

Spor Kulüplerinde Dijital Dönüşüm Sürecinde Siber Güvenlik ve Dijital Risk Yönetimi

İsmail ÖNER¹, Özgür KARATAŞ², Emine ÖZTÜRK KARATAŞ³

ÖZET

Amaç: Bu araştırmanın amacı, spor kulüplerinde dijital dönüşüm sürecinde siber güvenlik ve dijital risk yönetiminin incelenmesidir.

Yöntem: Araştırma, nitel araştırma yöntemlerinden doküman analizi tekniği kapsamında ele alınmıştır. Spor kulüplerinde dijital dönüşüm sürecinde siber güvenlik ve dijital risk yönetimi konularına ilişkin ulusal ve uluslararası akademik yayınlar, resmi raporlar ve yasal düzenlemeler detaylı biçimde incelenmiştir. Elde edilen veriler, tematik analiz yöntemiyle sınıflandırılarak sistematik bir biçimde yorumlanmıştır.

Bulgular: Araştırmada, spor kulüplerinin dijitalleşme süreciyle birlikte hem önemli fırsatlar hem de farklı risklerle karşı karşıya kaldıkları tespit edilmiştir. Dijital uygulamaların, taraftar etkileşimini artırma, hizmet sunumunu kolaylaştırma ve gelir yönetimini iyileştirme açısından önemli avantajlar sağladığı vurgulanmaktadır. Bu dönüşüm sürecinin, aynı zamanda kişisel veri güvenliği, teknik altyapı zafiyetleri, siber tehditlere açıklık ve kriz durumlarında yetersiz dijital iletişim gibi çeşitli yapısal sorunları da beraberinde getirdiği belirlenmiştir. Bununla birlikte birçok kulübün bu risklere karşı yeterli önleyici strateji geliştiremediğini ve kurumsal hazırlık düzeyinin düşük olduğu tespit edilmiştir.

Sonuç: Bu araştırma, spor kulüplerinin dijital dönüşüm sürecinde karşılaştıkları siber güvenlik tehditleri ile dijital risklerin yalnızca teknik boyutla sınırlı kalmayıp, aynı zamanda yönetsel ve stratejik boyutlar da taşıdığını göstermektedir. Dijital altyapı, veri güvenliği, ödeme sistemleri ve kriz iletişimi gibi alanlarda yaşanan yapısal zafiyetler, kulüplerin dijital tehditlere karşı direnç geliştirme kapasitesini sınırlamaktadır.

Anahtar Kelimeler: Dijitalleşme, Siber güvenlik, Spor kulüpleri, Dijital risk yönetimi, Veri koruma

ABSTRACT

Cyber Security and Digital Risk Management In The Digital Transformation Process Of Sports Clubs

Purpose: The purpose of this research is to examine cyber security and digital risk management in the digital transformation process of sports clubs.

Method: The research was conducted using the document analysis technique, one of the qualitative research methods. National and international academic publications, official reports and legal regulations concerning cyber security and digital risk management in the digital transformation process of sports clubs were examined in detail. The data obtained were classified using thematic analysis and interpreted systematically.

Results: The study found that sports clubs face both significant opportunities and various risks as they undergo digital transformation. It emphasises that digital applications offer important advantages in terms of increasing fan engagement, facilitating service delivery and improving revenue management. It was also determined that this transformation process brings with it various structural problems, such as personal data security, technical infrastructure weaknesses, vulnerability to cyber threats, and inadequate digital

¹ Bağımsız Araştırmacı, ORCID ID: 0000-0003-0332-2139, smailoner1@gmail.com

² İnönü Üniversitesi Spor Bilimleri Fakültesi, Spor Yöneticiliği Bölümü, Malatya/TÜRKİYE. ORCID NO: 0000-0002-7863-2898, ozgur.karatas@inonu.edu.tr

³ Malatya Turgut Özal Üniversitesi Sağlık Bilimleri Fakültesi, Egzersiz ve spor Bilimleri Bölümü, Malatya/TÜRKİYE. ORCID NO: 0000-0002-4142-5369, emine.karatas@ozal.edu.tr

communication in crisis situations. Furthermore, it was found that many clubs have failed to develop adequate preventive strategies against these risks and that their level of organisational preparedness is low.

Conclusion: This research demonstrates that the cyber security threats and digital risks encountered by sports clubs during their digital transformation process are not limited to technical aspects, but also involve managerial and strategic dimensions. Structural weaknesses in areas such as digital infrastructure, data security, payment systems and crisis communication limit clubs' capacity to develop resilience against digital threats.

