

Dijital Pazarlama Sistemlerinde Siber Güvenliğin Rolü ve Önemi

<https://doi.org/10.31006/gipad.1604902>

Bora GÜNDÜZYELİ*

Öz

Dijital pazarlama, ürün ve hizmetlerin dijital platformlar aracılığıyla, özellikle internet üzerinden tanıtımı ve satışının yapıldığı bir pazarlama yöntemidir. Bu süreçte sosyal medya, arama motorları ve e-posta pazarlama gibi çeşitli çevrimiçi kanallar kullanılmaktadır. Ancak, bu durum, pazarlama verilerinin bu kanallar üzerinden elektronik ortamda paylaşılmasını gerektirir. Diğer bilgi sistemlerinde olduğu gibi, dijital pazarlama sistemleri de siber tehdit ve saldırılara karşı risk altındadır. Bu nedenle, dijital pazarlama sistemlerini hedef alan siber tehdit ve saldırılara karşı alınacak güvenlik önlemleri büyük önem taşımaktadır. Bu çalışmanın amacı, dijital pazarlama sistemlerinde siber güvenliğin rolünü ve önemini incelemek ve dijital pazarlama sistemleri bağlamında siber güvenlik farkındalığının artırılmasına yönelik literatüre katkı sağlamaktır. Araştırmanın temel sorusu şu şekilde belirlenmiştir: "Dijital pazarlama sistemlerinde siber güvenlik önlemlerinin etkisi ve önemi nedir?" Araştırma, ulusal ve uluslararası literatür taramalarıyla gerçekleştirilmiştir. Araştırma sonuçları, dijital pazarlama yöntemlerinin sayısız teknolojik fırsat sunduğunu, ancak bu fırsatların aynı zamanda güvenlik risklerini de beraberinde getirdiğini ve bunun işletmeleri daha güçlü güvenlik önlemleri almaya zorladığını ortaya koymaktadır. Çalışma kapsamında, dijital pazarlama sistemlerinde bilgi güvenliğinin sağlanmasında, ulusal siber güvenlik testlerinden geçmiş ve yerli milli sertifikasyona sahip siber güvenlik ürünlerinin kullanımının önemi vurgulanmıştır. Bu araştırma, dijital pazarlama sistemleri ile siber güvenlik arasındaki kesişimi inceleyerek, dijital pazarlama sistemlerinin güvenliğini artırmada siber güvenlik farkındalığının kritik rolünü vurgulamakta ve literatüre önemli bir katkı sağlamaktadır.

Anahtar Kelimeler: Dijital Pazarlama, Siber Güvenlik, Bilgi Güvenliği, Siber Saldırı, Pazarlama Güvenliği.

The Role and Importance of Cybersecurity in Digital Marketing Systems

Abstract

Digital marketing is a marketing method through which products and services are promoted and sold, primarily via the internet and digital platforms. In this process, various online channels, such as social media, search engines, and email marketing, are used. However, this requires the sharing of marketing data in an electronic environment through these channels. Like other information systems, digital marketing systems are also vulnerable to cyber threats and attacks. Therefore, security measures against cyber threats and attacks targeting digital marketing systems are of great importance. The aim of this study is to examine the role and importance of cybersecurity in digital marketing systems and contribute to the literature regarding raising cybersecurity awareness in the context of digital marketing systems. The primary research question is as follows: "What is the impact and significance of cybersecurity measures in digital marketing systems?" The research has been conducted through a review of national and international literature. The results show that digital marketing methods offer

* Dr., Öğr. Üyesi, İstanbul Topkapı Üniversitesi, İktisadi, İdari ve Sosyal Bilimler Fakültesi, YBS.
boragunduziyeli@topkapi.edu.tr. ORCID: 0000-0001-5098-8713

numerous technological opportunities, but these opportunities also bring security risks, which force businesses to adopt stronger security measures. The study emphasizes the importance of using cybersecurity products that have passed national cybersecurity tests and have local national certifications in ensuring information security in digital marketing systems. This research contributes significantly to the literature by examining the intersection between digital marketing systems and cybersecurity and highlighting the critical role of cybersecurity awareness in enhancing the security of digital marketing systems.

Keywords: Digital Marketing, Cybersecurity, Information Security, Cyber Attack, Marketing Security.

Extended Abstract

This study examines the impact of information security on digital marketing processes, with a focus on the emerging role of Artificial Intelligence (AI) technologies in enhancing cybersecurity measures. As digital platforms have become central to marketing strategies, businesses face increasing threats from cyber-attacks, such as malware, identity theft, data breaches, and DDoS attacks. These threats pose significant risks not only to businesses' financial stability but also to their reputation and customer trust. The integration of cybersecurity measures is, therefore, essential to protect digital marketing efforts from these risks and to ensure the safety of sensitive data.

The research highlights the importance of robust cybersecurity strategies in safeguarding digital marketing activities. To prevent potential threats, businesses must adopt advanced technologies, such as firewalls, antivirus software, and encryption. In addition, regular cybersecurity training for employees is crucial in minimizing human errors, which are often a significant vulnerability in these systems. The study also explores how AI technologies, particularly machine learning, can be utilized to detect and respond to potential security threats. By analyzing user behavior patterns, AI can help detect anomalies and provide early warnings about possible cyber-attacks, thus enabling companies to take timely action.

The study also emphasizes the significant role of AI in the digital marketing domain, where it helps businesses better analyze customer interactions and identify security vulnerabilities. AI's ability to predict and manage cybersecurity threats offers businesses the opportunity to prepare for potential risks and to develop more effective digital marketing strategies in a secure environment. Machine learning and AI technologies are particularly beneficial in the context of mobile banking, IoT applications, and mobile apps, where security and user interaction are closely intertwined.

Furthermore, the research discusses the need for small and medium-sized enterprises (SMEs) to improve their cybersecurity awareness. Given their limited resources, SMEs should invest in cost-effective security solutions, such as cloud-based services, to protect their digital marketing strategies. Additionally, compliance with data privacy laws and regulations is critical for businesses to safeguard customer data and maintain trust.

Finally, the study outlines several strategic recommendations. It advocates for the continuous integration of AI technologies in digital marketing processes to enhance security measures. It also stresses the importance of a cybersecurity culture within organizations and calls for the development of security policies that comply with international standards. The study concludes by suggesting that businesses strengthen their cybersecurity infrastructure to safeguard their digital marketing operations and mitigate potential risks, ensuring sustainable growth in an increasingly digital world.

1. Giriř

Dijital pazarlama, firmaların internet üzerindeki varlıklarını ve diğerk dijital iletişim kanallarını kullanarak gerçekleřtirdikleri iletişim faaliyetlerini kapsar (řengöl, 2017). Ellis-Chadwick ve Chaffey (2012), dijital pazarlamayı internet ve dijital teknolojiler aracılığıyla gerçekleştirilen tüm pazarlama faaliyetleri olarak tanımlar ve bu süreçte dijital kanalların yanı sıra teknolojilerin entegrasyonunun önemine de vurgu yapar. Dijital pazarlama, son yıllarda hemen her organizasyon için karlı ve kritik bir sektör haline gelmişken, siber suçlardan korunmak için kişisel bilgilerin ve hesapların güvenliğinin sağlanması kaçınılmaz bir gereklilik olmuştur (Kumar, 2022). Teknolojik gelişmeler ve internetin yaygınlaşmasıyla insanların alışveriş, iletişim ve bankacılık işlemleri gibi alışkanlıkları değişirken, bu dönüşümle birlikte siber suç kavramı da hayatımıza girmiş ve teknolojiye uyum sağlamaya çalışan işletmeler siber tehditlerle karşı karşıya kalmıştır (Eroğlu, 2023). Özellikle bankacılık ve borsa işlemleri gibi finansal işlemler çevrimiçi platformlar aracılığıyla yapılmakta ve sanal para birimleri ile kripto paralara yönelik siber saldırılar artmaktadır. Bu durum, işletmelere yıllık milyonlarca dolarlık kayıplara yol açabilecek güvenlik açıklarını doğurmuştur (Aslan ve diğ., 2023). Kredi kartları, banka kartları ve ön ödemeli kartlar çevrimiçi işlemlerde yaygın ödeme yöntemi olsa da bu popülerlik dolandırıcılık mağduriyetlerini artırmıştır (Akdemir ve Yenal, 2020). Dijital pazarlama sistemlerinde sıklıkla kullanılan bu ödeme yöntemleri, güvenlik açıklarını ve siber suçları gündeme getirir. Pazarlamacılar müşteri verilerine daha fazla güveniyor, ancak firmalar bu verilerin olumsuz etkilerini anlayamamakta ve bu durum, müşterilerin güvenlik endişelerini artırabilmekte veya gerçek riskler oluşturabilmektedir (Martin ve diğ., 2017). Dijital pazarlama açısından, bu durum müşteri verilerinin toplanması ve kullanılmasında pazarlamacılara önemli fırsatlar sunarken, aynı zamanda siber güvenlik risklerini de beraberinde getirdiğini göstermektedir. Firmalar, pazarlama verilerinin güvenliğini yeterince sağlamazsa, müşterilerin kişisel bilgileri siber saldırılara açık hale gelebilmektedir. Bu durum, müşterilerin güvenlik endişelerini artırarak markanın itibarını zedeleyebilir. Ayrıca, verilerin kötüye kullanımı hukuki sonuçlara yol açabilir ve şirketlerin uzun vadede finansal kayıplara uğramasına neden olabilir. Bu nedenle dijital pazarlama stratejilerinde veri güvenliği önlemleri almak ve müşterilere güven veren bir ortam sağlamak büyük önem taşımaktadır. Dijital reklamcılığın gelişen dünyasında, tüketici verilerinin güvenliğini sağlamak için siber güvenlik entegrasyonu kritik hale gelmiştir (Geetha ve diğ., 2024). Dijital reklamcılık, kullanıcı verilerinin toplandığı ve paylaşıldığı bir alan olduğundan, bu verilerin korunması hem tüketici güvenliğini sağlamak hem de yasal yükümlülöklere uyum sağlamak açısından hayati önem taşır. Dolandırıcılık, ödeme bilgileri çalmak ve kimlik hırsızlığı gibi tehditler, dijital pazarlamanın güvenliğini tehlikeye atmaktadır. İşletmeler, müşterilerin finansal bilgilerini koruyarak güvenli bir dijital ortam sunmak zorundadır; bu da siber güvenlik önlemlerinin stratejilerin etkinliğini sürdürebilmesi için kritik olduğunu göstermektedir. Bu noktada, dijital pazarlama sistemlerinin siber güvenlik kapsamında değerlendirilmesi, bu tehditlere karşı etkili önlemler alabilmek için büyük önem taşımaktadır. Choong ve diğ. (2017) tarafından yapılan çalışmada bir şirketin bilgi ihlali duyurusunun ardından piyasa değerinin nasıl etkilendiğı incelenmiş ve çalışma neticesinde ihlal duyurusu sonrasında şirketin hisse senetlerinde küçük ama anlamlı bir değer kaybı yaşandığı ve bu olumsuz etkinin devam ettiğı bulunmuştur. Bu durum, şirketlerin bilgi güvenliğini korumalarının, piyasa değerlerini ve marka itibarlarını sürdürebilmek için kritik önemde olduğunu ortaya koymaktadır.

