TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SPORDA SİBER GÜVENLİĞİN ÖNEMİ

Namık BEKAR

BEDEN EĞİTİMİ VE SPOR ANABİLİM DALI
DOKTORA TEZİ

DANIŞMAN
Doç. Dr. Velittin BALCI

ANKARA
2023

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SAĞLIK BİLİMLERİ ENSTİTÜSÜ

SPORDA SİBER GÜVENLİĞİN ÖNEMİ

Namık BEKAR

BEDEN EĞİTİMİ VE SPOR ANABİLİM DALI

DOKTORA TEZİ

DANIŞMAN

Doç. Dr. Velittin BALCI

ANKARA

2023

ETİK BEYAN

Ankara Üniversitesi

Sağlık Bilimleri Enstitüsü Müdürlüğü'ne

Doktora tezi olarak hazırlayıp sunduğum, "Sporda Siber Güvenliğin Önemi" başlıklı tez; bilimsel ahlak ve değerlere uygun olarak tarafımdan yazılmıştır. Tezimin hipotezi, tümüyle tez danışmanım ve bana aittir. Tezde yer alan deneysel çalışma tarafımdan yapılmış olup; tüm cümleler ve yorumlar bana aittir.

Yukarıda belirtilen hususların doğruluğunu beyan ederim.

Öğrencinin Adı Soyadı : Namık BEKAR

Tarih :

İmza :

KABUL VE ONAY

Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Beden Eğitimi ve Spor Anabilim Dalında Namık BEKAR tarafından hazırlanan
"Sporda Siber Güvenliğin Önemi" adlı tez çalışması aşağıdaki jüri tarafından
DOKTORA TEZİ olarak OYBİRLİĞİ / OY ÇOKLUĞU ile kabul / ret edilmiştir.
Tez Savunma Tarihi
07/07/2023

İmza
Gazi Üniversitesi
Jüri Başkanı

İmza
Ankara Üniversitesi
Üye

İmza
Ankara Üniversitesi
Üye

İmza
Ankara Üniversitesi
Üye

İmza
Üniversitesi
Üye

Tez hakkında alınan jüri kararı, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Yönetim Kurulu tarafından onaylanmıştır.

İÇİNDEKİLER

ÖNSÖZ

Sporda teknoloji kullanımı, teknolojinin hızla gelişmesiyle birlikte sporcuların performansını artırmak, hakem kararlarını desteklemek, antrenman ve veri analizi yapmak gibi amaçlarla gerçekleştirilmektedir. Türkiye'de spor alanında teknoloji kullanımı da giderek artmaktadır. Yalnız teknolojik yetkinlikler kendiliğinden oluşmamakta, devlet, üniversite, sektör gibi tüm tarafların ve bir çok sosyoekonomik faktörün etkisinde evrimsel gelişmeden etkilenmektedir. Teknolojinin hızla gelişmesiyle birlikte güvenliği de önemli hale gelmektedir. Spor alanında teknolojinin ilerlemesi birçok açıdan fırsatlar sunduğu gibi tehlikeler ve tehditler de barındırmaktadır. Bu çalışmanın temel amacı, Türkiye için önümüzdeki yıllar için siber güvenlik teknolojisi öngörüsünü gerçekleştirmek ve jenerik öngörü modeli olan bulanık öngörü ve SWOT çerçevesini uygulayarak Türkiye için spor sektöründe siber güvenlik öngörüsü ön sonuçlarına göre somut politika önerileri belirlemektir.

Doktora eğitimimi, köklü bir kurum olan Ankara Üniversitesi'nde tamamlamamın mutluluğunu yaşıyorum. Eğitimim boyunca kıymetli hocalarımın spor bilimlerindeki tecrübelerinden olabildiğince yararlanmaya ve kendime dersler edinmeye çalıştım. Öncelikle değerli önerileri ve yardımları için tez danışmanım Doç. Dr. Velittin BALCI'ya ayrıca tez izleme sürecindeki rehberlik ve destekleri için Prof. Dr. Bülent GÜRBÜZ ve Prof. Dr. Azmi YETİM'e şükranlarımı sunarım.Tüm eğitim hayatım boyunca dişini tırnağına takıp beni bu günlere getiren, her anımda yanımda olan, en değerli varlıklarım, eşim,ablam, babama ve anneme teşekkür ederim.

SİMGELER VE KISALTMALAR

AB	Avrupa Birliği
ABD	Amerika Birleşik Devletleri
ARBİS	TUBİTAK Araştırıcı Bilgi Sistemi
BTYK	Bilim Teknoloji Yüksek Kurulu
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BYOD	Bring Your Own Device
BYOK	Bring Your Own Key
CIA	Central Intelligence Agency
CSP	Cloud Service Provider
DOD	ABD Savunma Bakanlığı
DDoS	Distributed Denial of Service
FwaaS	Firewall as a Service
GNU	Generation Next Unix
GPL	General Public Licence
GSYIH	Gayri Safi Yurt İçi Hasıla
GSMH	Gayri Safi Milli Hasıla
IAM	Identity and Access Management
IDaaS	Identity as a Service
IEEE	International Association of Electric and Electronic Engineering
IGA	Identity Governance and Administration
IoT	Internet of Things
IPS	Intrusion Prevention System
IT	Information Technology
JSON	JavaScript Object Notation
KOBİ	Küçük ve Orta Büyüklükteki İşletmeler
NAC	Network Access Control
NFV	Network Functions Virtualization
NGFW	Next-Generation Firewall

NIST	National Institute of Standards and Technology
OOB	Out-of-Band
OTP	One Time Password
OTT	Over-the-Top
PC	Personal Computer
PKI	Public Key Infrastructure
SCIM	System for Cross-Domain Identity Management
SDN	Software-Defined Networking
SGE	Siber Güvenlik Enstitüsü
SMS	Short Message Service
SSO	Single Sign On
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UTM	Unified Threat Management
VPN	Virtual Private Network

ŞEKİLLER

ÇİZELGELER

1. GİRİŞ

Spor, belirli kurallar çerçevesinde doğası gereği bir mücadele ve rekabet gerektiren bir aktivitedir. Bu rekabetin seviyesi yükseldikçe ve karşılığında kazanılan şeyler değiştikçe sektörde şiddet ve saldırganlık durumu ortaya çıkmaktadır. Çünkü bu şekilde spor sadece sahada kalmamakta, müsabaka öncesi ve sonrasına taşmakta, insan hayatının diğer mekân ve zamanlarının da mevzuu olmaktadır (Kuş ve Biçer, 2022).

Spor belki de insanlık tarihi kadar eski bir olgudur. İnsanlar başlangıçta kendilerini korumak ve güçlü olmak için spora yönlenmişlerse de sonraları fazla enerjilerini atmak, sağlıklarını korumak, boş zamanlarını değerlendirmek, birbirleri ile yarışmak, kabiliyet ve üstünlüklerini göstermek ve para kazanmak gibi amaçlarla yapmaya başlamışlardır.

Spora olumlu ve olumsuz bakış açılarına göre farklı tanımlamalar getirilmektedir (Savaş, 1989). Sporu, "tek başına, toplu ya da takım halinde yapılan kendine özgü kuralları, teknikleri olan, bedensel ve zihinsel yetilerin gelişiminin sağlayan, eğitici, eğlendirici uğraşı" olarak tanımlarken, Fişek ise kitleleri uyutan bir 'afyon' olarak tanımlamaktadır (Fişek,1985). Zaman içerisinde spora yüklenen veya spordan beklenen anlamlar değişmiş, bu doğrultuda spor bir endüstri halini almış ve tarafları oyunculardan öteye geçmiştir.

Zaman içerisinde spora yüklenen veya spordan beklenen anlamlar değişmiş, bu doğrultuda spor bir endüstri halini almış ve tarafları oyunculardan öteye geçmiştir. Oluşan spor endüstrisi sadece oynayanları değil; kulüp, medya, taraftarlar, taraftar dernekleri, kulüp yöneticileri, çalıştırıcılar, diğer kulüp çalışanları, hakemler, ilgili devlet kurumları, destekleyici-şirketler, güvenlik güçleri, amigolar, siyasiler gibi (Arıkan ve Çelik, 2007:113) birçok birimi içerisine dâhil etmiştir. Spor endüstrisi ilerlerken aynı zamanda teknolojik gelişmeleri de yaşanmıştır. Spor teknolojileri ise büyüleyici bir şekilde değişen teknolojinin getirilerindendir. Sahada

olup biteni daha açık ve anlaşılabilir bir şekilde ekranlarımıza getiren bu sistemler son 20 yıl içinde büyük gelişmeler gösterdi. Bu geliştirilen teknolojiler sayesinde spor dünyasının kuralları bile değişime uğrayarak yeniden yazılmasına sebep olmuştur (Novak, 1993). Temel anlamda spor dünyasında önemli değişmelere sebep olan ve sporu ayrıntıları ile evimizde bize sunma imkânı oluşturan teknolojiler gün geçtikçe gelişme kaydetmiştir (Savaş, 2023).

Teknolojinin gelişmesiyle birlikte spor ve teknoloji günümüzde artık birbirine eş değer kavramlar haline gelmiştir (Van Der Slıkke, 2023). Sporda teknolojinin gelişmesi hem pazarlama hem yayın hayatında taraflara farklı imkanlar sunmuştur. Bu bakımdan spor güvenliğide önemli hale gelmiştir. Teknoloji kullanımı, spor endüstirisinde verilerin toplanması, analizi, depolonması ve paylaşması gibi birçok süreci kolaylaştırır. Teknoloji güvenliği sağlanması günümüzde artık siber güvenlik kavramı hayatımıza girmiştir. Spor teknolojisi ve güvenliği olarak adlandırılan ve içinde bilgisayar sistemleri, online iletişim ağları ve kontrol sürecinin bulunduğu bilgi iletişim teknolojilerinin kurduğu bu devasa sistem, küresel ölçekte sosyal, ekonomik, politik ve kültürel bütünleşmenin bir parçası olarak hızla gelişmektedir (Tunca, 2019). Siber güvenlik, verilerin toplanması, analizi ve depolanması sırasında gizlilik, bütünlük ve erişebilirlik gibi güvenlik prensipleri gözetilmektedir. Özellikle spor alanında kişisel sağlık bilgileri gibi hassas verilerin güvenliği büyük önem taşır. Spor alanında siber güvenlik önlemleri, yetkisiz erişimden korunmayı, veri kaybını önlemeyi ve verilerin doğru ve güvenilir olmasını sağlamayı hedefler.

1.1. Sporda Siber Güvenliğin Temelleri

Teknoloji, belli amaçlara ulaşmada, belli sorunları çözmede, gözleme dayalı ve kanıtlanmış bilgilerin uygulanmasıdır (Demirel, 1993). Teknolojik gelişmeler, her alanla olduğu gibi sporla da kuvvetli bir etkileşim halindedir. Spor, birçok teknolojik gelişmeye ilham kaynağı olurken; birçok noktada da gelişen teknolojiden faydalanmaktadır. Bilim, mühendislik ve modern bilgi teknolojisinin gelişmesi, sporun her seviyesine ve her branşına etki etmekte, yaşanan rekabetin, yaşanan

mücadelenin ve alınan hazzın artmasına katkı sağlamaktadır (Yıldız ve Algün, 2022). Artan rekabet artan ilgiye sebep olmakta, artan ilginin karşılanması adına da tesisleri, organizasyonları, yayınları, ekipmanları ve sportif performansları geliştirmek adına teknolojiden yararlanılmaktadır. Teknolojik koşullar sporu etkilemekte; sporun, sporcunun ve organizasyonların güçlenmesine katkı sağlamaktadır. Bu katkı, teknoloji ile sporun ayrılmaz iki bileşen haline gelmesini sağlamaktadır (Can ve ark., 2011). Gelinen bu noktada da mevcut rekabet koşullarında başarılı olabilmenin, sahip olunan teknolojik güçle yakından ilişkili olduğu kabul edilmektedir (Şimşek ve Deveci, 2018).

Sporda teknoloji kullanımı, sporcuların performansını artırmak, antrenman verimliliğini artırmak, sakatlanma riskini azaltmak, izleyicilere daha zengin deneyimler sunmak ve sporun genel yönetimini geliştirmek gibi amaçlarla kullanılır. Spor teknolojisi, farklı spor dallarında ve profesyonel, amatör düzeylerde geniş bir şekilde de kullanılmaktadır.

Spor endüstrisinin ilerlemesi, teknolojideki hızlı gelişmeler ve dijital dönüşümle büyük ölçüde etkilenmiştir (Zhang ve ark., 2021). Spor endüstrisi, her yıl milyarlarca dolarlık bir pazar haline gelmiştir ve bu büyüme büyük ölçüde teknolojinin spor alanına entegrasyonu ile desteklenmiştir. Spor endüstrisinin ilerlemesinde teknolojinin rolünde örneklerden biride sporcu performansı ve sağlığında kullanılan giyilebilir cihazlar ve sensörler olabilir. Sporcuların performansını takip etmeye ve sağlık durumlarını izlemeye yardımcı olur. Bu veriler, antrenörlerin ve tıbbi personelin daha iyi kararlar almasına yardımcı olurken, sporcuların performansını artırır ve sakatlanma riskini azaltır.

Spor endüstirisi teknoloji birlikte Yeni İzleyici Deneyimleri: Teknoloji, izleyicilere oyunları ve etkinlikleri izleme şeklini değiştirdi. Sanal gerçeklik (VR) ve artırılmış gerçeklik (AR) gibi teknolojiler, izleyicilere daha etkileşimli ve immersif deneyimler sunar.Medya ve Yayınlar: Yayıncılık alanında teknolojik gelişmeler, spor etkinliklerinin daha geniş kitlelere ulaşmasına olanak tanır. Yüksek çözünürlüklü yayınlar, 360 derece kameralar ve çevrim içi yayın platformları, sporun daha

erişilebilir ve izlenebilir hale gelmesini sağlar.E-spor ve Dijital Sporlar: E-spor, geleneksel spor etkinliklerine kıyasla dijital platformlarda düzenlenen rekabetçi oyunlar ve turnuvalardır. Teknolojinin bu alandaki ilerlemesi, e-sporun hızla büyümesine ve milyonlarca kişiye ulaşmasına olanak sağlamıştır. Spor Yönetimi ve Veri Analitiği: Büyük veri analitiği ve yapay zeka, spor endüstrisindeki yönetim süreçlerini optimize etmeye yardımcı olur. Bilet satışı, pazarlama stratejileri ve taraftar katılımı gibi alanlarda veri analizi, daha etkili kararlar almayı sağlar. Sponsorluk ve Pazarlama: Teknoloji, sporcular ve takımlar arasında yeni sponsorluk fırsatları yaratırken, dijital pazarlama ve sosyal medya platformları, spor markalarının taraftarlarla etkileşimini artırmalarına yardımcı olur.Genel olarak, spor endüstrisi teknolojinin etkisiyle sürekli olarak değişmekte ve gelişmektedir. Bu teknolojik ilerlemeler, sporcuların performansını artırırken, izleyicilere daha etkileyici deneyimler sunar ve spor endüstrisinin daha geniş kitlelere ulaşmasını sağlar.

Siber güvenlik, bilgisayar sistemlerinin, ağların ve dijital ortamların siber tehditlere karşı korunması için alınan önlemleri ve uygulanan güvenlik politikalarını ifade eder. Siber güvenlik, bilgisayarlar, sunucular, ağlar, mobil cihazlar, yazılımlar ve diğer dijital sistemlerin kötü niyetli saldırılardan, veri ihlallerinden ve zararlı yazılımlardan korunmasını hedefler.

Siber güvenlik, bilgi güvenliği, ağ güvenliği, veri güvenliği ve sistem güvenliği gibi farklı alanları içerir. Temel olarak, siber güvenlik, siber saldırılara karşı korunma, siber tehditlerin tespit edilmesi, önlenmesi ve bunlara müdahale edilmesini içeren bir dizi teknik, yöntem ve süreçlerden oluşur.

Siber güvenlik, aşağıdaki amaçları gerçekleştirir:

Varlık Koruma: Bilgi, veri, sistemler ve diğer dijital varlıkların yetkisiz erişim, değişiklik veya yok olmaktan korunması.

Veri Gizliliği: Hassas ve kişisel verilerin yetkisiz kişilerin eline geçmesini engelleme.

Hizmet Sürekliliği: İş süreçlerinin, sistemlerin ve hizmetlerin kesintiye uğramadan çalışmasını sağlama.

Tehdit Tespiti: Potansiyel saldırıları, zayıflıkları ve diğer güvenlik açıklarını tespit etme.

Tehdit Önleme: Saldırıları engellemek için güvenlik önlemleri ve politikalarının uygulanması.

Olay Müdahalesi: Saldırıların tespit edilmesi durumunda hızlı ve etkili bir şekilde müdahale etme.

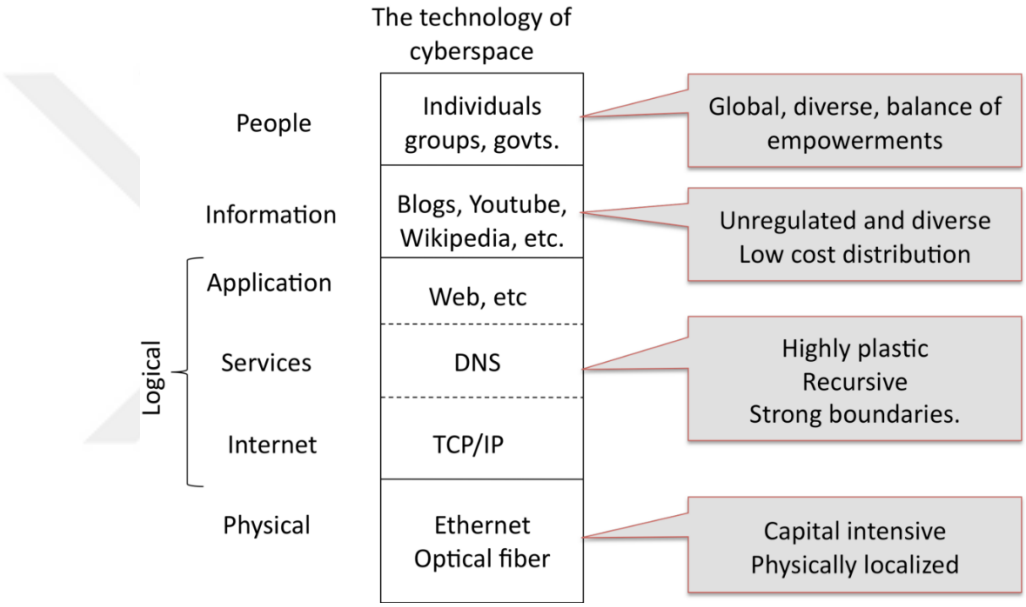
Siber güvenlik, bireylerin, kurumların, hükümetlerin ve toplumun dijital dünyadaki güvenliğini sağlamak için önemlidir. Güvenli bir dijital ortam, veri gizliliği, siber saldırılardan korunma ve siber suçların önlenmesi açısından kritik bir unsurdur.

Siber uzay, bilgisayar sistemlerinin, ağların ve dijital ortamların birbiriyle bağlantılı olduğu, elektronik iletişimin gerçekleştiği sanal bir ortamdır. İnternet, bilgisayar ağları ve diğer iletişim ağları üzerindeki dijital etkileşimleri ifade eder. Siber uzay, bilgi alışverişi, veri transferi, iletişim, ticaret, eğlence ve daha birçok faaliyetin gerçekleştiği dijital dünyayı kapsar.

Siber güvenlik ise, siber uzayda yer alan bilgisayar sistemlerini, ağları ve dijital ortamları tehditlere karşı korumak için alınan önlemleri içerir. Siber güvenlik, siber saldırılara, veri ihlallerine, kötü niyetli yazılımlara ve diğer siber tehditlere karşı koruma sağlar. Siber uzayda gerçekleşen iletişim, veri aktarımı ve diğer faaliyetlerin güvenliğini sağlamayı amaçlar.

Siber güvenlik, siber uzayın güvenli ve güvenilir bir ortam olmasını sağlamak için teknik, organizasyonel ve politik önlemleri içerir. Bu önlemler, güvenlik yazılımları ve donanımları, şifreleme, kimlik doğrulama, güvenlik protokolleri, güvenlik politikaları, eğitim ve farkındalık gibi çeşitli unsurları içerir.

Dolayısıyla, siber güvenlik, siber uzaydaki bilgisayar sistemlerini, ağları ve dijital ortamları tehditlere karşı korurken, siber uzayda gerçekleşen iletişim, veri aktarımı ve diğer faaliyetlerin güvenliğini sağlar.



Şekil 1.3. Siber Uzay Modeli (Clark, D. 2014).

Yukarıda Şekil 1.1'de belirtilen David Clark'ın siber uzay bileşenlerini İnsanlar,Bilgi, Mantıksal ve Fiziksel katmanlardan oluşturmuş. Katmanlar arası alışveriş ve etkileşim söz konusudur.

Spor, günümüzde büyük bir dijital dönüşüm yaşamaktadır ve bu da siber güvenlik konusunu önemli hale getirmektedir. Spor organizasyonları, takımlar, sporcular ve taraftarlar arasındaki iletişim ve veri paylaşımı giderek dijitalleşmektedir. Bu nedenle, sporun siber güvenlikteki yeri giderek artmaktadır. İşte sporun siber güvenlikteki rolü ve önemli konular:

Veri Güvenliği: Spor organizasyonları, takımlar ve sporcular, büyük miktarda veriye sahiptir. Bu veriler, oyuncu istatistikleri, performans analizleri, taktiksel bilgiler, finansal bilgiler, taraftar verileri ve daha fazlasını içerebilir. Bu verilerin gizliliği, bütünlüğü ve erişilebilirliği, siber güvenlik önlemleri ile korunmalıdır.

İş Sürekliliği: Spor organizasyonları ve takımları, teknolojiye dayalı altyapıları ve sistemleri kullanarak işlerini yürütür. Bu sistemlerin, maç yayınları, bilet satışı, veri analizi, pazarlama ve diğer faaliyetlerin kesintisiz devam etmesi için güvende olması gerekmektedir. Saldırılara karşı dirençli bir iş sürekliliği planı, siber güvenliğin önemli bir parçasıdır.

Taraftar Güvenliği: Spor organizasyonları, taraftarların dijital platformlar üzerinden maç izlemelerine, bilet satın almalarına, takımlarıyla iletişim kurmalarına ve sosyal medya üzerinden etkileşime geçmelerine olanak sağlar. Bu iletişim kanallarının güvenliği, taraftarların kişisel verilerinin ve finansal bilgilerinin korunması açısından kritiktir.

Fikri Mülkiyet ve Ticari Haklar: Spor organizasyonları, sponsorluk anlaşmaları, yayın hakları ve diğer ticari haklar üzerinde çalışır. Bu ticari hakların siber saldırılara karşı korunması ve izinsiz erişimden korunması önemlidir. Fikri mülkiyetin ve ticari hakların siber güvenlik önlemleri ile güvence altına alınması gerekmektedir.

Rekabet ve Manipülasyon: Spor dünyasında rekabet ve maç sonuçlarının manipülasyonu gibi sorunlar siber güvenlik konularını da içerir. İlgili tarafların, maç sonuçlarını veya diğer önemli bilgileri manipüle etmesini engellemek için siber güvenlik önlemleri alınmalıdır.

Spor dünyası, siber güvenlik tehditlerine karşı hazırlıklı olmalı ve güvenliğin sağlanması için uygun teknik ve organizasyonel önlemleri almalıdır. Bu, veri

güvenliği, ağ güvenliği, güvenlik eğitimi, izleme ve olay müdahalesi gibi alanları içeren kapsamlı bir siber güvenlik stratejisi gerektirir.

Şekil 1.2. Bilgi Güvenliği Anahtar Kavramları.

Spor alanında gizlilik, bütünlük ve erişebilirlik, siber güvenlik kavramlarıyla ilişkilendirilen temel değerlerdir. İşte bu değerlerin spor alanındaki anlamları:

Gizlilik (Confidentiality): Gizlilik, spor organizasyonları, takımlar, sporcular ve taraftarlar arasında paylaşılan bilgilerin gizli kalmasını sağlama prensibidir. Özel bilgilerin yetkisiz kişiler tarafından erişilmesini önlemek ve bilgilerin sadece ilgili kişilerin bilgisi dahilinde tutulmasını sağlamak, gizlilik değerinin önemli bir parçasıdır. Örneğin, oyuncu istatistikleri, taktiksel bilgiler, finansal bilgiler ve taraftar verileri gizlilik gerektiren bilgilerdir.

Bütünlük (Integrity): Bütünlük, spor alanında verilerin doğruluk, eksiksizlik ve değiştirilmemişlik durumunu ifade eder. Veri bütünlüğü, verilerin yetkisiz değişikliklere veya manipülasyonlara karşı korunmasını sağlar. Spor alanında bütünlük, özellikle skorlar, istatistikler, hakem kararları ve diğer önemli verilerin doğruluğunu ve güvenilirliğini sağlamak için önemlidir.

Erişebilirlik (Availability): Erişebilirlik, spor organizasyonları ve taraftarlar için bilgilere ve hizmetlere sorunsuz ve kesintisiz bir şekilde erişimi sağlama

prensibidir. Spor organizasyonlarının web siteleri, uygulamaları, bilet satış sistemleri, canlı yayınlar gibi hizmetlerin sürekli olarak kullanılabilir olması, erişebilirlik değerinin bir parçasıdır. Ayrıca, saldırılar veya diğer kesintiler durumunda hızlı bir şekilde sistemlerin tekrar kullanılabilir hale getirilmesi de erişebilirlik önemli bir unsurdur.

Bu değerler, spor alanında siber güvenlik stratejilerinin temelini oluşturur. Gizlilik, bütünlük ve erişebilirlik değerlerinin korunması, spor organizasyonlarının ve taraftarların güvenliğini ve güvenini sağlamak için önemlidir.

1.2. Amaç ve Gerekçe

Sporda yaygın teknoloji kullanımı, oyunları kaydetmek ve daha sonra dünya çapında anında yayınlamak için video kameraların entegrasyonu ile başladı. Yayın teknolojisi geliştikçe, takımlar ve oyuncular atletik performansı öğrenmek ve geliştirmek için videoları kullanmaya başladılar. Hakemler, aramaların geçerliliğini sağlamak için anlık tekrarları kullanmaya başladı ve MLB yayınları, grev bölgesini sanki gerçek dünyada varmış gibi ekranda göstermeye başladı. Ve şimdi, 21. yüzyılda, teknoloji sporda çok daha fazlasını yapmak için kullanılıyor.

Spor organizasyonları, bireysel sporcular hakkında hızlanma, kalp atış hızı ve uyku gibi verileri toplamaya başladı. Bu veriler, her zamankinden daha bireysel kılavuza daha yakın: Beyzbolda Kazanılan Koşu Ortalaması ve temel yüzde gibi istatistikler doğrudan oyun oynamakla ilgili olsa da, bu yeni veriler elektronik bir tıbbi kayıt işlevi görüyor ve performansı iyileştirmeyi ve yaralanmaları azaltmayı amaçlıyor. Ayrıca, Amerikan futbol kasklarındaki potansiyel sarsıntıları algılayan sensörler gibi tıbbi cihazlar sadece yaralanmaları önlemekle kalmaz, aynı zamanda hayat kurtarır.

Son on yılda büyük verinin patlaması, profesyonel sporcular gibi kamuya mal olmuş kişilerin özel bilgilerinin paylaşılmasının etiği üzerine bir tartışmayı ateşledi.

Sporcular artık medyada azalan mahremiyete ve organizasyonları veya takımları tarafından artan izlemeye tabidir ve bu nedenle çalışanlar yerine ticari mallar olarak ele alınabilir (Sanderson, 2009). Bazı sporcular bu tür izleme konusunda rahat olsa da, spor organizasyonları bireysel sporcular hakkında verileri ne ölçüde izlediklerini ve paylaştıklarını sporcularına her zaman net bir şekilde iletmezler (Evans, 2017).

Cihazlar ve veriler daha yaygın ve kullanışlı hale geldikçe, bu cihazların güvenliği ve ilişkili verilerin saklanması, sporcuların mahremiyeti ve güvenliği ve spor organizasyonlarının başarısı için çok önemlidir. Daha fazla veri elde edilirken, veri sistemlerini denetlemeye devam etmek, potansiyel ihlalleri izlemek ve başta sporcular olmak üzere tüm tarafları, verilerinin kullanımı ve dağıtımı ile ilgili hakları ve sorumlulukları hakkında bilgilendirmek önemlidir. Bu teknolojilerin kullanımı büyük faydalar sağlar, ancak bunların yanında riskler ve sorumluluklar da gelir.

Bu çalışmanın temel amacı, Türkiye için önümüzdeki yıllar için siber güvenlik teknolojisi öngörüsünü gerçekleştirmek ve jenerik öngörü modeli olan bulanık öngörü ve SWOT çerçevesini uygulayarak Türkiye için spor sektöründe siber güvenlik öngörüsü ön sonuçlarına göre somut politika önerileri belirlemektir.

1.3. Problemler

Sporda güvenliğin, yalnızca profesyonel sporlarla uğraşan sporcular ve çalışanlar için değil, herkes için etkileri vardır. Yeni teknolojilerden gelen veriler spor performansını artırabilirken, bu verilerin saklanması ve iletilmesiyle gelen gizlilik ve güvenlik endişeleri, yönetmelikler ve standartlar aracılığıyla topluluk tarafından tam olarak ele alınmamıştır. Hassas verilerin bilgisayar korsanları tarafından kamuya açıklanması, sporcuların, kuruluş üyelerinin yaşamlarını ve bilet satışları ile spor bahislerini çevreleyen pazarları etkileme potansiyeline sahiptir. Akıllı saatlerin ve diğer giyilebilir cihazların popülaritesi arttıkça, büyük şirketlerin depoladığı bireysel çalışan verilerinin artan miktarı büyük ölçüde artacaktır. Bu

nedenle, profesyonel sporcuların mahremiyetiyle ilgili etik tartışması, iş gücündeki çalışanlar için de aynı tartışmayı bilgilendirecektir.

Spor bilimlerinde verilerin aslında barından ortam siber uzaydır. Siber uzay, bireyler, kuruluşlar ve devletler dahil olmak üzere tüm aktörleri birbirine bağlayan sınırsız bir ortamdır. Siber uzaya artan ve hızlanan güven nedeniyle siber uzayın güvenliği öncelikli bir konu haline geliyor. Siber uzaydaki riskler ve tehditlerle mücadele etmek ve siber uzaydan yararlanma yeteneğini korumak için, siber güvenliğe yönelik politikalar, stratejiler ve planlar geliştirmek hayati önem taşır. (Akkuş, 2013).