Keywords: Digitalisation, Cyber security, Sports clubs, Digital risk management, Data protection

GİRİŞ

Günümüzde toplumsal ve endüstriyel yapılar, dijital teknolojilerdeki hızlı gelişmelere paralel olarak köklü bir dönüşüm süreci yaşamaktadır. Robotik sistemler, yapay zeka, sensör teknolojileri, nesnelerin interneti, endüstriyel otomasyon, bulut bilişim ve artırılmış gerçeklik gibi yenilikçi çözümler, yalnızca üretim ve hizmet sektörlerini değil; aynı zamanda sosyal etkileşim biçimlerini ve çalışma düzenlerini de derinden etkilemektedir (Ersöz ve Özmen, 2020). Bu teknolojik atılımlar, özellikle bulut bilişim ile uyum sürecinde dijitalleşmenin kapsamını genişletmiş; bunun sonucunda ise spor endüstrisi de bu dönüşümden doğrudan etkilenmiştir. Dijitalleşme, spor kulüplerinde yönetim, iletişim ve hizmet sunumu alanlarında önemli avantajlar sağlarken, aynı zamanda güvenlik açıkları ve dijital riskler gibi yeni tehdit alanlarını da ortaya çıkarmıştır.

Siber güvenlik yönetimi, belirsizlikleri donanım, yazılım ve psiko-bilişsel düzeylerde analiz ederek yönetilebilir risklere dönüştüren; dirençli bir toplum inşa etmek amacıyla çözülmesi gereken çok katmanlı zorlukları içeren disiplinlerarası bir alan olarak tanımlanmaktadır (Dacorogna ve Kratz, 2023). Bu yaklaşım, yalnızca teknik altyapının korunmasını değil, aynı zamanda bireylerin bilişsel tepkileri ile yönetsel karar alma süreçlerini de kapsayan geniş kapsamlı bir strateji gerektirmektedir. Dijitalleşmenin etkisiyle hızla dönüşen spor endüstrisinde de siber güvenlik yönetimi, kaçınılmaz bir gereklilik haline gelmiştir.

Dijital risk yönetimi ise, günümüzde risk analitiği ve dijital teknolojilerin sunduğu imkânlarla yalnızca sorunlar ortaya çıktıktan sonra müdahale etmeyi amaçlayan geleneksel anlayışın ötesine geçerek, karmaşık tehditlerin önleyici ve dinamik bir biçimde yönetilmesini sağlayan kritik bir yetkinlik alanıdır (Akmeşe, 2020). Bu yaklaşım, gelişmiş teknolojilerin uyumu, finansal ve faaliyet temelli risklerin önceden öngörülerek yönetilmesi ve güçlü bir yönetişim çerçevesinin oluşturulmasını gerektirmektedir. Chang (2024) göre, dijital yetkinliklerin geliştirilmesi ve erişilebilir dijital araçların etkin biçimde kullanılması, spor

organizasyonlarının hızla değişen dijital ortamda dirençli, sürdürülebilir ve rekabetçi kalmalarını mümkün kılmaktadır.

Spor kulüplerinin hem siber güvenlik yönetimini hem de dijital risk yönetimini birbirini tamamlayan stratejik alanlar olarak ele almaları büyük önem taşımaktadır. Dijital altyapıların güvenliğini sağlamak, sadece veri koruma açısından değil; aynı zamanda kulüplerin itibarını, ekonomik sürekliliğini ve taraftarla olan dijital bağına korumak açısından da önemlidir. Bu doğrultuda, teknolojiye uyum sağlayan, siber tehditlere karşı hazırlıklı olan ve dijital riskleri öngörülü biçimde yönetebilen kulüp yöneticileri, spor organizasyonlarının dijital çağda güçlü ve sürdürülebilir bir şekilde varlık göstermesini mümkün kılacaktır. Bu nedenle siber güvenlik ve dijital risk yönetimi, spor kulüplerinde dijital dönüşüm sürecinin temel bileşenlerinden biri olarak ele alınmalı; kurum içi strateji ve politika geliştirme süreçlerinin vazgeçilmez bir parçası haline getirilmelidir. Araştırmamızda spor kulüplerinin karşı karşıya olduğu dijital tehditleri ve siber güvenlik risklerini inceleyerek, bu risklerin etkin yönetimine yönelik stratejik yaklaşımları ortaya koymayı amaçlamaktadır.