Günümüzde, internetin ve mobil teknolojilerin hızla yaygınlaşmasıyla birlikte dijital pazarlama, işletmelere küresel pazarlara ulaşma ve tüketiciyle doğrudan etkileşimde bulunma imkânı tanımaktadır. Bu dönüşüm, geleneksel pazarlama yaklaşımlarının ötesine geçerek, ürün ve hizmetlerin dijital teknolojiler aracılığıyla tanıtılmasını, özellikle internet ve mobil

platformlar üzerinden yapılmasını içermektedir (Desai ve Vidyapeeth, 2019). Bugün, dijital pazarlama sistemlerinde Bilgi ve İletişim Teknolojilerine (BİT) ve özellikle de İnternete olan bağımlılığın giderek artmakta olduđu görülmektedir. Ayrıca, dijital teknolojilerin ve sosyal medyanın hızla gelişmesiyle birlikte, işletmelerin tüketicilerle daha interaktif ve doğrudan iletişim kurma imkânı artmıştır. Bu durum, pazarlama süreçlerini yeniden şekillendirmiş ve işletmelerin bu yeni ortamda rekabet avantajı elde edebilmesi için dijital platformları etkin bir şekilde kullanmaları gerektiğini ortaya koymuştur (Krishen ve diğ., 2021). Ancak bu durum aynı zamanda işletmeler için dijital pazarlama stratejilerinin ve çevrimiçi platformların etkin bir şekilde işletilmesi için önemli fırsatlar sunarken, aynı zamanda da bu sistemleri siber saldırılar ve çeşitli dijital tehditlere karşı savunmasız hale getirmektedir. Sosyal medya hesaplarından e-posta pazarlamasına kadar tüm dijital kanallar, siber suçlular tarafından hedef alınabilmekte ve bu durum markaların itibarını, müşteri verilerini ve iş süreçlerini riske atabilmektedir. Bu nedenle, dijital pazarlama stratejilerinin güvenliği, yalnızca pazarlama başarısı için değil, aynı zamanda markaların sürdürülebilirliği için de kritik öneme sahiptir. Siber saldırıların sıklığı ve kapsamı giderek artmakta, bu durum ekonomik faaliyetin her alanını etkilemekte ve sanayi ile işletmeleri tehlikeye atmaktadır (Aiman at al., 2021). Siber tehditler, dijital çağda her işletmenin karşılaşması gereken bir gerçeklik haline gelmiştir (Akhtar ve diğ., 2021).

Dijital pazarlama sistemlerine yönelik artan siber saldırı ve tehditler sadece bireysel işletmelerin değil, aynı zamanda ulusal düzeydeki güvenliğin de tehdit edilmesine yol açabilir. Özellikle büyük veri analizleri, e-ticaret sistemleri ve sosyal medya platformlarının manipülasyonu gibi durumlar, ekonomik istikrarı ve kamu düzenini doğrudan etkileyebilir. Kritik sektörlerde faaliyet gösteren büyük işletmelerin ya da devletle ilişkili kurumların dijital pazarlama ve veri yönetim sistemlerine yönelik siber saldırılar, enerji, sağlık veya finans gibi stratejik alanlarda önemli sorunlara yol açarak ulusal güvenliği tehdit edebilir. Özellikle e-ticaret sitelerindeki finansal bilgilerin üçüncü taraf hizmetlerle sürekli hedef haline gelmesi durumu dijital pazarlamanın güvenlik endişelerini artıran bir diğer faktördür (Rosário, 2023). Örneğin, bir hastane grubu dijital pazarlama sistemleri aracılığıyla hasta bilgilerini yönetirken, bir siber saldırgan bu sisteme sızarak hasta verilerini çalabilir ve sağlık hizmetlerinin aksamasına yol açarak ulusal güvenliği tehdit edebilir. Bu nedenle dijital pazarlama sistemlerinde alınacak güvenlik önlemleri, ulusal güvenliği de kapsayan geniş bir çerçevede ele alınmalıdır. Online alışverişte, tüketici güveni, alışveriş sitesinin güvenlik açıklarına sahip olması ve kullanıcıların ödeme işlemleri, kişisel verilerinin korunması gibi kritik süreçlerde kuralların ihlal edilebileceği algısını taşıması nedeniyle zedelenebilir, bu da tüketicilerin siteyi kullanmaktan kaçınmalarına yol açabilir (Akçacı ve Kurt, 2020).

Dijital pazarlama stratejileri, işletmelerin siber tehditlere karşı etkili bir savunma mekanizması oluşturmasını sağlayacak şekilde geliştirilmelidir (Şenyapar, 2024). Siber güvenlik, dijital pazarlamanın sürdürülebilir ve sorumlu iş operasyonlarının temelini oluşturur (Şenyapar, 2024). Ancak tüm bunlar ile birlikte artık siber güvenlik sadece Bilgi İşlem (BT) departmanının sorumluluğunda değildir. Şirketlerin hassas verileri sızdırıldığında veya sistemler saldırıya uğradığında, güvenli bir çevrimiçi ortamın korunmasında herkesin rolü olduğu açıktır (Kumar, 2022). Bu durum, işletmelerin siber güvenliği yalnızca teknik bir konu olarak görmek yerine, kurumsal kültürün bir parçası olarak ele almaları gerektiğini göstermektedir. E-ticaret sitelerindeki güvenlik ihlalleri, tüketicilerin mali ve hassas kişisel bilgilerini tehlikeye atmaktadır (Suh ve Han, 2003). Teknolojinin gelişmesiyle elektronik platformları kullanan tüketici sayısı artarken, kötü niyetli saldırganların bu platformlara illegal erişim girişimleri de hızla çoğalmaktadır (Gülmüş, 2010). Bu durum, dijital pazarlama faaliyetlerinin güvenliğini sağlamak için siber güvenlik önlemlerinin önemini artırırken,

kullanıcı verilerinin korunması ve markaların itibarının güvence altına alınması açısından bu alandaki arařtırmaların gerekliliğini ortaya koymaktadır.

Bu çalışmanın amacı dijital pazarlama sistemlerinde siber güvenliğin rolünün ve öneminin araştırılması ve bu bağlamda dijital pazarlama alanında siber güvenlik farkındalığının artırılmasına katkı sağlanması olarak belirlenmiştir. Çalışma, řu temel araştırma sorusunu ele almaktadır: "Dijital pazarlama sistemlerinde siber güvenlik önlemlerinin etkisi ve önemi nedir?" Çalışma bu araştırma sorusuna odaklanarak, dijital pazarlama alanındaki siber güvenliğin rolünü giderek artan önemi incelemektedir. Bu bağlamda arařtırmada öncelikle dijital pazarlama süreçlerinde karşılaşılan siber tehditler ile bu tehditlerin işletmelerin dijital pazarlama stratejilerine olan etkilerini ele almıştır. Müteakiben çalışmada siber güvenlik önlemlerinin dijital pazarlama stratejilerinin güvenli bir şekilde uygulanmasındaki kritik rolü ve işletmelerin bu tehditlere karşı daha hazırlıklı olabilmesi için gereken stratejik yaklaşımlar incelenmiştir. Çalışmada ayrıca Yapay Zekâ (YZ) teknolojilerinin siber güvenlikteki etkin rolü de araştırılmıştır. Çalışma neticesinde elde edilen bulgular çerçevesinde ayrıca dijital pazarlama sistemleri güvenliğinin sağlanmasında ulusal siber güvenlik testlerinden geçirilmiş, yerli ve milli sertifikasyona sahip siber güvenlik bilgi teknoloji ürünleri kullanılması hususuna da ayrıca dikkat çekilmiştir. Çalışmanın 2'nci bölümde arařtırmada kullanılan metodoloji detaylandırılmıştır. 3'üncü bölümde araştırma kapsamında elde edilen bulgulara yer verilmiştir. Çalışmanın 4'üncü ve son bölümünde ise araştırma neticesinde elde edilen bulgular doğrultusunda ulařılan sonuçlara yer verilmiştir.

