Perspektifleri Dergisi, 6*(2), 414-439.

Keser, H. & Yayla, H. G. (2021). Fatih projesi uygulanan okullardaki öğretmenlerin bilgi güvenliği farkındalık düzeylerinin incelenmesi. *Milli Eğitim Dergisi, 50*(229), 9-40.

Kruger, H. A.,& Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security, 25*(4), 289-296.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic Inquiry*. Newbury Park, CA: Sage.

Öğün, M. N. & Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi, 9*(18), 145-191.

Öz, Ö. (2020). Dijital liderlik: Dijital dünyada okul lideri olmak. *Uluslararası Liderlik Çalışmaları Dergisi: Kuram ve Uygulama, 3*(1), 45-57.

Öztürk, İ. & Çakır, R. (2022). Öğretmenlerin sınıf ortamında dijital oyunlardan yararlanmaları ve dijital veri güvenliği farkındalıkları. *Türkiye Bilimsel Araştırmalar Dergisi, 7*(1), 123-146.

Praveena, A., & Smys, S. (2017, Nisan). *Ensuring data security in cloud based social networks.* 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA), RVS Technical Campus, Coimbatore.

Simplilearn (2021). What is digital security: Overview, types, and applications explained. https://www.simplilearn.com/what-is-digital-security-article, Erişim Tarihi: 24.02.2023.

Solichin, A., & Ramadhan, E. W. (2017, Ekim). *Enhancing data security using DES-based cryptography and DCT-based steganography.* 3rd International Conference on Science in Information Technology (ICSITech), Universitas Pendidikan Indonesia, Bandung. Retrieved from https://ieeexplore.ieee.org/xpl/conhome/8241142/proceeding.

Şahinaslan E., Kantürk A., Şahinaslan Ö. & Borandağ E. (2009) *Kurumlarda bilgi güvenliği farkındalığı, önemi ve oluşturma yöntemleri*, XI. Akademik Bilişim Konferansı, Harran Üniversitesi, Şanlıurfa, 597-602.

Taha, N., & Dahabiyeh, L. (2021). College students information security awareness: a comparison between smartphones and computers. *Education and Information Technologies, 26*(2), 1721-1736.

Talan, T., & Aktürk C. (2021). Ortaöğretim öğrencilerinin dijital okuryazarlık ve bilgi güvenliği farkındalığı seviyelerinin incelenmesi. *Kahramanmaraş Sütçü İmam Üniversitesi Sosyal Bilimler Dergisi, 18*(1), 158-180. https://doi.org/10.33437/ksusbd.668255.

Tekerek, M. (2008). Bilgi güvenliği yönetimi. *KSÜ Fen ve Mühendislik Dergisi, 11*(1), 132.

ThinkTech, S. T. M. (2023). Siber Tehdit Durum Raporu. https://thinktech.stm.com.tr/tr/arastirma-ve-yayinlar?contenttype=siber-tehdit-durum-raporu

Ünver, M., Canbay, C. & Mirzaoğlu, A.G. (2009). *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler.* Ankara: Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı.

Vural, Y. & Sağıroğlu, Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. gazi üniversitesi, *Mühendislik Mimarlık Fakültesi Dergisi, 23*(2), 507-522.

Wagner, A. E. & Brooke, C. (2007). Wasting time: The mission impossible with respect to technologyoriented security approaches electronic. *Journal of Business Research Methods, 5*(2), 117-124.

Yıldırım, A. & Şimşek, H. (2018). *Sosyal bilimlerde nitel araştırma yöntemleri*. Ankara: Seçkin.

Yılmaz, E., Şahin, Y. L., & Akbulut, Y. (2015). Dijital veri güvenliği farkındalığı ölçeğinin geliştirilmesi. *AJIT-e: Academic Journal of Information Technology, 6*(21), 23-40.

Yılmaz, E., Şahin, Y. L. & Akbulut, Y. (2016). Öğretmenlerin dijital veri güvenliği farkındalığı. *Sakarya University Journal of Education, 6*(2), 26-45.

Yüksel, I. & Adıgüzel, A. (2011). A glance at standard development studies and accreditation process as sustaining tools for quality in teacher education in Turkey. *International Journal of Instruction, 4*(2), 39-50.