Literatür taramasına ve halka açık siber güvenlik stratejilerinin analizine dayanarak, ülkeler siber güvenlik alanı için nadiren öngörü metodolojileri uygulamaktadır. Ayrıca Delphi tabanlı öngörülerde siber güvenlik bir ana alan ya da tema olarak ele alınmamış, Japonya'nın 10. Öngörü Çalışması (Ogasawara, 2015) gibi siber güvenlik konularının sadece bir kısmı ICT alanı altında ele alınmıştır. Bazı durumlarda, yalnızca Nesnelerin İnterneti ve Avrupa Birliği içindeki bakım görevlerinin uyumlaştırılmasının ele alındığı European Foresight Cybersecurity gibi siber güvenlik öngörü tatbikatlarında yalnızca sınırlı siber güvenlik konuları ele alınmıştır (Siber Güvenlik Konseyi, 2016).

Türkiye'de siber güvenlik konularına devlet kademesinde 15 yılı aşkın bir süredir önem verilmekte olup e-Dönüşüm Türkiye Projesi ile 2003 yılına kadar resmi başvuruların ve aksiyonların başlatıldığı söylenebilir (Çifci, 2017). Daha sonra günümüze kadar birçok çalışma yapılmıştır. Siber güvenlikle ilgili en belirgin ve önemli adım, Türkiye Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014 (Ulaştırma ve Altyapı Bakanlığı, 2012) ve Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019'dur (Ulaştırma ve Altyapı Bakanlığı, 2016). Söz konusu stratejilerin ve eylem planlarının metodolojisi, kamu kurumlarını, kritik altyapı işletmecilerini, BİT sektörünü, üniversiteleri ve sivil toplum kuruluşlarını temsil eden kurum ve kuruluşlardan uzmanlarla toplantılar, çalıştaylar, seminerler ve konferanslar düzenlemekti (Şentürk ve ark., 2012), öngörü metodolojilerinden yoksundur. Ayrıca

hiçbir çalışma spor sektörüne değinmemiştir. Ama sporun günümüzde etkisi toplumsal sonuçlar doğrulmaktadır. İnsan topluluklarını millet yapan kültür unsurlarından biri de spordur. Spor kişisel olduğu kadar sosyal bir olaydır (Güven, 1992). Toplumların devamında, kültürlerinin korunması, kendilerini geliştirebilmeleri için başka yöntem, metot ve araçlar olduğu kadar spor ve sportif faaliyetler de etkili olmuştur. Topluma yön veren bir çizgisi olduğu ve topluma etkisi düşünüldüğünde nasıl bir savaş ve yokluk kadar etkisi siber savaşın savunma sanayisi kadar etkisi olmasa bir spor organizasyonda ve işletmeye saldırıları çok büyük etkileri olacaktır.

1.4. Araştırmanın Önemi

Günümüzün dijital dünyasında ekonomi, bilimsel faaliyetler, ticaret, iletişim ve sosyal yaşam, kötü niyetli aktörler tarafından hedef alınan "siber uzay" adı verilen ağ bağlantılı bir altyapı aracılığıyla birbirine bağlıdır (Sertçelik, 2015). Birbirine bağlı dünyada yıkıcı ve hatta yıkıcı siber saldırı tehlikesi büyüyor. Siber güvenlik, ulus devletlerin daha geniş ulusal güvenlik stratejilerindeki ana güvenlik endişelerinden biridir. Yeni teknolojik gelişmelerin siber güvenlikle ilgili uzun vadeli, stratejik yaklaşımlara ihtiyaç olduğu kabul edilmektedir (Siber Güvenlik Konseyi, 2016).

Kuruluşlar, şirketler, ortaklar, müşteriler ve rakipler tarafından mahçup olmamak, itibarlarını kaybetmemek ve dava edilmemek için veri ihlali olaylarını gizler. Bu işletmelerinden biride spor faaliyet ve kuruluşlardırçBununla birlikte siber saldırıların dünya çapında yüz milyarlarca dolarlık zarara yol açtığı farklı kaynaklar tarafından söyleniyor. IBM Security ve Ponemon Institute'un "2018 Cost of Data Breach Study" çalışmasına göre, dünyadaki bir veri ihlalinin spor kamuoyuna ortalama maliyeti 3,86 milyon ABD dolarıdır bu rakam 2017'ye göre %6,4 artış gösteriyor. (IBM, 2018) Veri ihlali maliyetleri, tarihindeki en yüksek ortalama toplam maliyet olan 2021'de 3,86 milyon dolardan 4,24 milyon dolara yükseldi (IBM, 2022). Veri ihlali olayları günümüzde giderek artmaktadır.

Bilişim ve iletişim teknolojilerinin günlük hayattan en kritik askeri sistemlere kadar her alanda kullanılmasıyla birlikte siber uzayın korunması ulus-devletlerin ulusal güvenliğinin önemli unsurlarından biri haline gelmiştir (Çifci, 2017). Günümüzde spor da aslında bu unsurlardan biridir. Sporun birleştirici bir rolü olduğu toplumu ve kültürüde temsil ettiğide mevcuttur. Dünyanın her yanında spor, ulusal ve uluslararası örgütler tarafından kontrol edilmektedir. Bu örgütler kuralları belirler, organizasyonların yapısını, katılımları ve ödülleri düzenler. Federasyonlar ve Uluslararası Olimpiyat Komitesi (IOC), her ülkede sadece bir oluşumu resmen tanırlar ve onları muhatap alırlar. Örneğin, yirminci yüzyılın ikinci yarısında IOC birkaç senesini Doğu-Batı Almanya, Kuzey-Güney Kore gibi meseleleri nasıl aşacağını karar vermeye çalışmakla geçirmiştir. Bir spor kurumunun tanınması, kaçınılmaz olarak rejimin tanınması anlamına gelmektedir. 1970'te Güney Afrika Cumhuriyeti'nin olimpiyatlardan çıkarılması meselesi ise tamamen ülkenin içinde bulunduğu sosyal ve ekonomik sistemden kaynaklanmaktadır (Taylor, 1986). Yani kısacası sporun siyasi etkisi hafiflenmeyecek ölçüdedir. Büyük bir siber saldırıların spor işletme ve organizasyonlara doğurduğu kurumsal ve ekonomik etkileri yıkıcı olacaktır. Sporun teknolojik gelişmeler ışık hızıyla ilerlerken bu gelişmelerin yol açtığı tehditlere, zayıflıklara ve risklere karşı önlem almak ve uygulamak büyük önem taşıyor. Bu amaçla spor sektöründe siber uzayın güvenliği, gerekli altyapının sağlanarak savunma ve saldırı kabiliyetlerinin kazanılması, ulaşılması gereken stratejik bir hedeftir.

1.5. Teknoloji Öngörüsü

1.5.1. Teknoloji Öngörüsünün Tanımı

Terminolojisi çoğunlukla tahmin ve öngörü ile karıştırılmaktadır (Keenan, 2000). "Forecast" sözcüğü; "Tahmin" şeklinde, "Foresight" sözcüğü "Öngörü" şeklinde tercüme dilimize yansımıştır. Forecast , mevcut veriden hareketle, gelecekte ne olacağı ile ilgili tahmin yürütmek anlamına gelmektedir. Tahminde tek bir gelecek

varsayımı ile geleceğe karşı pasif tavır vardır (Tümer, 2002). Öngörünün tahminden farklı özellikleri şunlardır,

- Tahmin, geçmişin gelecekte de devam edeceğine inanılan durumlarda göz önüne alınması

- Temel değişiklikler beklenmemesi,

- Ele alınan sorunun daha basit olması, sayısal tekniklerle optimize edilebilmesi.

- Mevcut eğilimlerle ilgili göreceli olarak kesinlik var olması.

- Gelecekle ilgili yorumların birbiriyle benzerlik göstermesi.

- Zaman ufkunun göreceli olarak kısa olmasıdır (Wehrmeyer ve ark., 2002).

Bu kapsamda etkili bir yöntem olan teknoloji öngörüsü geçmiş ve mevcut durumun gelecek için rehber olamadığı durumda aşağıdaki durumlar gözden geçirilmelidir.

- Sorun karmaşıktır.

- Değişimlerin bariz olma olasılığı yüksektir.

-Baskın eğilimler olgunlaşmış veya olumlu olmayabilir, bu sebeple analiz edilmesi gerekir.

- Zaman ufku göreceli olarak daha uzundur.

- Öngörü sadece analitik değil bununla birlikte yaratıcı da bir süreçtir. Tahminde "gelecek ne olacak?" sorusu, öngörüde katılımcıları daha aktif hale getirerek "hangi gelecekler mümkündür, bunlardan hangileri yararlı, hangileri tehlikelidir?" şeklinde yoruma dayalı sorulara dönüşür (Wehrmeyer ve ark., 2002). Buradan da anlaşılacağı gibi öngörü sadece bir uzmanın belirlediği bir çalışma değil

aynı zamanda çok sayıda değişkeni olan bir metotdur. Öngörü çalışmaları, geleceğe yönelik hem çok disiplinli hem de disiplinler arası faaliyetlerdir.

Literatürde “teknoloji”nin çeşitli tanımları bulunmaktadır.Bu tanımları analiz etmek, teknolojiyi tanımlayan bir dizi faktörü keşfeder.Teknolojinin temel özelliği “uygulamalı bilgi” olmasıdır (Phaal ve ark., 2001). Teknoloji, teknik problemleri belirleme yeteneği ile yeni konseptler yaratma ve kullanma ve bu problemlere değerli çözümler keşfetme yetkinliğini içerir. Yani bu sebeple hem becerileri hem de örtülü bilgiyi içerir (Molas-Galat, 1997).

Teknoloji Vadeli İşlem Analiz Yöntemleri Çalışma Grubu (TFAMWG) teknoloji odaklı tahmin yöntemlerini ve uygulamalarını entegre etmek için “teknoloji geleceği analizi” (TFA) şemsiye konseptini tanıttı. TFA, gelecekteki teknolojik gelişmeler hakkında bilgi toplamak için herhangi bir sistematik süreci ifade eder. Teknoloji zekası tahmini, yol haritası oluşturma, değerlendirme ve öngörü gibi birçok TFA biçimi bir arada bulunur (Porter ve ark., 2004). Aynı kavram “Geleceğe Yönelik Teknoloji Analizi” (FTA) (Haegeman ve ark., 2013) adlı başka bir terminoloji ile temsil edilmektedir.

Literatürde yer alan kavramlar arasında tahmin ve öngörü, teknoloji ile ilgili gelecekte yapılacak çalışmalarda en çok kullanılan terimlerdir. Meredith ve Mantel'e (1995) göre "teknoloji tahmini", "teknolojinin gelecekteki özelliklerini ve zamanlamasını tahmin etme sürecidir". Martin (1995), “teknoloji öngörüsünü” “stratejik araştırma alanlarını ve muhtemel olarak ortaya çıkan jenerik teknolojileri belirlemek amacıyla en büyük ekonomik ve sosyal faydaları sağlamak için bilim, teknoloji, ekonomi ve toplumun uzun vadeli geleceğine sistematik olarak bakma girişiminde yer alan bir süreç” olarak tanımlamaktadır. Teknoloji öngörüsü hakkında Porter ve arkadaşları (2004)’te, daha arzu edilir bir gelecek yaratmak için yönergeler belirlemek üzere gelecekteki teknolojik gelişmeleri ve bunların toplum ve çevre ile ilişkilerini belirlemeye yönelik sistematik bir süreç olarak tanımlamakatadır. Slaughter'a (1997) göre teknoloji öngörüsü, bir gelecek söylemi yaratmak için

gelecek kavramlarını kullanmak üzere geliştirilmesi ve uygulanması gereken "insan kapasitesi"dir.

1.5.2. Teknoloji Öngörüsünün Önemi

Teknoloji öngörüsü, gelecekteki teknolojik gelişmeleri tahmin etme ve analiz etme sürecidir. Önemi birkaç farklı açıdan değerlendirilebilir:

Planlama ve Strateji: Teknoloji öngörüsü, işletmelerin, kurumların ve hükümetlerin gelecekteki teknolojik trendleri belirlemelerine ve bu trendlere uygun planlar yapmalarına yardımcı olur. Gelecekteki teknolojik gelişmeler hakkında bilgi sahibi olmak, rekabet avantajı sağlamak ve stratejik kararları doğru bir şekilde almak için önemlidir.

Yatırım ve İnovasyon: Teknoloji öngörüsü, yatırımcıların ve girişimcilerin gelecekteki büyüme alanlarını ve fırsatları belirlemelerine yardımcı olur. Bu bilgiler doğrultusunda, yenilikçi ürünler ve hizmetler geliştirmek ve yeni pazarlara girmek için yatırımlar yapılabilir. Ayrıca, teknoloji öngörüsü, Ar-Ge faaliyetlerinin odak noktalarını belirlemede ve kaynakları doğru bir şekilde tahsis etmede de kullanılır.

Risklerin Azaltılması: Teknoloji öngörüsü, işletmelerin ve kurumların gelecekteki riskleri ve tehditleri tahmin etmelerine yardımcı olur. Örneğin, bir sektördeki teknolojik değişimler, bazı işlerin otomatikleştirilmesine veya dönüşmesine neden olabilir, bu da bazı çalışanların işlerini kaybetmelerine yol açabilir. Bu tür risklerin farkında olmak ve uygun önlemleri almak, etkilenen taraflar için daha iyi bir geçiş süreci sağlayabilir.

Toplum ve Etik: Teknoloji öngörüsü, toplumun gelecekteki teknolojik değişimlere adapte olabilmesi için önemlidir. Örneğin, yapay zeka, otomasyon ve robotik gibi teknolojilerin yaygınlaşmasıyla birlikte, iş gücü ve eğitim alanlarında değişiklikler olabilir. Bu değişikliklerin sosyal etkilerini ve toplumun bu süreçlere

nasıl uyum sağlayabileceğini öngörmek, politika yapıcılar, eğitimciler ve toplum liderleri için önemlidir.

Sonuç olarak, teknoloji öngörüsü, gelecekteki teknolojik değişimleri anlamak ve bu değişimlere uyum sağlamak için stratejik bir araçtır. İşletmeler, kurumlar ve toplumlar, rekabet avantajı elde etmek için inovatif çözüm yoludur.

Teknoloji öngörüsü, birçok alanda büyük bir etkiye sahip olabilir ve size birçok avantaj sağlayabilir. Öngörülerinizi doğru bir şekilde yaparak gelecekteki teknolojik değişimleri tahmin etmek, rekabet avantajı elde etmenize ve iş stratejilerinizi buna göre şekillendirmenize yardımcı olur.

İşletme açısından, teknoloji öngörüsü size gelecekteki pazar eğilimlerini belirleme, müşteri ihtiyaçlarını anlama ve buna göre ürün ve hizmetlerinizi geliştirme şansı verir. Ayrıca, yeni pazar fırsatlarını yakalama ve rakiplerinizden bir adım önde olma imkanı sunar.

Yatırımcılar için, teknoloji öngörüsü yatırım yapacakları sektörleri belirlemek ve gelecekte büyüme potansiyeli olan şirketlere odaklanmak açısından kritik öneme sahiptir. Doğru öngörülerle, yatırımlarınızı daha bilinçli bir şekilde yönlendirebilir ve risklerinizi azaltabilirsiniz.

Aynı şekilde, teknoloji öngörüsü girişimciler için de büyük bir önem taşır. İnovasyon ve yeni fikirler geliştirme sürecinde, gelecekteki teknolojik trendleri tahmin etmek, pazarda öncü olmanıza ve başarılı bir şekilde rekabet etmenize yardımcı olur.

Son olarak, teknoloji öngörüsü toplumun genelinde etkiler yaratır. Teknolojik değişimler iş gücü, eğitim, sağlık, ulaşım ve iletişim gibi birçok alanda etkiler yaratabilir. Bu değişimlere önceden hazırlıklı olmak, politika yapıcıları ve toplum

liderlerini geleceğe yönelik stratejiler oluşturmaya teşvik eder ve toplumun genel refahını artırır.

Sonuç olarak, teknoloji öngörüsü işletmeler, yatırımcılar, girişimciler ve toplumun genelinde önemli bir rol oynar. Doğru bir şekilde uygulandığında, gelecekteki teknolojik değişimlere adapte olmak, rekabet avantajı sağlamak ve toplumun refahını artırmak için önemli bir araçtır.

1.5.3. Teknoloji Öngörüsünün Tarihsel Süreci

Teknoloji öngörüsünün tarihsel gelişimi, insanların teknolojik değişimleri tahmin etme ve gelecekteki gelişmeler hakkında bilgi sahibi olma çabalarıyla başlar. İnsanlar, teknolojik ilerlemelerin yaratacağı etkileri anlamak ve gelecekteki gelişmelere hazırlıklı olmak için binlerce yıldır çeşitli yöntemler kullanmışlardır. İşte teknoloji öngörüsünün tarihsel gelişimi hakkında bazı önemli noktalar:

Antik Çağlardan Orta Çağa:

Antik çağlarda, bazı filozoflar ve düşünürler gelecekteki teknolojik gelişmelere dair tahminlerde bulunmuşlardır. Örneğin, Antik Yunan filozofu Heron, buhar gücüyle çalışan makinelerin olabileceğini ve otonom hareket edebilecek araçların inşa edilebileceğini öngörmüştür. Orta Çağ döneminde ise bazı bilginler, mekanik icatlar ve makineler konusunda fikirler geliştirmişlerdir (Kapır, 2022). Örneğin, Leonardo da Vinci'nin çizimlerinde helikopter, su altı aracı ve uçan makineler gibi fikirler bulunmaktadır.

Sanayi Devrimi ve Sonrası:

Sanayi Devrimi, teknolojik öngörülerin hız kazandığı bir dönemdir. Makineleşme ve endüstriyel üretimdeki büyük ilerlemeler, gelecekteki teknolojik değişimleri öngörmek için bir zemin oluşturmuştur. Bu dönemde, bilim ve

mühendislik alanlarındaki ilerlemelerle birlikte, öngörüler daha spesifik hale gelmiştir. Örneğin, 19. yüzyılda Jules Verne, kitaplarında deniz altı araçları, uzay seyahatleri ve diğer ileri teknolojiler hakkında tahminlerde bulunmuştur (Özdoğan, 2017).

Modern Dönem ve Teknoloji Öngörüsü Araçları:

20. yüzyılda, teknoloji öngörüsü daha bilimsel bir yaklaşım kazanmış ve çeşitli araçlar geliştirilmiştir. Bilim kurgu yazıları, trend analizi, Delphi metodu, senaryo analizi gibi teknikler kullanılmıştır. Aynı dönemde, teknolojik değişimleri tahmin etmek için uzmanlar ve akademisyenler arasında çalışmalar yapılmıştır. Teknoloji öngörüsü, hükümetler, kuruluşlar ve şirketler tarafından stratejik planlama ve karar verme süreçlerinde daha yaygın bir şekilde kullanılmaya başlanmaktadır.

Modern dönemde, teknoloji öngörüsü daha da önem kazanmış ve gelişmiştir. Bilgisayar ve iletişim teknolojilerindeki hızlı ilerlemeler, büyük veri analitiği ve yapay zeka gibi araçlar, teknoloji öngörüsünü daha kesin ve veri odaklı hale getirmiştir. Ayrıca, akademik kurumlar, araştırma enstitüleri ve özel şirketler teknoloji öngörüsü çalışmalarını yürütmek için uzman ekipler oluşturmuşlardır (Kapır, 2022).

Teknoloji öngörüsü için çeşitli metodolojiler ve yaklaşımlar geliştirilmiştir. Bunlardan bazıları şunlardır:

Trend Analizi: Geçmiş trendlerin analizi, gelecekteki teknolojik gelişmeleri tahmin etmede kullanılır. Belirli bir teknolojinin geçmiş performansı ve büyüme eğilimleri, gelecekteki trendleri tahmin etmek için bir gösterge olabilir (Soysal ve Ömürgönülşen, 2010).

Senaryo Analizi: Farklı olası senaryoların oluşturulması ve değerlendirilmesi, belirsizliklerle başa çıkmak ve gelecekteki teknolojik değişimleri anlamak için

kullanılan bir yöntemdir. Farklı senaryolar üzerinde çalışarak, olası fırsatlar ve riskler hakkında daha iyi bir anlayış geliştirilebilir (Karaman, 2022).

Delphi Metodu: Uzman görüşlerinin toplandığı ve uzmanların iteratif olarak fikirlerini paylaştığı bir yöntemdir. Birden fazla iterasyon ile uzlaşıya varılan tahminler oluşturulabilir (Yıldırım, 2006).

Büyük Veri Analitiği: Büyük veri kaynaklarının analizi, mevcut verilerden gelecekteki eğilimleri ve desenleri ortaya çıkarabilir. Büyük veri analitiği, teknoloji öngörüsünde daha kesin ve veri odaklı sonuçlar elde etmek için kullanılan bir araçtır.

Teknoloji öngörüsü, şirketlerin Ar-Ge faaliyetlerini yönlendirmelerine, yeni pazarlara girmelerine, rekabet avantajı elde etmelerine ve gelecekteki riskleri minimize etmelerine yardımcı olur. Aynı zamanda, hükümetlerin politika yapım süreçlerinde ve toplumun genel refahını artırmak için stratejiler oluşturmada da önemli bir rol oynar.

1.5.4. Teknoloji Öngörüsünün Amaçları

Teknoloji öngörüsünün temel amacı, gelecekteki teknolojik değişimleri tahmin etmek ve bu tahminlere dayanarak kararlar almak için bilgi sağlamaktır. Teknoloji öngörüsü, işletmeler, hükümetler, akademik kurumlar ve diğer paydaşlar için çeşitli amaçlar taşır. İşte teknoloji öngörüsünün bazı temel amaçları:

Gelecekteki Trendleri ve Fırsatları Belirlemek: Teknoloji öngörüsü, gelecekteki teknolojik trendleri belirlemek için kullanılır. Bu trendler, yeni pazar fırsatları ve büyüme potansiyelleri sunabilir. Teknoloji öngörüsü, işletmelerin bu trendlere önceden adapte olmalarını ve rekabet avantajı elde etmelerini sağlar.

Stratejik Planlama: Teknoloji öngörüsü, işletmelerin uzun vadeli stratejik planlama süreçlerine rehberlik eder. Gelecekteki teknolojik değişimleri tahmin etmek, işletmelere doğru kararlar alabilmeleri için bilgi sağlar. Bu da işletmelerin rekabetçi bir konumda kalabilmelerini ve başarılı olmalarını sağlar (Yıldırım, 2006).

Risk Yönetimi: Teknoloji öngörüsü, gelecekteki teknolojik riskleri belirlemek ve yönetmek için kullanılır. Öngörülen teknolojik değişimlere uyum sağlayamamak veya yeni gelişmeleri göz ardı etmek, işletmeler için risk oluşturabilir. Teknoloji öngörüsü, bu riskleri tanımlayarak işletmelerin önlem almasına yardımcı olur.

Yatırım Kararları: Teknoloji öngörüsü, yatırımcılar için önemlidir. Gelecekte büyüme potansiyeli olan sektörleri ve şirketleri belirlemek, yatırımların doğru şekilde yönlendirilmesine yardımcı olur. Ayrıca, yatırımların getirisini artırmak için yeni teknolojilere yatırım yapma stratejilerini belirlemek için kullanılır (Yıldırım, 2006).

Politika Oluşturma: Teknoloji öngörüsü, hükümetler ve politika yapıcılar için önemlidir. Gelecekteki teknolojik değişimleri öngörmek, politika yapıcıların geleceğe yönelik stratejiler oluşturmasına yardımcı olur. Bu stratejiler, toplumsal etkileri ve ekonomik gelişimi göz önünde bulundurarak teknoloji ile uyumlu politikaların geliştirilmesini sağlar (Yıldırım, 2006).

Teknoloji öngörüsü, bu amaçlar doğrultusunda gelecekteki teknolojik değişimleri anlamak ve doğru kararlar almak için kullanılır.

1.5.5. Teknoloji Öngörüsünde Kullanılan Yöntemler

Teknoloji öngörüsü, gelecekteki teknolojik değişimleri tahmin etmek ve analiz etmek için çeşitli yöntemler ve araçlar kullanır. İşte teknoloji öngörüsünde yaygın olarak kullanılan bazı yöntemler:

Trend Analizi: Geçmiş trendlerin analizi, gelecekteki teknolojik gelişmeleri tahmin etmede kullanılan bir yöntemdir. Belirli bir teknolojinin geçmiş performansı, büyüme eğilimleri ve benzeri faktörler gelecekteki trendleri tahmin etmek için bir gösterge olabilir. Bu analiz, istatistiksel veriler ve grafiklerin kullanılmasıyla yapılır.

Senaryo Analizi: Senaryo analizi, farklı olası gelecek senaryolarının oluşturulması ve değerlendirilmesini içeren bir yöntemdir. Bu senaryolar, teknolojik değişimlerin farklı hızlarda gerçekleştiği veya farklı faktörlerin etkili olduğu durumları yansıtabilir. Senaryo analizi, belirsizlikleri ele almak ve gelecekteki teknolojik değişimlerin olası sonuçlarını anlamak için kullanılır.

Delphi Metodu: Delphi metodu, uzmanların görüşlerinin toplandığı ve iteratif olarak fikirlerin paylaşıldığı bir yöntemdir. Uzmanlardan anketler veya görüş bildirimleri aracılığıyla bilgi toplanır ve bu bilgiler kullanılarak gelecekteki teknolojik değişimler hakkında tahminler oluşturulur. Delphi metodu, uzmanların farklı perspektiflerini birleştirmek ve uzlaşıya varılan tahminler üretmek için kullanılır.

Büyük Veri Analitiği: Büyük veri analitiği, büyük veri kaynaklarının analizi ve modelleme tekniklerinin kullanılmasıyla gelecekteki teknolojik eğilimleri ve desenleri ortaya çıkarmak için kullanılan bir yöntemdir. Büyük veri analitiği, milyonlarca veri noktasını analiz ederek trendleri belirlemek, öngörüler yapmak ve gelecekteki teknolojik değişimleri tahmin etmek için güçlü bir araçtır.

Uzman Görüşleri ve Literatür Taraması: Teknoloji öngörüsünde uzman görüşleri ve literatür taraması da önemli bir rol oynar. Uzmanların teknoloji alanındaki bilgileri ve deneyimleri, gelecekteki gelişmeler hakkında önemli bir kaynak olabilir. Ayrıca, bilimsel makaleler, raporlar ve teknoloji haberleri gibi kaynaklar da teknoloji öngörüsü için kullanılabilir (Yıldırım, 2006).

Bu yöntemler, teknoloji öngörüsünde kullanılan temel araçlar olmakla birlikte, öngörülerin doğruluğunu artırmak için birbiriyle kombinasyon halinde de kullanılabilir. Teknoloji öngörüsü süreci, yöntemlerin seçimi ve uygulanması, veri toplama ve analiz süreçleri gibi adımlardan oluşur.

Keenan (2000) tarafından yapılan çalışma, öngörü yöntemlerinin genel bir görünümünü oluşturmak için çeşitli öngörü alanlarını ve yöntemlerini sınıflandırmıştır. Bu sınıflandırma, farklı öngörü yöntemlerinin kategorilere ayrılmasını ve bu yöntemlerin nasıl kullanıldığını açıklamayı amaçlamıştır.

Keenan'ın öngörü yöntemleri için genel görünümü aşağıdaki gibi oluşturmuştur:

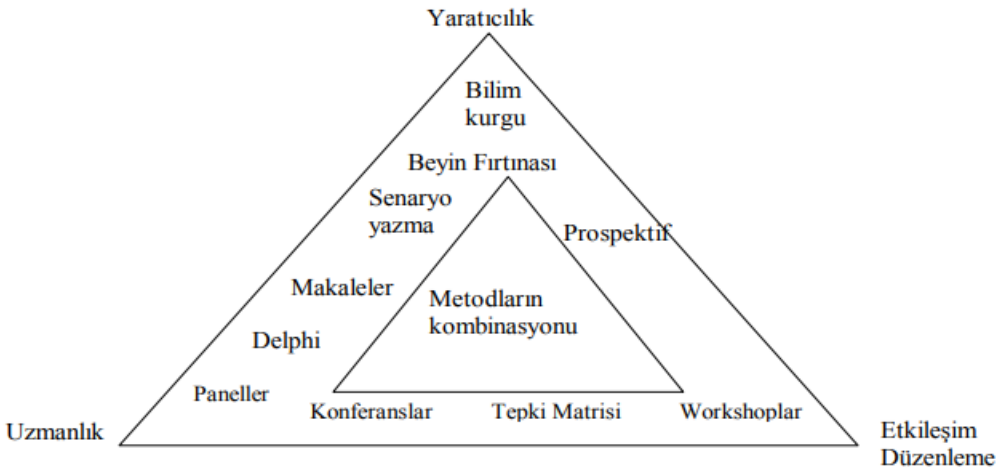
Kalitatif Öngörü Yöntemleri: Kalitatif öngörü yöntemleri, uzman görüşlerine, uzman panellerine veya uzman mülakatlarına dayalı olarak gelecekteki olayları ve trendleri tahmin etmeye odaklanır. Bu yöntemler, uzmanların bilgi ve deneyimlerinden yararlanarak öngörüler elde etmeyi amaçlar. Örnekler arasında Delphi yöntemi, uzman paneli, senaryo analizi ve görüş anketleri bulunur.

Kvantitatif Öngörü Yöntemleri: Kvantitatif öngörü yöntemleri, istatistiksel verilere, matematiksel modellere ve nicel analizlere dayalı olarak gelecekteki olayları tahmin etmeyi hedefler. Bu yöntemler, geçmiş verileri analiz ederek gelecekteki trendleri ve ilişkileri belirlemeyi amaçlar. Örnekler arasında zaman serisi analizi, regresyon analizi, simülasyon modelleri ve yapay sinir ağları bulunur.

Karma Yöntemler: Karma yöntemler, kalitatif ve kvantitatif öngörü yöntemlerinin birleştirilmesini içerir. Bu yöntemler, farklı yaklaşımların bir araya getirilerek daha kapsamlı ve sağlam öngörüler elde edilmesini amaçlar. Örnek olarak, uzman görüşlerinin niceliksel olarak değerlendirilmesi veya kvantitatif modellerin kalitatif senaryolarla birleştirilmesi verilebilir.

Yaratıcı Öngörü Yöntemleri: Yaratıcı öngörü yöntemleri, hayal gücünü ve yaratıcılığı teşvik ederek yenilikçi ve radikal öngörüler elde etmeyi hedefler. Bu yöntemler, çeşitli yaratıcı düşünme tekniklerini kullanarak farklı perspektiflerden geleceğe dair fikirler geliştirmeyi amaçlar. Örnekler arasında senaryo yazımı, özgür yazım, hikaye anlatımı ve çizimler bulunur.

Keenan'ın sınıflandırması, öngörü yöntemlerinin çeşitliliğini ve farklı yaklaşımlarını ortaya koymayı amaçlamaktadır. Bu genel görünüm, öngörü çalışmalarında kullanılan yöntemlerin anlaşılmasına ve seçilmesine yardımcı olabilir. Keenan'ın sınıflandırması Şekil 1.3'de gösterilmiştir.