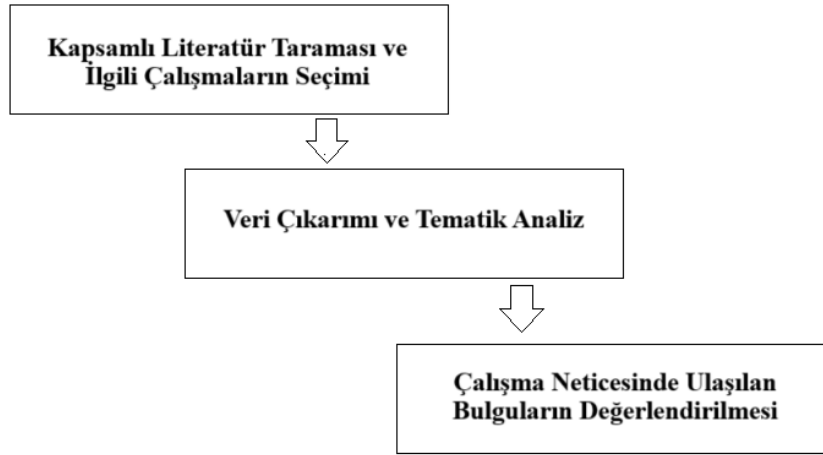
2. Çalışmanın Metodolojisi

Arařtırmada nitel bir yöntem kullanılmış ve literatür taraması yapılmıştır. Kaptan (1995, s. 59) bu yöntemi, olayların, grupların, kurumların vb. çeşitli alanların ne olduğunu ve bu sırada gerçekleşen eylemleri daha iyi anlayabilmek ve aktarabilmek amacıyla aralarındaki ilişkinin açıklandığı bir unsur olarak görmektedir. Bu bağlamda arařtırmanın amacı doğrultusunda ařağıdaki sorulara nitel araştırma ile yanıt aranmıştır:

- Dijital pazarlama stratejileri ile siber güvenlik arasındaki ilişki neden bu kadar kritik bir rol oynamaktadır?
- Dijital pazarlama süreçlerinde siber güvenlik tehditleri ve korunma yöntemleri nelerdir?
- Yapay Zeka'nın (YZ) dijital pazarlamada siber güvenlik üzerindeki etkileri nelerdir?
- Dijital pazarlama stratejilerinin ulusal güvenlik üzerindeki rolü nedir?

Arařtırmada kapsamlı bir analiz sağlamak amacıyla nitel araştırma yöntemi kullanılmıştır. Arařtırmada belirlenen araştırma sorularını ele almak amacıyla "Dijital Pazarlama", "Siber Güvenlik" ve "Bilgi Güvenliğı" anahtar arama terimleri kullanılarak Google Scholar, Scopus ve Web of Science gibi çeşitli akademik veri tabanlarında kapsamlı bir literatür taraması yapılmıştır. Bu veri tabanları aracılığıyla başlangıçta toplamda 47 makale belirlenmiştir. Araştırma, Ocak 2000 ile Aralık 2024 tarihleri arasında yayımlanan hakemli dergi makaleleriyle sınırlı tutulmuştur. Bu makalelerden, araştırma konusu ile ilgisi olmayan çalışmalar hariç tutulmuş ve tekrarlar kaldırılmıştır. İncelemenin güvenilirliğı ve kalitesini sağlamak için yalnızca hakemli makalelere yer verilmiştir. Bu süreç sonucunda analiz için bu makalelerden oluşan nihai bir set elde edilmiştir. Bu çalışmanın araştırma modeli literatür taraması ile geliştirilmiş olup kullanılan model Şekil 1'de sunulmuştur. İnceleme süreci, ilgili çalışmaların tanımlanması ve seçilmesiyle başlamış, ardından veri çıkarımı ve tematik analiz yapılmıştır. Seçilen makaleler, yöntemsel kalite, araştırma soruları ile ilgili olma durumu ve

yapay zekanın dijital pazarlamadaki sürdürülebilirlik üzerindeki etkisini anlamaya katkıları açısından değerlendirilmiştir. Son olarak, bulgular sentezlenmiş ve çalışmada sunulmuştur.



Şekil 1. Önerilen Araştırma Modeli

Araştırma sonucunda elde edilen bulgular, dijital pazarlama sistemlerinde güçlü bir siber güvenlik çerçevesinin gerekliliğini ortaya koymaktadır. Çalışmada elde edilen bulgular neticesinde yapılan öneriler arasında, dijital pazarlama sistemlerinde yerli ve ulusal siber güvenlik testlerinden geçirilmiş, ulusal sertifikasyona sahip ve akredite güvenlik danışmanlık şirketleri tarafından tasarlanmış ve test edilmiş yerli dijital pazarlama araçları ve çözümleri kullanılması gerektiği hususuna özellikle vurgu yapılmıştır.

3. Bulgular

3.1. Dijital Pazarlama ve Siber Güvenlik: Fırsatlar ve Riskler

Pazarlama, günümüzün karmaşık iş dünyasında üç büyük güç tarafından dönüştürülmektedir: Teknolojik eğilimler, sosyoekonomik eğilimler ve jeopolitik eğilimler (Rust, 2020). Bu dinamikler, pazarlama stratejilerinin evrimini doğrudan etkilemektedir. Özellikle teknolojik eğilimler, dijital dünyanın her yönünü etkileyerek işletmelerin pazarlama stratejilerinde köklü değişikliklere yol açmıştır. Geleneksel pazarlama, genellikle ürün, fiyat, yer ve promosyon (4P) modeline dayanarak şekillenir ve bu model, stratejilerin geliştirilmesinde kritik bir çerçeve sunar (Armstrong ve diğ., 2014). Ancak dijital çağın başlamasıyla birlikte pazarlamanın bu geleneksel yapıdan uzaklaşmaya başladığı ve dijital kanallar aracılığıyla daha hedeflenmiş ve etkileşimli bir hale geldiği gözlemlenmiştir (Desai ve Vidyapeeth, 2019). Dijital pazarlama, yalnızca teknolojik bir yenilik değil, aynı zamanda pazarlama felsefesinde de bir değişim sürecini başlatmıştır. Bu dönüşüm, markaların daha birebir ve kişiselleştirilmiş stratejilerle müşterilere ulaşmasını sağlamış ve böylece müşteri deneyimini ve markaların etkinliğini artırmıştır. Örneğin, cep telefonları, görüntülü reklamlar ve çeşitli dijital medya kanalları gibi dijital teknolojiler pazarlama faaliyetlerini daha dinamik ve katılımcı hale getirmiştir (Deiss ve Henneberry, 2020). Dijital pazarlama stratejilerinin bu denli güçlü etkileri, aynı zamanda dijital ortamın getirdiği güvenlik tehditlerine karşı daha dikkatli olunmasını zorunlu kılmaktadır. Dijital pazarlama ile birlikte gelen bu yeni fırsatlar, işletmelerin verilerini, müşteri bilgilerini ve çevrimiçi varlıklarını daha hassas hale getirmiştir. Desai ve Vidyapeeth (2019) tarafından yapılan çalışmada dijital pazarlamanın avantajları olarak gerçek zamanlı sonuçlar, küresel erişim, kişiselleştirilmiş tanıtım ve hedefleme yetenekleri öne çıkarken, dezavantajları da

internet bağımlılığı, yüksek rekabet, güven sorunları ve satış dönüşüm zorlukları olarak belirtilmiştir.

Dijital pazarlamanın hızlı dönüşümü, işletmelere geniş müşteri kitlelerine ulaşma olanağı sunsa da bu genişlemenin beraberinde getirdiğı güvenlik riskleri de oldukça önemlidir. Günümüzde pazarlama faaliyetlerinin dijital platformlarda yoğunlaşması durumu her ne kadar işletmeler için büyük fırsatlar sunsa da bu durum aynı zamanda çeşitli bilgi güvenliği tehdit ve risklerini de beraberinde getirmektedir. Dijital pazarlama stratejileri veriye dayalı kararlar almayı ve geniş kitlelere ulaşmayı kolaylaştırırken, diğer taraftan dijital pazarlama sistemlerini siber saldırı ve tehditlere maruz bırakabilir. Günümüzde dijital kanallar üzerinden işletmelerin müşteri verilerini toplaması ve reklam hizmetlerini sunması, onları aynı zamanda siber saldırılara karşı daha açık hale getirmektedir. İşletmelerin dijital platformlarda faaliyetlerini sürdürebilmesi için gizlilik, bütünlük ve erişilebilirlik ilkelerinin sağlanması büyük önem taşır. CIA üçgeni olarak da bilinen bu ilkeler, esasen bilgi güvenliğinin sağlanması gereken temel unsurlardır ve siber güvenliğin en önemli işlevlerini oluştururlar (Stallings ve Brown, 2008). Bu ilkelerden birinin eksik olması bile tüm sistemin güvenliğinin tehdit altında olması anlamına gelir. Örneğin, bir e-ticaret platformunda gizlilik ilkesi, kullanıcı verilerinin sadece yetkili kişiler tarafından erişilmesini sağlarken, bütünlük ilkesi verilerin bozulmadan, doğru bir şekilde korunmasını temin eder. Erişilebilirlik ise kullanıcıların doğru bilgilere her an ulaşabilmesini garanti eder. Bu ilkeler, dijital pazarlama stratejilerinin güvenli bir şekilde işlemesi için kritik öneme sahiptir.