YÖNTEM

Araştırma Modeli

Nitel araştırma yaklaşımıyla gerçekleştirilen bu çalışmada veriler, doküman incelemesi yoluyla elde edilmiştir. Araştırılmak istenen konu hakkında bilgi sağlayan her türlü yazılı materyale doküman denir (Balcı, 2018). Dokümanlar gerçeğin birer yansımalarıdır ve herhangi bir çalışmayı desteklemek için kullanılabilecekleri gibi bizzat çalışmanın inceleme amacını da teşkil edebilirler (May ve Perry, 2022). Doküman analizi, mevcut kayıt ve belgelerin incelenmesi yoluyla veri elde etme sürecidir. Bu yöntem, belirli bir amaca yönelik olarak kaynakların bulunması, okunması, not alınması ve değerlendirilmesi aşamalarını kapsamaktadır (Karasar, 2005).

Veri Analizi

Araştırmada, spor kulüplerinin karşı karşıya kaldığı dijital tehditleri, siber güvenlik risklerini ve dijital risk yönetimi stratejilerini anlamaya yönelik çeşitli akademik kaynaklar, yasal düzenlemeler ve resmi raporlar incelenmiştir. Özellikle Türkiye’de yürürlükte olan Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği’nin Genel Veri Koruma Tüzüğü gibi veri koruma mevzuatları, uluslararası hakemli dergilerde yayımlanmış bilimsel makaleler, spor yönetimi alanındaki güncel araştırmalar ve siber güvenlik odaklı raporlar temel

dokümanlar olarak değerlendirilmiştir. Bu dokümanlar, konuya ilişkin anlamlı temaların belirlenmesi amacıyla tematik analiz yöntemiyle çözümlenmiş ve veriler belirli kategoriler altında sınıflandırılarak yorumlanmıştır. Bu süreç, araştırmanın kuramsal altyapısını güçlendirmenin yanı sıra, spor kulüplerine dijital güvenlik bağlamında yol gösterici öneriler sunma amacı da taşımaktadır.

BULGULAR

Bu araştırmada, spor kulüplerinin dijitalleşme sürecinde karşılaştığı başlıca siber güvenlik riskleri ve dijital kriz yönetimi incelenmiştir. Aşağıda bu kapsamda elde edilen bulgular, dört ana temada sunulmuştur: taraftar verilerinin korunması, kulüp dijital altyapılarındaki güvenlik açıkları, online biletleme ve ödeme sistemlerine ilişkin tehditler ve kriz durumunda dijital itibar yönetimi. Bu temalar, spor kulüplerinde dijital dönüşüm sürecinde siber güvenlik ve dijital risk yönetimi açısından karşılaşılan başlıca risk alanlarını ve yönetimsel öncelikleri ortaya koymaktadır.

Taraftar Verilerinin Korunması

Dijitalleşmenin spor endüstrisinde yaygınlaşmasıyla birlikte taraftarlara ait kişisel verilerin toplanması, işlenmesi ve saklanması süreçleri kritik bir boyut kazanmıştır. Kuruluşların çevrimiçi gizliliği sağlam bir şekilde sürdürmeleri ve hem bireysel hem de kurumsal verileri kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı saldırıları, siber korsanlık ve veri casusluğu gibi dış kaynaklı tehditlere karşı korumaları stratejik bir zorunluluk teşkil etmektedir (Grover, 2023). Özellikle taraftar bağlılığına yönelik dijital stratejiler, mobil uygulamalar ve biletleme sistemleri aracılığıyla elde edilen hassas verilerin güvenliği; yalnızca yasal düzenlemelere uyum açısından değil, aynı zamanda taraftar güveni ve kulüp itibarının sürdürülebilirliği açısından da büyük önem arz etmektedir.

Ataman (2025) tarafından sunulan sektörel analizde, spor kulüplerinin taraftar verilerini yönetme biçimlerinin siber güvenlik açısından ciddi zaafılar içerdiği vurgulanmaktadır. Taraftar bağlılığına yönelik dijital stratejiler, mobil uygulamalar ve sosyal medya etkileşimleri aracılığıyla toplanan kişisel verilerin, güçlü şifreleme protokolleri ve çok faktörlü kimlik doğrulama sistemleriyle korunmadığı durumlarda yüksek risk taşıdığı belirtilmiştir. Raporda, kimlik avı, oturum ele geçirme ve veri sızıntısı gibi tehditlerin son yıllarda spor kulüplerine yönelik saldırılarda artış gösterdiği, bu durumun taraftar güvenliğini ve dijital itibar algısını doğrudan etkilediği ifade edilmektedir. Ayrıca, kulüplerin yasal düzenlemelere uyumunun teknik önlemlerle desteklenmediği takdirde, sadece hukuki değil,

aynı zamanda günlük işleyişleri ve iletişim süreçleri açısından da ciddi risklerle karşı karşıya kalacakları vurgulanmaktadır.