Şekil 1.3. Öngörü Methodlarının Keenan Sınıflandırılması (Keenan, 2000).

Cuhls, öngörü yöntemlerini sınıflandırmak için "Cuhls Sınıflandırması" adı verilen bir model geliştirmiştir. Bu sınıflandırma, öngörü yöntemlerini beş ana kategoriye ayırır. İşte Cuhls Sınıflandırması'na göre öngörü yöntemlerinin kategorileri:

Dışsal Yöntemler (Exogenous Methods): Bu yöntemler, öngörüleri dış faktörlerin analizi ve değerlendirmesi yoluyla yapar. Örneğin, uzman görüşleri, anketler, Delphi metodu gibi dışsal verilere dayalı yöntemler bu kategoriye girer. Bu

yöntemler, gelecekteki eğilimleri ve değişkenleri anlamak için dışarıdan bilgi ve perspektiflerin kullanılmasına odaklanır.

İçsel Yöntemler (Endogenous Methods): Bu yöntemler, öngörüleri geçmiş ve mevcut verilerin analizi yoluyla yapar. İstatistiksel analiz, trend analizi, regresyon analizi gibi içsel verilere dayalı yöntemler bu kategoriye girer. Bu yöntemler, geçmiş eğilimlerin ve verilerin gelecekteki davranışları tahmin etmek için kullanılmasına odaklanır.

Türetme Yöntemleri (Derivative Methods): Bu yöntemler, öngörüleri matematiksel veya istatistiksel modellerin kullanımıyla yapar. Örneğin, zaman serisi analizi, stokastik süreçler, yapay sinir ağları gibi yöntemler bu kategoriye girer. Bu yöntemler, geçmiş verilere dayanarak gelecekteki değerleri ve trendleri tahmin etmek için matematiksel modelleme ve analiz yapar.

Normatif Yöntemler (Normative Methods): Bu yöntemler, öngörüleri belirli bir norm veya hedefe göre yapar. Örneğin, senaryo analizi, hedeflerin belirlendiği planlama süreçleri gibi yöntemler bu kategoriye girer. Bu yöntemler, farklı senaryoların ve hedeflerin etkilerini değerlendirerek gelecekteki durumları tahmin etmeye çalışır.

Yaratıcı Yöntemler (Creative Methods): Bu yöntemler, öngörüleri yaratıcı ve yenilikçi düşünce süreçlerini kullanarak yapar. Örneğin, zihinsel haritalama, senaryo planlaması, çıkarım ve sezgisel düşünce gibi yöntemler bu kategoriye girer. Bu yöntemler, alternatif gelecek senaryolarını keşfetmeye ve farklı perspektiflerden öngörüler geliştirmeye odaklanır.

Cuhls Sınıflandırması, farklı öngörü yöntemlerinin çeşitli yaklaşımları temsil etmesini sağlar ve öngörü çalışmalarının genel bir çerçevesini sunar. Bu sınıflandırma, öngörü yöntemlerini anlamak, seçmek ve uygulamak için bir rehber

sağlar. Ancak, her yöntemin kendi avantajları ve sınırlamaları vardır ve doğru yöntemin seçilmesi öngörü çalışmasının amaçlarına ve bağlamına bağlıdır.

1.5.5.1. Delphi Yöntemi

Delphi yöntemi, belirsizliklerin ve karmaşıklıkların olduğu konularda uzmanların fikirlerini toplamak ve uzlaşmaya varmak amacıyla kullanılan bir araştırma yöntemidir. Bu yöntem, katılımcıların anonim olarak fikirlerini paylaşmasını sağlar ve sonuçları sistematik bir şekilde değerlendirir.

Delphi yöntemi genellikle aşağıdaki adımları içerir:

Panelin oluşturulması: Yöntemde kullanılacak uzman paneli oluşturulur. Bu panel, konuyla ilgili uzmanlar, akademisyenler, endüstri liderleri veya ilgili paydaşlardan oluşabilir.

Soru hazırlığı: Panel üyelerine yöneltilmek üzere sorular hazırlanır. Bu sorular, öngörülen konu veya sorunla ilgili bilgi, görüş ve tahminlerin alınmasını amaçlar.

İlk tur anketi: Panel üyelerine soruların yöneltilmesi için anketler hazırlanır. Panel üyeleri, kendi görüşlerini, tahminlerini veya değerlendirmelerini anonim olarak paylaşırlar.

Geri bildirim: İlk tur anketlerinin sonuçları toplanır ve panel üyelerine geri bildirim yapılır. Bu geri bildirim, diğer panel üyelerinin görüşlerini öğrenme ve karşılıklı etkileşim için kullanılır.

İkinci tur anketi: İlk turdaki sonuçlara dayanarak, panel üyelerine ikinci bir ankete katılmaları ve fikirlerini yeniden değerlendirmeleri istenir. İlk turdaki görüşler

üzerinde uzlaşmaya varmak veya belirli konuları daha ayrıntılı bir şekilde ele almak için ek sorular da eklenebilir.

Tekrar eden turlar: İkinci turun sonuçları değerlendirilir ve gerektiğinde üçüncü, dördüncü ve daha fazla tur yapılabilir. Her turda panel üyeleri arasında bir uzlaşma sağlanmaya çalışılır.

Sonuçların analizi: Tüm tur sonuçları toplanır ve analiz edilir. Ortak görüşler, eğilimler, farklılıklar ve uzlaşma noktaları belirlenir.

Delphi yöntemi, uzman görüşlerini sistemli bir şekilde toplamak, farklı perspektifleri bir araya getirmek ve belirsizlikleri azaltmak için etkili bir yöntemdir. Özellikle gelecek tahminleri, stratejik planlama, politika oluşturma ve karmaşık karar verme süreçlerinde yaygın olarak kullanılmaktadır.

Delphi yöntemi, diğer araştırma yöntemlerinden farklı olarak bazı öne çıkan özelliklere sahiptir:

Anonimlik: Delphi yönteminde panel üyeleri anonim olarak fikirlerini paylaşırlar. Bu, katılımcıların açık ve dürüst bir şekilde düşüncelerini ifade etmelerini sağlar. Anonimlik, hiyerarşi veya baskı unsurlarının etkisini azaltır ve daha özgür bir fikir alışverişi sağlar.

Uzman Görüşlerinin Derlenmesi: Delphi yöntemi, konuyla ilgili uzmanların fikirlerini bir araya getirerek geniş bir uzmanlık perspektifi sunar. Birden fazla uzmanın görüşlerinin birleşimiyle daha kapsamlı ve detaylı bir sonuç elde etmek mümkündür.

Geri Bildirim: Delphi yönteminde, panel üyeleri her turda geri bildirim alır. Bu geri bildirim, panel üyelerinin diğer üyelerin görüşlerini gözden geçirmelerini ve

kendi fikirlerini yeniden değerlendirmelerini sağlar. Bu sayede daha sağlıklı ve bilinçli bir uzlaşma sağlanabilir.

Çoklu Tur: Delphi yöntemi genellikle birden fazla turdan oluşur. Her turda panel üyeleri fikirlerini yeniden değerlendirir ve yeni bir ankete katılır. Bu, fikirlerin gelişmesine ve uzlaşmanın sağlanmasına yardımcı olur.

Karmaşık ve Belirsiz Konular İçin Uygunluk: Delphi yöntemi, karmaşık ve belirsiz konularda kullanılmak üzere tasarlanmıştır. Bu yöntem, gelecek tahminleri, politika oluşturma veya stratejik planlama gibi alanlarda belirsizliklerle başa çıkmak ve uzman görüşlerini sistematik bir şekilde toplamak için etkilidir.

Delphi yöntemi, geniş bir katılımcı grubunun fikirlerini toplamak, farklı perspektifleri değerlendirmek ve ortak bir uzlaşma noktası bulmak için kullanılan bir yöntemdir. Anonimlik, uzman görüşlerinin derlenmesi, geri bildirim, çoklu tur ve uygunluk sağlama gibi özellikleriyle ön plana çıkar.

1.5.5.2. Bulanık Delphi Yöntemi

Bulanık Delphi yöntemi, belirsizlik içeren konuların analiz edilmesi ve gelecek tahminlerinin yapılması için kullanılan bir tekniktir. Genellikle aşağıdaki adımları içerir:

1. Sorunun tanımlanması ve araştırmanın kapsamının belirlenmesi: Bu adımda, analiz edilecek sorun net bir şekilde tanımlanır ve çalışmanın kapsamı belirlenir. Bu, analizin amacını, hedeflerini ve araştırmanın odak noktasını içerir.

2. Uzman panelinin oluşturulması: Bu adımda, uzmanlardan oluşan bir panel oluşturulur. Uzmanlar, analiz edilecek sorunla ilgili bilgi ve deneyime sahip kişilerdir. Panel genellikle birden fazla uzmandan oluşur ve farklı bakış açıları, uzmanlık alanları ve deneyim seviyelerini kapsar.

3. Anket tasarımı: Bu adımda, uzmanlara gönderilecek anketlerin tasarımı yapılır. Ankette, bulanık mantık ifadeleri ve bulanık sayılar kullanılabilir. Ankette, sorunla ilgili sorular, öneriler veya tahminler bulunabilir. Anketteki soruların net ve anlaşılır olması önemlidir.

4. Uzmanlara anketlerin gönderilmesi: Anketteki sorular uzmanlara gönderilir. Uzmanlardan, sorulara bulanık mantık ifadeleriyle yanıt vermeleri istenir. Uzmanlar, kendi bilgi düzeyleri ve belirsizlik toleranslarına göre yanıtlarını belirler.

5. Yanıtların toplanması ve analizi: Uzmanlardan gelen yanıtlar toplanır. Bu yanıtlar daha sonra analiz edilir. Bulanık mantık prensipleri kullanılarak uzmanların farklı görüşlerinin birleştirilmesi ve konsensüsün sağlanması hedeflenir. Bu adımda, belirsizliklerin ele alınması ve yanıtların yorumlanması da önemlidir.

6. Sonuçların raporlanması: Analiz sonuçları rapor haline getirilir. Bu raporda, uzmanların görüşleri, bulanık mantık ifadeleri ve tahminler yer alabilir. Rapor, sorunun analizini, bulunan sonuçları ve önerileri içerebilir.

Bulanık Delphi yöntemi, adımların spesifik duruma bağlı olarak değişebileceği esnek bir yöntemdir. Bu adımlar, belirsizlik içeren sorunların analiz edilmesi ve gelecek tahminlerinin yapılması için genel bir rehber niteliği taşır.

1.5.6. Bölgesel /Uluslararası Uygulamalar

1.5.6.1. UNİDO

Birleşmiş Milletler Sınai Kalkınma Teşkilatı (United Nations Industrial Development Organization - UNIDO), sanayi sektörünün sürdürülebilir ve kapsayıcı kalkınmasını teşvik etmek amacıyla faaliyet gösteren bir Birleşmiş Milletler kuruluşudur.

UNIDO, 1966 yılında kurulmuş olup merkezi Viyana, Avusturya'dadır. Teşkilatın temel amacı, sanayi sektörünün geliştirilmesi yoluyla ekonomik büyümeyi teşvik etmek, yoksulluğu azaltmak, iş imkanları yaratmak ve sürdürülebilir kalkınmayı desteklemektir (Başlar, 2012).

UNIDO'nun faaliyetleri, üye ülkelerin ihtiyaçlarına göre belirlenen stratejiler ve programlar üzerinden yürütülür. Teşkilat, teknik destek, kapasite geliştirme, politika danışmanlığı, bilgi paylaşımı ve işbirliği faaliyetleri gibi çeşitli araçlar kullanarak üye ülkelerin sanayi sektörlerini güçlendirmeyi hedefler.

UNIDO'nun çalışma alanları arasında enerji verimliliği, çevresel sürdürülebilirlik, sanayi politikaları, endüstriyel altyapı, teknoloji transferi, kadın girişimciliği ve küçük ve orta ölçekli işletmelerin desteklenmesi yer almaktadır.

Teşkilat, üye ülkelerle işbirliği yaparak projeler yürütür, politika önerilerinde bulunur, teknik uzmanlık sağlar ve uluslararası platformlarda sanayi kalkınmasıyla ilgili konuları gündeme getirir. UNIDO'nun çalışmaları, sürdürülebilir kalkınma hedeflerine ulaşma çabalarına katkıda bulunmayı amaçlar. Birleşmiş Milletler Sınai Kalkınma Teşkilatı (UNIDO) ve Türk İşbirliği ve Koordinasyon Ajansı Başkanlığı (TİKA) arasında işbirliği, Türkiye'nin kalkınma yardımlarının etkin ve verimli bir şekilde yönetilmesi ve uygulanması amacıyla gerçekleşmektedir (Başlar, 2012).

TİKA, Türkiye'nin kalkınma yardımlarını koordine eden ve yürüten bir ajans olarak faaliyet gösterirken, UNIDO ise sanayi sektörünün sürdürülebilir kalkınmasını teşvik etmek amacıyla çalışan bir Birleşmiş Milletler kuruluşudur. İki kuruluş arasındaki işbirliği, Türkiye'nin sanayi sektörünün geliştirilmesi ve sürdürülebilir kalkınma alanında daha etkili ve verimli bir şekilde çalışmasını hedefler.

UNIDO ve TİKA arasındaki işbirliği çerçevesinde, ortak projeler yürütülerek sanayi sektörünün güçlendirilmesi, endüstriyel altyapının geliştirilmesi, teknoloji transferi, enerji verimliliği ve çevresel sürdürülebilirlik gibi konularda çalışmalar

yapılmaktadır. Bu işbirliği, üye ülkelerde sanayi sektörünün kalkınmasına yönelik projelerin uygulanması, teknik destek sağlanması, kapasite geliştirme faaliyetleri ve bilgi paylaşımı gibi alanları kapsar (Demirkaya ve Çelik, 2021)

UNIDO ve TİKA arasındaki işbirliği, Türkiye'nin sanayi ve kalkınma alanında birikimi ve deneyiminden faydalanarak, UNIDO'nun küresel çalışmalarına katkıda bulunmayı amaçlar. İki kuruluş arasındaki işbirliği projeleri, uluslararası kalkınma ve sürdürülebilir kalkınma hedeflerine ulaşmayı desteklemektedir**.**

1.5.6.2. Avrupa Birliği

Avrupa Birliği (AB), geleceğe yönelik öngörü çalışmalarını çeşitli şekillerde yürütmektedir. Bu çalışmalar, AB'nin politika yapıcılarına, karar vericilere ve paydaşlara bilgi sağlamak, stratejik planlama yapmak ve politika geliştirme süreçlerine katkıda bulunmak amacıyla gerçekleştirilir. İşte AB'nin öngörü çalışmalarını desteklemek için kullandığı bazı araçlar:

AB Foresight Platformu: AB Komisyonu, geleceği şekillendiren konuları analiz etmek ve politika önceliklerini belirlemek amacıyla AB Foresight Platformu'nu oluşturmuştur. Bu platform, AB içinde ve dışında gerçekleştirilen öngörü çalışmalarını bir araya getirir, bilgi paylaşımı sağlar ve ortak bir stratejik görünüm oluşturmayı amaçlar (Popper ve Teichler, 2011)

Avrupa Geleceği İçin Uzun Vadeli Vizyon Çalışması: AB Komisyonu, Avrupa'nın geleceğiyle ilgili uzun vadeli bir vizyon oluşturmak için çalışmalar yürütmektedir. Bu vizyon, 2050 yılına kadar olan dönemde AB'nin hedefleri, değerleri ve politikaları üzerinde odaklanır.

Araştırma ve İnovasyon Programları: AB, Horizon Europe gibi araştırma ve inovasyon programları aracılığıyla geleceğe yönelik öngörü çalışmalarını destekler. Bu programlar, ileri teknolojiler, sosyal ve ekonomik değişimler, iklim değişikliği ve

enerji dönüşümü gibi konuları inceleyerek AB'nin politika ve stratejilerine katkıda bulunmayı hedefler.

Stratejik Planlama Dokümanları: AB, stratejik planlama dokümanları aracılığıyla geleceğe yönelik öngörülerini ve politika önceliklerini açıklar. Örneğin, Avrupa Yeşil Mutabakatı ve Dijital Dönüşüm Stratejisi gibi belgeler, AB'nin gelecekteki hedeflerini ve politikalarını belirlemek için öngörü çalışmalarından yararlanır (Popper ve Teichler, 2011).

Bu örnekler, AB'nin geleceğe yönelik öngörü çalışmalarına örnek teşkil etmektedir. AB, değişen dünya koşullarına uyum sağlamak, gelecekteki zorluklara hazırlıklı olmak ve sürdürülebilir kalkınmayı desteklemek için sürekli olarak öngörü çalışmalarını kullanmaktadır.

1.5.7. Ulusal Uygulamalar

1.5.7.1. Japonya'nın Beşinci "Delphi" Envanteri

Japonya'nın Beşinci "Delphi" Envanteri, Japonya'nın bilim ve teknoloji alanındaki geleceğe yönelik öngörülerini içeren bir çalışmadır. Bu envanter, Japonya'nın Bilim ve Teknoloji Politikası Konseyi tarafından yürütülen bir girişimdir.

Japonya'nın Beşinci "Delphi" Envanteri, Japonya'nın bilim ve teknoloji politikalarının belirlenmesi ve stratejik planlaması için önemli bir kaynak olarak kullanılmaktadır. Çalışma, geniş bir uzman topluluğunun katılımıyla gerçekleştirilen bir anket yöntemi olan Delphi yöntemi kullanılarak gerçekleştirilir (Yıldırım, 2006).

Bu envanterde, Japonya'nın bilim ve teknoloji alanında gelecekteki öncelikleri, hedefleri ve politika alanlarını belirlemek için uzman görüşleri toplanır.

Uzmanlar, belirli teknoloji alanlarına, trendlere, yeniliklere ve diğer faktörlere ilişkin bilgilerini ve öngörülerini paylaşırlar. Bu bilgiler, Japonya'nın bilim ve teknoloji politikalarının şekillenmesinde ve stratejik planlamada kullanılır.

Japonya'nın Beşinci "Delphi" Envanteri, Japonya'nın bilim ve teknoloji alanında rekabetçi bir konumda kalmasını sağlamak, ekonomik büyümeyi desteklemek ve toplumsal ihtiyaçlara cevap vermek amacıyla gerçekleştirilir. Sonuçları, politika yapıcılar, araştırmacılar, endüstri liderleri ve diğer paydaşlar için bir yol haritası sunar ve Japonya'nın bilim ve teknoloji stratejilerini belirlemede rehberlik eder (Kocakulah ve Upson, 2004).

1.5.7.2. ABD'de yürütülen Öngörü Çalışmaları

ABD'de öngörü çalışmaları, birçok kurum, kuruluş ve akademik çevre tarafından yürütülen geniş kapsamlı bir faaliyettir. İşte ABD'de yürütülen öngörü çalışmalarının bazı örnekleri:

ABD Ulusal İstihbarat Konseyi: ABD Ulusal İstihbarat Konseyi (National Intelligence Council, NIC), ABD Başkanı'na ve hükümetine stratejik öngörüler sunan bir kuruluştur. NIC, küresel politika, ekonomi, teknoloji, güvenlik ve diğer konuları analiz eder ve uzun vadeli öngörüler geliştirir.

RAND Corporation: RAND Corporation, savunma, güvenlik, sağlık, eğitim, enerji ve diğer birçok alanla ilgili öngörü çalışmaları yürüten bağımsız bir araştırma kuruluşudur. RAND, ABD hükümetine ve diğer paydaşlara politika önerileri sunmak için analitik yöntemler kullanır (Brodie, 2011).

Brookings Enstitüsü: Brookings Enstitüsü, ekonomi, dış politika, sosyal politika ve diğer alanlarda öngörü çalışmaları yapan bir düşünce kuruluşudur. Enstitü, gelecekteki eğilimleri ve politika seçeneklerini analiz eder ve politika yapıcılar için bilgi sağlar (Milletler,2005).

ABD Savunma Bakanlığı (DoD): ABD Savunma Bakanlığı, güvenlik, askeri teknoloji ve strateji alanlarında öngörü çalışmaları yürütür. Örneğin, Pentagon'un gelecekteki savunma ihtiyaçlarını belirlemek için "Geleceğin Savunma Görünümü" raporları yayınlanır (Sezgin ve Sezgin, 2018).

Teknoloji Şirketleri ve Araştırma Kuruluşları: ABD'deki teknoloji şirketleri, öngörü çalışmalarını kendi bünyelerinde yürütür. Örneğin, Google, Microsoft, IBM gibi büyük teknoloji şirketleri, gelecekteki teknoloji trendleri, yapay zeka, bulut bilişim, otomasyon gibi konuları analiz eder ve politika yapıcılar için önemli bilgiler sağlar.

Bu sadece birkaç örnek olup, ABD'de öngörü çalışmaları çok çeşitli kurumlar ve kuruluşlar tarafından gerçekleştirilir. Bu çalışmalar, gelecekteki trendleri belirlemek, politika yapıcıları bilgilendirmek, stratejik planlama yapmak ve karar verme süreçlerine rehberlik etmek amacıyla yürütülür.

1.5.7.3. Almanya’nın 21. Yüzyıl Teknoloji Öngörüsü Çalışması

Almanya'nın 21. Yüzyıl Teknoloji Öngörüsü Çalışması, Almanya Federal Eğitim ve Araştırma Bakanlığı (BMBF) tarafından yürütülen bir girişimdir. Bu çalışma, Almanya'nın bilim, teknoloji ve yenilik alanındaki geleceğine yönelik öngörülerin belirlenmesi ve stratejik planlamanın yapılması amacıyla gerçekleştirilir.

Yüzyıl Teknoloji Öngörüsü Çalışması, geniş bir paydaş topluluğunun katılımıyla gerçekleştirilen bir süreçtir. Bu süreçte, akademisyenler, uzmanlar, endüstri temsilcileri, sivil toplum kuruluşları ve diğer ilgili paydaşlar bir araya gelerek gelecekteki teknolojik eğilimleri ve yenilik potansiyellerini tartışır ve analiz eder (Cuhls, 2008).

Çalışma kapsamında, Almanya'nın öncelikli alanları, teknolojik yetenekleri, sosyal ve ekonomik değişimleri ve sürdürülebilir kalkınma hedeflerini göz önünde

bulundurarak bir dizi senaryo oluşturulur. Bu senaryolar, farklı gelecek vizyonlarını ve potansiyel gelişim yollarını temsil eder.

Yüzyıl Teknoloji Öngörüsü Çalışması, Almanya'nın bilim ve teknoloji politikalarının belirlenmesinde ve stratejik planlamasında önemli bir rol oynar. Çalışmanın sonuçları, politika yapıcılar ve karar vericiler için bir yol haritası sunar ve Almanya'nın rekabetçi bir konumda kalması, inovasyon kapasitesini güçlendirmesi ve toplumsal ihtiyaçlara yanıt vermesi için rehberlik eder (Cuhls, 2008).

1.5.7.4. İngiltere'deki Teknolojik Öngörü Çalışmaları

İngiltere'de çeşitli kurumlar ve kuruluşlar tarafından yürütülen teknolojik öngörü çalışmaları bulunmaktadır. İşte bazı örnekler:

İngiltere Hükümeti - İleri Araştırma Projeleri Ajansı (ARPA): İngiltere hükümeti, ARPA aracılığıyla gelecekteki teknolojik eğilimleri belirlemek ve öngörüler oluşturmak için çalışmalar yürütür. ARPA, özellikle savunma, enerji, sağlık ve iletişim gibi stratejik alanlarda öncelikli teknolojik hedefler belirler (Miles, 2010).

İngiltere İleri Araştırma Merkezi (UKRI): UKRI, çeşitli araştırma konseylerini ve araştırma finansman ajanslarını bünyesinde barındıran bir kuruluştur. UKRI, bilimsel ve teknolojik öngörüler yapmak, araştırma ve inovasyon politikalarını belirlemek ve araştırma fonlarını yönlendirmek amacıyla çalışmalar yürütür (Smith ve Wynne, 2022).

İngiltere Bilim ve Teknoloji Tesisleri Konseyi (STFC): STFC, bilim ve teknoloji alanında öngörü çalışmaları yapar ve gelecekteki araştırma altyapısı ihtiyaçlarını belirler. STFC, bilim, mühendislik, astronomi, parçacık fiziği ve uzay bilimi gibi alanlarda öngörü çalışmalarına liderlik eder (Smith ve Wynne, 2022).

İngiltere Teknoloji Stratejisi Kurulu (TSB): TSB, teknolojik öngörüler yaparak İngiltere'nin rekabet gücünü artırmayı hedefleyen bir kuruluştur. TSB, gelecekteki teknoloji trendlerini izler, inovasyonu teşvik eder ve endüstri ve akademik işbirliğini destekler (Willetts, 2013).

İngiltere Teknoloji ve Strateji Kurumu (Technology and Strategy Board): Technology and Strategy Board, teknolojik öngörüler yaparak İngiltere'nin yenilikçilik ve rekabet gücünü geliştirmeyi amaçlar. Kurum, gelecekteki teknolojik eğilimleri analiz eder, araştırma ve inovasyon programlarına yönlendirme yapar ve teknoloji odaklı stratejik planlamayı destekler.

Bu kurumlar ve kuruluşlar, İngiltere'nin bilim, teknoloji ve inovasyon alanında öngörü çalışmaları yaparak ülkenin rekabet gücünü artırmayı, sürdürülebilir kalkınmayı desteklemeyi ve toplumsal ihtiyaçlara cevap vermeyi hedefler. Bu çalışmalar, politika yapıcılar, endüstri liderleri ve akademisyenler için yol haritası ve stratejik bilgi sağlar.

1.5.8. Sektörel Uygulama Örnekleri

Delphi yöntemi, bir konudaki uzmanların görüşlerini toplamak ve gelecekteki trendleri, olası senaryoları veya belirli bir sektördeki gelişmeleri tahmin etmek için yaygın olarak kullanılan bir yöntemdir. İşte Delphi yönteminin sektörel uygulama örneklerinden bazıları:

Teknoloji Sektörü: Teknoloji sektöründe, Delphi yöntemi yeni teknolojilerin keşfi, teknoloji trendlerinin belirlenmesi, gelecekteki teknolojik gelişmelerin tahmin edilmesi ve inovasyon stratejilerinin oluşturulması için kullanılabilir. Örneğin, yapay zeka, robotik, nesnelerin interneti gibi teknolojik alanlarda uzmanların görüşleri toplanarak gelecekteki eğilimler ve etkiler tahmin edilebilir.

Enerji Sektörü: Enerji sektöründe Delphi yöntemi, enerji kaynaklarının gelecekteki talebi, enerji politikaları, yenilenebilir enerji kaynaklarının benimsenmesi ve enerji verimliliği gibi konularda uzmanların görüşlerini değerlendirmek için kullanılabilir. Bu şekilde, enerji sektöründeki değişimler ve gelecekteki enerji dönüşümüne yönelik öngörüler elde edilebilir (Di Zio ve Maretti, 2014).

Sağlık Sektörü: Sağlık sektöründe Delphi yöntemi, sağlık hizmetlerinin gelecekteki talebi, sağlık politikaları, hastalıkların yayılımı, sağlık teknolojilerinin gelişimi gibi konularda uzmanların görüşlerini toplamak için kullanılabilir. Bu şekilde, sağlık sektöründe ortaya çıkabilecek değişiklikler ve sağlık sistemlerinin gelecekteki ihtiyaçlarına yönelik öngörüler elde edilebilir (Sangal ve ark., 2022).

Finans Sektörü: Finans sektöründe Delphi yöntemi, ekonomik trendler, finansal piyasaların gelecekteki performansı, risk yönetimi stratejileri gibi konularda finansal uzmanların görüşlerini toplamak için kullanılabilir. Bu şekilde, finansal kararlar ve yatırım stratejileri için gelecekteki belirsizliklerin azaltılmasına yardımcı olacak öngörüler elde edilebilir (KUO ve CHEN, 2008).

Ulaşım ve Lojistik Sektörü: Ulaşım ve lojistik sektöründe Delphi yöntemi, ulaşım sistemlerinin gelecekteki talebi, sürdürülebilirlik, otomasyon ve lojistik operasyonların gelişimi gibi konularda uzmanların görüşlerini toplamak için kullanılabilir. Bu şekilde, ulaşım ve lojistik sektöründe meydana gelebilecek değişimler ve sektöre yönelik stratejik kararlar için öngörüler elde edilebilir.

Bu örnekler, Delphi yönteminin çeşitli sektörlerde kullanılabileceğini göstermektedir. Ancak, Delphi yöntemi genel olarak belirli bir konu veya sektöre odaklanmış olabilir ve uygulama alanı çeşitlilik gösterebilir. Bu çalışmada spor sektöründe ait bir uygulama olacaktır. Delphi yöntemi, spor sektöründe de kullanılabilecek bir öngörü yöntemidir. Spor sektöründe Delphi yöntemi, gelecekteki spor trendleri, spor etkinliklerinin organizasyonu, spor pazarlaması, sporcu performansı ve spor tesisleri gibi konuları değerlendirmek için kullanılabilir. İşte Delphi yönteminin spor sektörüne ait bir uygulama örneği:

Spor Trendleri: Delphi yöntemi, spor sektöründeki uzmanların görüşlerini toplayarak gelecekteki spor trendlerini belirlemek için kullanılabilir. Bu, spor organizasyonları, spor giyim ve ekipmanları, spor teknolojileri ve sporcu performansı gibi alanlarda öngörüler elde etmek için değerli bir araç olabilir. Örneğin, uzman görüşleri ile gelecekteki popüler spor türleri, egzersiz trendleri, spor etkinliklerinin evrimi ve diğer sporla ilgili konular hakkında bilgi edinilebilir (Young ve Ross, 2000).

Delphi yöntemi, spor sektöründe trendleri öngörmek, stratejik planlama yapmak ve karar vermek için bir araç olarak kullanılabilir. Bu şekilde, spor organizasyonları, spor kulüpleri, spor markaları ve diğer sporla ilgili kuruluşlar, gelecekteki değişimlere uyum sağlamak ve rekabet avantajı elde etmek için sağlam bir temele dayanan öngörülere sahip olabilirler.

1.6. Sporda Bilişim Teknolojisi Kullanımı

Sporda bilişim teknolojisi, birçok farklı alanda kullanılan çeşitli teknolojik araç ve yöntemlerin spor alanına uygulanmasıdır. Sporda bilişim teknolojisi kullanımının bazı örnekleri şunlardır:

Veri Analitiği: Sporcuların performansını ve takımın taktiksel stratejilerini analiz etmek için veri analitiği kullanılır. Oyuncuların istatistiksel verileri, hareket izleme sistemleri, sensörler ve diğer kaynaklardan toplanır ve analiz edilerek eğilimler, zayıf yönler ve iyileştirme alanları belirlenir (Korkut, 2022).