Siber güvenlik tehdidi, yalnızca işletmelerin iç süreçlerine zarar vermekle kalmaz, aynı zamanda işletmelerin pazarlama stratejilerinin başarısını da doğrudan etkiler. Siber savaş, elektronik ağlarda, bilgisayar sistemlerinde, iletişim ağlarında ve bilgi depolama cihazlarında gerçekleşen bir savaş şeklidir (Johnson, 2015). Siber güvenlik, dijital pazarlamanın etkinliğini sürdürülebilir kılmak için kritik bir rol oynamaktadır. Siber güvenlik, bilgi güvenliği kavramını bir adım öteye taşıyarak sadece veri korumayı değil, tüm dijital varlıkları, ağları ve dijital altyapıları da kapsar (Von Solms ve Niekerk, 2013). Siber güvenliğin temel ilkeleri arasında gizlilik, bütünlük ve erişilebilirlik yer almaktadır (Simmonds ve diğ., 2004). Gizlilik, bilgilere yalnızca yetkili kişilerin erişmesini sağlarken, bütünlük, bilginin bozulmadan ve doğru bir şekilde korunmasını ifade eder. Erişilebilirlik ilkesi ise, bilgiye ihtiyaç duyan kişilerin bu bilgilere zamanında ve güvenli bir şekilde ulaşabilmesini amaçlar. Dijital pazarlama stratejileri, bu ilkelerle doğrudan ilişkili olup, kullanıcı verilerinin ve müşteri bilgilerinin güvenliğini sağlamadan başarılı olamaz. Dijital pazarlama stratejilerinin artan kullanımıyla birlikte, işletmelerin karşılaştığı güvenlik tehditlerinin çeşitliliği ve boyutu da önemli bir sorun haline gelmiştir. Günümüzde siber tehdit ve saldırıların giderek arttığı görülmektedir. Siber alan, her geçen gün genişleyerek kimlik avı ve DDoS saldırıları gibi çeşitli tehditleri içinde barındıran bir ortam haline gelmektedir (Karasoy, 2022). Cisco'nun raporuna göre, 2023 yılı itibarıyla DDoS saldırı sayısının 7,9 milyondan 15 milyona çıkması öngörülmektedir (Cisco Annual Internet Report, 2018–2023). Pazarlama sistemlerini hedef alan siber saldırılar, hizmet kesintilerine yol açarken aynı zamanda markaların çevrimiçi güvenliklerini de riske atmaktadır. Bu tehditlere karşı dijital pazarlama stratejilerinde siber güvenlik önlemlerinin uygulanması büyük bir önem taşımaktadır. Günümüzde, işletmelerin kişisel veriler ve ticari sırlar gibi hassas bilgilerin çalınma tehditlerine karşı güvenli sistemlere ihtiyaçları olduğu açıktır (Buhas ve diğ., 2021). Bu güvenlik önlemleri, dijital pazarlama stratejilerinin etkinliğini artırır ve yatırımın geri dönüşünü olumlu yönde etkiler (Obitovich ve Utkirovna, 2023). Artan dolandırıcılık tehditlerine karşı güvenlik önlemleri (sanal kart, ek şifreleme, EMV standartları) geliştirilmiş olsa da internet üzerindeki kredi kartı dolandırıcılığı tamamen sona erdirilememiştir ve dolandırıcılar sürekli yeni yöntemler bulmaktadır (Akdemir ve Yenal, 2020). Esasen, bu durum,

dijital ortamda artan dolandırıcılık tehditlerine karřı geliştirilen güvenlik önlemlerine rağmen, dolandırıcıların sürekli olarak yeni yöntemler bulup bu önlemleri aşmaya çalıştığını ve internet üzerindeki kredi kartı dolandırıcılığının tamamen ortadan kaldırılamadığını göstermektedir.

Tablo 1. Dijital Pazarlama Stratejileri ve Siber Güvenlik İliřkisini İnceleyen Çalışmalar

Çalışma Bilgileri	Yazar(lar)	Yıl	Yöntem	Sonuçlar
Pazarlama Stratejilerinin Evrimi ve Dijital Pazarlama	Rust (2020)	2020	Literatür İncelemesi	Teknolojik eğilimlerin pazarlama stratejilerinde köklü deęişikliklere yol açtığı vurgulanmıştır.
Dijital Pazarlama ve Teknolojik Yenilikler	Armstrong ve diğ. (2014)	2014	Literatür İncelemesi	Dijital pazarlamanın geleneksel pazarlama yapılarına göre daha etkileşimli olduđu belirtilmiştir.
Dijital Pazarlamanın Avantajları ve Dezavantajları	Desai ve Vidyapeeth (2019)	2019	Anket Çalışması	Avantajlar: Gerçek zamanlı sonuçlar, küresel erişim, kişiselleştirilmiş tanıtım. Dezavantajlar: İnternet bağımlılığı, yüksek rekabet, güvenlik sorunları.
Dijital Pazarlama ve Siber Güvenlik İliřkisi	Deiss ve Henneberry (2020)	2020	Literatür İncelemesi	Dijital pazarlamanın getirdiğı güvenlik tehditlerine dikkat çekilmiş ve siber güvenlik önlemlerinin önemine vurgu yapılmıştır.
Siber Güvenlik ve Dijital Pazarlama Stratejileri	Stallings ve Brown (2008)	2008	Literatür İncelemesi	Siber güvenlik ilkelerinin (gizlilik, bütünlük, erişilebilirlik) dijital pazarlama için kritik olduđu belirtilmiştir.
Dijital Pazarlama Stratejileri ve Güvenlik Tehditleri	Johnson (2015)	2015	Kavramsal Çalışma	Siber güvenlik tehditlerinin dijital pazarlamanın etkinliğini olumsuz etkileyebileceğı vurgulanmıştır.
Siber Güvenlik ve Dijital Varlıklar	Von Solms ve Niekerk (2013)	2013	Literatür İncelemesi	Dijital varlıkların güvenliği için siber güvenlik önlemlerinin gerekliliğı açıklanmıştır.
Pazarlama Sistemlerini Hedef Alan Siber Saldırıları	Karasoy (2022)	2022	Literatür İncelemesi	DDoS saldırılarının arttığı, pazarlama sistemlerinin hedef alındığı ve güvenlik önlemlerinin artırılması gerektiğı belirtilmiştir.
Siber Güvenlik Önlemleri ve Dijital Pazarlama	Obitovich ve Utkirovna (2023)	2023	Literatür İncelemesi	Siber güvenlik önlemlerinin dijital pazarlama stratejilerinin etkinliğini artırdığı ifade edilmiştir.
Dijital Dolandırıcılık ve Güvenlik Önlemleri	Akdemir ve Yenal (2020)	2020	Literatür İncelemesi	Dijital dolandırıcılıkla mücadele için yeni güvenlik önlemleri geliştirilmiş olsa da, dolandırıcıların sürekli yeni yöntemler bulduđu belirtilmiştir.

Görüldüğü üzere Tablo 1’de incelenen çalışmalarda, dijital pazarlama stratejilerinin gelişen teknolojiyle birlikte dönüşüm geçirdiğini, ancak bu dönüşümün beraberinde çeşitli siber güvenlik tehditlerini de beraberinde getirdiğini ortaya koymaktadır. 2020 yılında Rust, teknolojik eğilimlerin pazarlama stratejilerini nasıl dönüřtürdüğüne dair bulgular sunarken, Armstrong ve diğ. (2014) dijital pazarlamanın geleneksel yapıları nasıl etkileřtirdiğini vurgulamıştır. Desai ve Vidyapeeth (2019) ise dijital pazarlamanın gerçek zamanlı sonuçlar ve küresel erişim gibi avantajlarını belirtmiş, ancak internet bağımlılığı ve güvenlik sorunları gibi dezavantajlara da dikkat çekmiştir. Deiss ve Henneberry (2020), dijital pazarlamanın getirdiğı

güvenlik tehditlerine karşı siber güvenlik önlemlerinin önemini vurgulamışken, Stallings ve Brown (2008) siber güvenlik ilkelerinin dijital pazarlama için kritik olduğunu açıklamıştır. Johnson (2015), dijital pazarlamanın etkinliğini olumsuz etkileyebilecek siber güvenlik tehditlerini tartışmış, Von Solms ve Niekerk (2013) ise dijital varlıkların güvenliği için siber güvenlik önlemlerinin gerekliliğine dikkat çekmiştir. Diğer çalışmalarda, Karasoy (2022) DDoS saldırılarının artışı ve pazarlama sistemlerinin hedef alındığını belirtmiş, Obitovich ve Utkirovna (2023) ise dijital pazarlama stratejilerinin etkinliğini artırmak için siber güvenlik önlemlerinin gerekliliğini vurgulamıştır. Son olarak, Akdemir ve Yenal (2020), dijital dolandırıcılıkla mücadele için güvenlik önlemleri geliştirilse de dolandırıcıların yeni yöntemler bulmaya devam ettiğini ifade etmiştir. Bu çalışmalar, dijital pazarlama stratejilerinin güvenliğini sağlamak için siber güvenlik önlemlerinin hayati bir rol oynadığını göstermektedir. Bu durum, dijital pazarlama stratejilerinin günümüzde işletmeler için büyük fırsatlar sunarken, beraberinde önemli güvenlik risklerini de getirdiğini ortaya koymaktadır. Teknolojik ilerlemelerle birlikte dijital platformlarda yapılan pazarlama faaliyetleri, müşteri verilerinin toplanması ve kullanılmasıyla artan siber güvenlik tehditlerine açık hale gelmiştir. Özellikle gizlilik, bütünlük ve erişilebilirlik ilkeleri, dijital pazarlama stratejilerinin güvenli bir şekilde işlenmesini sağlamak için kritik önem taşır. Siber güvenlik önlemleri olmadan, işletmeler pazarlama kampanyalarını etkili bir şekilde yürütemez ve müşteri güvenliğini riske atabilirler. Bu nedenle, dijital pazarlama stratejileri ile siber güvenlik arasındaki ilişki, işletmelerin dijital varlıklarını koruma ve başarılı bir pazarlama performansı sergileme yetenekleri açısından hayati bir rol oynamaktadır.