Kulüp Dijital Altyapılarında Güvenlik Açıkları

Günümüzde spor kulüplerinin faaliyetlerini yürüttüğü dijital altyapılar; web siteleri, e-posta sunucuları, mobil uygulamalar ve veri yönetim sistemlerini içerecek şekilde oldukça geniş bir yapıya sahiptir. Bu sistemler, teknik kusurlar, yetersiz yapılandırmalar ve yönetsel aksaklıklar nedeniyle çeşitli güvenlik tehditlerine karşı savunmasız kalmaktadır. Dijital sistemlerin otomatik tehdit tespiti, risk önceliklendirmesi ve yeni siber tehditlere adaptasyon gibi işlevleri yerine getirebilmesi, etkili bir yönetim süreci gerektirirken; birçok kulüp bu alanda kaynak, insan gücü ve veri yönetimi gibi sınırlılıklar nedeniyle yetersiz kalmaktadır (Mahinay ve Teleron, 2023).

NCC Group (2024) tarafından profesyonel spor organizasyonlarında gerçekleştirilen saha araştırmaları ve yönetici görüşmeleri, kulüplerin dijital altyapılarındaki güvenlik zaaflarına odaklanmaktadır. Çalışma, web siteleri, e-posta sunucuları, mobil uygulamalar ve veri yönetim sistemleri gibi dijital bileşenlerin teknik, yapılandırma ve yönetsel eksiklikler nedeniyle sürekli siber tehditlere karşı savunmasız kaldığını ortaya koymuştur. Araştırmada, otomatik tehdit tespiti, risk önceliklendirmesi ve yeni siber tehditlere adaptasyon gibi kritik işlevlerin yerine getirilebilmesi için etkili bir siber güvenlik yönetim sürecinin zorunlu olduğu vurgulanmıştır. Birçok kulüpte bu yeterliliğin sağlanamadığı; kaynak yetersizliği, sınırlı personel kapasitesi ve veri yönetimi eksiklikleri nedeniyle temel güvenlik uygulamalarının bile ihmal edildiği belirlenmiştir.

Online Biletleme, Ödeme Sistemleri ve Siber Tehditler

Spor organizasyonlarının dijitalleşme sürecinde önemli bir yere sahip olan çevrimiçi biletleme ve ödeme sistemleri, hem taraftar deneyimini kolaylaştırmakta hem de kulüplerin gelir yönetimini daha etkin hale getirmektedir. Bu sistemler, beraberinde çeşitli siber tehditleri de gündeme getirmektedir. Özellikle veri ihlalleri, kimlik hırsızlığı, ödeme sahtekârlığı ve sistem güvenlik açıkları gibi riskler, kullanıcı güvenliğini ve kulüplerin kurumsal itibarını tehdit etmektedir. Etkili bir siber güvenlik altyapısı oluşturulması büyük önem taşımaktadır. Gelişmiş şifreleme teknikleri, çok faktörlü kimlik doğrulama, yapay zeka destekli dolandırıcılık tespiti sistemleri ve güvenli ödeme protokolleri bu sürecin temel unsurlarını oluşturmaktadır. Bununla birlikte, bu teknolojilerin başarılı bir şekilde uygulanabilmesi, sadece teknik yeterlilikle değil; aynı zamanda güçlü yasal uyum politikaları ve kullanıcı dostu arayüz tasarımlarıyla da bağlantılıdır (Urs, 2015).

Bucea-Manea-Țoniș ve arkadaşlarının (2025) çalışmasında, spor endüstrisinin dijitalleşme süreciyle birlikte artan online biletleme ve ödeme sistemlerinin siber güvenlik açısından ciddi riskler barındırdığı ortaya konmuştur. Özellikle merkezi yapıdaki geleneksel ödeme altyapılarının, veri manipülasyonu, sahtecilik ve yetkisiz erişim gibi tehditlere karşı savunmasız olduğu vurgulanmıştır. Çalışmada, bu tür güvenlik açıklarının azaltılabilmesi için blok zincir tabanlı biletleme sistemlerinin kullanımının önemine dikkat çekilmiştir. Blok zincir tabanlı sistemler, her işlemin değiştirilemez şekilde kaydedildiği, şeffaf biçimde izlenebildiği ve tek bir merkeze bağlı olmadan güvence altına alındığı bir yapı sunmaktadır. Bu özellikleri sayesinde, biletlerin sahteciliğini önlemekte, taraftarların ve kulüplerin finansal verilerini korumakta ve işlem güvenliğini artırmaktadır (Murathan ve Murathan, 2019). Bu güvenli ve merkeziyetsiz yapı, biletleme süreçlerinde sahteciliğin önlenmesine yönelik yenilikçi çözümler sunmaktadır. Blok zinciri temelli biletleme sistemlerinde her bilet, değiştirilemez token (NFT) teknolojisi sayesinde benzersiz bir dijital varlık olarak tanımlanmakta ve yalnızca yetkilendirilmiş sahipleri tarafından kullanılabilir (Pilkington, 2016). Elde edilen bulgular, spor kulüplerinin yalnızca kullanıcı deneyimini iyileştirmeye yönelik dijital çözümler geliştirmelerinin yeterli olmadığını; aynı zamanda finansal veri güvenliğini sağlamak için yenilikçi ve sürdürülebilir teknolojik altyapılara yönelmeleri gerektiğini göstermektedir.