Video Analizi: Spor müsabakalarının ve antrenmanların video kayıtları, teknik analizler ve taktiksel incelemeler için kullanılır. Video analizi yazılımları, antrenörlerin ve sporcuların maçları veya antrenmanları geri sararak hareketleri, stratejileri ve hataları analiz etmelerini sağlar (Baykan, 2022).

Hareket İzleme Sistemleri: Sporcuların hareketlerini ve vücut mekaniğini izlemek için kullanılan sistemlerdir. Bu sistemler, giyilebilir sensörler, kamera sistemleri veya radar teknolojisi gibi farklı yöntemleri kullanabilir. Hareket izleme sistemleri, sporcuların teknik becerilerini analiz etmek, yaralanma risklerini değerlendirmek ve performanslarını optimize etmek için kullanılır (Tozkoparan ve Karaduman, 2022).

Elektronik Ölçüm Cihazları: Spor müsabakalarında kullanılan elektronik ölçüm cihazları, örneğin tenis maçlarında kullanılan hattı geçip geçmediği belirleyen sistemler veya atletizm yarışmalarında kullanılan zamanlama sistemleri gibi, doğruluk ve hassasiyet sağlamak için kullanılır (Akyıldız ve Yıldız, 2020).

Sanal Gerçeklik (VR) ve Artırılmış Gerçeklik (AR): Sanal gerçeklik ve artırılmış gerçeklik teknolojileri, sporculara ve antrenörlere gerçekçi simülasyonlar sunarak antrenmanları ve taktiksel çalışmaları iyileştirmek için kullanılır. Ayrıca, sporseverlere etkileşimli deneyimler sunmak ve maçları farklı bir perspektiften izlemelerini sağlamak için de kullanılabilir.Ayrıca e-sporda sanal gerçeklik yaratılarak bir spor karşılaştırma yapılmaktadır. E-Sporun paydaşları olarak ifade edilebilecek oyun üreten firmalar ve yayımcıları, takım sahipleri ve oyuncular, sponsor firmalar, organizatörler, koçlar, izleyiciler ve menajerler ile bir endüstri haline geldiği söylenebilir (Yükçü ve Kaplanoğlu, 2018).

Sporcuların İzlenmesi ve İzleme Sistemleri: GPS izleme cihazları, hareket sensörleri ve diğer izleme sistemleri kullanılarak sporcuların performansı takip edilir. Bu sistemler, sporcuların hızı, mesafe, kalori tüketimi gibi verileri ölçer ve antrenman programlarının tasarlanmasında ve iyileştirilmesinde kullanılır.

Spor Ekipmanları ve Malzemeleri: Bilişim teknolojisi, spor ekipmanlarının ve malzemelerinin tasarım ve geliştirilmesinde kullanılır. Örneğin, tenis raketleri, golf sopaları, bisikletler gibi spor ekipmanları, bilgisayar simülasyonları ve modellerle optimize edilir ve performansı artırıcı özelliklere sahip olur.

Spor Yayıncılığı ve İnteraktif Deneyimler: Bilişim teknolojisi, spor etkinliklerinin yayınlanması ve interaktif deneyimlerin sunulması için kullanılır. İnternet ve mobil uygulamalar aracılığıyla spor müsabakaları canlı yayınlanır, istatistikler ve anlık bilgiler sunulur, izleyicilerle etkileşim sağlanır.

Bu sadece birkaç örnek olup, spor alanında bilişim teknolojisi kullanımı sürekli olarak gelişmektedir. Teknoloji, sporcuların performansını artırmak, antrenmanları optimize etmek, takım stratejilerini geliştirmek ve taraftar deneyimini zenginleştirmek için kullanılmaktadır.

1.6.1. Sporda Alanında Bilişim Teknolojisinin Ekonomik Önemi

Sporda bilişim teknolojisinin ekonomik önemi oldukça büyüktür. İşte sporda bilişim teknolojisinin ekonomiye katkılarından bazıları:

Pazarlama ve Gelir Olanakları: Bilişim teknolojisi, spor kulüpleri ve organizasyonlar için yeni pazarlama ve gelir fırsatları sunar. Örneğin, dijital medya ve sosyal medya platformları aracılığıyla, spor organizasyonları markalarını tanıtabilir, taraftarlarla etkileşim kurabilir ve sponsorluk anlaşmaları yapabilir. Ayrıca, çevrimiçi mağazalar ve bilet satış platformları üzerinden ürün ve hizmetlerin satışı da gerçekleştirilebilir (Özdengül ve Aydın, 2022).

Yayın Hakları ve Medya Gelirleri: Bilişim teknolojisi, spor etkinliklerinin canlı yayınlanması ve dijital medya platformları üzerinden izlenebilmesini sağlar. Bu, spor organizasyonlarına ve kulüplere yayın haklarından kaynaklanan gelirlerin artmasını sağlar. Aynı zamanda, reklam gelirleri ve sponsorluk anlaşmaları da bu yayın platformları üzerinden elde edilebilir (Özdengül ve Aydın, 2022).

Veri Analizi ve Performans Geliştirme: Bilişim teknolojisi, sporcuların performansını analiz etmek ve geliştirmek için kullanılır. Veri analizi araçları ve sensörler, sporcuların hareketlerini, hızlarını, kalp atışlarını ve diğer performans

göstergelerini ölçer (Bakır ve Müniroğlu, 2007). Bu veriler, antrenman programlarının ve stratejilerin iyileştirilmesine yardımcı olur ve sporcuların daha iyi sonuçlar elde etmelerini sağlar. İyi performans gösteren sporcuların ve takımların başarıları, sponsorluk anlaşmaları ve reklam gelirlerini artırabilir.

Ekipman Geliştirme ve Satışı: Bilişim teknolojisi, spor ekipmanlarının ve malzemelerinin tasarım ve geliştirilmesinde kullanılır. Bilgisayar simülasyonları, sensörler ve diğer teknolojilerle ekipmanlar optimize edilir ve sporcuların performansını artıracak özelliklere sahip hale getirilir. Gelişmiş ekipmanlar, talep ve satışlarını artırarak spor endüstrisine ekonomik katkı sağlar (Akyıldız ve Yıldız, 2020).

İnteraktif Deneyimler ve Abonelik Modelleri: Bilişim teknolojisi, spor izleyicilerine interaktif deneyimler sunar. Mobil uygulamalar, sanal gerçeklik ve artırılmış gerçeklik gibi teknolojilerle izleyiciler, spor etkinliklerini daha yakından takip edebilir, istatistiklere erişebilir ve etkileşimde bulunabilir. Ayrıca, bazı spor organizasyonları abonelik modelleri sunarak, izleyicilere özel içerik ve deneyimler sunar ve bu da ekonomik getiriler sağlar (İçten ve Güngör, 2017).

Bu faktörler, sporda bilişim teknolojisinin ekonomik olarak önemini artırır ve spor endüstrisine büyük katkılar sağlar.

1.6.2. Sporda Bilişimin Küreselleşmeye Etkisi

Sporda bilişim teknolojisinin küreselleşmeye etkisi oldukça büyük olmuştur. İşte sporda bilişimin küreselleşmeye olan etkilerinden bazıları:

Küresel İletişim: Bilişim teknolojisi, sporla ilgili haberlerin, bilgilerin ve etkinliklerin hızla küresel düzeyde paylaşılmasını sağlar. Sosyal medya, dijital yayın platformları ve spor web siteleri aracılığıyla spor haberleri anında tüm dünyaya

ulaşır. Bu da sporun daha geniş bir kitleye ulaşmasını ve küresel bir iletişim ağı oluşturmasını sağlar (Kubat, 2021).

Uzaktan İzleme ve Erişim: Bilişim teknolojisi, spor etkinliklerini canlı olarak izlemek için uzaktan erişim imkanı sağlar. Spor müsabakaları, çevrimiçi yayın platformları aracılığıyla dünyanın herhangi bir yerinden izlenebilir. Bu da insanların farklı kültürlerden ve coğrafyalardan spor etkinliklerine erişebilmesini sağlar ve küresel bir izleyici kitlesi oluşturur.

Küresel Transferler ve Takımlar: Bilişim teknolojisi, sporcuların transfer süreçlerini ve takım oluşturma süreçlerini kolaylaştırır. İnternet ve diğer iletişim teknolojileri, spor kulüplerinin dünya genelindeki yetenekli sporcuları keşfetmesine ve transfer görüşmelerini yapmasına yardımcı olur. Bu da farklı ülkelerden sporcuların farklı takımlara transferini ve küresel takımların oluşmasını sağlar.

Küresel Veri Paylaşımı ve Analizi: Bilişim teknolojisi, spor performansıyla ilgili verilerin küresel düzeyde paylaşılmasını ve analiz edilmesini sağlar. Antrenörler, takımlar ve uzmanlar, farklı ülkelerden elde edilen verileri paylaşarak en iyi uygulamaları öğrenir ve performansı geliştirmek için yeni yöntemler keşfeder (Appelqvist ve ark., 2013).

İnteraktif Deneyimler: Bilişim teknolojisi, spor izleyicilerine interaktif deneyimler sunar. Sanal gerçeklik, artırılmış gerçeklik ve diğer teknolojilerle, izleyiciler spor etkinliklerine katılmış gibi hissedebilir ve etkileşimde bulunabilir. Bu da sporun küresel bir deneyim haline gelmesini sağlar (İçten ve Güngör, 2017).

Bu etkiler, sporda bilişim teknolojisinin küresel düzeyde daha fazla bağlantı, erişim ve etkileşim sağladığını göstermektedir. Spor, küresel bir fenomen haline gelerek farklı kültürlerin bir araya gelmesine ve sporun daha geniş bir kitleye ulaşmasına katkıda bulunur.

1.6.3. Dünyada Spor Bilişimi Sektörü

Dünyada spor bilişimi sektörü, hızla gelişen ve büyüyen bir sektördür. Spor organizasyonları, kulüpler, federasyonlar, medya şirketleri ve teknoloji firmaları arasında giderek artan bir talep ve ilgiyle karşılaşmaktadır. İşte spor bilişimi sektörünün bazı özellikleri:

Veri Analitiği ve Performans Optimizasyonu: Spor bilişimi sektörü, veri analitiği ve performans optimizasyonu konularında büyük bir rol oynar. Sporcuların performansını analiz etmek, antrenman programlarını optimize etmek ve takım performansını geliştirmek için veri analitiği ve ölçüm araçları kullanılır. Bu, sporculardan elde edilen verilerin toplanması, analizi ve kullanılmasıyla gerçekleştirilir.

Canlı Yayın ve İnteraktif Deneyimler: Spor bilişimi sektörü, canlı yayın ve dijital medya teknolojileri konusunda da büyük bir etkiye sahiptir. Spor etkinliklerinin canlı olarak yayınlanması, sosyal medya platformları üzerinden izlenmesi ve izleyicilere interaktif deneyimler sunulması yaygın hale gelmiştir. İzleyiciler, istatistiklere erişebilir, çoklu kamera açılarından maçları izleyebilir ve etkinliklere katılan diğer izleyicilerle etkileşimde bulunabilir.

E-ticaret ve Lisanslama: Spor bilişimi sektörü, e-ticaret ve lisanslama konularında da önemli bir rol oynar. Spor kulüpleri ve organizasyonlar, dijital platformlar aracılığıyla ürün ve hizmetlerini satışa sunar. Lisanslı ürünlerin satışı da önemli bir gelir kaynağı haline gelmiştir. Ayrıca, spor bilişimi sektörü, spor markalarının dijital pazarlama stratejileri ve sponsorluk anlaşmaları konularında da aktif bir rol oynar.

Sağlık ve Performans Takibi: Spor bilişimi sektörü, sporcuların sağlık ve performans takibinde önemli bir rol oynar. Akıllı saatler, sporcu takip sistemleri ve diğer sağlık teknolojileri, sporcuların fiziksel aktivitelerini ve sağlık durumlarını

takip etmelerine yardımcı olur. Bu veriler, sporcuların performanslarını izlemelerine ve gerektiğinde iyileştirmeler yapmalarına olanak tanır (Ráthonyi ve ark., 2018).

Spor İçerik Yönetimi ve Analitiği: Spor bilişimi sektörü, spor içerik yönetimi ve analitiği konularında da önemli bir rol oynar. Spor medya şirketleri, dijital platformlar üzerinden spor içeriği sunar ve izleyicilerin ilgi alanlarına göre kişiselleştirilmiş içerikler sunar. Ayrıca, izleyici davranışlarının analizi ve kullanıcı verilerinin değerlendirilmesi, pazarlama stratejilerini ve içerik yönetimini şekillendirir (Liu ve Zou, 2021).

Dünya genelinde spor bilişimi sektörü hızla büyümekte ve teknolojik gelişmelerle birlikte daha da ilerlemektedir. Spor endüstrisinde bilişim teknolojilerinin kullanımı, etkinliklerin daha erişilebilir hale gelmesini sağlamakta ve izleyicilerle daha interaktif deneyimler yaşanmasına olanak tanımaktadır.

1.6.4. Türkiye'de Spor Bilişimi Sektörü

Türkiye'de spor bilişimi sektörü, son yıllarda önemli bir gelişme göstermektedir. Spor kulüpleri, federasyonlar, medya şirketleri ve teknoloji firmaları arasında artan bir ilgi ve yatırım söz konusudur. Türkiye'deki spor bilişimi sektörünün dijital medya ve canlı yayınları bulunmaktadır. Türkiye'de spor etkinliklerinin dijital platformlar aracılığıyla canlı olarak yayınlanması yaygınlaşmıştır. Spor kulüpleri ve federasyonlar, kendi dijital kanallarını oluşturarak maçları, röportajları ve diğer içerikleri izleyicilere sunar. Ayrıca, sosyal medya platformları üzerinden etkinliklere ilişkin içerikler paylaşılır ve izleyicilerle etkileşim sağlanır. Türkiye Radyo Televizyon Kurumu Türkiye'deki spor canlı yayın sayısını artırarak TRT Spor kanalına ek olarak TRT SPOR Yıldız, 21 Eylül 2019'da TRT Spor 2 HD ismiyle test yayınlarına başlayıp, 19 Mayıs 2021'den itibaren normal yayına geçiş yapmıştır (Trtspor, 2019). Ayrıca son on yılda Türkiye'de çok sayıda spor kanalı dijital platformlarda ve uydu yayınlarında kanal sayısı artırmıştır (Budak, 2019).

Türkiye'deki spor bilişimi sektörü, veri analitiği ve performans takibi konularında da gelişme göstermektedir. Spor kulüpleri, sporcuların antrenman verilerini ve performans istatistiklerini toplayarak analiz eder ve antrenman programlarını optimize etmeye çalışır. Bu sayede sporcuların performanslarının artırılması hedeflenir.

Türkiye'de spor bilişimi sektörü, e-ticaret ve lisanslama konularında da önemli bir yer tutar. Spor kulüpleri, resmi web siteleri veya dijital platformlar üzerinden lisanslı ürünlerin satışını yapar. Taraftarlara özel ürünler, giyim ve eşyaların satışı ile gelir elde edilir. Bu özellikle Türkiye'de büyük kitleye hitap eden dört büyük aracığı satışları ve sponsorlar gelirleri oldukça fazladır (Tolan, 2014).

Türkiye'deki spor bilişimi sektörü, mobil uygulamalar ve interaktif deneyimler konusunda da ilerlemektedir. Spor kulüpleri ve federasyonlar, kendi mobil uygulamalarını kullanarak taraftarlara özel içerikler sunar, maç takibi yapma imkanı sağlar ve etkileşimli deneyimler sunar.

Türkiye'deki spor bilişimi sektörü, daha fazla yenilik ve yatırım ile büyümeye devam etmektedir. Teknolojik gelişmelerin ve dijitalleşmenin hız kazandığı bir dönemde, sporun dijital dünyayla entegrasyonu önemli bir rol oynamaktadır.

Bütün bunlar Türkiye'de spor sektörünün popüleritisi ve pazar payı ile kullanılan sistemlerdir.Fakar şuana kadar yerli ve milli ürünler pazarda çokda görünmemektedir.Bu yüzden dışsal bağlılık söz konusudur.

1.7. Sporda Siber Güvenlik Teknolojisi

Sporun her alanında olduğu gibi spor hekimliğinden tutun spor kulüplerine kadar sporcuların yaralanmaları önlemek ve atletik performansı iyileştirmek için veri alışverişinin kullanılması özellikle sporcular için yararlı olabilir. Bununla birlikte, güvenlik açıkları ve bu verileri çevreleyen güvenlik düzenlemelerinin olmaması,

sporcular ve kişisel mahremiyetlerinin yanı sıra oyun sonuçlarına ilişkin bahisler, bilet satışları ve reklam sözleşmeleri dahil olmak üzere oyunu çevreleyen pazar için bir risk oluşturmaktadır.

Oyunlar ve antrenmanlar sırasında gerçek zamanlı veri aktarımı anında teşhise olanak sağlasa da, aktarılan verilerin çalınma ve cezai amaçlarla kullanılma riski vardır. Özel atletik verilerin önceki veri ihlallerini araştırmak, sporda büyük verilerin kullanımına ilişkin etik kaygıları ve güvenlik risklerini analiz etmek ve spor organizasyonlarının siber güvenlik çabalarını iyileştirmeleri için eylemler planlanmalıdır (Greenwald, 2017).

1.7.1. Siber Güvenliğin Tarihçesi

Siber güvenlik tarihçesi ve gelişimi ile bilişim teknolojileri alanında yer alan önemli konulardan birisidir. Ülkemizde bilgisayarlar 1960 yılında Kara yolları genel müdürlüğünde devasa büyüklükteki IBM-650 kullanılmaya başlandı. Başlarda tüm dünyada da olduğu üzere bir takım hesaplama işlemleri için kullanılan bilgisayarlar Windows 95 ile birlikte bilgisayarın sıkıcı mavi ekranından kurtulup ilgi çekici bir hal almaya başladı. 1981 yılında ilk kişisel bilgisayarlar IBM tarafından piyasaya sürüldü. Artık bilgisayar çantaya sığacak kadar küçüldü. Bilgisayar kullanıcı sayısı da buna bağlı olarak hızla artmaya başladı. İlk piyasaya sürülen işletim sistemleri internet alt yapısı bakımından savunmasız bir durumdaydı.

Siber güvenlik duvarı veya virüs programı gibi kavramlar ortada yoktu. İşletim sistemi üreticileri bilgisayar kullanıcılarının birbirlerinin verilerine sızabileceğini hiç düşünmemişlerdi. Yada her sistemin bir arka kapısı vardır hiçbir sistem kusursuz değildir kavramlarıyla daha karşılaşmamışlardı. İlk hackerler eğitimin ve öğretimin gerçekleştiği üniversitelerde ortaya çıktı. Bu hackerler başka kullanıcıların bilgisayarlarına girip kullanıcının yapabileceği her türlü işlemi yapabiliyorlardı. Bunun üzerine işletim sistemleri için ilk kez güvenlik duvarını (firewall) geliştirildi. Ancak bu güvenlik duvarları o kadar yetersizdi ki sürekli aynı

kapıyı kullanan hackerler artık güvenlik duvarının etrafından dolaşıp arka kapıdan erişimi sağladılar.

1986 yılında kamu, kişisel ve tüzel kişilerin bilgisayarlarına yoğun bir şekilde saldırı yapılması Amerikan hükumetini harekete geçirdi ve izinsiz olarak başka bilgisayarlara erişim sağlayan hackerlere hapis cezası uygulanacağına karar verildi. Solucan ve trojen adı verilen bir çok zararlı yazılımla bilgisayarlarda hasar bırakan hackerlar binlerce bilgisayara zarar vermişlerdir. İlerleyen yıllarda bu gibi durumların artması ile IBM 1989 yılında ilk anti virüs programını yazdı. Virüslere karşı hem güvenlik duvarı hem de anti virüs programı kullanılmaya başlandı (Uslu, 2007).

1994 yılında web tarayıcıları üretildi. Bu gelişmeyle birlikte hackerlar ile kullanıcıların yüz yüze etkileşime gireceği alanın alt yapısı oluştu. Bilinçsiz internet kullanıcılarının kişisel bilgilerinin web üzerinden paylaşılması birçok sorunu da beraberinde getirdi. 1998 yılından itibaren basit ve belirli kalıpları olan hackerler artık trojenler (Truva atı) yardımı ile kullanıcıların bilgisayarlarında güvenlik zafiyeti yaratarak hackerlerin bilgisayar sistemlerine sızmasını kolaylaştırmışlardır. 1999 yılında Windows 98 ile bir çok güvenlik açığı kapatıldı ve yeni daha az güvenlik zafiyeti bulunan firewall güvenlik duvarı oluşturuldu. Artık ağ ve benzeri alanlar üzerinde erişim sağlayamayan hackerler e-posta yoluyla kullanıcının kendi rızası ile güvenlik zafiyeti oluşturmaya başladılar.

2000 yılında yeni yöntemler üreten bilgisayar korsanları web sitelerine DOS saldırıları yapmaya başladılar. Sunucular bu kadar yoğun iletiye cevap veremeyince işlevini yerine getiremez hale geldiler. Hackerler kullanıcıların kredi kartı bilgilerini çalmaya başladılar. Bilgisayar korsanları hep bir adım öndeydiler. Yakın geçmişte özgün olarak yazılan birçok anti virüs yazılımı bu gün büyük ölçüde hackerleri durdurmuş gibi. Şimdilerde çok iyi yazılım bilgisine sahip hackerler kendilerini zor güvenlik duvarlarını aşmak için pek çaba göstermiyorlar. İnsan psikolojisini ve insanın yapay zekadan farklı olarak her etkiye verdiği tepkiyi göz önünde bulundurursak. Hackerler yüz yüze veya iletişim yolları ile insanları dolandırıp onları

mağdur etmeye devam etmektedir. Tek fark yapay zeka ile vakit kaybetmeyi bir kenara bırakıp insan gibi bir değişkeni gözlemleyerek dolandırıcılık yöntemlerine başvurmaktadırlar.

1.7.2. Sporda Siber Güvenlik Teknolojileri ve Ürünleri

Sporda siber güvenlik teknolojileri ve ürünleri, spor organizasyonlarının ve sporcuların dijital güvenliklerini korumak için kullanılan çeşitli araçlar ve yöntemlerdir. İşte bazı örnekler:

Güvenlik Yazılımları: Spor organizasyonları ve sporcular, siber saldırılara karşı korunmak için güvenlik yazılımları kullanır. Bu yazılımlar, virüs ve kötü amaçlı yazılımları tespit etmek, ağ güvenliğini sağlamak, veri şifrelemesi yapmak ve yetkilendirme süreçlerini yönetmek gibi işlevlere sahiptir.

İzleme ve Analiz Sistemleri: Spor organizasyonları, dijital ortamda gerçekleşen faaliyetleri izlemek ve analiz etmek için izleme ve analiz sistemleri kullanır. Bu sistemler, ağ trafiğini ve kullanıcı etkinliklerini izleyerek anormal durumları tespit eder ve siber saldırılara karşı erken uyarı sistemleri sağlar.

İki Faktörlü Kimlik Doğrulama: İki faktörlü kimlik doğrulama, sporcuların ve spor organizasyonlarının hesaplarının güvenliğini artırmak için kullanılan bir teknolojidir. Bu yöntemde, kullanıcılar sadece parola değil, aynı zamanda bir ikincil doğrulama faktörü (örneğin, SMS doğrulama kodu, biyometrik veriler vb.) kullanarak kimliklerini doğrularlar.

Ağ Güvenliği Ekipmanları: Spor organizasyonları, ağ güvenliğini sağlamak için çeşitli ekipmanlar kullanır. Bunlar arasında güvenlik duvarları, saldırı tespit ve önleme sistemleri (IDS/IPS), sanal özel ağ (VPN) teknolojileri ve güvenli yönlendiriciler yer alır.

Veri Şifreleme: Sporcuların ve spor organizasyonlarının hassas verilerini korumak için veri şifreleme teknolojileri kullanılır. Bu teknolojiler, verilerin şifrelenerek izinsiz erişime karşı korunmasını sağlar ve veri güvenliğini sağlar. (Yılmaz ve Balli, 2016).

Eğitim ve Farkındalık Programları: Spor organizasyonları ve sporcular, siber güvenlik konusunda eğitim programlarına ve farkındalık kampanyalarına katılır. Bu programlar, kullanıcıların güvenli internet kullanımı konusunda bilinçlenmelerini sağlar, phishing gibi saldırıları tanımalarını öğretir ve güvenli davranış alışkanlıklarını teşvik eder.

Bu örnekler, spor organizasyonları ve sporcuların siber güvenlik teknolojileri ve ürünleri kullanarak dijital güvenliklerini sağlamak için kullandıkları bazı araçları göstermektedir. Her bir spor organizasyonu veya sporcu, ihtiyaçlarına ve bütçesine uygun olan teknolojileri seçebilir ve uygulayabilir. Bu çalışmada bu ürünlerin daha fazlasını genişleterek anlatacağız.

1.7.2.1. Ağ Güvenliği

Spor organizasyon ve şirketlerde ağ güvenliği, ağ altyapısını yetkisiz erişime, yanlış kullanıma, arıza, değişiklik, imha veya yanlış bilgilendirmeye karşı korumak için gerek donanım gerek yazılım olarak önleyici önlemlerin alınması işlemidir. Spor işletmelerinde veya organizayonlarında güvenli bir platform oluşturularak, bilgisayarlar, kullanıcılar ve programlar için izin verilen kritik işlevlerin güvenli bir ortamda gerçekleştirilmesi sağlanır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Ağ Politika Yönetimi, Güvenlik Duvarı, Ağ İzleme, Saldırı Önleme Sistemleri, Toplu Saldırı Yönetimi vb.

1.7.2.1.1. Ağ Politika Yönetimi (Network Policy Management)

1.7.2.1.1.1. Ağ Güvenlik İlke Yönetimi (Network Security Policy Management)

Ağ Güvenlik İlke Yönetimi (Network Security Policy Management) Ağ Güvenlik İlke Yönetimi sağlayıcıları, kural performansını optimize etmek ve yönetim iş akışını değiştirmek, uyumluluk için kuralları kontrol etmek ve birden çok ağ yolu üzerinde dağıtılan bir ağ haritasını görselleştirmek için analitik araçlar sağlar.

1.7.2.1.1.2. Ağ Erişim Denetimi (Network Access Control)

Bir ağ erişim denetimi (NAC) işlemi, tüm aygıtların ve kullanıcıların erişimini denetlemek için ağa politikalar ekler. Politikalar, cihaz ve / veya kullanıcı kimlik doğrulamasına ve uç nokta yapılandırmasına bağlı olabilir.

1.7.2.1.1.3. Yazılım Tanımlı Güvenlik (Software-Defined Security)

Yazılım Tanımlı Güvenlik bir çatı terimdir. Güvenlik politika yönetiminin soyutlaştırılmasından fayda sağlayan teknolojilerin birleşiminden oluşmaktadır. Lokasyondan bağımsız olarak iş yükü ve bilgi korunması, güvenlik kontrollerinin risk profiline göre ayarlanması gibi özellikleri mevcuttur.

1.7.2.1.1.4. Ağ İzleme ve Adli Bilişim (Network Monitoring and Forensics)

Ağ izleme, bir bilgisayar ağını ve bileşenlerini sürekli olarak izleyen ve ağ yöneticisine (e-posta, SMS veya diğer alarmlar aracılığıyla) kesinti veya başka bir sorun olması durumunda bunu bildiren bir sistemin kullanılmasıdır. Ağ adli bilişimi,

güvenlik saldırılarının veya diğer sorunlu olayların kaynağını keşfetmek için ağ olaylarının yakalanması, kaydedilmesi ve analiz edilmesidir

1.7.2.1.2. Ağ Güvenlik Duvarı (Network Firewall)

1.7.2.1.2.1. Hizmet Olarak Güvenlik Duvarı (Firewall as a Service)

Hizmet Olarak Güvenlik Duvarı (FwaaS) bulut bazlı servis veya hibrit çözüm (bulut&geliştirme uygulamaları) olarak servis veren güvenlik duvarıdır. FwaaS'in vaatleri; merkezcil yönetim biçimini öne çıkararak, daha çok kurumsal güvenlik duvarı özellikleri kullanmak ve güvenlik incelemelerini bir bulut altyapısına kısmen ya da tamamen aktararak, daha basit ve daha esnek mimari sağlamaktır.

1.7.2.1.2.2. Yeni Nesil Güvenlik Duvarları (Next-Generation Firewalls)

Yeni Nesil Güvenlik Duvarları (NGFW), port/protokol incelemesinin ötesinde, uygulama ekleme seviyesindeki incelemeyi durdurma ve güvenlik açığının önlemesi gibi güvenlik duvarı dışından da bilgi getirebilen, derin paket inceleyici güvenlik duvarlarıdır. Bu ekstra güvenlik duvarı bilgi servisleri bulut bazlı gelişmiş tehdit tespiti ve tehdit bilgisini içerir. NGFW, bağımsız tehdit önleme sistemleri veya birleşik tehdit yönetimi ile karıştırılmamalıdır.

1.7.2.1.2.3. Durum Denetlemeli Güvenlik Duvarları (Stateful Firewalls)

Durum Denetlemeli Güvenlik Duvarı: "Durum" kullanımı bağlantının nasıl kullanıldığı hakkında daha güvenli bilgi verirken; eski güvenlik duvarları sadece internet protokol (IP) adres kaynağı, varış noktası ve portlarını kullanmaktaydı. Durumsal güvenlik duvarları; kaynak IP, varış IP, kullanılan portlar ve kaynak ile hedefin arasındaki geçmiş etkileşimlere dayalı paket filtreleme ve kontroller

bulundurur. Durum denetlemeli güvenlik duvarları; yönlendirici ve servis sağlayıcı bulut altyapısı (IaaS) dahil pek çok teknolojide yer alabilir.

1.7.2.1.3. Saldırı Önleme Sistemi (IPS)

1.7.2.1.3.1. Ağ Saldırı Önleme Sistemi (Network IPS)

Bir ağ saldırı önleme sistemi (IPS) sıralı, derin paket inceleme gereçleri ile teknolojik gelişmeleri kullanarak saldırıları ve istenmeyen trafiği belirler, engeller ve bunlara karşı koruma sağlar. Ağ IPS'leri gelecek nesil IPS'leri (NGIPS) gibi kullanıcı veya uygulama içeriklerine yaptırım uygulamaz.

1.7.2.1.3.2. Yeni Nesil Saldırı Önleme Sistemi (Next-Generation IPS)

Yeni nesil saldırı önleme sistemleri, birinci nesil saldırı önleme sistemi (IPS) yeteneklerine ek olarak, uygulama bilinci ve tam yığın görünürlük, içerik ve bağlam farkındalığı, yeni bilgi kaynaklarını entegre etmek için yolar sağlar.

1.7.2.1.3.3. Dağıtık Hizmet Dışı Bırakma Savunması (DDoS Defense)

Dağıtık Hizmet Dışı Bırakma saldırılarında, internetin iş amaçlı kullanımına engel olmak veya şirketlerden para koparmaya çalışmak için pek çok teknik kullanılır. Hackerlık, siyasal veya sosyal amaçlı olarak düşünüldüğünde, DDOS saldırganları için motivasyon kaynaklarından biridir. DDoS savunma ürünleri ve servisleri, bu tip saldırıları tespit eder ve azaltır.