3.2. Dijital Pazarlama Süreçlerinde Karşılaşılan Siber Güvenlik Tehditleri ve Savunma Stratejileri

Siber saldırılar, siber ortamda yer alan bilgileri istismar etmek, bozmak, değiřtirmek, sistemlere erişimi engellemek veya zarar vermek amacıyla gerçekleştirilen faaliyetlerdir (Çiftçi, 2013). Günümüzde siber tehditler genellikle çeřitli dijital kanallar aracılığıyla gerçekleştirilir. Özellikle dijital pazarlama ortamında karşılaşılan tipik siber saldırılar arasında kötü amaçlı yazılım bulaşması, tarayıcı korsanlığı, veri ve hassas bilgilerin çalınması, kimlik hırsızlığı, sahte haber yayılması, DDoS saldırıları ve WordPress kötü amaçlı yazılımları gibi tehditler bulunmaktadır. Ancak dijital pazarlama profesyonellerinin çoğu bu tehditlerin tamamını bilmemektedir ve yeni saldırı türlerine karşı hazırlıksızdır (Kumar, 2022). Bu bağlamda, siber güvenlik tehditlerinin sürekli evrim geçirdiğı bir ortamda dijital pazarlama uzmanlarının tehditlere karşı proaktif bir yaklaşım benimsemeleri çok önemlidir. Günümüzde siber tehditler, sadece bireysel bilgileri çalmaktan çok daha fazlasını hedeflemektedir. Örneğın, kötü amaçlı yazılım (malware) ve fidye yazılımları (ransomware) gibi tehditler doğrudan işletmelerin operasyonlarını durdurma veya önemli verileri şifreleyerek fidye talep etme amacı gütmektedir. Ayrıca oltalama (phishing) ve SMS ile oltalama (smishing) gibi yöntemlerle kullanıcılar kimlik hırsızlığı ve dolandırıcılıkla karşı karşıya kalabilirler (Bucovetchi ve Vevera, 2024). Bu tür saldırılar dijital pazarlama stratejileriyle doğrudan ilişkili olup, hedeflenen firmaların müşteri verilerini, finansal bilgilerini ve marka itibarını tehdit etmektedir. Bu nedenle dijital pazarlama profesyonellerinin siber güvenlik stratejileri geliřtirmeleri, dijital platformlarda güvenli işlemler sağlayabilmek için son derece önemlidir. Siber güvenlik stratejileri, yalnızca teknik değil, aynı zamanda organizasyonel düzeyde de uygulanması gereken önlemler içermektedir. Etkili bir siber güvenlik stratejisi, dijital pazarlamada yalnızca mali zararları ve hassas verilerin yetkisiz erişim veya kaybını önlemekle kalmayıp, aynı zamanda müşteri güveni ve sadakatini sağlamak için de kritik öneme sahiptir (İlyas ve diğ., 2021). Tüketicilerin kişisel verilerinin güvenliği ve gizliliğı ile ilgili artan endişeleri, dijital pazarlamanın gelecekte daha dikkatli bir

řekilde yapılandırılmasını zorunlu kılmaktadır (řenyapar, 2024). Bunun yanı sıra dijital pazarlama alanındaki platformlar ve ödeme sistemleri, siber tehditlere karřı her zaman güncel güvenlik önlemleri ile korunmalıdır (Konyeha, 2020). Geliřmekte olan ölkelerde teknoloji altyapısının zayıflığı nedeniyle siber tehditlere karřı daha savunmasız kalınmaktadır (Dubovyk, 2022). Bu durum, geliřmekte olan ölkelerde faaliyet gösteren dijital pazarlama firmaları için büyük bir risk oluřturmakta olup, siber güvenlik önlemlerinin güçlendirilmesi gerekliliğini ortaya koymaktadır. Küçük ve orta ölçekli řetmeler (KOBİ'ler), genellikle daha sınırlı kaynaklara sahip olduklarından dijital pazarlama süreçlerinde siber güvenlik önlemlerini yeterince uygulamamakta ve bu durum onları siber saldırılara karřı savunmasız hale getirmektedir (Chidukwani ve diğ., 2022). Dijital pazarlama süreçlerinin yaygınlařmasıyla birlikte, artan siber güvenlik olayları, řetmeleri, özellikle küçük ve orta ölçekli řetmeleri (KOBİ'ler) ekonomik zayıflama riskiyle karřı karřıya bırakmaktadır (Schwieger ve Ladwig, 2022). Bu bağlamda KOBİ'lerin dijital pazarlama stratejilerini koruyabilmek için güçlü siber güvenlik önlemleri almaları ve bu alanın potansiyel tehditlerine karřı hazırlıklı olmaları çok önemlidir. Bu nedenle KOBİ'lerin dijital pazarlama stratejilerini korumak için gerekli güvenlik önlemlerini alması hem marka itibarlarını korumaları hem de müşteri güvenini kazanmaları açısından kritik bir öneme sahiptir.

İstenmeyen e-postalar (spam), dijital pazarlama bağlamında hem fırsatlar hem de ciddi riskler barındırır. Dijital pazarlama stratejilerinin önemli bir parçası olan e-posta pazarlama, markaların doğrudan hedef kitlelerine ulaşmasını sağlar. Ancak bu tür e-posta kampanyaları, siber güvenlik tehditlerine karřı savunmasız olabilir. E-posta içeriklerinde yer alan zararlı yazılımlar, kullanıcıların bilgisayarlarına veya ağlarına sızarak büyük zararlar verebilir. Örneğin, virüsler, Truva atları veya SCADA sistemlerine yönelik saldırılar, özellikle büyük řetmelerin altyapılarını hedef alabilir ve ciddi veri kayıplarına ya da sistem çökmesine yol açabilir. İstenmeyen e-postalar bazen reklam ya da propaganda aracı olurken, bazen de eklerindeki virüs, Truva atı veya SCADA sistemlerini hedef alan zararlı yazılımlar aracılığıyla bireysel varlıklara ve ülke varlıklarına ciddi zararlar verebilir ve bu yazılımlar bilgisayardan bilgisayara, ölkeden ölkeye yayılabilir (Kaya, 2013). Bu durumu dijital pazarlama ile ilişkilendirdiğimizde, siber güvenlik tehditleri doğrudan pazarlama faaliyetlerinin güvenliğini etkiler. Özellikle markaların, kullanıcı verilerini toplama ve işleme süreçlerinde yüksek güvenlik önlemleri alması gerekir. Eğer bu e-posta saldırıları bir marka ile ilişkilendirilirse, markanın itibarı zarar görebilir, müşteri güveni sarsılabilir ve hukuki sonuçlarla karşılaşılabilir. Ayrıca, zararlı yazılımlar bilgisayarlar arasında yayılarak daha geniş kitlelere ulaşabileceği için, bir e-posta kampanyasında kullanılan veritabanlarının güvenliği büyük önem taşır. Dijital pazarlama stratejilerinde kullanılan e-posta gibi dijital iletişim kanallarının siber güvenlik riskleri, markaların güvenliğini ve itibarını tehdit edebilir, müşteri verilerinin korunmasını zorlaştırabilir ve dolayısıyla marka güvenliği ile siber güvenlik arasındaki ilişki son derece güçlüdür. Bu nedenle, dijital pazarlama uygulamaları sırasında siber güvenlik önlemleri almak, markaların uzun vadeli başarısı ve güvenilirliği için kritik öneme sahiptir. Veri ihlalleri, firmanın piyasa değerini etkiler ve toparlanma, müşteri tepkilerine bağlıdır (Kirk ve Noguera, 2019). Bu durum esasen, bir řirketin veri ihlali yařaması durumunda, bu olayın řirketin piyasa değerini olumsuz řekilde etkileyebileceğini belirtmektedir. Veri ihlali, müşteri ve yatırımcı güvenliğini sarsarak, řirketin değer kaybetmesine neden olabilir. Ancak, řirketin toparlanma süreci, müşterilerin ve diğeri paydařların gösterdiği tepkiyle doğrudan ilişkilidir. Yani, eğer řirket veri ihlaliinden sonra müşteri güvenliğini yeniden kazanmak için etkili adımlar atarsa, piyasa değeri zamanla eski seviyelere dönebilir. Veri ihlalleri meydana geldiğinde, pazarlamacıların markayı ve itibarını koruma konusunda önemli bir rolü vardır (Whitler ve Farris, 2017). Pazarlamacılar, markanın güvenliğini ve itibarını koruyabilmek için doğru iletişim stratejileri geliřtirerek, müşterilere řeffaf ve güven verici mesajlar iletebilir, süreci etkili bir

řekilde yönetebilir ve marka imajını yeniden inşa etmeye çalışabilirler. Bu, müşteri güvenliğini yeniden kazanmak ve markanın olumsuz etkilerden mümkün olduđunca az etkilenmesini sağlamak aısından kritik bir öneme sahiptir.

Tablo 2, dijital pazarlama süreçlerine yönelik olası siber saldırı türlerini ve bu saldırılara karşı alınabilecek önlemleri özetlemektedir. Örneđin, virüsler ve solucanlar, müşteri verilerini çalabilir veya sistemlerin çalışmasını engelleyebilir. Truva atları ve casus yazılımlar ise kullanıcıların hassas bilgilerini elde etmek amacıyla kullanılabilirken, DDoS saldırıları web sitelerinin erişilebilirliğini tehdit ederek pazarlama faaliyetlerini durdurabilir.

Tablo-2: Siber Saldırı Türleri ve Yöntemleri

Saldırı Türü	Aıklama
Virüsler	Kötücül yazılımlar; kendilerini kopyalayarak diđer sistemlere yayılırlar.
Solucanlar	Kendi başına kopyalanarak ađ üzerinden yayılan kötü programlar.
Truva Atları	Gizlice zararlı yazılımlar; içten sızarak güvenliđi ihlal ederler.
Mantık Bombaları	Belirli bir programda zararlı kod barındırarak veri silme veya deđiřtirme amacı güderler.
İstem Dıřı Elektronik Postalar	Spam e-postalar; genellikle reklam amaçlıdır.
Klavye İşlem Kayıt Ediciler	Kullanıcı klavye işlemlerini kaydederek yetkisiz kişilere gönderir.
Casus Yazılımlar	Kullanıcı bilgisi olmadan veri kopyalayıp transfer eden zararlı yazılımlar.
DDoS Saldırıları	Ađ iletişimini engelleyerek hizmetlere erişimi durduran yoğun veri gönderimi.
Sosyal Mühendislik	İnsan hatalarını manipüle ederek gizli bilgilere erişim sağlama tekniđi.
Diđer Saldırı Türleri	Yeni tehditler sürekli ortaya çıkmakta; çeřitlilik ve sürekli gelişim göstermektedir.