Kriz Durumunda Dijital İtibar Yönetimi

Dijital platformlar ve sosyal medya, kamuoyu algısını ve paydaş katılımını giderek daha fazla şekillendirdikçe, dijital itibar yönetimi spor kulüpleri açısından stratejik bir unsur haline gelmiştir. Etkili dijital stratejiler, yalnızca kulüplerin kurumsal itibarını korumakla sınırlı kalmamakta; aynı zamanda marka değerini artırmakta, taraftar bağlılığını güçlendirmekte ve özellikle kriz anlarında hızlı, tutarlı ve güven verici iletişim kurulmasını mümkün kılmaktadır. Bu süreçte kulüplerin dijital medya içeriklerini şeffaflık, tutarlılık ve etkileşim odaklı bir yaklaşımla yönetmeleri; potansiyel itibar risklerini önceden öngörebilmeleri ve bu risklere karşı hazırlıklı olmaları büyük önem taşımaktadır (Stegmann ve ark., 2024).

Stegmann ve Lang (2025) tarafından gerçekleştirilen kapsamlı bir literatür taramasında, spor kulüplerinin dijital itibar yönetimi ve kriz iletişimi süreçlerinde dijital medya içeriklerini şeffaf, tutarlı ve etkileşim odaklı şekilde yönetmelerinin stratejik öneme sahip olduğu vurgulanmaktadır. Çalışma, kriz dönemlerinde dijital platformlar aracılığıyla yayılan yanlış veya eksik bilgi akışlarının kamuoyu algısını hızla olumsuz etkileyebileceğini, buna karşılık dengeli içerik ve gerçek zamanlı iletişim ile itibarın korunabileceğini

göstermektedir. Ayrıca şeffaflık, tutarlılık ve kullanıcı etkileşimi eksenindeki dijital stratejiler, hem paydaş güveninin artırılmasına hem de markanın itibar değerinin korunmasına katkı sağlamaktadır. Bu bulgular ışığında, spor kulüplerinin potansiyel itibar risklerini önceden öngörmeleri ve kriz iletişimi stratejilerini uyumlu biçimde dijital mecralar üzerinden yürütmeleri gerektiği sonucuna ulaşılmıştır.

TARTIŞMA

Bu çalışmada elde edilen bulgular, spor kulüplerinin dijitalleşme sürecinde karşılaştığı siber güvenlik riskleri, veri koruma gereklilikleri, dijital hizmet altyapılarındaki zafiyetler ve kriz anlarında dijital itibar yönetimi gibi çok katmanlı konuların, güncel teknolojik gelişmeler ve mevzuat çerçevesinde yeniden değerlendirilmesini zorunlu kıldığını ortaya koymaktadır. Bu doğrultuda Zhou ve Huang'ın (2021) çalışmasında vurgulandığı üzere, yapay zeka temelli sistemler, spor organizasyonlarındaki risk faktörlerinin sınıflandırılmasında önemli avantajlar sunmaktadır. İlgili çalışmaya göre, risklerin %20'si insan ve saha koşullarından, %6,56'sı ise sosyal faktörlerden kaynaklanmaktadır. Bu bulgular, yapay zekânın özellikle öngörülebilir ve ölçülebilir risk alanlarında etkili müdahale stratejileri geliştirme konusunda güçlü bir araç olduğunu ortaya koymaktadır. Dolayısıyla, spor kulüplerinin dijital risk yönetimi süreçlerinde yapay zekâ teknolojilerinden yararlanmaları, sürdürülebilir ve güvenli bir dijital altyapı oluşturma açısından kritik bir gereklilik haline gelmiştir. Bununla birlikte Wang ve arkadaşları (2023) Çin'de spor hizmetleri sektörünün yüksek kaliteli gelişimini sürdürebilmesi için, özellikle büyük ölçekli etkinliklerde dijital teknolojilere dayalı risk yönetimi uygulamalarının acil bir ihtiyaç haline geldiğini belirtmektedir. Dijital teknolojilerin yalnızca veri analizi ve öngörüye katkı sağlamadığı, aynı zamanda kriz senaryolarının modellenmesi ve operasyonel süreçlerin güvenliğinin sağlanmasında da kritik bir rol oynadığı söylenebilir.