1.7.2.1.3.4. Birleşik Tehdit Yönetimi (UTM)

Birleşik tehdit yönetimi platformları, özellikle küçük veya orta ölçekli işletmelerde kullanılan, çok fonksiyonlu ağ güvenlik uygulamalarıdır. Özellik kullanılabilirliği büyümekte olup, diğer ağ güvenlik teknolojilerinin yeni özelliklerini alabilir; fakat daha fazla özellik geçerli kılındığında performası yavaşlamaktadır. Bu yüzden başlıca UTM kullanılan durumlar, personel üretkenliği ve internet güvenliğidir. Fonksiyonların hiçbiri türünün en iyisi olamazken, UTM ürünleri düşük maliyet ihtiyacını karşılar.

1.7.2.1.4. Yazılım Tanımlı Ağlar ve Ağ Fonksiyonu Sanallaştırma (SDN and NFV Security)

1.7.2.1.4.1. Yazılım Tanımlı Çevre (Software-Defined Perimeter)

Yazılım Tanımlı Çevre (YTÇ), güvenli bölgede yer alan, farklı şeylerden oluşan, ağ bağlantılı katılımcıların mantıksal setini tanımlar. Kaynaklar genellikle açık erişime gizlidir, güvenlik aracıları aracılığıyla erişim sınırlıdır ve saldırılabilir alanı azaltır.

1.7.2.1.4.2. Ağ Anahtarı Güvenliği (Security in the Switch)

Ağ Anahtarı Güvenliği, mevcut ağ güvenlik kontrollerini, ağ ve diğer altyapı ürünlerinin içerisine dahil eder. Bu da ağ güvenlik sınıflandırması ve iç ağ güvenlik fonksiyonlarını ayrık gereçlerden ziyade ağ yapısının parçası olarak uygulayarak, maliyet düşürülmesini sağlar. Bu teknoloji sanallaştırma, ağ fonksiyon sanallaştırması (NFV) ve uygulama tanımlı ağ kurma (SDN) sayesinde geliştmiştir.

1.7.2.2. Son Kullanıcı Güvenlik Tespiti ve Koruma

Son Kullanıcı Güvenlik Tespiti ve Koruma, mobil aygıtlar, dizüstü bilgisayarlar ve masaüstü bilgisayarlar gibi son kullanıcı aygıtları olarak tanımlanan çeşitli uç noktaları bir ağda güvence altına alma işlemidir. Bir spor kurumunda veya organizasyonda veri merkezinde donanım olarak bulunan sunucular da uç nokta olarak kabul edilmektedir.Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Güvenli Ağ Geçidi, Kötü Amaçlı Yazılım Analizi, Korunmuş Mobil Tarayıcılar, Mobil Uygulama Sıkılaştırma vb.

1.7.2.2.1. Güvenli Ağ Geçitleri (Secure Web Gateways)

Güvenli Ağ Geçitleri (GAG) URL filtreleme, gelişmiş tehdit koruması (GTK), kötü amaçlı yazılım bulunması ve uygulama kontrol teknolojisinden faydalanarak; organizasyonları korur ve politika uyumluluğunu devam ettirir. GAG'ler geliştirme uygulamaları (donanım ve sanal), bulut bazlı servisler veya hibrit çözümler (bulut&geliştirme) olarak servis edilir.

1.7.2.2.2. Uygulama Kontrol (Application Control)

Uygulama beyaz listeleri olarak da adlandırılan uygulama kontrol çözümleri, genellikle uç noktası ve bulut işyükü koruma platformlarıyla birlikte kullanılabilen bir uç nokta koruması (masaüstü ve sunucu) türüdür.

- Basit çözümler: kodun çalışıp çalışmaması gerektiğinin kontrolünü sağlar.
- Detaylı çözümler: uygulamanın çalıştığı anda ne yaptığı ve hangi sistem kaynakları ile entegre olduğunun kontrolünü sağlar.

1.7.2.2.3. Ağ Koruması (Network Sandboxing)

Network sandbox ları, ağ trafiğini izleyerek şüpheli gördükleri nesneleri (çalıştırılabilir kodlar, Microsoft Office dosyaları, Javascript kodları vb.) sanal ortama taşıyarak izole edilmelerini sağlar. Sanal ortamdaki nesneler analiz edilir ve önem derecelerine göre puanlandırılır.

1.7.2.2.4. İmza Tabanlı Olmayan Zararlı Yazılım Analizi (Non-Signature Malware Analysis)

1.7.2.4. Mesajlaşma ve İletişim Güvenliği

Mesaj güvenliği cihazınızdaki mesajların şifrelenmesi ve böylece yalnızca alıcı tarafından okunabilmesi için uygulanır. İletişim güvenliği, yetkili olmayan önlemcilerin, telekomünikasyona anlaşılır bir biçimde erişmelerini önleme disiplinidir.

1.7.2.4.1. Mobil Ses Koruması (Mobile Voice Protection)

Mobil ses koruması teknolojileri, mobil ve kablosuz ağlarda iletilen, mobil araçlarda başlayan ve sonlanan sesli haberleşmelerin gizliliğini ve bütünlüğünü sağlar. Mobil ses koruması içeren araçlar genellikle mobil cihazlarda bulunan bağımsız uygulama şeklinde gelmektedir.

1.7.2.3.2. Güvenli Mesajlaşma (Secure Texting)

Güvenli mesajlaşma teknolojileri, mobil cihazlardan gönderilen veya alınan ve kablosuz veya mobil şebekelerde iletilen anında mesajlaşma ve SMS'in gizliliğini

ve bütünlüğünü sağlar. Mobil metin koruması sağlayan araçlar genellikle bir taşınabilir aygıtta bulunan bağımsız bir uygulama biçimindedir.

1.7.2.3.3. Mobil Sanal Özel Ağlar (Mobile Virtual Private Networks)

Mobil sanal özel ağlar (VPN'ler) istemci ağ geçitleri ve araç setlerinden oluşur ve son derece güvenilmez uzak bağlantılarda ve akıllı telefonlar ve tabletler içeren mobil kullanım durumlarıyla çalışacak şekilde optimize edilmiştir. Mobil VPN'ler, SSL ve IPsec'in halefi olan Aktarım Katmanı Güvenliği (TLS) çevresinde oluşturulabilir. İstemcide, tarayıcı aracılığıyla çağrılan veya platform API'ları aracılığıyla çağrılan uygulamaları ve kapsayıcıları içine gömülebilirler.

1.7.2.4. Veri Güvenliği

Veri güvenliği, bilgisayarlara, veritabanlarına ve web sitelerine yetkisiz erişimi önlemek için uygulanan koruyucu dijital gizlilik önlemlerini ifade eder. Veri güvenliği ayrıca verileri bozulmalardan korur. Veri Güvenliği, Veri Tabanı Güvenliği, Verileri Ortadan Kaldırma, Veri Kaçakçılığını Önleme gibi alt alanlara ayrılabilir. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Statik/Dinamik Veri Maskeleme, Veri Dağılım Algoritmaları, Veri Temizleme, Veritabanı Şifreleme vb.

1.7.2.4.1. Veri Güvenliği (Data Security)

1.7.2.4.1.1. Statik Veri Maskeleme (Static Data Masking)

Veri maskeleme, yazılım testleri ve kullanıcı eğitimleri gibi amaçlar için kullanılabilen, bir kuruluşun verisinin yapısal olarak benzer ancak özgün olmayan versiyonunun oluşturulması için bir yöntemdir. Amaç, gerçek veriler gerekli

olmadığı zaman, benzer verilerle işlem yaparak gerçek verileri korumaktır. Statik Veri Maskeleme, durağan verilerin korunmasını sağlar.

1.7.2.4.1.2. Dinamik Veri Maskeleme (Dynamic Data Masking)

Veri maskeleme, yazılım testleri ve kullanıcı eğitimleri gibi amaçlar için kullanılabilen, bir kuruluşun verisinin yapısal olarak benzer ancak özgün olmayan versiyonunun oluşturulması için bir yöntemdir. Amaç, gerçek veriler gerekli olmadığı zaman, benzer verilerle işlem yaparak gerçek verileri korumaktır. Dinamik veri maskeleme (DVM), üretilen verinin gerçek zamanlı maskelenmesini amaçlayan bir teknolojidir. DVM, istemcinin hassas verilere erişememesi için veri akışını değiştirir; orijinal üretim verilerinde herhangi bir değişiklik yapılmaz.

1.7.2.4.1.3. Biçim Koruma Şifreleme (Format Preserving Encryption)

Biçim koruma şifrelemesi (FPE) araçları, durağan verileri, ilişkisel veritabanı yönetim sistemleri (RDBMS'ler), veri ambarları, büyük veriler ve Hadoop, Cassandra ve MongoDB gibi NoSQL veritabanlarında kullanılan alanlardaki verileri korumak için kullanılır.

1.7.2.4.1.4. Bilgi Dağıtma Algoriatmaları (Information Dispersal Algorithms)

Bilgi dağıtma algoritmaları, bilgiyi parçalı olarak (yani dağınık) birden çok yerde depolamak için bir metodoloji sağlar, böylece lokal kesinti durumunda bilgi korunur ve tek bir yerde yetkisiz veri erişiminin olması erişimi yapana kişiye kullanışlı bilgi sağlamaz.

1.7.2.4.1.5. Belirtkeleme (Tokenization)

Belirtkeleme, bir ödeme kartı numarası gibi bir hassas verinin bir parçasının, belirteç olarak bilinen yedek değeri değiştirdiği bir işlemi ifade eder. "Vaultless" simgeleşme kullanılmadığı sürece, hassas verilerin merkezi bir konumda güvenli bir şekilde depolanması ve korunması gerekir.

1.7.2.4.1.6. Birlikte Çalışabilir Depolama Şifreleme (Interoperable Storage Encryption)

Endüstri standartlarına dayanan ve sürücü denetleyicilerine yerleştirilen birlikte çalışabilir depolama şifrelemesi, güvenli yığın depolama sürücülerinin performansını önemli ölçüde artırabilir. Standart şifreli sürücüler (SED'ler) için vitrin teknolojisi Opal Güvenlik Alt Sınıf Sistemi (SSC) 'dir.

1.7.2.4.1.7. Güvenilir Taşınabilir Depolama Güvenliği (Trusted Portable Storage Security)

Güvenilir taşınabilir depolama güvenlik aygıtları, genelde USB konektörlü bir flash bellek cihazında sunulan sağlam güvenlik politikalarını uygulamak üzere tasarlanmış yerleşik erişim denetimleri ve şifrelemeye sahip, bağımsız bir ortam sistemidir.

1.7.2.4.1.8. Veri Güvenliği İçin Blockchain (Blockchain for Data Security)

Blockchain, değer değişim işlemlerinin, bloklara sıralı olarak gruplandığı dağıtılmış bir teknolojidir. Blockchain özellikli veri güvenliği uygulamaları,

merkezileştirilmiş arbitrallere güvenmeden, güven ve esneklik sağlamak için alternatif yöntemler sunar ve dijital varlıkları takip eder.

1.7.2.4.1.9. Gizlilik Yönetim Araçları (Privacy Management Tools)

Gizlilik yönetim araçları, kuruluşların gizlilik etkisi değerlendirmelerini yürütmesine ve gizlilik düzenlemelerinin gereklerine karşı işleme faaliyetlerini kontrol etmesine yardımcı olur. Kişisel bilgilerin veri akışlarını analiz ve dokumante etmekte, gizlilik politikalarının dağıtımını desteklemekte ve kullanıcı farkındalığını izlemektedir.

1.7.2.4.2. Veri İmha (Data Disposal)

1.7.2.4.2.1. Veri Temizleme (Data Sanitization)

Veri temizleme, tüm verileri bir okuma / yazma ortamından güvenilir bir şekilde ve tamamen çıkararak, artık okunamayan veya kurtarılamaz hale getirmek için sürekli uygulanan bir işlemdir.

1.7.2.4.2.2. Mobil Cihazlar İçin Veri Elden Çıkarma Araçları (Data Disposal Tools for Mobile Devices)

Mobil cihazlar için veri elden çıkarma araçları, mobil aygıtların güvenli bir şekilde hizmet dışı kalmasını sağlayan ve veri silinmesini sağlayan silme teknolojilerini kullanır.

1.7.2.4.3. Veritabanı Güvenliği (Database Security)

1.7.2.4.3.1. Veritabanı Denetim ve Koruma (Database Audit and Protection)

Veritabanı denetim ve koruma (DAP) araçları, ilişkisel veritabanı yönetim sistemleri (RDBMS'ler) için veri güvenliği ilkeleri, kullanıcı etkinliği izleme ve veri korumasının merkezi yönetimini sağlar.

1.7.2.4.3.2. Veritabanı Şifreleme (Database Encryption)

Veritabanı şifreleme araçları ilişkisel veritabanı yönetim sistemlerini (RDBMS) korumak için kullanılır. Şifreleme, saldırı veya içeriden istismar riskini en aza indirmeye yardımcı olmak ve yöneticilerin ve yetkisiz kullanıcıların erişimini engelleyerek uyumluluk sorunlarını ortadan kaldırmayı sağlar. Operasyonel olarak şifreleme, durağan bir tabloyu veya veritabanı örneğini koruyabilir.

1.7.2.4.4. Veri Kaçağı Önleme / İç Tehdit Savunma (DLP / Inside Threat Protection)

1.7.2.4.4.1. Veri Kaybını Önleme (Data Loss Preventation)

Veri kaybını önleme bir işlemin yapıldığı andaki içeriğe ve bağlama dayalı bir politikanın dinamik uygulamasıdır. DLP, yanlışlıkla veya kazara veri kaybı riskini ve izleme, filtreleme, engelleme ve iyileştirme özelliklerini kullanarak hassas verilere maruz kalma riskini ele alır.

1.7.2.4.4.2. E-posta için İçerik Tanıyan Veri Kaybını Önleme (Content-Aware DLP for Email)

E-posta için içerik tanıyan veri kaybını önleme (VKÖ), tüm kurumda değil sadece bir e-posta sisteminde kullanılmak üzere VKÖ politikaları oluşturma amacıyla kullanıldığı için entegre bir VKÖ dağıtımı olarak düşünülür.

1.7.2.4.4.3. İçerik Tanıyan Mobil Veri Kaybını Önleme (Content-Aware Mobile DLP)

İçerik tanıyan mobil veri kaybını önleme, yasal uyumluluk, fikri mülkiyet gibi hassas verileri koruyan mevcut DLP ürünlerinin mobil için genişletilmiş halidir.hassas içerikler mobil cihaza kaydedilir, mobil cihaz tarafından buluta yüklenir veya web mail vb. uygulamalar ile gönderilir.

1.7.2.5. Bulut Güvenliği

Bulut güvenliği, çevrimiçi depolanan verilerin hırsızlığa, kaçağa ve silinmesine karşı korunmasıdır. Bulut güvenlik sağlama yöntemleri, güvenlik duvarları, penetrasyon testleri, şaşırtma, sanal özel ağların (VPN) kullanımı ve genel İnternet bağlantılarını kullanmaktan kaçınmayı içerir. Bulut güvenliği hem fiziksel hem de mantıksal güvenliği ele alır ve farklı hizmet modellerinin nasıl yerine getirildiğini (genel-özel-hybrid) belirtir. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Bulut Erişim Güvenlik Aracısı, Yüksek Güvenceli Arakatmanlar, Saas Güvenlik Yönetimi, IaaS Container Şifreleme vb.

Bulut Erişim Güvenlik Aracıları (Cloud Access Security Brokers)

Bulut erişim güvenlik aracıları, kurum güvenlik denetimlerine müdahale etmek ve ilkeleri uygulamak için bulut hizmeti tüketicileri ile bulut hizmeti

sağlayıcıları arasında aracılık yapan kurum içi veya bulut tabanlı güvenlik ilkesi uygulama noktalarıdır. Bulut Erişim Güvenlik Aracı platformları, bulut hizmeti bulma, bulut sağlayıcı risk derecelendirmeleri, tek oturum açma, yetkilendirme, aygıt profillemesi, şifreleme, tokenization, hassas veri izleme, kullanıcı davranışı izleme gibi birden çok güvenlik ilkesini birleştirir.

Yüksek Güvenilirlikli Hypervisor (High-Assurance Hypervisors)

Yüksek güvenilirlikli bir hypervisor, müdahale edilmemiş veya ele geçirilmemiş yüksek bir güven seviyesi oluşturulmasını sağlayan hypervisor dur. Yüksek güvence sağlandıktan sonra kritik öneme sahip iş yükleri ve hassas veriler güvence altına alınır.

Bulut Veri Koruma Ağ Geçitleri (Cloud Data Protection Gateways)

Bulut veri koruma ağ geçitleri, proxy vasıtasıyla bulut SaaS sağlayıcısına akarken yapılandırılmış ve yapılandırılmamış verilere şifreleme, maskeleme veya tokenization uygulayarak bir vekil kurabilir. Bulut veri koruma ağ geçidi işlevi, birkaç bulut erişim güvenlik aracısı çözümüne eklenmektedir. Uygulama kullanıcıları, diğer bulut kiracıları, SaaS yöneticileri ve bilgisayar korsanlarının bulut hizmetine yetkisiz erişimi önler ve SaaS kullanırken veri ikameti gereksinimlerini karşılamaya yardımcı olur. SaaS Platform Güvenlik Yönetimi (SaaS Platform Security Management).

SaaS platform güvenlik yönetimi araçları, bir veya daha fazla SaaS hizmeti içinde veri erişimi ve kullanıcı etkinliği üzerinde kontrol sağlayan bir yönetişim gösterge tablosunu uygulamak için SaaS sağlayıcılarının API'lerini kullanır. Bu tür mekanizmalar tipik olarak bulut erişim güvenlik aracısı ürünlerinin bir bileşeni olarak sağlanır ancak birkaç niş SPSM satıcısı, bir veya az sayıdaki SaaS uygulamasını hedef alan ürünler sunmaya devam etmektedir.

Hizmet Olarak Altyapı Konteyner Şifrelemesi (IaaS Container Encryption)

Hizmet olarak altyapı konteyner şifrelemesi, IaaS sağlayıcılarının barındırdığı iş yüklerinde, uygulama tarafında olmayan bir şekilde IaaS sağlayıcı altyapısında bulunan iş yükü tarafından depolanan verileri şifrelemek için kullanılan şifreleme teknolojisinin kullanılmasıdır. Kurumlar, şifre çözme anahtarlarına erişimi kontrol ederek, IaaS iş yükleri tarafından kullanılan ve oluşturulan verileri, komşu kiracılardan, bulut hizmeti sağlayıcısı yöneticilerinden ve IaaS sağlayıcının olası bilgisayar korsanlarından koruyabilirler.

1.7.2.6. Güvenlik Analizleri ve İstihbarat

Güvenlik Analizi, büyük risk teşkil eden olayları anlamak için güvenlik olaylarını toplamak ve analiiz etmek amaçlı bilgi teknolojisi kullanımıdır. Çoğunlukla büyük miktarda veri toplayarak çalışır ve önleyici tedbirlerin zamanında alınabilmesi için tehdit kalıpları yaratmada kullanır. Düzgün bir analiz, tehditin kök nedenleri hakkında derinlemesine bilgi sağlar. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Kullanıcı ve Davranış Analizi, Ağ Trafik Analizi, Sahtecilik Tespiti vb.

Kullanıcı ve Varlık Davranış Analizi (User and Entity Behavior Analytics)

Kullanıcı ve varlık davranış analizi olarak bilinen UEBA aslında kullanıcı ve kimliklerin kullanım modellerini profil analizi ile öğrenip daha sonra anormal davranışların sergilenmesinde durumunda bunların raporlanmasını sağlar. Örnek vermek gerekir ise, bir banka kartı ile sürekli Türkiye'de alış veriş yapılıyor iken, aynı kart Amerika kökenli amazon.com sitesinde kullanılırsa banka bunun normal bir davranış olmadığını tespit eder ve hemen kart sahibini arayarak bu alış verişin kart sahibinin bilgisi dahilinde olup olmadığını doğrular.

Ağ Trafik Analizi (Network Traffic Analysis)

Ağ trafiği analizi teknolojisi, kurumsal ağdaki şüpheli etkinlikleri tespit etmek için istatistiksel analiz, makine öğrenmesi, meta veri ve içerik denetimi yöntemlerini kullanır. Genellikle ihlal olayları sonrası yapılır. Birçok NTA satıcısı, tüm ağın izlenmesi yerine LAN segmenti izleme konusunda uzmanlaşmaktadır.

Tehdit İstihbarat Platformları (Threat Intelligence Platforms)

Tehdit İstihbarat Platformları (TIP), savunma eylemlerinin önceliklendirilmesini desteklemek ve saldırı önleme, tespit ve yanıt vermeye yardımcı olmak için gerçek zamanlı olarak güvenlik tehdidi verilerini toplamak, ilişkilendirmek, kategorilere ayırmak, paylaşmak ve bütünleştirmek için kullanılır. Ayrıca bu platformlar SIEM, EDR, IPS ve güvenlik duvarı gibi mevcut güvenlik teknolojileri ve süreçleri ile entegre olabilirler.

Dolandırıcılık Tespiti ve İşlem Güvenliği (Fraud Detection and Transaction Security)

Fraud Detection (Dolandırıcılık Tespiti), müşterilerin ve kurumun bilgilerini, varlıklarını, hesaplarını ve (hesap) işlemlerini gerçek zamanlı, gerçeğe yakın zamanlı veya kullanıcı aktivitelerini toplu analiz etme yöntemiyle tespitini sağlar. Kullanıcı aktivitesi şüpheli olmadığı sürece müdahale edilemez.

Aldatma Teknolojisi (Deception Technology)

Aldatma teknolojisi, ağa sızmış olan bir saldırganın ağa zarar vermesini önlemek için tasarlanmış olan güvenlik araçları ve tekniklerini kapsar. Bu teknoloji saldırganın yönünü şaşırtmak için tuzak bir sistem kullanmakta, saldırganın hedefine ulaşmasını geciktirmekte veya önlemekte olan sistemlerdir (Han ve ark., 2017). Ayrıca bu teknolojiler atak analizi ve forensics (adli analiz) yaparak saldırganların davranışlarını tespit etmenizi sağlar. Spor alanın bu teknolojinin kullanımı kurumsal firmaları bilişim alanında bir adım öne alır.

1.7.2.7. Güvenlik Operasyonları, Olay Yönetimi ve Adli Bilişim

Bir güvenlik operasyon merkezi (SOC), örgütsel ve teknik düzeyde güvenlik konularını ele alan merkezi bir birimdir. Bir bina veya tesis içindeki bir SOC, personelin veri işleme teknolojisini kullanarak siteyi denetlediği merkezi bir konumdur. Olay yönetimi (ICM), bir organizasyonun gelecekte yeniden oluşumunu önlemek için tehlikeleri tanımlama, analiz etme ve düzeltme faaliyetlerini tanımlayan bir terimdir. Yapısal bir organizasyon içindeki bu olaylar normalde olayla mücadele ekibi (IRT) veya bir olay yönetimi ekibi (IMT) tarafından ele alınır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: SIEM (Bilgi Güvenliği Olay Yönetimi), Kriz Yönetim Platformları vb.

Bilgi Güvenliği ve Olay Yönetimi (SIEM), bir organizasyonun veya kurumun ağında gerçekleşen olayları izleme, analiz etme ve yönetme yeteneklerini sağlayan bir bilişim teknolojisi ve yöntemler bütünüdür. SIEM, güvenlik olaylarından kaynaklanan tehditleri tespit etmek, saldırıları önlemek veya hızla yanıt vermek için kullanılır.

SIEM sistemleri, farklı kaynaklardan (ağ cihazları, sunucular, uygulamalar, veritabanları vb.) gelen güvenlik olaylarını toplar, depolar, analiz eder ve raporlar. Bu olaylar arasında güvenlik ihlalleri, saldırı girişimleri, yetkisiz erişim denemeleri, kötü amaçlı yazılım tespitleri, sisteme ait hatalar ve diğer potansiyel tehditler yer alabilir.

SIEM sistemleri genellikle aşağıdaki temel bileşenlere sahiptir:

Veri Toplama: SIEM, farklı kaynaklardan (güvenlik cihazları, log kayıtları, ağ trafiği vb.) güvenlik olaylarını toplar. Bu veriler genellikle günlük dosyaları veya sistem logları şeklinde gelir.

Veri Analizi: Toplanan veriler, analiz algoritmaları ve kurallar kullanılarak incelenir. Bu analizler, potansiyel tehditleri tespit etmek ve anormal aktiviteleri belirlemek için yapılır. Örneğin, belirli bir IP adresinden gelen yoğun ağ trafiği veya kullanıcı hesaplarından yapılan anormal etkinlikler gibi durumlar tespit edilebilir.

Olay Yönetimi: SIEM sistemleri, tespit edilen olayları yönetmek ve yanıt vermek için iş akışı yönetimi ve otomatik bildirim mekanizmaları sağlar. Sistem, güvenlik ekiplerine olayları bildirebilir, durumları takip edebilir ve gerekli aksiyonları yönlendirebilir.

Raporlama ve İzleme: SIEM sistemleri, güvenlik olayları hakkında detaylı raporlar ve analizler üretebilir. Bu raporlar, güvenlik durumunu izlemek, uyumluluk gereksinimlerini karşılamak ve olaylara ilişkin trendleri görmek için kullanılabilir.

SIEM sistemleri, güvenlik olaylarını hızlı bir şekilde tespit etmek, yanıt vermek ve gelecekteki saldırıları önlemek için büyük önem taşır. Güvenlik operasyonlarına katkı sağlayarak bilgi güvenliğini artırır ve kuruluşlara daha etkili bir olay yönetimi imkanı sunar.Kriz/Olay Yönetimi Platformları (Crisis/Incident Management Platforms).

Kriz/Olay yönetimi platformları, iş kesintileri, hizmette aksama gibi olaylara karşı müdahale ve iyileştirme gibi tedbirleri yönetmek için kullanılır. Kriz halinde iletişim, kurtarma planı veri havuzu, iş gücü planlama, devlet kurumu raporlaması gibi fonksiyonaliteleri içerir.

Adli Bilişim

Adli Bilişim, kanun önünde sunmak amacıyla, belirli bir bilgi işlem cihazından elde edilen kanıtları toplamak ve muhafaza etmek için soruşturma ve analiz tekniklerinin uygulanmasıdır. Adli Bilişimin amacı, bir bilgi işlem aygıtında

tam olarak neler olduğunu ve kimin sorumlu olduğunu bulmak için gerekli kanıtları toplamak ve bunları belgelendirmektir.

1.7.2.8. Güvenlik Risk ve Uyum Yönetimi

Uyum riski, bir kurumun, kanun ve yönetmeliklere, iç politika veya öngörülen en iyi uygulamaları uyarınca hareket etmemesi durumunda karşı karşıya kaldıkları yasal cezalar, istihkak kaybı ve maddi kayıplara maruz kalma olayıdır. Bu kategoride yer alan örnek teknolojileri / ürünleri şu şekilde sıralayabiliriz: Konfigürasyon Denetimi, Yazılım Bileşim Analizi, BT Risk Yönetimi, Sosyal Risk Yönetimi vb.

Yapılandırma Denetleme (Configuration Auditing)

Yapılandırma denetleme araçları, sunucular, uygulamalar, veritabanları ve ağ aygıtları arasında, iç ve genel bulut altyapısında değişiklik algılama ve yapılandırma değerlendirmesi sağlar. Şirkete özgü ilkeler veya endüstri tarafından tanınan güvenlik yapılandırma değerlendirme şablonları (örneğin, NIST), sistemin denetim, sıkılaştırma veya kullanılabilirlik açısından doğruluğunu korur. Bazıları iyileştirme için yapılandırma yönetimi araçları ile çalışırken bazıları istenilen bir duruma dönüştürülebilir.

Yazılım Bileşimi Analizi (Software Composition Analysis)

Yazılım bileşimi analizi aşağıdaki görevleri gerçekleştirir:

- Güvenlik ve / veya işlevsellik açığı olan veya uygun lisanslamayı gerektiren bileşenleri algılamak için uygulama bileşimini analiz eder.

- Kurumsal yazılım tedarik zincirinin yalnızca güvenli bileşenleri içerdiğinden ve bu nedenle güvenli uygulama geliştirme ve kurma işlemini desteklediğinden emin olmaya yardımcı olur.

Risk Yönetimi Risk Management)

BT Risk Yönetimi Çözümleri (IT Risk Management Solutions)

BT risk yönetimi çözümleri, BT riskinin ve güvenlik ekiplerinin riske dayalı karar vermeyi desteklemek için kullandığı işlevleri ve iş akışlarını desteklemektedir. Bu çözümlerin beş kritik özelliği şunlardır:

- Politika Yönetimi
- Kontrol Eşleme ve Raporlama
- Güvenlik İşlemleri Analizi ve Raporlaması
- BT Risk Değerlendirmesi
- Olay Yönetimi

Dijital Risk Yönetimi (Digital Risk Management)

Dijital risk yönetimi (DRY), bulut, mobil, sosyal, büyük veriler, üçüncü parti teknoloji sağlayıcıları, operasyonel teknoloji (OT) ve Nesnelerin İnterneti (IoT) gibi dijital iş bileşenleri ile ilişkili risklerin yönetimini kolaylaştırır.

BT Tedarikçi Risk Yönetimi (IT Vendor Risk Management)

BT tedarikçi risk yönetimi, BT sağlayıcılarının ve servis sağlayıcıların kullanılmasının iş kesintisi veya iş performansı üzerinde olumsuz bir etki için kabul

edilemez bir potansiyel yaratmamasını sağlayan bir yöntemdir. BT tedarikçi risk yönetimi teknolojisi, satıcılarla ilgili riske maruziyeti değerlendiren, izleyen ve yöneten kuruluşları destekler.

Operasyonel Risk Yönetimi (Operational Risk Management)

Operasyonel risk yönetimi çözümleri daha kapsamlı bir kurumsal risk yönetimi (ERM) programı kapsamında desteklemektedir. Operasyonel riskler, Gartner tarafından "günlük taktik ticari faaliyetlerin belirsizliğinin yanı sıra yetersiz veya başarısız iç süreçler, insanlar veya sistemler veya dış olaylardan kaynaklanan risk olaylarıyla ilgili" riskler olarak tanımlanır.

Endüstriyel Operasyonel Risk Yönetimi (Industrial Operational Risk Management)

Endüstriyel operasyonel risk yönetimi uygulamaları, yetersiz veya başarısız iç süreçler ve sistemler, insan faktörleri veya dış olaylardan kaynaklanan zarar riski dahil olmak üzere operasyonel riskin belirlenmesi, değerlendirilmesi, hafifletilmesi, izlenmesi ve kontrol edilmesi süreçlerini desteklemek üzere tasarlanmıştır.