Siber saldırılar karşısında savunma stratejileri geliřtirmek işletmeler için hayati öneme sahiptir. Bir siber güvenlik planına yatırım yapmak, şirketlerin imajını güçlendirir, güçlü bir siber güvenlik sistemi sağlar ve müşterilerin kişisel bilgilerini koruyarak SQL enjeksiyon saldırıları, Hizmet Reddi (DoS) saldırıları ve şifre kırma gibi siber tehditlere karşı koruma sağlar (Kumar, 2022). Bu tür saldırılara karşı etkili koruma sağlamak için işletmelerin güvenlik politikalarını sürekli olarak güncelleyip dinamik tutmaları gerekmektedir (Çetin ve diđer., 2015). Siber tehdit ve saldırılardan korunmak için çeřitli teknik ve yöntemler kullanılabilir. Şifreleme, antivirüs yazılımları, güvenlik duvarları (firewall), sayısal imzalar, VPN'ler, vekil sunucular (proxy), saldırı tespit sistemleri ve zayıflık inceleme araçları gibi yöntemler dijital pazarlama alanındaki işletmelerin karşılařtığı risklere karşı savunma mekanizmalarını güçlendirebilir (Tablo 3). Bu yöntemler, siber güvenliđi sağlamak için kritik öneme sahiptir ve dijital pazarlama faaliyetlerini sürdüren işletmelerin bu araçları etkin bir řekilde kullanması gerekmektedir.

Tablo-3: Savunma Mekanizmaları

Tedbir/Yöntem	Açıklama
Şifreleme	Düz metinleri şifreli hale getirerek yalnızca yetkililerin erişimine açar.
Antivirüs Yazılımları	Virüsleri tespit edip, önleyerek sistemleri koruyan yazılımlardır.
Güvenlik Duvarı (Firewall)	Ağ trafiğini kontrol ederek güvenlik politikalarına göre denetim sağlar.
Sayısal İmza	Elektronik belgelerin gönderici ve alıcısını doğrulayan, belgelerin güvenilirliğini artıran bir sistemdir.
Özel Sanal Ağlar (VPN)	İnternet üzerinden güvenli iletişim sağlayarak verileri şifreleyip korur.
Vekil Sunucular (Proxy)	İki ağ arasında dolaylı geçiş sağlayarak güvenliğini artırır.
Saldırı Tespit Sistemleri	Sistem aktivitelerini analiz ederek güvenlik zaafalarını tespit eden ve alarm veren sistemlerdir.
Zayıflık İnceleme Araçları	Sistem ve ağların güvenlik zayıflıklarını belirleyip analiz eden araçlardır.

Dijital pazarlama süreçlerinde karşılaşılan siber güvenlik tehditleri, kötü amaçlı yazılımlar, kimlik hırsızlığı, veri ihlalleri, DDoS saldırıları ve oltalama gibi çeşitli saldırı türlerini içermektedir. Bu tehditler, işletmelerin müşteri verilerini, finansal bilgilerini ve marka itibarını riske atabilir. Dijital pazarlama profesyonellerinin bu tür saldırılara karşı proaktif bir yaklaşım benimsemesi ve siber güvenlik stratejileri geliştirmesi büyük önem taşımaktadır. Güçlü şifreleme, antivirüs yazılımları, güvenlik duvarları, VPN kullanımı ve düzenli sistem güncellemeleri gibi yöntemlerle bu tehditlere karşı etkili koruma sağlanabilir. Ayrıca, özellikle küçük ve orta ölçekli işletmelerin (KOBİ'ler) sınırlı kaynaklarla bu tür önlemleri almaları hem marka güvenliğini hem de müşteri güvenini sağlamak açısından kritik bir öneme sahiptir. Dijital pazarlamanın sürdürülebilirliği için siber güvenlik, işletmelerin stratejik bir parçası haline gelmelidir.

3.3. Yapay Zekâ (YZ) Teknolojilerinin Dijital Pazarlamada Siber Güvenlik Üzerindeki Etkisi ve Rolü

Günümüzde YZ, neredeyse hayatımızın hemen her alanını dönüştüren bir teknoloji olarak dijital pazarlama süreçlerinde de siber güvenliği önemli ölçüde dönüştüren bir teknoloji olarak öne çıkmaktadır. Özellikle dijital pazarlamada güvenliği artırma ve tehditlere karşı hızlı yanıt verme kapasitesini geliştirme noktasında YZ, kritik bir rol oynamaktadır. YZ'nin siber güvenlik alanına entegrasyonu, tehdit tespiti ve yönetimi konusunda önemli avantajlar sağlamaktadır (Şenyapar, 2024). Dijital pazarlama alanında YZ teknolojileri, kullanıcıların çevrimiçi davranışlarını analiz ederek anomali tespiti yapabilir ve bu sayede potansiyel tehditlere karşı önceden uyarı vererek müdahalede bulunabilir. Bu durum, şirketlere olası saldırılara karşı daha hızlı ve etkili yanıt verme imkânı tanır. YZ'nin sunduğu bu çözümler, dijital pazarlama stratejilerinin güvenli bir ortamda yürütülmesini sağlayan altyapıyı güçlendirmek için de önemli fırsatlar sunmaktadır. YZ teknolojilerinin, siber güvenlik tehditlerini öngörme ve yönetme becerisi, dijital pazarlamanın gelecekte karşılaşılabileceği risklere karşı hazırlıklı olmayı mümkün kılmaktadır. Bu alandaki gelişmeler, özellikle mobil bankacılık, IoT uygulamaları ve mobil uygulamalar gibi dijital pazarlama bileşenlerinde makine öğrenimi ve YZ'nin etkili kullanımını göstermektedir (Krishen ve diğ., 2021). YZ, bu teknolojilerin kullanımıyla şirketlere müşteri etkileşimlerini daha iyi analiz etme ve güvenlik açıklarını daha etkin bir şekilde tespit etme yeteneği sunmaktadır.

Bir diğer önemli gelişme ise dijital pazarlamanın siber güvenlik risklerine karşı direnç kazanması için YZ'nin sunduğu makine öğrenimi ve YZ destekli analizlerdir. Şirketlerin dijital

platformlarda daha güvenli bir ortam yaratabilmesi için bilgi teknolojileri altyapılarını güçlendirmeleri gerektiđi vurgulanmaktadır (Ansari ve diğ., 2022). YZ'nin dijital pazarlama stratejilerinde ve siber güvenlik önlemlerinde kullanılmasının, veri güvenliđini sağlamada büyük katkı sunduđu bir gerçektir. Bu teknoloji, yalnızca siber tehditlere karşı daha dayanıklı olmayı deđil, aynı zamanda veri hırsızlıđı gibi kritik konularla mücadele etmek için de önemli bir araçtır (Buhas ve diğ., 2024). Nalbant ve Aydın (2024)'a göre, dijital pazarlamada YZ'nin sunduđu avantajlar arasında yüksek veri toplama ve analitik kapasitesiyle potansiyel müşterileri daha doğru bir şekilde belirleyebilme imkânı bulunmaktadır. Bu durum, dijital pazarlama stratejilerinin etkinliđini artırırken, kullanıcı deneyimlerini iyileřtiren sanal asistanlar gibi teknolojilerin de önünü açmaktadır. Ancak, bu avantajlara rađmen internet erişimi sınırlı olan bölgelerde yařanan sorunlar ve dijital pazarlamanın gerçek satışlarla ilişkisinin belirsizliđi gibi dezavantajlar da mevcuttur. YZ'nin dijital pazarlama süreçlerinde siber güvenliđi sağlamadaki rolü oldukça büyüktür. Bu teknoloji hem güvenlik tehditlerini tespit etme hem de bu tehditlere karşı stratejik yanıtlar geliştirme konusunda önemli fırsatlar sunmaktadır. Ancak, YZ'nin bu faydaları sađlarken, aynı zamanda dijital pazarlamanın gerçek satışlarla olan ilişkisini netleřtirmek ve internet erişiminde yařanan zorlukları aşmak için dikkatli bir entegrasyon süreci gereklidir. řirketlerin, YZ teknolojilerini kullanarak güvenlik önlemlerini güçlendirmeleri, dijital pazarlama stratejilerinin etkinliđini artırırken siber riskleri de en aza indirecektir.

YZ, dijital pazarlama süreçlerinde siber güvenliđi dönüřtüren önemli bir teknoloji olarak öne çıkmaktadır. YZ, siber tehditlerin tespiti ve yönetimi konusunda büyük avantajlar sunarak řirketlerin potansiyel saldırılara karşı daha hızlı ve etkili yanıtlar vermesini sađlar. YZ, kullanıcı davranışlarını analiz etme yeteneđi sayesinde tehditleri önceden tespit etme imkânı tanır, böylece dijital pazarlama stratejilerinin güvenli bir ortamda uygulanmasını garanti eder. YZ'nin sunduđu makine öğrenimi ve analitik yetenekler, veri güvenliđini artırırken aynı zamanda dijital pazarlamanın etkinliđini de güçlendirir. Ancak, YZ'nin bu avantajları sađlarken internet erişimi sınırlı bölgelerde yařanan sorunlar ve dijital pazarlamanın gerçek satışlarla ilişkisinin net olmaması gibi zorluklarla da karşılaşmaktadır. YZ, dijital pazarlama alanında siber güvenliđi artırmada kritik bir rol oynamaktadır ve bu teknoloji, řirketlerin dijital pazarlama stratejilerinde karşılaşılabilen risklere karşı daha hazırlıklı olmalarını sađlar.