Santos'un (2023) ifade ettiği gibi, dijital çağda spor yönetimi; dijital dönüşümler ve yıkıcı yeniliklerden doğrudan etkilenen, sporun “uberleşmesi” potansiyelini taşıyan kalıcı bir yönetsel dönüşüm süreci içerisinde. Dolayısıyla, spor kulüplerinin yapay zekâ ve dijital teknolojilere dayalı risk yönetimi stratejilerini benimsemeleri, hem yerel hem de küresel düzeyde sürdürülebilir ve dirençli bir spor ekosisteminin inşası açısından stratejik bir zorunluluk haline gelmiştir.

Kişisel verilerin güvenliği günümüzde en önemli meselelerden biri haline gelmiştir. Özellikle bu verilerin çeşitli amaçlarla kullanılması, beraberinde ciddi riskleri de getirmektedir. İnternetin ve bilişim sistemlerinin yaygınlaşmasıyla birlikte, kişisel verilerin

dijital ortamda işlenmesi artmış; bu durum, dolandırıcılık ve hırsızlık gibi suçların da dijital mecralara taşınmasına zemin hazırlamıştır. Üstünel ve Alkurt (2015), çalışmalarında bilişim sistemleri aracılığıyla işlenen dolandırıcılık ve hırsızlık suçlarının günümüzde en kolay işlenebilen suçlar arasında yer aldığını belirtmektedir. Bu durum, dijital çağda kişisel verilerin korunmasına yönelik etkili güvenlik önlemlerinin gerekliliğini ortaya koymaktadır.

Spor kulüplerinin dijital altyapıları, veri odaklı modeller ve çevrimiçi etkileşim arttıkça ciddi güvenlik ve etik risklerle karşı karşıya kalmaktadır. Bu risklerin önlenmesi; gelişmiş güvenlik uygulamaları, çözümlerin deneysel olarak doğrulanması ve hem kulüpleri hem de taraftarları koruyacak güçlü bir etik çerçevenin oluşturulmasını gerektirmektedir (Nešić, 2018).

Diğer yandan, dijital ödemeler ve çevrim içi biletleme sistemleri gibi kullanıcı etkileşimine açık dijital hizmet alanlarında siber tehditlerin artışı dikkat çekmektedir. Özellikle spor organizasyonlarına ait platformlarda ödeme güvenliği, taraftar verilerinin korunması ve sahte bağlantılarla yönlendirme gibi riskler, spor kulüpleri açısından öncelikli bir güvenlik sorunu haline gelmiştir. Bu kapsamda, veri şifreleme teknolojileri, çok faktörlü kimlik doğrulama yöntemleri, yapay zeka destekli dolandırıcılık tespit sistemleri ile Kişisel Verilerin Korunması Kanunu ve Avrupa Birliği Genel Veri Koruma Tüzüğü gibi yasal düzenlemelere tam uyum, dijital ödemelerde hem güvenliğin artırılması hem de sistemin sürdürülebilirliğinin sağlanması açısından kritik öneme sahiptir (Praveen, 2024). Spor kulüplerinin bu tür gelişmiş siber güvenlik önlemlerini dijital sistemlerine uyarlamaları, kullanıcı güvenliğini tesis etmek ve dijital tehditlere karşı dirençli kalabilmek adına stratejik bir gerekliliktir.

Kriz anlarında dijital itibar, kuruluşların kamuoyuna yönelik etkili ve güven verici yanıtlar geliştirmesinde kritik bir rol oynamaktadır. Özellikle sosyal medyada yayılan sahte haberler karşısında, kuruluşların kriz iletişim stratejilerini şeffaflık, özgünlük ve duyarlılık ilkeleriyle uyarlamaları büyük önem taşımaktadır. Gasana (2024), çalışmasında bu yaklaşımın hem dijital ortamda güveni teşvik ettiğini hem de krizlere karşı daha dirençli bir iletişim zemini oluşturduğunu ifade etmektedir.