Yönetilen Entegre Risk Yönetimi Çözümü (Managed Integrated Risk Management)

Solution Yönetilen entegre risk yönetimi çözümü , bir kuruluştaki risk bileşenlerini bütünleştirir ve yönetir. Bu, sağlayıcının tek bir harici sistem ve süreç grubu aracılığıyla alıcının kurumsal boyuttaki teknolojisi ve iş süreçleri (uygulamalar, mimari, güvenceler ve risk kontrolleri) hakkında bilgi toplamak ve daha sonra yönetilen YERY hizmetlerini müşterilere sunmak için yönetilen hizmetleri kullanmayı içerir.

Sosyal Medya Risk Yönetimi (Social Risk Management)

Sosyal medya riski yönetimi (SMRY) uygulamaları, sosyal medyanın iş süreçlerine dahil edilmesiyle ilgili belirsizliğin etkilerini, düzenlemelere ve politikalara uyumu, sosyal medyanın ve diğer dinamik içeriğin düzenleyici uyumluluk, yasal gereksinimler ve iş hedeflerine yönelik riskler açısından analizi için gerekli süreçleri sağlamaktadır.

1.7.2.9. Uygulama ve İnternet Güvenliği

Uygulama güvenliği, güvenlik açıklarını tespit ederek ve önleyerek bir uygulamanın güvenliğini artırmak için alınan önlemleri kapsar. Web uygulaması güvenliği, özellikle web sitelerinin, web uygulamalarının ve web servislerinin güvenliğini sağlayan Bilgi Güvenliği'nin bir dalıdır. Web uygulaması güvenliği, yüksek düzeyde, uygulama güvenliği ilkelerini benimser, ancak bunları özellikle İnternet ve Web sistemlerine uygular.

Web Uygulama Güvenlik Duvarı ve Uygulama Güvenliği (WAF and Application Security)

RASP (Runtime Application Self-Protection)

Çalışma zamanı uygulama özkaynağı koruması (RASP), bir uygulama çalışma zamanı ortamında yerleşik olan veya daha sonra eklenen bir güvenlik teknolojisidir. Uygulama davranışlarını izleyebilir, uygulama yürütmeyi denetleyebilir, ayrıca gerçek zamanlı saldırıları tespit edebilir ve önleyebilir.

Uygulama Koruması (Application Shielding)

Uygulama koruması, uygulama düzeyindeki saldırıların etkin bir şekilde önlenmesi ve tespit edilmesi için doğrudan güvenlik işlevselliği eklemek için kullanılan bir dizi teknolojiyi belirtir. Özellikle mobil uygulamaları korumak için tercih edilmektedir.

Web Uygulama Güvenlik Duvarı (Web Application Firewalls)

Bir web uygulama güvenlik duvarı (WAF), web uygulamaları ve web API'lerini korumak için web sunucularının önünde konumlandırılmış bir tespit ve önleme teknolojisidir. Birçok WGD, daha doğru koruma için olumsuz ("imzalar") ve pozitif ("beyaz liste") güvenlik modellerinin bir kombinasyonunu içerir.

Aracı API (Mediated APIs) Aracı

API, bir API'nin sanallaştırılmış, yönetilen, korunan ve bir ara katmanı tarafından zenginleştirilmiş bir tasarım modelidir. Bu katman, artan çeviklik, kullanılabilirlik, performans, güvenlik ve kontrol için ilkeyi uygulayabilir ve API etkileşimine yetenekler katabilir. Aracı API, bir hizmetin, alan modelini doğrudan yansıtan "iç API" yi ve belirli istemci gereksinimlerini desteklemek üzere uyarlanmış bir veya daha fazla "dış API" yi ortaya koymasını sağlar.

Hizmet Olarak Uygulama Güvenliği (Application Security as a Service)

Test hizmetlerinin, genellikle internet üzerinden aboneliğe dayalı fiyatlandırma modeliyle uzaktan çalışan üçüncü parti profesyonel güvenlik sağlayıcılarına devredildiği bir teslimat modelidir.

Uygulama Gizleme (Application Obfuscation)

Uygulama gizleme, uygulamayı ve içinde bulunan fikri mülkiyeti sızma, ters mühendislik ve hack işlemlerinden koruma amaçlı teknolojileri içermektedir.

Gömülü Yazılım ve Sistem Güvenliği (Embedded Software and Systems Security)

Gömülü yazılım ve sistemler güvenliği, donanım ve gömülü yazılımı tehlikeye atılmış saldırılardan korumak ve bu sistemlerin işlediği verilerin bütünlüğünü ve gizliliğini sağlamak için mühendisler ve geliştiriciler için tasarlanmış teknoloji ve uygulamaları sunar. Bu sistemler hem fiziksel hem de dijital saldırılara maruz kalabilirler.

Zafiyet Denetimi (Vulnerability Assesment)

Açıklık Değerlendirme (Vulnerability Assessment)

Güvenlik açığı değerlendirmesi ürünleri ve hizmetleri kurumsal BT ortamlarını değerlendirir ve aşağıdaki özellikleri gerçekleştirir:

- Aygıt, işletim sistemi ve yazılım güvenlik açıklarının keşfedilmesi ve tanımlanması
- Güvenlik açığı koşullarının temelini oluşturmak ve eğilim oluşturmak
- BT varlıklarının güvenlik konfigürasyonunu belirleme ve raporlama
- Ağa bağlı BT ve OT varlıklarının keşfedilmesi ve raporlanması
- Özel uygunluk raporlaması ve kontrol çerçevelerini destekleme
- Risk değerlendirme
- BT operasyon grupları tarafından iyileştirmenin desteklenmesi

Uygulama Güvenlik Açığı Korelasyon (Application Vulnerability Correlation)

Uygulama Güvenlik Açığı Korelasyon araçları, Statik ve Dinamik test araçlarından gelen iyileştirmelerin analizi ve önceliklendirilmesi sonrası merkezi bir uygulamaya girdi sağlanmasını sağlar.

Penetrasyon Testi (Network Penetration Testing Tools)

Penetrasyon testi, güvenlik açıklarını bulmak ve onları, aygıt rollerini, güven ilişkilerini, erişilebilir ağ hizmetlerini ve olası güvenlik açıklarını eşleştirmek ve onları hedef sistemlere erişmek için kullanmak için çok aşamalı saldırı senaryolarını kullanır. Penetrasyon test araçları, yüksek riskli güvenlik açıklarının önceliklendirilmesi ve mevcut savunmaların savunmasızlığını göstermek için yol gösterici bir etkiye sahiptir.

Kitle Kaynak Güvenlik Test Platofmrları (Crowdsourced Security Testing Platforms)

Kitlekaynak güvenlik test platformları, güvenlik açıklarını belirlemek için geniş güvenlik testi uygulayıcılarından yararlanarak penetrasyon testi ve / veya uygulama güvenlik testinin kitlelere yönlendirilmesine olanak tanıyan bir SaaS platformu sağlar. CSSTP'ler sıklıkla, platformlarının bir parçası olarak ödül programı yönetim hizmetleri sunar.

İnteraktif Uygulama Güvenlik Testi (Interactive Application Security Testing)

İnteraktif uygulama güvenlik testi, uygulama güvenliği testinin doğruluğunu arttırmak için dinamik uygulama güvenlik testi ve statik analiz güvenlik test tekniklerini birleştiren teknolojidir.

Mobil Uygulama Gülvenliği Testi (Mobile Application Security Testing)

Mobil uygulama güvenliği testi (MAST), güvenlik açıklarını tanımlamak için kodlama, tasarım, paketleme, dağıtım ve çalışma zamanı koşulları için mobil uygulamaları analiz eder. Mobil Uygulama Onaylama Çözümü (MARS) olarak kullanıldığında, MAST, bir kuruluşun güvenlik ilkeleriyle çakışan uygulama işlevlerine de işaret edebilir.

Statik Uygulama Güvenliği Testi (Static Application Security Testing)

Statik Uygulama Güvenlik Testi, uygulama kaynak kodu, bayt kodu ve binary dosyaları analiz etmek üzere tasarlanmış bir dizi teknolojidir.

Dinamik Uygulama Güvenliği Testi (Dynamic Application Security Testing)

Dinamik uygulama güvenliği testi (DUGT) teknolojileri, bir uygulamadaki güvenlik açığına işaret eden koşulları çalışma durumunda algılamak için tasarlanmıştır. Bazı dinamik test çözümleri özellikle web dışı protokol ve veri hataları için tasarlanmıştır

Software Development Life Cycle Security

Yazılım Geliştirme Yaşam Döngüsü (SDLC), ilk fizibilite çalışmasından tamamlanan başvurunun sürdürülmesine kadar bir bilgi sistemi geliştirme projesinde yer alan aşamaları tanımlayan, proje yönetiminde kullanılan kavramsal bir modeldir.

DevSecOps (DevSecOps)

DevSecOps, geliştiricileri, operasyon ekibini ve işletme ekiplerini birlikte çalışmaya teşvik eden yazılım geliştirmeye yönelik bir yaklaşımdır; böylece, kuruluş yazılımları daha hızlı geliştirir, kullanıcı talebine daha duyarlı olur ve sonuç olarak gelirini en üst düzeye çıkarabilir

1.7.2.10. Mobil ve Taşınabilir Cihaz Yönetimi Güvenliği

Mobil güvenlik, akıllı telefonların, tabletlerin, dizüstü bilgisayarların ve diğer taşınabilir bilgi işlem cihazlarının ve bunlarun bağlandığı ağların, tehdit ve zayıf noktalardan korunmasıdır. Cihazın kaybedilmesi, cihazdan dışarıya izinsiz veri transferi, zararlı yazılım atakları gibi konular mobil güvenlik kapsamında değerlendirilir.

Kurumsal Mobilite Yönetim Sistemleri (Enterprise Mobility Management Suites)

Kurumsal Mobilite Yönetim Sistemleri, mobil aygıtların işletmelerin sistemlerine güvenli bir şekilde entegre edilmesini sağlar. Bu sistemler aygıtları kuruluşların politikalarına uymak, uygulamaları güvenli hale getirmek ve dağıtmak, kuruluş verilerini korumak ve isteğe bağlı olarak bağlamsal güven sağlamak için yapılandırır.

Kurumsal Mobil Yönetimi Güvenliği (EMM Security)

Kurumsal mobil yönetimi (EMM) ürünleri ve hizmetleri, mobil cihazları kurumsal BT uç nokta sistemi yaşam döngüsüne entegre eder. EMM araçları mobil politikaların merkezi olarak uygulanmasını sağlar. Örnek olarak, jailbreak algılama ve uzaktan silme gibi cihaz politikalarının yanı sıra veri erişimi, uygulama yönetimi ve mobil kimlik için daha geniş politikalar verilebilir.

Kendi Cihazınızı Getirin (BYOD)

Kendi cihazınızı getirin (BYOD), çalışanların, iş ortaklarının ve diğer kullanıcıların, kurumsal uygulamaların yürütülmesi ve verilere erişmek için kişisel olarak seçilmiş ve satın alınmış bir istemci cihazı kullanmalarını sağlayan son nokta dağıtım stratejisidir. Genellikle akıllı telefonları ve tabletleri kapsar, ancak strateji

PC'ler için de kullanılabilir. Çalışanın cihazına, yerel vergi düzenlemelerine, işgücü gereksinimlerine ve şirket politikasına bağlı olarak, bir sübvansiyon içerebilir.

Mobil Cihazlar İçin Kullanıcı Kimlik Doğrulaması (User Authentication to Mobile Devices)

Mobil cihazlar için kullanıcı kimlik doğrulaması, cihazın kendisine erişen kullanıcının kimliğini doğrulayan çeşitli yöntemleri kapsar. Kısa sayısal PIN'ler ve alfa sayısal şifreler sıradanlaşmakta; grafik desenler ve biyometrik yöntemler daha yaygın hale gelmektedir.

Mobil Tehdit Savunma (Mobile Threat Defense)

Mobil tehdit savunma araçları (MTS), işletmeleri mobil platformlardaki tehditlerden korur. MTDS çözümleri, aygıt (davranışsal anomali algılama ve güvenlik açığı değerlendirmeleri aracılığıyla), uygulama (kod analizi yoluyla) ve ağ (ağ trafiğini izleyerek ve şüpheli ağları otomatik olarak mobil aygıtlardan devre dışı bırakarak) üç düzeyde güvenlik sağlar.

Mobil Uygulama Sıkılaştırma (Mobile Application Hardening)

Mobil Uygulama Sıkılaştırma teknolojileri, mobil uygulamaları tersine mühendislik ve yeniden paketleme saldırılarına karşı korur. Yeniden Paketleme: Android cihazlarda çok yaygın bir saldırı türüdür. Böyle bir saldırıda, saldırganlar uygulama pazarlarından indirilen popüler bir uygulamayı değiştirir, uygulama kodlarına ters mühendislik yaparlar, bazı kötü amaçlı yazılım (payload) ekler ve sonra değiştirilen uygulamayı uygulama pazarlarına yüklerler.

Korumalı Mobil Tarayıcılar (Protected Mobile Browsers)

Korumalı mobil tarayıcılar, tüketici ve kurumsal portallar gibi web tabanlı kaynaklara erişmek için veri güvenliği ve katman koruma katmanları ekleyerek veri kaybını önlemeye ve varsayılan tarayıcıların ötesinde yeteneklerle güvenlik ilkelerini uygulamaya yardımcı olur.

Mobil Platform Sağlık Kontrolü (Mobile Platform Health Checks)

Mobil platform sağlık kontrolü, bir aygıtın güvenlik durumunu doğrulamak ve muhtemel tehlikeleri belirlemek için kullanılan yöntemlerdir. Mobil platform sağlık kontrolleri, uygulamalarda gömülü olabilecek yazılım geliştirme kitleri şeklinde gelir.

Güvenilir Mobil Ortam (Trusted Mobile Environments)

Güvenilir mobil ortamlar, güvenlik özelliklerini yazılım temelli güvenlik mekanizmalarından daha yüksek düzeyde güven altına almak için bir mobil cihaza (akıllı telefon veya tablet) gömülü veya bağlı bir özel donanıma dayanır.

Mobil Açıklık Yönetim Araçları (Mobile Vulnerability Management Tools)

Mobil açıklık yönetim araçları aşağıdaki yetenkleri sağlar:

- Mobil işletim sistemlerinde (işletim sistemleri), yazılım ve uygulamalarda bulunan güvenlik açıklarının tanımlanması, sınıflandırılması ve düzeltilmesine yardımcı olmak

- Mobil varlıkların riskinin değerlendirilmesi ve raporlanmasına izin verilmesini sağlamak

Tüketici Mobil Güvenlik Uygulamaları (Consumer Mobile Security Apps)

Tüketici mobil güvenlik uygulamaları, mobil cihazları güvenlik tehditlerine karşı korur ve kullanıcıların gizlilik ve cihaz performansını yönetmesine yardımcı olur. Antivirüs taramaları, gizlilik yönetimi, aygıt performans optimizasyonu ve hırsızlığa karşı koruma gibi özellikler içerir. Böyle uygulamaları aslında çoğu spor kulubu veya işletme tercih etmez ama her bir veri işleyen personel içim gerekebilir.

1.7.2.11. Endüstriyel / IoT Sistemleri Güvenliği

Endüstriyel güvenlik, endüstriyel kontrol sistemlerinin korunması, endüstri ortamlarında makine ve ilgili cihazların çalışmasını izlemek ve kontrol etmek için tasarlanmış entegre donanım ve yazılım içeren bir çalışma alanıdır. IoT güvenliği, nesnelerin internette bağlı cihazların ve ağların korunması ile ilgili çalışma alanıdır. Spor sektöründe sporcuların kullandığı giyimdeki cihazlar aslında bu alana dahildir.

IoT Security

Nesnelerin İnterneti Kimlik Doğrulaması (Internet of Things Authentication)

Nesnelerin kimlik doğrulaması, bir IoT ortamında çalışan aygıtlar, uygulamalar, bulut hizmetleri veya ağ geçitleri gibi diğer varlıklarla etkileşime giren bir nesnenin kimliğine güven oluşturmanın mekanizmasıdır. IoT'deki "nesneler" için kimlik doğrulama, IoT aygıtlarının potansiyel kaynak kısıtlamaları, içinde faaliyet gösterdikleri ağların bant genişliği sınırlamaları ve çeşitli IoT varlıkları arasındaki etkileşimin mekanize olması nedeniyle günümüzde yaygın olan kullanıcı kimlik doğrulama yöntemlerinden farklı ve daha karmaşıktır.

Operasyonel Teknoloji Güvenliği (Operational Technology Security) Operasyonel teknoloji (OT) güvenliği, endüstriyel otomasyon ve kontrol sistemleri,

süreçleri ve organizasyonları için sayısal ve fiziksel güvenliğin yönetilmesi, geliştirilmesi, yönetimi ve işletilmesidir.

1.7.3. Dünya'da Siber Güvenlik Sektörü

En iyi siber güvenlik yatırımı yapan ülkeler, siber güvenlik alanına büyük önem veren ve bu alanda kaynakları aktif bir şekilde yönlendiren ülkelerdir. İşte siber güvenlik yatırımlarıyla öne çıkan bazı ülkeler:

İsrail: İsrail, siber güvenlik alanında dünya çapında tanınan bir liderdir. Yüksek teknolojiye dayalı siber güvenlik şirketleri ve araştırma merkezleriyle bilinir. İsrail hükümeti, siber güvenlik yatırımlarını teşvik etmek ve sektörü desteklemek için çeşitli politikalar uygulamaktadır (Adamsky, 2017).

ABD: ABD, siber güvenlik alanında önemli bir oyuncudur. Hem kamu sektörü hem de özel sektördeki büyük teknoloji şirketleri ve siber güvenlik firmalarıyla dikkat çeker. ABD hükümeti, siber güvenlik alanında yatırımları teşvik etmek, ulusal güvenliği sağlamak ve özel sektörle işbirliğini desteklemek için çeşitli girişimlerde bulunmaktadır (Eckert, 2005).

Çin: Çin, siber güvenlik alanında önemli yatırımlar yapan bir ülkedir. Çin hükümeti, siber güvenlik teknolojilerini geliştirmek, ulusal siber güvenliği sağlamak ve yerel siber güvenlik şirketlerini desteklemek için çeşitli politikalar uygulamaktadır. Ayrıca, Çinli teknoloji şirketleri siber güvenlik alanında önemli inovasyonlar yapmaktadır (Austin, 2018).

Almanya: Almanya, siber güvenlik alanında ciddi yatırımlar yapan ve ulusal siber güvenlik stratejisine önem veren bir ülkedir. Almanya hükümeti, siber saldırılara karşı koruma, siber suçlarla mücadele ve kritik altyapı güvenliği gibi konularda yatırımlar yapmaktadır. Ayrıca, Almanya'da siber güvenlik şirketleri ve araştırma merkezleri de aktiftir (Ulmer, 2021).

İngiltere: İngiltere, siber güvenlik konusunda güçlü bir ekosisteme sahip olan ülkelerden biridir. İngiliz hükümeti, siber güvenlik sektörünü desteklemek ve ulusal güvenliği sağlamak için çeşitli yatırımlar yapmaktadır. Ayrıca, İngiltere'de birçok siber güvenlik şirketi, araştırma merkezi ve eğitim kurumu bulunmaktadır (Sabillon, ve ark., 2016).

Bu ülkeler, siber güvenlik konusunda yapılan yatırımlar ve politikalarıyla öne çıkan örneklerdir. Ancak, siber güvenlik konusundaki yatırımlar sürekli olarak değişebilir ve farklı ülkeler farklı dönemlerde öncü olabilir.

En iyi siber güvenlik yatırımı yapan ülkelerde birçok teknoloji firması bulunmaktadır. İşte bazı örnekler:

ABD:

Cisco Systems

Palo Alto Networks

Symantec

McAfee

FireEye

Fortinet

İsrail:

Check Point Software Technologies

CyberArk

NSO Group

Radware

Argus Cyber Security

Çin:

Huawei

360 Enterprise Security Group

Tencent

Alibaba Cloud

Baidu Security

Almanya:

Siemens

Deutsche Telekom

G DATA Software

Compu Group Medical

Secunet Security Networks

İngiltere:

Darktrace

Sophos

BAE Systems Applied Intelligence

NCC Group

BT Group

Bu listedeki şirketler, siber güvenlik alanında faaliyet gösteren önde gelen firmalardan bazılarıdır. Ancak, siber güvenlik alanında sürekli olarak yeni şirketler ve teknolojiler geliştirilmektedir. Bu nedenle, siber güvenlik sektörünün dinamik doğası göz önüne alındığında, listede yer almayan birçok başarılı teknoloji firması da mevcut olabilir.

1.7.3.1. Gelişen ve Gelişmekte Olan Ülkelerde Siber Güvenlik Sektörü

İngiltere'de Siber Güvenlik

İngiltere, siber güvenlik alanında önemli ilerlemeler kaydetmiştir. Ülke, siber tehditlere karşı önlemler almak, siber saldırıları önlemek ve siber güvenlik kapasitesini güçlendirmek için çeşitli adımlar atmıştır. İşte İngiltere'nin siber güvenlik alanında ilerleme kaydetmesine yönelik bazı önemli adımlar:

Ulusal Siber Güvenlik Stratejisi: İngiltere, 2011 yılında Ulusal Siber Güvenlik Stratejisi'ni oluşturarak siber güvenlik konusundaki vizyonunu belirlemiştir. Bu strateji, siber tehditlere karşı korunma, siber suçla mücadele, siber güvenlik kapasitesinin geliştirilmesi ve ulusal altyapının korunması gibi alanları kapsamaktadır. Strateji, siber güvenlik konusundaki politika ve eylemlerin belirlenmesini sağlamıştır.

Ulusal Siber Güvenlik Merkezi: İngiltere, 2016 yılında Ulusal Siber Güvenlik Merkezi'ni (NCSC) kurarak siber güvenlik faaliyetlerini merkezi bir yapı altında toplamıştır. NCSC, siber tehditleri izlemek, siber saldırıları önlemek, siber güvenlik konusunda rehberlik sağlamak ve kriz durumlarında müdahale etmek gibi görevleri

yerine getirmektedir. NCSC, kamu kurumları, özel sektör ve vatandaşlar arasında işbirliği ve bilgi paylaşımını teşvik etmektedir.

Kamu-Özel İşbirliği: İngiltere, siber güvenlik alanında kamu-özel işbirliğini teşvik etmektedir. Özellikle kritik altyapı sağlayıcılarıyla işbirliği yaparak siber güvenlik standartlarının iyileştirilmesi ve siber tehditlere karşı etkili önlemler alınması hedeflenmektedir. Ayrıca, siber güvenlik konusunda özel sektörle işbirliği yaparak en iyi uygulamaların paylaşılması ve bilgi güvenliği kültürünün yaygınlaştırılması amaçlanmaktadır.

Eğitim ve Farkındalık: İngiltere, siber güvenlik eğitimi ve farkındalık konularında da ilerleme kaydetmiştir. Özellikle, siber güvenlik alanında yetkin uzmanların yetiştirilmesi için eğitim programları ve sertifikasyonlar sağlanmaktadır. Ayrıca, siber güvenlik farkındalığını artırmak amacıyla kampanyalar düzenlenmekte ve bilinçlendirme faaliyetleri yürütülmektedir.

Bu adımlar, İngiltere'nin siber güvenlik alanında ilerleme kaydetmesine yönelik örneklerdir. Ülke, siber tehditlerin hızla arttığı bir ortamda, siber güvenlik konusunda politika, teknoloji ve işbirliği alanlarında sürekli olarak gelişmeye ve yenilik yapmaya devam etmektedir.

İsrail'de Siber Güvenlik

İsrail, siber güvenlik konusunda dünya çapında tanınan bir lider ülkedir. Ülke, hem siber güvenlik teknolojileri geliştirme hem de siber saldırılara karşı korunma konusunda büyük bir başarı göstermiştir. İsrail'in siber güvenlik alanındaki durumu aşağıdaki faktörlerle açıklanabilir:

İnovasyon ve Teknoloji Odaklılık: İsrail, siber güvenlik alanında inovasyona ve teknolojiye büyük bir önem vermektedir. Ülke, yüksek teknoloji şirketleri, girişimler ve araştırma kurumlarıyla yoğun bir ekosisteme sahiptir. İsrail, siber

güvenlik teknolojilerinde önemli ilerlemeler kaydetmiş ve dünya çapında tanınmış şirketlerin ortaya çıkmasına katkıda bulunmuştur.

Savunma ve İstihbarat Yetenekleri: İsrail, güvenlik ve istihbarat alanında derin bir uzmanlığa sahiptir. Bu bilgi birikimi, siber güvenlikte de büyük avantaj sağlamaktadır. İsrail, ulusal siber güvenlik ajansları, birimler ve özel sektör işbirliği ile siber saldırılara karşı etkin bir şekilde savunma yapmaktadır. Ülke, sürekli olarak siber saldırıları izlemekte, tehditleri analiz etmekte ve hızlı bir şekilde müdahale etmektedir.

Eğitim ve İnsan Kaynağı: İsrail, siber güvenlik konusunda yetenekli insan kaynağına sahiptir. Üniversitelerdeki siber güvenlik programları ve eğitim kurumları, nitelikli uzmanların yetişmesini sağlamaktadır. Ayrıca, İsrail Silahlı Kuvvetleri'ndeki askeri eğitim programları da siber güvenlik yeteneklerini güçlendirmektedir.

İşbirliği ve Uluslararası İlişkiler: İsrail, siber güvenlik konusunda uluslararası işbirliğine büyük önem vermektedir. Ülke, diğer ülkelerle, uluslararası kuruluşlarla ve özel sektör paydaşlarıyla bilgi paylaşımı, ortak egzersizler ve siber güvenlik politikalarının geliştirilmesi konularında aktif olarak işbirliği yapmaktadır. İsrail, uluslararası konferanslara ev sahipliği yapmakta ve siber güvenlikte en iyi uygulamaların paylaşılmasına öncülük etmektedir.

Bu faktörler birleştiğinde, İsrail'in siber güvenlik alanında güçlü bir durumda olduğunu söyleyebiliriz. Ülke, siber saldırılara karşı savunma kapasitesini geliştirirken aynı zamanda yenilikçi çözümler üretmeye devam etmektedir.

Singapur'da Siber Güvenlik

Singapur, siber güvenlik konusunda önemli ilerlemeler kaydeden ve dünya çapında tanınan bir ülke olarak öne çıkmaktadır. Ülke, siber tehditlerle başa çıkmak, dijital altyapıyı korumak ve siber güvenlik kapasitesini güçlendirmek için çeşitli

adımlar atmıştır. Singapur'un siber güvenlik alanında ilerleme kaydetmesine yönelik bazı önemli faktörler şunlardır:

Stratejik Planlama ve Politika: Singapur, siber güvenlik konusunda stratejik bir planlama ve politika çerçevesi oluşturmuştur. Ulusal Siber Güvenlik Stratejisi ve Master Plan gibi belgeler, siber güvenlik hedeflerini ve politikalarını belirlemektedir. Bu çerçeve, siber güvenlik konusundaki politika ve eylemlerin belirlenmesini ve koordinasyonunu sağlamaktadır. (Yıldırım ve Adalı, 2017)

Yatırım ve Altyapı: Singapur, siber güvenliği bir öncelik olarak görmekte ve buna uygun yatırımlar yapmaktadır. Ülke, siber güvenlik altyapısını güçlendirmek, tehditleri tespit etmek ve saldırılara karşı korunma sağlamak için önemli adımlar atmıştır. Bunlar arasında siber tehdit bilgi paylaşım platformları, siber savunma merkezleri ve siber güvenlik operasyon merkezleri bulunmaktadır.

İnsan Kaynağı ve Eğitim: Singapur, siber güvenlik alanında nitelikli insan kaynağı yetiştirmeye büyük önem vermektedir. Ülke, siber güvenlik eğitim programları, sertifikasyonlar ve sektörle işbirliği yaparak uzmanların yetişmesini desteklemektedir. Ayrıca, siber güvenlik farkındalığını artırmak için kamuoyu eğitim kampanyaları düzenlenmektedir.

İşbirliği ve Uluslararası İlişkiler: Singapur, siber güvenlik alanında uluslararası işbirliğine önem veren bir ülkedir. Çeşitli ülkeler, özel sektör kuruluşları ve uluslararası kuruluşlarla işbirliği yaparak bilgi paylaşımını teşvik etmektedir. Singapur, uluslararası konferanslara ev sahipliği yapmakta ve siber güvenlikte en iyi uygulamaları paylaşmaktadır.

Bu faktörler, Singapur'un siber güvenlik alanında ilerleme kaydetmesine katkıda bulunmuştur. Ülke, hem ulusal siber güvenlik kapasitesini güçlendirmekte hem de diğer ülkelerle işbirliği yaparak küresel siber güvenlik ortamının gelişimine katkı sağlamaktadır.

1.7.4. Türkiye’de Siber Güvenlik Sektörü

Türkiye'de siber güvenlik sektöründe yapılan politik ve stratejik olaylar aşağıdaki gibi sıralanabilir:

Siber Güvenlik Kanunu: Türkiye, 2016 yılında Siber Güvenlik Kanunu'nu kabul etmiştir. Bu kanun, siber güvenlik alanında hukuki düzenlemeleri belirlemiş ve siber suçlarla mücadele edilmesini sağlamıştır. Kanun, kritik altyapıların korunması, siber saldırıların tespiti ve önlenmesi, siber güvenlik olaylarının yönetimi gibi konuları kapsamaktadır.

Ulusal Siber Güvenlik Stratejisi ve Eylem Planı: Türkiye, 2013 yılında Ulusal Siber Güvenlik Stratejisi ve 2016-2019 dönemi için Ulusal Siber Güvenlik Eylem Planı'nı belirlemiştir. Bu strateji ve eylem planı, siber güvenlik politikalarını ve hedefleri belirlemekte, kamu, özel sektör ve akademik kuruluşlar arasında işbirliğini teşvik etmekte ve siber güvenlik farkındalığını artırmayı hedeflemektedir.

Siber Güvenlik Merkezi: Türkiye, Kamu Siber Güvenlik Kurumu (KSGM) bünyesinde Siber Güvenlik Merkezi'ni kurmuştur. Bu merkez, siber saldırıları izlemek, tehditleri analiz etmek, siber güvenlik olaylarına müdahale etmek ve bilgi paylaşımını sağlamak gibi görevleri yerine getirmektedir. Ayrıca, merkez, siber güvenlik konusunda yetenek geliştirme çalışmaları da yürütmektedir.

Siber Güvenlik Operasyon Merkezi: Türkiye, siber güvenlik olaylarını hızlı bir şekilde tespit etmek ve müdahale etmek için Siber Güvenlik Operasyon Merkezi'ni faaliyete geçirmiştir. Bu merkez, devlet kurumları ve kritik altyapı sağlayıcıları arasında siber güvenlik olaylarına müdahaleyi koordine etmektedir.