3.4. Dijital Pazarlama Stratejilerinin Ulusal Ekonomiye Etkileri

Dijital pazarlama stratejileri, řetmelerin küresel pazarlarda başarılı olabilmesi için kritik öneme sahiptir. Ancak bu stratejiler, yalnızca řetmeler deđil, ulusal güvenlik açısından da büyük bir rol oynamaktadır. Dijital platformlar, e-ticaret ve çevrimiçi hizmetler gibi sektörlerin gelişmesine olanak tanırken, bu sistemlerin güvenliđi, ülkenin ekonomik istikrarını doğrudan etkileyebilir. Dijital pazarlama faaliyetlerine yönelik siber saldırılar, finansal verilerin çalınması, e-ticaret platformlarının çökmesi gibi durumlarla ulusal ekonomiye ciddi zararlar verebilir. Ayrıca, dijital pazarlamanın devletin dijital altyapılarıyla iç içe geçmesi, ulusal güvenlik açısından yeni riskler yaratmaktadır. Kamu hizmetlerine yönelik siber saldırılar, toplumsal huzursuzluklara ve kamu düzeninin bozulmasına yol açabilir. Dijital pazarlama stratejilerinin ulusal güvenlik üzerindeki etkisi, özellikle devlet destekli dijital platformların siber saldırılara karşı savunmasız olmasıyla daha belirgin hale gelmektedir. Bu sistemlere yönelik güvenlik ihlalleri, kamu hizmetlerine erişimi engelleyebilir ve ulusal güvenliđi tehdit edebilir. Dijital pazarlama stratejilerinin ulusal ekonomi ve güvenlik üzerindeki bu etkisi, dijital ekonominin gelişimi ve ulusal siber güvenlik stratejilerinin önemini de ortaya koymaktadır. Huzaizi ve diğ. (2021) tarafından yapılan çalışmada, girişimcilerin işlerini yönetirken iyi siber güvenlik bilgisine sahip olmanın, doğru uygulamaları oluşturabilmek için hayati önem taşıdıđı

sonucuna varılmıřtır. Bu durum, dijital pazarlamada siber güvenlik aısından zellikle veri koruma, müşteri güvenlięi ve marka itibarını saęlamada kritik bir rol oynamaktadır.

Dijital dönüşüm çağında, dijital ekonominin büyümesi, ülkelerin siber tehditlere karşı korunmasını saęlamak ve dijital ekonominin sürekli büyümesini desteklemek aısından kritik öneme sahiptir (Teoh ve Mahmood, 2017). Ayrıca, büyük veri ve YZ teknolojileri dijital pazarlama stratejilerinde kullanılırken, kötü niyetli kişiler tarafından ele geçirilirse, ulusal güvenlięi tehdit eden bilgi manipölasyonları ve veri alınmalarına yol aabilir. Dijital ortamda ekonomik güvenlik, birey, toplum veya devletin sanal dünyada normal işleyişini sürdürebilmesi için gerekli güvenlik, istikrar ve öngörülebilirlięi saęlamanın yanı sıra, sanal ve gerçek dünyada zarar verebilecek faktörlerden korunmasını ifade eder (Digilina ve Bishenov, 2024). Bu bağlamda dijital pazarlama stratejilerinin ulusal ekonomi ve güvenlik üzerindeki etkileri de önemli bir konu haline gelmektedir. Dijital platformların ve e-ticaretin gelişmesiyle birlikte, bu sistemlerin güvenlięi, ülkelerin ekonomik istikrarını doğrudan etkileyebilir. Yüksek büyüme oranları gösteren dijital ekonomi, aynı zamanda bu sektörlerin siber tehditlere karşı savunmasız hale gelmesi riskiyle karşı karşıyadır. Türkiye’de 2023 yılında e-ticaret hacmi bir önceki yıla göre %115,15 artarak 1,85 trilyon Türk lirasına (77,89 milyar dolar) ulaşmış ve işlem sayısı %22,25 artarak 5,87 milyar adede çıkmıştır (T.C. Ticaret Bakanlığı, 2024). Bu büyüme, dijital ekonominin potansiyelini ve ulusal güvenliğe olan etkisini gözler önüne sermektedir. Dijital platformlar, e-ticaretin yanı sıra finansal verilerin güvenlięi ve siber saldırılara karşı korunma ihtiyacını da beraberinde getirmektedir. Yine de dijital ekonominin bu denli büyümesi, siber güvenlik stratejilerinin önemini de artırmaktadır. Bu noktada, dijital ortamda ekonomik güvenlięi saęlama sorununun, hükümetlerin önemli rol oynadığı bir mesele haline geldięi anlaşılmaktadır. Hükümetler, dijital çağda ekonomik güvenlięi saęlama konusunda merkezi bir rol oynarlar çünkü toplumsal irade ve hedeflere odaklanarak, toplumun dijital ortamda gelişim yönünü belirlerler (Digilina ve Bishenov, 2024). Savaş hali ve COVID-19 pandemisinin etkisiyle Ukrayna’da dijital pazarlama, sosyal-ekonomik ve politik krizlerin tetiklemesiyle ciddi şekilde destabilize olmuş ve Ukrayna’nın dijital pazarlama stratejileri ile küresel dijital teknolojilerle etkileşim becerilerini olumsuz yönde etkilemiştir (Dubovyk ve dię., 2022). Bu durum, dijital pazarlamanın ulusal ekonomi ve güvenlik üzerinde yaratabileceęi potansiyel riskleri gözler önüne seriyor ve dijital altyapıların ne kadar kritik hale geldięini göstermektedir. Ayrıca dijital pazarlama stratejilerinin ulusal ekonomi ve güvenlik üzerindeki etkisinin büyüklüğünü de ortaya koymaktadır. Dijital altyapıların korunması ve siber güvenlik önlemlerinin güçlendirilmesi hem işletmelerin hem de ulusal güvenliğin korunması aısından kritik öneme sahiptir.

4. Sonuç ve Öneriler

Bu çalışmada dijital pazarlama süreçlerinde bilgi güvenlięinin etkisi, rolü ve önemi incelenmiş ve dijital pazarlama profesyonellerine yönelik çeşitli öneriler sunulmuştur. Siber tehditler ve saldırılar, işletmelerin dijital platformlarda gerçekleřtirdięi pazarlama faaliyetlerini tehlikeye atabilir ve ciddi finansal zararlara yol aabilir. Bu nedenle dijital pazarlama profesyonellerinin siber güvenlik stratejilerini güçlendirmeleri, müşteri güvenlięini kazanmak ve marka itibarını korumak aısından büyük önem taşımaktadır. Araştırma, dijital pazarlama süreçlerinde karşılaşılan başlıca siber tehditlerin kötü amaçlı yazılımlar, kimlik hırsızlığı, veri ihlalleri ve DDoS saldırıları gibi çeşitli türlerde olduęunu ortaya koymaktadır. Ayrıca, Yapay Zekâ (YZ) teknolojilerinin dijital pazarlama alanında siber güvenlik tehditlerini tespit etme ve yönetme noktasında önemli avantajlar sunduęu görülmektedir.

Çalıřmada elde edilen bulgular dođrultusunda ařađıdaki öneriler getirilebilir:

- İřletmelerin Siber Güvenlik Stratejilerini Güçlendirmeleri: Dijital pazarlama profesyonelleri, siber tehditlere karřı daha proaktif bir yaklařım benimseyebilir. Bunun için güncel güvenlik yazılımları, güvenlik duvarları (firewall), antivirüs yazılımları ve řifreleme yöntemlerini kullanabilirler. Ayrıca, řirket içindeki çalışanlara yönelik siber güvenlik eğitimleri vererek insan hatalarını minimize etmeyi hedefleyebilirler.
- Yapay Zekâ (YZ) Teknolojilerinin Entegre Edilmesi: Dijital pazarlama süreçlerinde YZ'nin potansiyelinden faydalanmak, řirketlerin güvenlik tehditlerini erken tespit etme ve hızlı yanıt verme yeteneklerini artırabilir. YZ tabanlı makine öğrenimi sistemleri, dijital pazarlama faaliyetlerinde kullanıcı davranıřlarını analiz ederek anomali tespiti yapabilir ve potansiyel tehditlere karřı uyarılar sağlayabilir. Bu nedenle, YZ teknolojilerinin dijital pazarlama güvenlik stratejilerine entegre edilmesi önerilmektedir.
- Küçük ve Orta Ölçekli İřletmelerin (KOBİ) Siber Güvenlik Bilinçlenmesi: KOBİ'ler, dijital pazarlama süreçlerinde siber güvenlik önlemlerine daha fazla yatırım yaparak, güvenlik uzmanlarından destek alabilirler. Ayrıca, maliyet etkin alternatifler arasında bulut tabanlı güvenlik çözümleri gibi seçeneklere yönelerek dijital pazarlama güvenliklerini artırabilirler.
- Veri Gizliliđi ve Yasal Düzenlemelere Uyumluluk: Dijital pazarlamanın sürdürülebilirliđi, müşteri verilerinin güvenliđi ve gizliliđi ile doğrudan iliřkilidir. Bu nedenle, iřletmelerin veri gizliliđi yasalarına ve düzenlemelere uyum sağlamaları büyük önem tařır.
- Siber Güvenlik Kültürünün Yaygınlařtırılması: Siber güvenlik sadece teknik bir sorumluluk deđil, aynı zamanda organizasyonel bir kültürdür. İřletmeler, tüm çalışanlarını siber güvenlik konusunda bilinçlendirerek bu kültürü kurum genelinde yaygınlařtırabilirler.
- Uluslararası Standartlara Uygun Güvenlik Politikaları Geliřtirilmesi: Uluslararası pazarlarda faaliyet gösteren iřletmeler, dijital pazarlama stratejilerini uygularken global güvenlik standartlarına uygun politikalar geliřtirebilirler.
- Ulusal Güvenlik Testlerinden Geçmiř Yerli ve Milli Siber Güvenlik Teknolojilerinin Kullanımı: Dijital pazarlama sistemlerinde güçlü bir siber güvenlik çerçevesi oluřturulması gerektiđi ortaya çıkmıřtır. Ayrıca, yerli ve milli siber güvenlik teknolojilerinin kullanımı, yalnızca dijital pazarlama süreçlerinin güvenliđini artırmakla kalmaz, aynı zamanda ülke içindeki siber güvenlik ekosistemini güçlendirmeye ve yerli teknoloji üretimini teřvik etmeye katkı sağlar.