SONUÇ ve ÖNERİLER

Spor kulüplerinde dijitalleşmenin yalnızca teknolojik uyumla sınırlı kalmaması gerektiğini, aynı zamanda veri güvenliği ve altyapı bütünlüğü açısından kapsamlı stratejiler geliştirilmesinin zorunlu olduğunu göstermektedir. Taraftar verilerinin korunmasına yönelik

uygulamaların çoğu yasal çerçeveye uyum sağlama noktasında olumlu bir eğilim sergilese de, özellikle üçüncü taraf hizmet sağlayıcılarla veri paylaşımı ve denetim mekanizmalarının yetersizliği ciddi bir güvenlik açığı oluşturmaktadır. Bununla birlikte, kulüp dijital altyapılarında tespit edilen güncelleme eksiklikleri, zayıf parola uygulamaları ve VPN kullanımındaki yetersizlikler; sistematik siber tehditlere karşı savunmasızlık riskini artırmaktadır. Bu nedenle, dijital güvenliğin sürdürülebilirliği için kulüplerin yalnızca teknik çözümlere değil, aynı zamanda kurumsal farkındalığı artıran, çok katmanlı ve bütüncül bir siber güvenlik kültürü geliştirmeye odaklanmaları büyük önem taşımaktadır.

Spor kulüplerinde dijitalleşen biletleme ve ödeme sistemlerinin sunduğu kolaylıkların yanında ciddi siber tehdit risklerini de beraberinde getirdiğini ortaya koymuştur. Kredi kartı bilgilerinin hedef alındığı saldırılar, sahte bağlantılar ve sosyal medya kaynaklı veri sızıntıları, kullanıcı güvenliğini zedelerken, kulüplerin dijital altyapısındaki zafiyetleri gözler önüne sermektedir. Bu nedenle, çok katmanlı güvenlik protokolleri, yapay zekâ tabanlı tehdit analizleri ve yasal uyum politikaları gibi unsurların sistematik biçimde entegre edilmesi kritik önem taşımaktadır. Öte yandan, dijital çağda kulüplerin itibarlarının büyük ölçüde çevrimiçi platformlarda şekillenmesi, kriz anlarında dijital iletişim stratejilerinin şeffaflık, hız ve güvenilirlik ilkeleriyle yürütülmesini zorunlu kılmaktadır. Araştırmada, kulüplerin büyük bölümünün kriz senaryolarına hazırlıksız olduğu ve dijital itibar yönetimi konusunun kurumsal düzeyde yapılandırılmadığı saptanmıştır.

Spor kulüplerinin dijitalleşme sürecinde karşılaştıkları siber güvenlik ve dijital risklerin yalnızca teknik çözümlerle değil, kurumsal bilinç ve stratejik planlamayla yönetilmesi gerektiği açıkça ortaya çıkmaktadır. Veri güvenliğinden ödeme sistemlerine, dijital altyapıdan kriz iletişimine kadar her alanda çok katmanlı, sürdürülebilir ve uyumlu bir güvenlik kültürü geliştirilmesi önemlidir. Spor kulüplerinin, dijital tehditleri yalnızca bir güvenlik sorunu olarak değil, aynı zamanda taraftar ilişkileri, marka itibarı ve finansal süreklilik açısından stratejik bir yönetim konusu olarak ele almaları gerekmektedir. Spor kulüplerinin dijital dönüşüm sürecine uyum sağlayacak kurumsal eğitim ve gelişim programlarının dijital çağın gerekliliklerine uygun biçimde yeniden yapılandırılması, kulüplerin dijital direncini ve sürdürülebilir rekabet gücünü artırmada önemli bir adım olacaktır.

Öneriler

- Spor kulüpleri, siber tehditlere karşı dijital güvenlik politikaları oluşturmmalıdır. Bu kapsamda yazılımlar güncellenmeli, güçlü parolalar kullanılmalı, VPN ve çok faktörlü kimlik doğrulama uygulanmalıdır.
- Taraftar verilerinin işlendiği platformlar düzenli olarak denetlenmelidir. Üçüncü taraf hizmet sağlayıcılarla yapılan iş birlikleri yasal sözleşmelerle güvence altına alınmalıdır.
- Kulüpler, veri analitiği ve yapay zekâ ile erken uyarı sistemleri geliştirmelidir. Risk sınıflandırması ve saldırı modellemeleri yapılmalıdır.
- Tüm personel düzenli siber güvenlik eğitimi almalıdır. Bu eğitimler, insan hatalarını azaltarak dijital sistemlerin korunmasına katkı sağlamalıdır.