Kamu-Özel İşbirliği: Türkiye, kamu ve özel sektör arasında siber güvenlik konusunda işbirliğini teşvik etmektedir. Özellikle kritik altyapı sağlayıcıları ve özel sektör firmalarıyla işbirliği protokolleri imzalanmıştır. Bu işbirliği çerçevesinde, bilgi paylaşımı, ortak tatbikatlar ve siber güvenlik önlemlerinin iyileştirilmesi hedeflenmektedir.

Uluslararası İlişkiler: Türkiye, siber güvenlik konusunda uluslararası işbirliğine önem vermektedir. Ülke, farklı ülkeler, uluslararası kuruluşlar ve sektör paydaşlarıyla bilgi paylaşımı, ortak egzersizler, teknoloji transferi ve en iyi uygulamaların paylaşılması için işbirliği yapmaktadır. Türkiye, uluslararası siber güvenlik konferanslarına ev sahipliği yapmış ve bu alanda aktif bir rol oynamaktadır.

Bu politik ve stratejik olaylar, Türkiye'nin siber güvenlik sektörünün gelişimine ve ulusal siber güvenlik kapasitesinin güçlenmesine katkıda bulunmuştur.

Türkiye, gelişmekte olan ülkeler arasında siber güvenlik konusunda önemli adımlar atmış ve ilerleme kaydetmiş bir ülkedir. Türkiye'nin siber güvenlikteki durumu aşağıdaki şekillerde değerlendirilebilir:

Yasal ve Kurumsal Altyapı: Türkiye, Siber Güvenlik Kanunu gibi önemli yasal düzenlemeleri hayata geçirmiş ve siber güvenlikle ilgili kurumsal yapıları oluşturmuştur. Kamu Siber Güvenlik Kurumu (KSGM), Siber Güvenlik Merkezi ve Siber Güvenlik Operasyon Merkezi gibi kurumlar, siber güvenlik konusunda koordinasyon, izleme ve müdahale görevlerini yerine getirmektedir.

Eğitim ve İnsan Kaynağı: Türkiye, siber güvenlik konusunda yetişmiş insan kaynağına yönelik önemli adımlar atmaktadır. Üniversitelerde siber güvenlik bölümleri ve sertifika programları açılmış, öğrencilerin ve profesyonellerin siber güvenlik alanında eğitim alması teşvik edilmektedir. Ayrıca, siber güvenlik farkındalığını artırmak amacıyla eğitim ve bilinçlendirme kampanyaları düzenlenmektedir.

İşbirliği ve Ortak Projeler: Türkiye, siber güvenlik konusunda ulusal ve uluslararası düzeyde işbirliği projelerine aktif olarak katılmaktadır. Özellikle NATO Cyber Defence Centre of Excellence gibi uluslararası kuruluşlarla işbirliği yapmakta, ortak tatbikatlar düzenlemekte ve bilgi paylaşımını sağlamaktadır. Ayrıca, kamu-özel sektör işbirliği de siber güvenlik konusunda önemli adımlar atılmasını sağlamaktadır.

Kritik Altyapı Güvenliği: Türkiye, kritik altyapıların siber saldırılara karşı korunması konusunda önemli adımlar atmaktadır. Özellikle enerji, finans, iletişim gibi kritik sektörlerin siber güvenliğini sağlamak için gerekli önlemler alınmaktadır. Siber saldırıların tespiti, olaylara müdahale ve kurtarma kapasitesi geliştirilerek kritik altyapıların güvenliği sağlanmaktadır.

Türkiye'nin siber güvenlik alanında gelişmekte olan ülkeler arasında önemli bir konuma sahip olduğu söylenebilir. Ancak, sürekli olarak değişen siber tehditler karşısında sürekli güncellenen bir strateji ve yatırım yapma ihtiyacı bulunmaktadır. Türkiye'nin siber güvenlik kapasitesini daha da güçlendirmek için ileri teknolojilerin kullanımı, uluslararası işbirliği ve siber güvenlik kültürünün yaygınlaştırılması gibi alanlarda çalışmalarına devam etmesi önemlidir.

1.8. Sporda Siber Güvenlik Saldırı Yöntemleri ve Açıklıklar

1.8.1. Oltalama Saldırıları

Oltalama, saldırganların, e-posta, sohbet veya diğer iletişim kanallarında saygın bir varlık veya kişi gibi maskelenerek kullanıcının giriş kimlik bilgileri veya hesap bilgileri gibi bilgilerini öğrenmeye çalıştıkları dolandırıcılık biçimidir. Bir ağ geçidi e-posta filtresi, toplu olarak hedeflenen oltalama e-postalarını yakalayarak kullanıcıların gelen kutularına ulaşan oltalama e-postalarının sayısını azaltır. Web güvenlik ağ geçitleri de kullanıcıların kötü amaçlı bir bağlantı hedefine ulaşmasını engelleyerek bir başka savunma katmanı sağlayabilir Web Güvenlik Ağ Geçitleri, istenilen URL'leri, kötü amaçlı yazılım dağıtımından şüphelenilen ve sürekli

güncellenen bir veritabanından kontrol ederek çalışırlar. Bu tip saldırıları organizatör şirket personellerine veya spor külüp işletmelerine yönelik olduğu gibi veri işleyen perosnele yönelikte hedefli olabilirler.

1.8.2. Fidyeci Yazılımlar

Fidyeci yazılım, kurbanının bilgisayarındaki verilerin genellikle şifreleme yöntemiyle kilitlendiği ve fidye verilen veriler şifresiz hale getirilmeden önce ödeme talep edilen kötü amaçlı yazılımdır. Fidyeci yazılım saldırılarının nedeni neredeyse her zaman parasaldır ve diğer saldırı türlerinden farklı olarak, kurban genellikle bir istismarın meydana geldiği konusunda bilgilendirilir ve kurbana saldırıdan kurtulma talimatları verilir. Spor işletme ve organizasyonlarda fidye saldırılarına karşı koruma sağlamak için uzmanlar kullanıcıları bilgisayar aygıtlarını düzenli olarak yedeklemeyi ve düzenli olarak virüsten koruma yazılımını güncellemeyi tavsiye etmektedir.

1.8.3. Servis Engelleme Saldırıların

Servis Engelleme saldırısı, bir saldırgan yasal kullanıcının hedef bilgisayar sistemlerine, aygıtlarına veya diğer ağ kaynaklarına erişmesini engelleyen bir işlem başlatması durumunda ortaya çıkan bir güvenlik olayıdır. Bir DoS saldırısı yaşandığından şüphelenildiğinde, işletmelerin gerçek bir DoS saldırısı mı yoksa başka bir faktörün neden olduğu performans düşüşü olup olmadığını belirlemek için İnternet servis sağlayıcısına (ISS) başvurmaları gerekir. ISS, kötü amaçlı trafiği yeniden yönlendirerek veya azaltarak saldırının hafifletilmesine yardımcı olabilir ve saldırının etkisini azaltmak için yük dengeleyici kullanabilir.

1.8.4. Gelişmiş Tehdit Saldırıları

Gelişmiş tehdit saldırısı (APT), yetkisiz bir kişinin bir ağa erişmesini ve orada uzun süre tespit edilmeden kalmasını sağlayan bir ağ saldırısıdır. APT saldırısının amacı, ağa veya organizasyona zarar vermek yerine verileri çalmaktır. APT saldırıları, ulusal savunma, imalat ve finans endüstrisi gibi yüksek değerli bilgiye sahip sektörlerdeki kuruluşları hedef almaktadır. APT saldırılarını tanımlamak zor olsa da, verilerin çalınması hiçbir zaman tamamen görünmez olamaz. Giden verideki anormalliklerin tespit edilmesi belki de ağ yöneticisinin, ağının bir APT saldırısının hedefi olduğunu keşfetmesinin en iyi yoludur.

1.8.5. Yetki Yükseltme Saldırıları

Yetki yükseltme saldırısı, saldırganın ağa ve ilişkili veri/uygulamalara ayrıcalıklı erişimini sağlamak için programlama hatalarından veya tasarım kusurlarından yararlandığı bir tür ağ saldırısıdır. Dikey yetki yükseltme, saldırganın kendisine daha yüksek ayrıcalıklar tanımasını gerektirir. Bu,spor işletme ve organizasyonlarında genellikle, saldırganın yetkisiz kod çalıştırmasına izin veren çekirdek düzeyinde işlemler gerçekleştirerek elde edilir. Yatay yetki yükseltme, saldırganın daha önce verilen yetkileri kullanmasını gerektirir, ancak benzer ayrıcalıklara sahip başka bir kullanıcının kimliğinin ele geçirildiğini varsaymaktadır. Örneğin, başka bir kişinin çevrimiçi uygulumada hakem yetkisinin hesabına erişen biri, yatay yetki yükseltmiş olur.

1.8.6. Truva Atı Saldırıları

Truva atı zararsız görünen, ancak oldukça zararlı olan bir programdır. Genellikle, kötü niyetli program, masum görünümlü bir e-posta eki veya bir oyun gibi ücretsiz bir programın içine gizlidir. Kullanıcı Truva atını indirdiğinde içeride gizlenmiş zararlı yazılım da indirilir.Kötü niyetli kod, bilgisayar içine girdikten

sonra, saldırganın gerçekleştirmek üzere tasarladığı herhangi bir görevi yerine getirebilir.Truva atı yazılımının bulaşmasına engel olmak için, kullanıcılar virüsten koruma yazılımlarını güncel tutmalı, dosyaları veya programları güvenilmeyen kaynaklardan asla indirmemeli ve açmadan önce virüsten koruma yazılımıyla yeni dosyaları taramalıdır.

1.8.7. İnternet Uygulamalarına Saldırılar

1.8.8. Casus Yazılımlar ile Saldırılar

Casus yazılım, son kullanıcı bilgisi olmadan bir bilgi işlem cihazına kurulmuş bir yazılımdır. Bu tür yazılımlar, bazen nispeten zararsız nedenlerle kurulmuş olsalar bile, son kullanıcının gizliliğini ihlal edebilir ve istismar edilme potansiyeline sahiptir. Kullanıcılar, casus yazılımları önlemek için yalnızca güvenilir kaynaklardan yazılım yüklemeli, yazılım yüklerken tüm açıklamaları okumalı, açılır pencerelere tıklanmamalı ve tarayıcı, işletim sistemi ve uygulama yazılımlarını güncel tutmalıdır.

1.8.9. Solucan Yazılım ile Saldırılar

Bir bilgisayar solucanın amacı, bulaştığı sistemde aktif olarak kalmak ve kendini yeni sistemlere bulaştırmaktır. Solucanlar genellikle bir işletim sisteminin kullanıcıya açık olmayan parçalarını kullanırlar. Solucanlar yalnızca kontrol sistem kaynaklarını fazla tüketmesi, diğer görevleri yavaşlatması veya durdurması durumunda fark edilir.

1.8.10. Karışık Tehdit Saldırılar

Karışık tehdit, birden fazla zararlı yazılım türündeki unsurları birleştiren ve genellikle hasarın şiddetini ve bulaşma hızını artırmak için birden fazla saldırı

vektörü kullanan bir istismar saldırısıdır. Nimda, CodeRed, Bugbear ve Conficker birkaç iyi bilinen örnektir. Virüs, solucan veya Truva atları olarak tanımlanabilmelerine rağmen, günümüzdeki istismar saldırıları karışık tehdit örnekleridir. Uzmanlar, karışık tehditlerden korunmak için ağ yöneticilerini yama yönetimi konusunda dikkatli olmaya, iyi güvenlik duvarı ürünlerini kullanmaya ve korumaya, ve kullanıcıları doğru e-posta kullanımı ve çevrimiçi davranış konusunda eğitmeye davet etmektedir.

1.8.11. Mobil Zararlı Yazılım

Mobil casus zararlı yazılımı, son kullanıcının bilgisi veya izni olmaksızın son kullanıcının eylemleri hakkındaki bilgileri izleyen ve kaydeden yazılım programıdır. Son kullanıcı, izleme yazılımının kurulu olduğunun farkındaysa, yazılım casus yazılım olarak değerlendirilmez. Casus yazılımları bulmak ve kaldırmak için antispyware koruması içeren virüsten koruma yazılımı kullanılmalıdır

1.8.12. Ortadaki Adam Saldırı

Ortadaki Adam saldırısı, saldırganın, doğrudan birbirleriyle iletişim halinde olduklarını düşünen iki taraf arasındaki mesajları gizlice yakaladığı ve bu durumdan faydalandığı bir saldırı türüdür. Bu saldırılar, hassas bilgilerin gerçek zamanlı olarak değiştirilmesine olanak sağlaması sebebiyle çevrimiçi güvenlik için ciddi bir tehdit oluşturmaktadır. Çevrimiçi bankacılık ve e-ticaret siteleri sıklıkla Ortadaki Adam saldırılarının hedefi olur, böylece saldırgan oturum açma kimlik bilgileri ve diğer hassas verileri ele geçirebilir.

1.8.13. SSL / TLS Altsürüme Zorlama

POODLE açıklığı kullanılarak yapılan SSL / TLS Altsürüme Zorlama saldırıları, şifreleme ve kimlik doğrulama için Güvenli Soket Katmanı (SSL) 3.0

protokolüne dayanan tarayıcı tabanlı iletişimi hedef almaktadır. TLS (Taşıma Katmanı Güvenliği) protokolü, SSL protokülünün yerini alsa da, TLS bağlantısı yapılamayan durumlarda birçok tarayıcı SSL protokolünü kullanmaya devam etmektedir. Bu tarz durumlarda saldırgan POODLE açıklığını kullanarak tarayıcıyı SSL 3.0 kullanmaya zorlar. Bu saldırıdan korunmak için ağ yöneticilerinin sunucu yazılımlarının TLS'in en son sürümünü desteklediğini ve düzgün şekilde yapılandırıldığını kontrol etmeleri gerekir.

1.8.14. Kontrol Dışı Registry Kayıtların

Dosyasız kötücül saldırılarda güncel bir trend, Windows kayıt defterine kod enjekte etmektir. Bu saldırıların çoğu, bir e-posta iletisinde bir dosya veya bağlantı olarak gönderilir. Bağlantı veya ek tıklandığında, zararlı yazılım yükünü Windows kayıt defterine yazar ve sonra kaybolur. Bu tür yeni dosyasız saldırılara karşı korunmak için antivirüsün güncellenmesi yeterli değildir

1.8.15. Bellek Tabanlı Saldırılar

Dosyasız zararlı yazılım, yalnızca bellekte bulunan kötü amaçlı koddur. Zararlı yazılım doğrudan RAM'e yazılır. Kod, daha sonra exploit için kullanılan iexplore.exe veya javaw.exe gibi çalışan bir işleme enjekte edilir. Bu tarz saldırılardan korunmak için işletim sistemi tarafından çalıştırılan tüm yeni süreçlerin doğrulanması, beyaz - kara liste kontrolünün düzenli olarak yapılması gerekmektedir

1.8.16. Tuş Kaydedicilerden (klavye, Ekran, Ağ) Saldırıları

Tuş kaydedici, belirli bir bilgisayarın klavyesinde yazılan her tuş vuruşunu izlemek ve kaydetmek için kullanılan bir gözetleme teknolojisidir. Tuş kaydedici yazılımı iPhone ve Android cihazları gibi akıllı telefonlarda da kullanılabilir. Tuş kaydediciler genellikle siber suçlular tarafından kişisel olarak tanımlanabilir bilgileri,

kimlik bilgilerini ve hassas kurumsal verileri çalmak için bir casus yazılım aracı olarak kullanılır. Antikeylogger yazılımı, ortak tuş kaydedici özelliklerini bir control listesi ile karşılaştırarak, yazılım tabanlı tuş kaydedicileri tespit etmek için dizayn edilmiştir.

1.8.17. Polimorfik Zararlı Yazılımlar

Polimorfik zararlı yazılımlar, sürekli olarak değişen bir virüs, solucan, trojan veya casus yazılım gibi zararlı, yıkıcı veya müdahaleci bilgisayar yazılımları olup, bu yazılımların anti-malware programları ile tespit edilmesi oldukça zordur. Kötü amaçlı kodun evrimi, dosya adı değişiklikleri, sıkıştırma ve değişken anahtarlarla şifreleme gibi çeşitli şekillerde oluşabilir. Polimorfik zararlı yazılımlarla mücadelede en iyi yöntem çoklu ve çeşitli engelleme, filtreleme, algılama ve ortadan kaldırma programları kullanmaktır. Bu programlar güncel tutulmalı ve olabildiğince sık çalıştırılmalı, (varsa) otomatik koruma özellikleri etkinleştirilmiş olmalıdır.

1.8.18. Proses Sömürülmesi Engellenmesi

Prosess Sömürülmesi saldırılarının en çok bilinen türü, tarayıcılarda arabellek aşımı saldırılarıdır. Bir program veya işlem, sabit uzunlukta bir bellek bloğuna veya arabelleğe daha fazla veri yazmaya çalıştığında arabellek taşması oluşur. Bir arabellek taşması kullanmak, bir saldırganın prosesleri kontrol etmesine, kilitlemesine veya değişkenlerini değiştirmesine olanak tanır. Ürün satıcıları, keşfedilen arabellek taşması güvenlik açıklarını gidermek için yazılım güncellemeleri yayınlarlar, ancak keşfedilen güvenlik açığı ile dağıtılan güncelleme arasındaki süre risk oluşturmaya devam etmektedir.

1.8.19. Rootkits Korunma

Spor kuruluşları artık dijitalleşme boyutunda hizmet sundukları için hepside veri akışlarını bilgisayar veya dijital platformlarda sağlamaktadır. Rootkit, bir bilgisayara veya yazılımının başka bir şekilde izin verilmeyen bir alanına (örneğin, yetkisiz bir kullanıcıya) erişim sağlamak için tasarlanmış ve genellikle varlığını veya diğer yazılımların varlığını maskeleyen, genellikle kötü amaçlı olan bir bilgisayar yazılımı koleksiyonudur (Mcafee, 2006). Genellikle, bir sistem kırıcı, bilinen güvenlik açığından yararlanarak veya bir parola kırarak kullanıcı düzeyinde erişim elde ettikten sonra bilgisayara bir rootkit yükler. Spor şirketi veya kuruluşta sistemde ve sunucularda rootkit kurulduktan sonra, saldırganın saldırıya maruz kalmasını maskeleme ve bilgisayara ve muhtemelen ağdaki diğer makinelere root kullanıcı edinerek elde etme veya ayrıcalıklı erişim hakkı kazanmasına olanak tanır. Rootkit algılandığı takdirde kurtulmanın tek yolu sunucu ve ya bilgisayardaki önce karantinaya alıp sabit diski tamemen silmek ve işletim sistemini yeniden kurmaktır (Kim ve ark., 2012).

1.8.20. Gömülü Yazılım Sömürülerine Saldırma

Spor karşılaması esnasında, spor ilgili organizasyonda yada kurum veya kulüplerde gömülü sistemler, internet ve kablosuz erişim noktaları, IP kameralar, güvenlik sistemleri, hızı ayarlayıcılar, dronlar ve endüstriyel kontrol sistemleri gibi çok çeşitli cihazlarda bulunabilir. Futbol karşılaşmalarından tutun bir sürü spor karşılaşmasında taraftara yayını daha kaliteli göüruntü sunabilmek için dronlar veya çok sayıda farklı türde gömülü kameralar kullanılmaktadır. Hack işlemi aslında, gömülü sistemin ROM çipleri üzerinde veya donımsal yazılımı üzerinde gerçekleştirilebilir (Rabaiotti ve Hargreaves, 2010).

1.8.21. Hatalı Konfigürasyon Açıklıkları

Spor alanında kullanabilecek dijital platform ve uygulamalarını yanlış veya hatalı yapılandırma açıklarını kullanarak, kablolu veya kablosuz ağ saldırı üzerinden gerçekleşir. Spor karşılaşmasında kullanılan birbiri ile uyumlu olmayan donanım ve yazılımın, ağ altyapısını saldırıya karşı savunmasız hale getirme olasılığı vardır (Hansman ve Hunt, 2005). Bu tür saldırıları engellemek için konfigürasyonun doğru yapıldığı kontrol edilmelidir. Örneğin bir stadyumda bütün haberleşmede kullanılan bilgisayar ortamlarının haberleşmesini sağlayan ağ alt yapısı vardır. Bu tür sistemler aslında kullanıcılar arası birbirne kapalı olmalıdır. Bir taraftar Ethernet kablolu bir alana giriş yapabilir veya taraftarın hizmet verilen noktada bu tür kablolama yapılmış olabilir. Kötü niyetli bir taraftar veya kullanıcı kablosunuda kendi getirip stadyumunda hizmet veren skorboardan tutun yayın sağlayan kuruluşun kameralarına kadar hizmete ulaşıp hizmet veremez hale getirebilir. Aynı şekilde stadyumda hizmet veren ağ ortamında kullanılan anahtar değiştiriciler hatalı konfigüre edilebilir. Maç devam ederken bir anda hizmet kesintisine neden olabilir.

1.8.22. Fiziksel veya Kaba Kuvvet Yöntemli Saldırılar

Spor ilgili kurum ya kuruluşlara dijital sahada büyük zarar verebilecek, saldırgan tarafından çok sayıda veri elde edibilme saldırı yöntemlerinden biri olan fiziksel veya kaba kuvvet yöntemli saldırılarıdır. Aslında fiziksel saldırı burada bir başka kişinin bedenini hedef alan her türlü saldırıdan gibi yaralama, tekme tokat atma, bir aletle vurma, gibi birebir teması işleyen saldırılar değildir. Buradaki fiziksel kelimesinin anlamı hedef ile aynı yerde bulunan bir saldırganın kullanabileceği güvenlik açıklarının toplamıdır. Fiziksel saldırı alanı, kötü niyetli çalışanlar, sosyal mühendislik saldırılarını kullanan kişiler vb. tarafından sömürülebilen sürekli deneme yanılma yoluyla parola ve kullanıcı adlarını ele geçirme yöntemleridir (Kara, 2019). Sporla ilgili kurum ya da kuruluşlar veya organizasyon sorumluları çalıştıkları dijital bilişim şirketleriyle ilgili her türlü teknojik alt yapıyı kullanırken özellikle web veya sanal ortamdaki uygulamalarında bu tür saldırılara kapalı olmalıdır. Spor

kuruluşunda kullanılan her hangi bir platform dışardan erişim sağlanabilir buda bir zaafiyete sebep olabilir. Örneğin Türkiye Futbol Federasyonu web sayfası aynı zamanda hem bilgilendirme ortamı taşıdığı için hem taraftar yada vatandaşlar tarafından kullanbilmekte iken aynı zamanda hakem, gözlemci veya mejaerlere karşılaşma içinde görevli olabilecek çalışanlara hizmet vermektedir (https://fys.tff.org/). Bu tür uygulam ortamları dışarıdan erişime açıktır. Sürekli paralo ve şifre kaba kuvvet saldırısı kullanıp hakemlere ait veriler elde edebilir maç içi veya görevlilerke ilgili kötü niyetli futbol karşılaşmasını zor duruma sokabilecek sebeplere neden olabilirler. Spor alanında kullanabilecek fiziksel saldırı veya kaba kuvvet saldırı alanı azaltmaya yönelik en iyi uygulamalar, güvenli kimlik doğrulamayı sınırlandırmak, iki faktörlü doğrulama yöntemi kullanmak veya sabit sürücüleri ve eski donanımları atmadan önce sıfırlamak ve değerli bilgileri ortada bırakmaktan kaçınmaktır (Andrade ve ark., 2016).

1.8.23. Sosyal Mühendislik Saldırıları

Sosyal mühendislik, insan etkileşimine büyük ölçüde dayanan ve teknolojiyi kullanarak ya da kullanmadan normal şartlar altında sahip olunamayacak bilgilerin elde edilme şeklidir (Mitnick ve Simon, 2013). Spor dünyası dahil olmak üzere dijital dünyada birçok sosyal mühendislik sömürüsü, insanların yardımcı olmaya istekli olmalarından kaynaklanmaktadır (Watson, 2014). Bilişim alanındaki güvenlik uzmanları, bilişim teknolojilerin departmanlarının sosyal mühendislik tekniklerini kullanan sızma testlerini düzenli olarak gerçekleştirmelerini önerir. Bu testler, spor organizasyonun ve kuruluşun yöneticileri bilgilerinden tutun web sayfalarına kadar hangi kullanıcı çeşitleri tarafından belirli saldırı türleri için en fazla risk oluşturduğunu öğrenmelerine yardımcı olabilmektedir. Ayrıca sosyal mühendislik saldırıları deneyerek aynı zamanda spor şirket veya kuruluşta hangi çalışanın ek eğitime ihtiyaç duyduğunu da belirlemekte yardımcı olmaktadır. Bu tür saldırılara sporla ilgili kurum ya kuruluşlara dışardan olabildiği gibi spor şirketlerini kullanarakta taraftar ya da hedef kitleye yönelik yapılabilir. Örneğin 2008 Pekin Olimpiyatlarında yüzlerce hedef kitle kurban seçilerek, sahte bir Pekin Olimpiyatları

web sitesi görüümü veren siteden büyük miktarlarda para kaybetti. Site bir bilet satıcısı imajı verilmiş gibi görünüp de aslında vatandaşların kredi kartı bilgilerini ve diğer kişisel bilgileri çalan siteydi (Trendmicro, 2015).

1.8.24. Kötü Niyetli Kullanıcılar

Kötü niyetli kişiler veya kullanıcılar (içerdeki saldırganlar), yetkili ve güvenli kullanıcı imajı oluşturarak kulüp veya sporculara ait hassas bilgileri elde etmeye spor kulubu veya kuruluşunun herhangi bir verisine ulaşmaya çalışırlar (Bowen ve diğ., 2009). Kötü niyetli kullanıcılar, hangi verinin nerede nasıl formatta olduğunu bildikleri için ve bu verilere güvenilir olarak erişebildiklerinden, bilgi teknolojileri ve bilgi güvenliği profesyonelleri, kötü niyetli kullanıcıları tespit etmekte zorlanmaktadır. Çünkü kullanıcı içeridedir ve isteği bilgileri yetkisi dahilinde bile elde edebilmektedir. Spor dünyasında kulüplerde ve kuruluşlardan aslında bu tip kullanıcıların sayısı oldukça fazla olabilmektedir. Bu nedenledir ki kurum ve kuruluşa işe başlamadan önce güvenlik soruşturması yapılabilmesi bir nebze olsun önem olarak alınabilmektedir. Kaynağın insan olduğu yerde davranış ve niyetler her han değişebilir. Ayrıca spor kulüp ve şirketten memnun olmayan çalışan veya sporcu bu durumu verilerini kullanabilmektedir. Basın karşısında açıklanacak bilgiler şirketin itibarini zedeleyebilmektedir.

2. GEREÇ VE YÖNTEM

Dünyadaki ve Türkiye'deki öngörü çalışmaları sonucunda, "siber güvenlik" teknolojisi kritik bir teknoloji olarak kabul edilmesine rağmen Türkiye'de siber güvenlik teknolojisine odaklanmış bir çalışma bulunmadığından siber güvenlik teknolojisi için ulusal bir vizyon oluşturacak öngörü çalışmasının bilimsel ve toplumsal yararları olduğu görülmüştür. Bu uygulamada özetle Bulanık Delphi araştırması ve SWOT (Güçlü ve zayıf yanlar, fırsatlar ve tehditler) analizi teknikleri kullanılmış, elde edilen sonuçlar doğrultusunda siber güvenlik teknolojisinin Türkiye'de gelişimini sağlayacak düzenlemeleri içermektedir.

Delphi anketi uygulaması Delphi araştırması; Çekirdek Uzman Grubu ve Bulanık Delphi Anketleri şeklinde 2 fazlı (aşamalı) karma bir yöntemle yürütülmüştür. Araştırmada, bulanık Delphi anketi için soruların oluşturulması, literatür taramasına, uzman görüşmelerine, derinlemesine (Bireysel) görüşme uyarlama ve benimseme tekniğine dayanıyordur. Anket komut dosyası oluşturma süreci, normal anket komut dosyasının oluşturulmasına benzerdir. Kullanılan likert ölçeği anket ve araştırmacılar tarafından izin düzeyi, aşama düzeyi ve ilgi düzeyi olarak ölçülecek olana göre gerekli olan araştırma sorularının gerekliliklerine dayanmaktadır. Bu çalışmada kullanılacak araçlar, araştırma tasarımı çerçevesinde açıklandığı gibi her aşamanın amacına bağlıdır. İlk adım olarak araştırmada, araç geliştirme sürecindeki yapıları ve öğeleri geliştirmek için veri toplamak üzere birebir nitel araştırma tekniklerinden olan yüz yüze görüşme yaklaşımını kullanacaklardır. Araştırma görüşmesi, iki taraf arasında yapılan ve çalışmayla ilgili olan ve belirli bir içeriğe odaklanan konuşmalar olarak tanımlanabilir ve nesnel tanımlama, tahmin veya sistematik olarak açıklama olarak belirlenir (Sang, 2010). Yüzyüze görüşmeleri, zaman ve yer bakımından senkronize iletişim ile karakterize edilir. Bu eşzamanlı iletişim nedeniyle, başka hiçbir görüşme yönteminde olmadığı gibi, yüze yüze birebir görüşmeleri sosyal ipuçlarından yararlanır. Görüşülen kişinin sesi, tonlaması, beden dili vb. gibi sosyal ipuçları, görüşmeciye, görüşülen kişinin bir soruya verdiği sözlü yanıta eklenebilecek pek çok ek bilgi verebilir. Elbette sosyal ipuçlarının değeri,

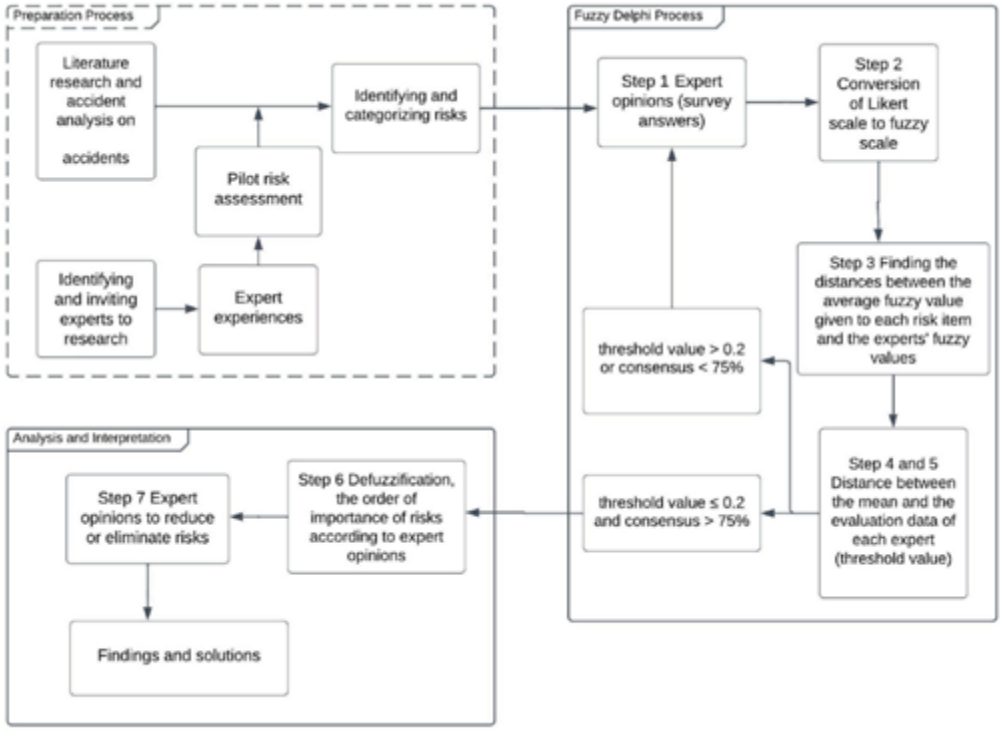
görüşmecinin görüşülen kişiden ne bilmek istediğine de bağlıdır. Görüşmeci, örneğin işçi sendikasına karşı tavrını öğrenmek istediği bir özne ve yeri doldurulamaz bir kişi olarak görülüyorsa, o zaman sosyal ipuçları çok önemlidir. Görüşmeci, konu olarak uzmanla hiçbir ilgisi olmayan şeyler veya kişiler hakkında bir uzmanla görüştüğünde, sosyal ipuçları daha az önemli hale gelir (Emans, 1986). Öte yandan, bu görünürlük, görüşmeci davranışıyla görüşmeciyi özel bir yöne yönlendirdiğinde rahatsız edici görüşmeci etkilerine yol açabilir. Bu dezavantaj, bir görüşme protokolü kullanılarak ve görüşmecinin bu etkinin farkında olmasıyla azaltılabilir. Bu aşamada çekirdek uzman grubunu oluşturulmuş yüzyüze görüşem tekniği kullanılmıştır. Görüşülen uzmanların özellikleri araştırmaya uygun olarak seçilmiştir.