Sonuç olarak, dijital pazarlama sistemlerine yönelik siber tehditlere karřı alınacak önlemler ve stratejik yaklařımlar, dijital pazarlamanın sürdürülebilirliđi ve güvenliđi açısından kritik bir rol oynamaktadır. İřletmeler, dijital pazarlama profesyonelleri olarak siber güvenlik stratejilerini sürekli olarak güncelleyip geliřtirdiklerinde, dijital pazarlama ekosistemindeki riskleri minimize edebilir ve rekabet avantajı elde edebilirler.

Kaynakça

- Aiman A. H., Ahmad Tajuddin, S. N. A., Bahari, K. A., Manan, K. A., & Abd Mubin, N. N. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. *Asian Culture and History*, 13(2), 20.
- Akçacı, T., & Kurt, F. B. (2020). Online Süpermarket Alıřveriřinde Tüketici Güven Faktörü. *Dicle Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 10(20), 414-433.

- Akdemir, N., & Yenal, S. (2020). Card-not-present fraud victimization: A routine activities approach to understand the risk factors. *Güvenlik Bilimleri Dergisi*, 9(1), 243-268.
- Akhtar, S., Sheorey, P. A., Bhattacharya, S., & VV, A. K. (2021). Cyber security solutions for businesses in financial services: Challenges, opportunities, and the way Forward. *International Journal of Business Intelligence Research (IJBIR)*, 12(1), 82-97.
- Ansari, M. F., Dash, B., Sharma, P., & Yathiraju, N. (2022). The impact and limitations of artificial intelligence in cybersecurity: a literature review. *International Journal of Advanced Research in Computer and Communication Engineering*.
- Armstrong, G., Adam, S., Denize, S., & Kotler, P. (2014). *Principles of marketing*. Pearson Australia.
- Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions. *Electronics*, 12(6), 1333.
- Bucovetchi, O., & Vevera, A. V. (2024). Perspective Chapter: Organizational Resilience toward Managing Risks in Digital Marketing.
- Buhas, V., Ponomarenko, I., Bugas, V., Ramskyi, A., & Sokolov, V. (2021). Using Machine Learning Techniques to Increase the Effectiveness of Cybersecurity. *Cybersecurity Providing in Information and Telecommunication Systems II 2021*, 3188(2), 273-281.
- Chidukwani, A., Zander, S., & Koutsakis, P. (2022). A survey on the cyber security of small-to-medium businesses: challenges, research focus and recommendations. *IEEE Access*, 10, 85701-85719.
- Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. *Journal of Marketing Development and Competitiveness*, 11(1), 59-68.
- Cisco, U. (2020). Cisco annual internet report (2018–2023) white paper. Cisco: San Jose, CA, USA, 10(1), 1-35.
- Çetin, H., Gundak, İ., & Çetin, H. H. (2015). E-iřletme güvenliğı ve siber saldırılar üzerine bir arařtırma. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 6(2), 223-240.
- Çiftçi, H. (2013). Her yönüyle siber savaş. TÜBİTAK.
- Deiss, R., & Henneberry, R. (2020). *Digital marketing for dummies*. John Wiley & Sons.
- Desai, V., & Vidyapeeth, B. (2019). Digital marketing: A review. *International Journal of Trend in Scientific Research and Development*, 5(5), 196-200.
- Digilina, O. B., & Bishenov, A. S. (2024). Economic Security in the Digital Age. In *Development of International Entrepreneurship Based on Corporate Accounting and Reporting According to IFRS* (Vol. 33, pp. 155-162). Emerald Publishing Limited.
- Dubovyk, T., Buchatska, I., Zerkal, A., & Lebedchenko, V. (2022). Digital marketing in the condition of wartime posture in Ukraine. *International Journal of Computer Science and Network Security*, 22(7), 206-212.
- Ellis-Chadwick, F., & Chaffey, D. (2012). *Digital marketing: strategy, implementation and practice*. Pearson.

- Erođlu, C. (2023). İřletmelerin Maruz Kaldığı Siber Suçların Boyutu. *Güvenlik Bilimleri Dergisi*, 12(1), 69-96.
- Geetha, B. T., Usman, M., Randhawa, N., Pipliwal, L., Maheshwari, K., & Kapila, N. (2024, March). Revolutionizing the dynamics of digital marketing by including cybersecurity measures and safeguarding consumer data. In 2024 International Conference on Trends in Quantum Computing and Emerging Business Technologies (pp. 1-5). IEEE.
- Gülmüş, M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.
- Huzaizi, A. H. A., Tajuddin, S. N. A. A., Bahari, K. A., Manan, K. A., & Abd Mubin, N. N. (2021). Cyber-security culture towards digital marketing communications among small and medium-sized (SME) entrepreneurs. *Asian Culture and History*, 13(2), 1-20.
- Ilyas, G. B., Munir, A. R., Tamsah, H., Mustafa, H., & Yusriadi, Y. (2021). The influence of digital marketing and customer perceived value through customer satisfaction on customer loyalty. Pt. 2 J. Legal Ethical & Regul. Issues, 24, 1.
- Karasoy, H. A. (2022). Yeni Nesil Savaş ve Siber İstihbarat. *Güvenlik Bilimleri Dergisi*, 11(1), 223-240.
- Kirk, G., & Noguera, J. (2019). Strategic marketing and cybersecurity: The case of data breaches. *Issues in Information Systems*, 20(3).
- Krishen, A. S., Dwivedi, Y. K., Bindu, N., & Kumar, K. S. (2021). A broad overview of interactive digital marketing: A bibliometric network analysis. *Journal of Business Research*, 131, 183-195.
- Johnson, T. A. (Ed.). (2015). Cybersecurity: Protecting critical infrastructures from cyber attack and cyber warfare. CRC Press.
- Obitovich, K. M., & Utkirovna, E. S. (2023, December). Quantifying the Impact of Cyber Security Risks on Digital Marketing ROI: A Case Study Analysis. In International Conference on Next Generation Wired/Wireless Networking (pp. 387-397). Cham: Springer Nature Switzerland.
- Kaptan, S. (1995). Bilimsel araştırma teknikleri ve istatistik teknikleri. Rehber Yayınevi.
- Kaya, M. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri Dergisi*, 9(18), 145-181.
- Konyeha, S. (2020). Exploring cybersecurity threats in digital marketing. *NIPES-Journal of Science and Technology Research*, 2(3).
- Kumar, S., Pallathadka, H., & Pallathadka, L. K. (2022). An analysis of cyber security threats in digital marketing. *Journal of Critical Reviews*, 9(03), 85-94.
- Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, 81(1), 36-58.
- Nalbant, K. G., & Aydın, S. (2024). Geçmişten Günümüze Geleneksel Pazarlamadan Dijitalleşen Pazarlamaya Evrilen Süreçte Yapay Zekâ ve Metaverse Faktörleri. *Pazarlama ve Pazarlama Arařtırmaları Dergisi*, 17(2), 231-258.
- Rosário, A. T., & Dias, J. C. (2023). How has data-driven marketing evolved: Challenges and opportunities with emerging technologies. *International Journal of Information Management Data Insights*, 3(2), 100203.

- Rust, R. T. (2020). The future of marketing. *International Journal of Research in Marketing*, 37(1), 15-26.
- Schwieger, D., & Ladwig, C. (2022). Cyber Insurance Concepts for the MIS and Business Curriculum. *Information Systems Education Journal*, 20(5), 54-66.
- Simmonds, A., Sandilands, P., & Van Ekert, L. (2004). An ontology for network security attacks. In *Applied Computing: Second Asian Applied Computing Conference, AACC 2004*, Kathmandu, Nepal, October 29-31, 2004. Proceedings 2 (pp. 317-323). Springer Berlin Heidelberg.
- Stallings, W., & Brown, L. (2008). *Computer Security Principles and Practices* second edition.
- Suh, B., & Han, I. (2003). The impact of customer trust and perception of security control on the acceptance of electronic commerce. *International Journal of electronic commerce*, 7(3), 135-161.
- řengöl, O. (2017). 2 Saatte A'dan Z'ye Dijital Pazarlama. CERES Yayınları.
- řenyapar, H. N. D. (2024). Digital Marketing in the Age of Cyber Threats: A Comprehensive Guide to Cybersecurity Practices. *The Journal of Social Science*, 8(15), 1-10.
- T.C. Ticaret Bakanlığı. (2024, Ekim 19). Duyurular. <https://ticaret.gov.tr/duyurular>. Eriřim tarihi: Aralık 2024.
- Teoh, C. S., & Mahmood, A. K. (2017, July). National cyber security strategies for digital economy. In *2017 International Conference on Research and Innovation in Information Systems (ICRIIS)* (pp. 1-6). IEEE.
- Von Solms, R., Van Niekerk, J. (2013). From information security to cyber security. *computers & security*, 38, 97-102.
- Whitler, K. A., & Farris, P. W. (2017). The impact of cyber attacks on brand image: Why proactive marketing expertise is needed for managing data breaches. *Journal of Advertising Research*, 57(1), 3-9.