KAYNAKLAR

- Akmeşe, S. (2020). Kamuda dijital dönüşümün siber güvenlik ve dijital güvence boyutları ve iç denetimin rolü. *Denetişim*, (20), 108-119.
- Ataman, A. (2025). Why cybersecurity in sports is more important than ever. AIMultiple. <https://aimultiple.com/cybersecurity-in-sports> Erişim Tarihi: 29.07.2025
- Balcı, A. (2018). Sosyal bilimlerde araştırma yöntem, teknik ve ilkeler. Ankara: Pegem Akademi.
- Bucea-Manea-Țoniș, R., Antonescu, A. G., & Mihăilă, C. (2025). Blockchain in sports: A comparative analysis of applications and perceptions in football and basketball. *Applied Sciences*, 15(12), 6829.
- Chang, K. (2024). Risk management in sport for athletes towards a successful sporting program. *International Journal of Education and Humanities*. <https://doi.org/10.54097/g5gs1702>.
- Dacorogna, M., & Kratz, M. (2023). Managing cyber risk, a science in the making. *Scandinavian Actuarial Journal*, 2023(10), 1000-1021.
- Ersöz, B., & Özmen, M. (2020). Dijitalleşme ve bilişim teknolojilerinin çalışanlar üzerindeki etkileri. *AJIT-e: Academic Journal of Information Technology*, 11(42), 170-179.
- Gasana, K. (2024). Crisis communication and reputation management in the age of fake news. *Journal of Public Relations*, 3(1), 28-39.

- Grover, H. S. (2023). Data protection: Need? Indeed. *Journal of Indian Society of Periodontology*, 27(1), 3.
- Karasar, N. (2005). *Bilimsel araştırma yöntemi*. Ankara: Nobel Yayın Dağıtım.
- Mahinay, J., & Teleron, J. (2023). Navigating the labyrinth: Unraveling security threats and vulnerabilities in network infrastructures. *International Journal of Advanced Research in Science, Communication and Technology*. <https://doi.org/10.48175/ijarset-13874>.
- May, T., & Perry, B. (2022). *Social research: Issues, methods and process*. London: McGraw-Hill Education.
- Murathan, T., & Murathan, F. (2019). Spor sektöründe blok zinciri uygulamaları. *Gaziantep Üniversitesi Spor Bilimleri Dergisi*, 4(1), 64-74.
- Nešić, M. (2018). Sports club as a factor in security management of a sport event. *Poslovna ekonomija*, 12(2), 128-140.
- NCC Group. (2024). *Cyber threats in sport: The hidden opponent*. Oxford: University of Oxford Researcher Strategy Consultancy in collaboration with Phoenix Sport & Media Group. Erişim adresi: https://www.nccgroup.com/media/zugjppis/cyber-threats-in-sport-whitepaper_final.pdf Erişim tarihi: 30.07.2025
- Pilkington, M. (2016). Blockchain technology: principles and applications. In *Research handbook on digital transformations* (ss. 225-253). Cheltenham: Edward Elgar Publishing.
- Praveen, T. (2024). Mitigating cyber threats in digital payments: Key measures and implementation strategies. *International Journal of Scientific Research and Engineering Trends*, 10(5), ISSN 2395-566X.
- Santos, A. (2023). What is sports management in the digital age?. *Revista intercontinental de gestão desportiva*. <https://doi.org/10.51995/2237-3373.v13i3e110060>.
- Stegmann, P., Ströbel, T., & Woratschek, H. (2024). Categorizing engagement behavior in sport brand communities—an empirical study informed by social practice theory. *Sport Management Review*, 27(4), 544-571.
- Stegmann, P., & Lang, G. (2025). Digital transformation in voluntary sports organizations: A scoping review on multi-level drivers, promoting factors, forms and consequences. *Current Issues in Sport Science (CISS)*, 10(2), 053-053.
- Urs, B. A. (2015). Security issues and solutions in e-payment systems. *Fiat Iustitia*, (1).

- Üstünel, R., & Alkurt, Z. (2015). Futbolda şiddet ve düzensizliğin önlenmesi için 6222 sayılı yasanın getirdiği yeni bir uygulama: Elektronik bilet ve yaşanan sorunlar. *Kara Harp Okulu Bilim Dergisi*, 21(1).
- Zhou, W., & Huang, Q. (2021). Risk management of community sports based on AI technology. In *Journal of Physics: Conference Series* (Vol. 1852, No. 4, p. 042092). Bristol: IOP Publishing.
- Wang, J., Shen, J., Chen, X., & Zhang, J. (2023). A study on the application of digital technology in large-scale events risk management. *Proceedings of the 2nd International Conference on Big Data Economy and Digital Management, (BDEDM 2023)*, January 6–8, 2023, Changsha, China. <https://doi.org/10.4108/eai.6-1-2023.2330329>