Çekirdek uzman grubu siber güvenlik teknolojisiyle ilgili bilgi sahibi olan, aynı zamanda Türkiye'de siber güvenlik teknolojisi ve sektörüne yön veren, büyük çaplı veya kritik alanlarda faaliyet gösteren kuruluşlarda yetkili sektör temsilcileri/siber güvenlik profesyonellerinden ve akademiden konuyla ilgili yüksek düzey uzmanlardan (7 siber güvenlik uzmanı, 2 sektör temsilcisi, 3 akademisyen) oluşturulmuştur. Bu grup, çalışmaya her aşamada ve gönüllü olarak zaman ayırmak ve katkıda bulunmak durumunda olacağından kendilerine önce bir brifing verilmiş ve bu konuda taahhütleri alınmıştır. Çekirdek uzman grubuyla birlikte görüşmeler sonucunda swot analiz oluşturulmuş ve delphi ifadeleri belirlenmiştir. Belirlenen delphi ifadeleri bulgular kısmında detaylandırılmıştır.

İkinci aşama olarak Bulanık Delphi sürecinde dilsel değişkenler kullanılarak ölçülecek değişkenler için değerlendirme kriterlerinin önemini belirlemek üzere davet edilen uzman sayısının K olduğu varsayılır. Uzmanlar ile yapılabilecek yöntemler arasında, bir seminer veya çalıştay yürütmek ve dahil olan bilimsel uzmanları davet etmek, her uzmanla yüz yüze görüşmek ve anket yapılan alanlarda belirlenen uzmanlar gibi e-posta yoluyla çevrimiçi yaymak gibi olabilir (Mohd Ridhuan Mohd Jamil, Saedah Siraj, Zaharah Hussin), Nurulrabihah Mat Noh, 2014). Araştırmada bu adımda her uzmanda yüz yüze görüşmek olarak belirlenmiştir. Uygun uzman sayısı konusunda 10 ila 15 kişi arasında iki farklı görüş vardır (Adler, M.& Ziglio, 1996), Jones ve Twiss (1978) toplam 10 ila 100 uzman önermiştir. Bu

çalışma için araştırmacılar, literatür taramasına dayanarak önceden belirlenen 87 uzmanı seçildi. Bir Bulanık Delphi paneli, belirli bir konu üzerinde görüş paylaşan uzmanlardan oluşan bir gruptur. Bu paylaşım, bir dizi yapılandırılmış araştırma süreci turu aracılığıyla fikir birliğine yol açar. Bu araştırmada, uzmanların hem politika yapıcılar, hem akademisyenler hem de kendi bakış açılarına dayalı olarak siber güvenlik konusunda paydaş yönetimi konusunda uzman görüşlere sahip oldukları görülmektedir. Bu çalışmanın uzmanları, siber güvenlik ve spor sektörü düşüldüğünde oynadıkları rol açısından heterojenliği sağlamak için özel bir amaç göz önünde bulundurularak özenle seçilmiştir. Böylece siber güvenlik uzay ortamı konusunda faaliyet gösteren kurumları temsil edecek uzmanlar seçilmiştir. Türkiye'deki tüm spor sektörü siber güvenlik uzay ortamlarından, yani Yüksek Öğrenim Sektörü, Kamu sektörü ve Özel sektörden uzmanların dahil edilmesine özen gösterildi.

Bu çalışmada kullanılan Fuzzy Delphi yönteminin hazırlanma ve uygulama süreçleri Şekil 2.1'de özetlenmiştir. Belton ve ark. (2019), en az 5 uzman kullanılmalı; 5 ile 20 arası yeterli olabilir, ancak mümkünse daha fazlasını kullanmak faydalıdır. Sonuçta bu çalışmaya çekirdek uzman grubu olarak 12 uzman katılmıştır. Spor sektöründe siber güvenlik üzerine uzmanlar, IT ve siber güvenlik üzerine uzun yıllar çalışmış ve sahada deneyimli siber güvenlik konusunda akademik çalışmalar yayınlamış ya da spor bilişim üzerine akademik yayını bulunan uzmanlarından oluşturulmuştur. Uzmanlara ilişkin detaylar bulgular ve analiz bölümünde yer verilmiş olup Çizelge 3.7'de gösterilmiştir. Çalışmada her bir uzmanla birebir görüşme yapılmış, spor sektöründeki bilişimden bahsedilmiş daha önceden yaşanan büyük kayıplara neden olaylar uzmanlara sunulmuştur. Uzmanlardan bunun nedenlerini raporlarda listelemeleri istenerek bir pilot risk değerlendirmesi yapılmıştır.



Şekil 2.1. Bulanık Delphi yönteminin süreçleri.

Verdikleri cevaplardan uzmanlardan için 25 adet sporda siber güvenlik nedeni belirlendi. Daha sonra uzmanlar bu siber güvenlik nedenlerini "Tamamen katılıyorum"dan "Tamamen Katılmıyorum"a doğru beşli Likert ölçeğinde derecelendirmeleri istenmiştir. Anket çevrimiçi olarak sunuldu ve uzmanlar birbirlerini etkilemediklerinden emin olmak için farklı fiziksel konumlarda bulundular. Uzmanlar araştırmaya gönüllü olarak katıldıkları için sıklıkla çevrimiçi anket kullanılmaktadır (Kınalı, 2022). Daha sonra, cevaplar Likert ölçeğinden bulanık bir ölçeğe dönüştürüldü. Formülasyon detayları aşağıdaki Fuzzy Delphi yöntemi adımlarında açıklanmıştır. Cheng ve Lin'e (2002) göre, her bir uzmanın ortalama ile değerlendirme verileri arasındaki mesafe eşik değer olan 0,2'den küçükse, tüm uzmanların fikir birliğine vardığı kabul edilir. Ek olarak, grup konsensüs yüzdesi %75'in üzerindeyse süreç 5. adıma geçebilir; aksi halde yeni bir anket turu gereklidir (Chu ve Hwang, 2008; Hammons, 1995). Uzmanların verdiği yanıtlara göre sporda siber güvenlik nedenleri uzmanlara geri sunuldu. Bir sonraki adımda bu nedenlerin ortadan kaldırılması veya nedenlerinin azaltılması konusunda uzman görüşleri alınmıştır. Son olarak, bulgular ve çözümler sunuldu.

Bulanık Delphi yöntemi adımları.

Adım 1: Likert ölçeklerini kullanarak çeşitli faktörlere göre değerlendirme kriterlerinin önemini belirlemek için K uzman davet edilir.

Adım 2: Likert ölçekli sayılar, Çizelge 2.1'de önerildiği gibi üçgen bulanık sayılara dönüştürülür.

Çizelge 2.1. Her bir kriter için Bulanık ölçek eşdeğerlerinin önem ağırlığı.

Likert Ölçeği	**Bulanık Ölçeği**		
5=Tamamen Katılıyorum	0,6	0,8	1
4= Katılıyorum	0,4	0,6	0,8
3= Kararsızım	0,2	0,4	0,6
2= Katılmıyorum	0	0,2	0,4
1= Tamamen Katılmıyorum	0	0	0,2

Bulanık numaralar r_i^k ;k uzmanının i riskine verdiği üçgen bulanık ortalamaları gösterir.

r_i^k=

$$\tilde{r}_i^k = \frac{1}{K}\left[\tilde{r}_i^1 + \tilde{r}_i^2 + \ldots + \tilde{r}_i^k\right](i = 1, \ldots, m)\text{and}(k = 1, \ldots, K) = (m_1, m_2, m_3)$$

Adım 3: Sporda siber güvenlik adına riskine dayalı olarak her bir risk faktörü için verilen cevapların üçgen bulanık ortalamaları (r_i) ve bulanık değerleri (r_i^k) arasındaki mesafeyi hesaplamak için vertex yöntemi kullanılır (C. T. Chen, 2000).

$\tilde{m}$ = (m1, m2, m3) and n = (n1, n2, n3)

Bu iki bulanık sayı arasındaki mesafe (d) şu şekilde ifade edilir:

$$d(\tilde{m}, \tilde{n}) = \sqrt{\frac{1}{3}\left[(m_1 - n_1)^2 + (m_2 - n_2)^2 + (m_3 - n_3)^2\right]}$$

Adım 4: Grup konsensüs yüzdesini hesaplamak için her bir uzmanın ortalama ve değerlendirme verileri arasındaki mesafe belirlenir.

Adım 5: Bulanık değerlendirmelerin eklenmesi şu şekilde ifade edilir:

$$\widetilde{A} = \begin{bmatrix} \widetilde{A_1} \\ \widetilde{A_2} \\ \dots \\ \widetilde{A_m} \end{bmatrix} (\widetilde{A} = \widetilde{r}_{i1} + \widetilde{r}_{i2} + \dots + \widetilde{r}_{i3})$$

$$i = 1, \dots, m$$

Adım 6: Durulaştırma gerçekleştirilir. Risklerin önem sırası aşağıdaki şekilde ifade edilerek belirlenir:

$$\widetilde{A}_i = \frac{1}{3}(a_{i1} + a_{i2} + a_{i3})$$

Her risk ai'nin önem sırası sayısal değerlere göre belirlenir.

Adım 7: Tüm uzman görüşlerinin değerlendirilmesi sonucunda ortaya çıkan sporda siber güvenlik risklerin önem sıralaması uzmanlara bildirilir ve risklerin azaltılması veya ortadan kaldırılması konusunda uzmanlara danışılır.

Ayrıca çekirdek uzman grupla birlikte SWOT çalışması yürütülmüştür, Türk Silahlı Kuvvetleri, hükümet, akademi ve siber güvenlik şirketlerinden 10 uzmanın katılımıyla her bir uzmanla yüz yüze görüşme ile SWOT analizler belirlenmiştir. SWOT analizinde, güçlü ve zayıf yönler Türkiye'nin içsel nitelikleri iken, fırsat ve tehditler siber güvenlik ekosistemini etkileyen dış etkenlerdir. Güçlü, zayıf yönler, fırsatlar ve tehditler araştırmacı tarafından hazırlanmış çekirdek çalışma grubuyla

birlikte birbirebir görüşmelerden elde edilen görüşlerdir çalıştay sırasında katılımcılara dağıtılmıştır (Çizelge 2.2'den Çizelge 2.5'e). Katılımcılardan ek ifadeler yazmaları ve hepsine öncelik vermeleri istenmiştir.

Çizelge 2.2. Türkiye'nin Güçlü Yönleri (Araştırmacı tarafından önceden yazılmış beyanlar).

Güçlü yönler	**Öncelik**
Genç ve girişimci insan gücü	
Uluslararası topluma entegre bir bilim ve teknoloji camiası	
SSM (Sanayi ve Teknoloji Bakanlığı), TÜBİTAK (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu) ve ilgili bakanlıklar gibi kurumlar, ortaya konan stratejileri hayata geçirmek için önemli yürütme organların varlığı	
Ülkemizin dünyanın en büyük 20 ekonomisi arasında olması	
Siber güvenlik alanına yönelik devlet desteklerinin varlığı	
Teknolojik Uluslararası arenaya açılmış sanayi	
Kişisel verileri, fikir ve eserleri koruma altına alan yasal altyapının varlığı (Fikir ve Sanat Eserleri Kanunu ve Kişisel Verilerin Korunması Kanunu vb.)	
İleri teknolojiye hakim olan ve bunu etkin bir şekilde kullanabilen genç nüfus	
Siber güvenliğe yönelik güçlü politik destek	
Millîlik duygusunun sahiplenilmesi	
Ucuz İş gücü	
Ek Güçlü yönler (Kendi düşünceniz)	

Çizelge 2.3. Türkiye'nin Zayıf Yönleri (Araştırmacı tarafından önceden yazılmış beyanlar).

Zayıf yönler	**Öncelik**
Sosyal Yetişmiş insan kaynağı eksikliği	
Eğitim ve öğretimdeki aksaklıklar	
Siber güvenliğin üzerine inşa edildiği bilişim teknolojilerinde (özellikle donanım açısından) yurt dışına bağımlılık	
Spor Organizator ve Kurumların, siber güvenlik açısından gerçek ihtiyaçlarının farkında olmaması	
Bilgi sistemleri ve siber güvenliğe yönelik millî ürün ve teknolojilerin azlığı	
Kamu, sanayi ve akademik camia arası iş birliğinin zayıf olması	
İş birliği kültürünün eksikliği	
Siber güvenlik alanında kurumsal yetkinliklerin (teşkilat, altyapı, personel, kaynak) yetersiz olması	
Çok sayıda firmanın az sayıdaki belirli siber güvenlik ürün ve hizmetlerine odaklanması spordaki alanı fark etmemesi	
Sporda siber güvenliğe yönelik verilerin eksikliği	
Spor sektöründe yetersiz mevzuat ve yasal çerçeve	
Ek Güçlü yönler (Kendi düşünceniz)	

Çizelge 2.4. Türkiye'nin Fırsat Yönleri (Araştırmacı tarafından önceden yazılmış beyanlar).

Fırsatlar	Öncelik
Siber tehditlerin artması ve daha karmaşık hâle gelmesi nedeniyle siber güvenliğe olan ihtiyacın artması	
Ülkemiz dâhil, dünyadaki çoğu ülkede siber güvenliğin, millî güvenliğin unsurları arasında kabul edilmesi	
Sosyal, teknolojik, ekonomik, çevresel ve politik faktörlerin doğurduğu siber güvenlik ihtiyaçları	
Siber güvenliğin doğası gereği, yerli ürünlere olan ihtiyaç	
Teknolojinin hayatın her alanına nüfuz etmesi ve kullanımının artması	
Kamu ve özel sektörün siber güvenlik alanına yatırım yapma istek ve iradesi	
Siber tehditlerin hızlı bir şekilde gelişmesi	
İç ve dış pazarın genişliği	
İnternet üzerinden verilen sayısal servislerin hayatın her alanına (sporda sağlık, pazarlama, bilgi paylaşımı vb.) nüfuz etmesi	
Siber güvenlik sistemlerinin kurumsal olarak tesis edilmesinde eksikliklerin olması	
Teknoparkların ve teknokentlerin gelişiyor olması	
Ek Güçlü yönler (Kendi düşünceniz)	

Çizelge 2.5. Türkiye'nin Tehdit Yönleri (Araştırmacı tarafından önceden yazılmış beyanlar).

Tehditler	Öncelik
Ar-Ge'ye olması gerekenden daha az yatırım yapılması	
Milli ürünlere olan güven eksikliği	
Global firmaların hükümette yaptığı lobiler	
Yasal Kamu ihale mevzuatı gereği, maliyetin kaliteden önce değerlendirilmesi	
Ekonomik Yabancı ürünlerin pazarın büyük kısmına hâkim olması	
Politik Gelişmiş siber güvenlik ürün ve teknolojilerinin satışına yönelik kısıtlamaların getirilmesi	
Teknolojik Bulut bilişime dayalı teknolojilerin yaygınlaşması ve bu alanda yabancı firmaların hâkimiyeti	
Kolay para kazanmaya hevesli bir kültürün yerleşmeye başlaması	
Beyin göçü	
Ülkedeki Ekonomik istikrarsızlık	
Metodolojik çalışmaya karşı direnç gösterilmesi ve bunun ulusal bir kültür özelliği olduğuna olan yanlış inanç	
Ek Güçlü yönler (Kendi düşünceniz)	

3. BULGULAR

3.1. SWOT Analiz Sonuçları

Katılımcılar, araştırmacı tarafından hazırlanan önceden yazılmış SWOT konularına öncelik verdiler ve ifadelerini eklemeleri teşvik edildi. Çalıştayın ardından konular, katılımcıların verdiği öncelik puanlarına göre araştırmacı tarafından sıralanmıştır. Sonuçlara göre, Türkiye'nin zayıf yönleri güçlü yönlerinden daha fazla, fırsatları ise tehditlerinden çok daha fazladır. Faktörlerin sayıları Çizelge 3.1'de gösterilmektedir. Ayrıca swot analiz sosyal, teknolojik, ekolojik, politik, ekonomik, hukuki ve etik alt faktörlerine bağlı olarak dağıtıldı.

Sosyal Faktörler: Bulunduğun stratejik konum gereği kültürel yapı iş ve işleyişte ki değişimi ön plana çıkarmaktadır.Nüfus artış hızı, eğitim seviyesi, yaşam biçimi, tüketici davranışları kapsar.

Teknolojik Faktörler: Teknolojinin kuruluşlara yansıtılması ayak uydurması önemli bir noktayı oluşturur İletişimdeki yenilikler, Sunucu ya da internet maliyetleri ve oluşabilecek değişiklikler,İnovasyonlar, Üretilen yeni teknolojiler vb.

Ekolojik Faktörler: iklim, hava koşulları, Küresel iklim değişikliği, Çevre dostu ürün ve uygulamalar Doğal afetler

Politik Faktörler: Hükümetin uyguladığı uygulayacağı güncel ve ilgili konuların inceleneceği başlıktır. Bunlardan bir kaçı vergiler, maliye politikaları, teşvikler, krediler, uluslararası ilişkiler, seçim ve sonuçlarıdır. Siyası olarak önceden tahmin edilemese de gündemi takip ederek öngörülerde bulunulabilir. Bu tip durumları politik faktör olarak değerlendirilir.

Ekonomik Faktörler: Ekonomik değişimler, kuruluşları bir fiil etkilemekte ve ekonomiye karşı belirli önlemler almak için duruş sergilenebilir.Ekonomik durumları, enflasyon oranları, vergi oranları, borsanın durumu, işçi maliyetleri gibi başlıkları kapsar.

Hukuki Faktörler: İş Kanunu, Ticaret Kanunu, Sağlık ve Güvenlik yasaları, Telif Hakkı ve Paten Yasaları, Yasalar Davalar gibi olayları kapsar.

Etik Faktörler: Etik, insanların bütün davranış ve eylemlerinin temelini araştırır. Kültürler, normlar, değerler, demografik yapı, ülkelerin standartları kapsar.

Çizelge 3.1. Spor sektöründe siber güvenlikte Türkiye'de SWOT Analizi.

	Güçlü Yönleri	**Zayıf Yönleri**	**Fırsatlar**	**Tehditler**	**G+F**	**Z+T**
Sosyal	7	8	9	8	16	16
Teknolojik	2	8	10	3	12	11
Ekolojik	0	1	1	3	1	4
Politik	4	1	5	4	9	5
Ekonomik	2	4	4	7	6	11
Hukuki	1	2	2	2	3	4
Etik	2	1	1	0	3	1
Toplam	18	25	32	27	50	53

3.1.1. Türkiye'nin Güçlü Yanları

Araştırmaya katılan uzmanlar yazılan mevcut 10 güçlü yöne 8 adet daha güçlü yön daha ekledi. Türkiye'nin spor sektöründe siber güvenlik açısından güçlü yönleri, uzmanlar tarafından belirlenen önem (öncelik) sırasına göre Çizelge 3.2'de verilmektedir. Bu sıralamaya aynı zamanda sosyal, teknolojik, ekolojik, politik, ekonomik, hukuki ve etik alt faktörlerine bağlı olarak dağıtıldı.

Çizelge 3.2. Spor sektöründe siber güvenlikte Türkiye'de Güçlü Yönleri.

No	Faktör	Güçlü Yönleri
1.	Politik	Siber güvenliğe yönelik güçlü politik destek
2.	Sosyal	İleri teknolojiye hakim olan ve bunu etkin bir şekilde kullanabilen genç nüfus
3.	Sosyal	Uluslararası topluma entegre bir bilim ve teknoloji camia sahip olması
4.	Politik	Siber güvenlik alanına yönelik devlet desteklerinin varlığı
5.	Teknolojik	Teknolojik Uluslararası arenaya açılmış sanayi
6.	Etik	Millîlik duygusunun sahiplenilmesi
7.	Sosyal	Genç ve girişimci insan gücü
8.	Politik	Ortaya konan stratejileri gerçekleştirebilecek kurumların varlığı (SSM, TÜBİTAK, Bakanlıklar vb.)
9.	Politik	Türkiye, siber güvenlik konusunda uluslararası işbirliklerine önem vermesi
10.	Teknolojik	Saldırılara hızlı bir şekilde müdahale etme ve zararları en aza indirme konusunda güçlü bir kapasiteye sahip olması
11.	Sosyal	Nüfusun büyük bir bölümünün siber güvenliğin önemi hakkında farkındalık düzeylerinin yüksek olması
12.	Ekonomik	Spor sektöründe gelirin fazla olması
13.	Sosyal	Siber güvenlik alanında yetişmiş insan kaynağının güçlü olması
14.	Etik	Spora olan ilginin fazla olması
15.	Sosyal	Bilinçlenmeyi teşvik etmek ve önleyici tedbirler almak için çaba gösteri
16.	Sosyal	Birçok üniversite ve eğitim kurumu, siber güvenlik alanında kaliteli eğitim programlar
17.	Hukuki	Kişisel verileri, fikir ve eserleri koruma altına alan yasal altyapının varlığı (Fikir ve Sanat Eserleri Kanunu ve Kişisel Verilerin Korunması Kanunu vb.)
18.	Ekonomik	Ülkemizin dünyanın en büyük 20 ekonomisi arasında olması

3.1.2. Türkiye'nin Zayıf Yanları

Araştırmaya katılan uzmanlar yazılan mevcut 10 zayıf yöne 15 adet daha zayıf yan daha ekledi. Türkiye'nin spor sektöründe siber güvenlik açısından zayıf yanları, uzmanlar tarafından belirlenen önem (öncelik) sırasına göre Çizelge 3.3'de verilmektedir. Bu sıralamaya aynı zamanda sosyal, teknolojik, ekolojik, politik, ekonomik, hukuki ve etik alt faktörlerine bağlı olarak dağıtıldı.

Çizelge 3.3. Spor sektöründe siber güvenlikte Türkiye'de Zayıf Yönleri.

No	Faktör	Zayıf Yönleri
1.	Ekonomik	Mili Ekonomik sorunlar (Artan Enflasyon, satın alma gücü azalması, işsizlik, TL değer kaybı)
2.	Sosyal	Yetişmiş insan kaynağı eksikliği
3.	Teknolojik	Siber güvenliğin üzerine inşa edildiği bilişim teknolojilerinde (özellikle donanım açısından) yurt dışına bağımlılık
4.	Sosyal	Spor organizasyonları, sporcular ve diğer ilgili taraflar arasında güvenlik bilinci ve eğitim eksikliği olması
5.	Teknolojik	Araştırmaya yönelik verilerin eksikliği
6.	Sosyal	İş birliği kültürünün eksikliği
7.	Sosyal	Kurumların, siber güvenlik açısından gerçek ihtiyaçlarının farkında olmaması
8.	Teknolojik	Bilgi sistemleri ve siber güvenliğe yönelik millî ürün ve teknolojilerin azlığı
9.	Ekonomik	Sınırlı Kaynaklar: Sporda siber güvenlik için ayrılan bütçe ve kaynaklar sınırlı olması
10.	Ekonomik	Yabancı ürünler pazarın çoğuna hakim olması
11.	Teknolojik	Spor organizasyonları kullandığı dijital altyapılar, güvenlik açıklarına sahip olması
12.	Sosyal	Sporcular ve diğer ilgili taraflar arasında bilinçsiz kullanıcı davranışları
13.	Sosyal	Farkındalık ve Eğitim Eksikliği
14.	Sosyal	Sporcular, antrenörler, yöneticiler ve diğer ilgili taraflar siber güvenlik konusunda yeterli eğitim almamış olması
15.	Teknolojik	Hızlı Teknolojik Değişim
16.	Teknolojik	Sporcuların kullandığı dijital altyapılar, güvenlik açıklarına sahip olması
17.	Politik	Çok sayıda firmanın az sayıdaki belirli siber güvenlik ürün ve hizmetlerine odaklanması
18.	Ekonomik	Tedarik zinciri güvenliği; Spor kuruluşları, genellikle çeşitli tedarikçi ve iş ortaklarıyla çalışır, tedarik zinciri üzerindeki zayıflıklar
19.	Teknolojik	Spor alanında hızlı teknolojik değişim
20.	Etik	Fikir ve eserlerin korunmasına ilişkin ilkelere uygun kişisel eksiklikler
21.	Ekolojik	Türkiye, coğrafi konumu, jeopolitik faktörler ve diğer nedenlerle siber casusluk veya devlet destekli saldırılara maruz kalması
22.	Sosyal	Insan kaynagina yatirimin gerekenden az olmasi
23.	Teknolojik	Spor alanında ki dijitalleşmenin yeterli olmaması.
24.	Hukuki	Uluslararası alanda sporda siber tehditlere ve siber olaylara karşı yetersiz mevzuat
25.	Hukuki	Yasal mekanizmaların işleyişindeki sorunlar

3.1.3. Türkiye'nin Fırsatları

Araştırmaya katılan uzmanlar yazılan mevcut 10 adet fırsatlara 22 adet daha ekledi. Türkiye'nin spor sektöründe siber güvenlik açısından fırsatları, uzmanlar tarafından belirlenen önem (öncelik) sırasına göre Çizelge 3.4'de verilmektedir. Bu sıralamaya aynı zamanda sosyal, teknolojik, ekolojik, politik, ekonomik, hukuki ve etik alt faktörlerine bağlı olarak dağıtıldı.

Çizelge 3.4. Spor sektöründe siber güvenlikte Türkiye'de Fırsatları.

No	Faktör	Fırsatlar
1.	Sosyal	Teknolojinin hayatın her alanına nüfuz etmesi ve kullanımının artması
2.	Sosyal	Sosyal, teknolojik, ekonomik, çevresel ve politik faktörlerin doğurduğu siber güvenlik ihtiyaçları
3.	Teknolojik	Siber güvenliğin doğası gereği, yerli ürünlere olan ihtiyaç
4.	Politik	Ülkemiz dâhil, dünyadaki çoğu ülkede siber güvenliğin, millî güvenliğin unsurları arasında kabul edilmesi
5.	Sosyal	Genç Nufüs
6.	Ekonomik	Kamu ve özel sektörün siber güvenlik alanına yatırım yapma istek ve iradesi
7.	Sosyal	İnternet üzerinden verilen sayısal servislerin hayatın her alanına (sağlık, alışveriş, bilgi paylaşımı vb.) nüfuz etmesi
8.	Ekonomik	İç ve dış pazarın genişliği
9.	Teknolojik	Siber güvenlik sistemlerinin kurumsal olarak tesis edilmesinde eksikliklerin olması
10.	Teknolojik	Siber tehditlerin hızlı bir şekilde gelişmesi
11.	Sosyal	Türkiye, spor endüstrisinde hızla büyüyen ve gelişen bir ülke olması
12.	Teknolojik	Türkiye'deki spor alanında yenilikçi teknoloji uygulamaları hızla yayılıyor olması
13.	Sosyal	Türkiye'deki spor alanında siber güvenlik bilincinin artması ve eğitim ihtiyacının karşılanması gerektiği
14.	Politik	Türkiye'deki spor alanında siber güvenlikle ilgili işbirliği ve ortaklık olanakları bulunması
15.	Politik	Hükümeti, siber güvenlik konusunda önemli adımlar atmaktası
16.	Ekonomik	Spor organizasyonlarına ve kurumlarına daha fazla yatırım yapılmasını
17.	Teknolojik	Düşük siber güvenlik ürün geliştirme yetenekleri
18.	Politik	Ülkelerin karşı karşıya kaldığı siber olaylar ve suçlar
19.	Teknolojik	Akıllı spor nesnelerin yaygın kullanımı (top, spor eşyaları vb.)
20.	Teknolojik	AI, makine öğrenimi ve derin öğrenme yöntemleri
21.	Teknolojik	Veri gizliliğini korumak için teknolojilerin önemi
22.	Teknolojik	Küresel internet erişiminin yaygın kullanımı
23.	Sosyal	Gizliliğe artan vurgu
24.	Sosyal	Siber güvenlik için eğitim ihtiyaçları
25.	Politik	Başta Müslüman ülkeler olmak üzere bölge ülkelerine rol model olarak ürün ve hizmet ihraç etme imkanı
26.	Ekolojik	Rusya ve coğrafi yakınlık arasındaki işbirliğine erişim
27.	Hukuki	Siber suçlarla ilgili ulusal ve uluslararası mevzuatın oluşturulması ve yaygınlaştırılması
28.	Hukuki	Kişisel verileri işleyen sistemlerin güvenlik kriterlerine uygunluğu konusunda uluslarda (örn. ABD) ve ülke topluluklarında (örn. Avrupa Birliği) yeni düzenlemeler
29.	Sosyal	Ülkelerin karşı karşıya kaldığı siber olaylar ve suçlar
30.	Teknolojik	Siber güvenlik hizmetlerini uzaktan sağlama yeteneği
31.	Ekonomik	Türkiye'de ve dünyada artan satın alma gücü
32.	Etik	Siber saldırıdan çok siber güvenliğe milli vurgu

3.1.4. Türkiye’nin Tehditleri

Araştırmaya katılan uzmanlar yazılan mevcut 10 gülü yöne 8 adet daha güçlü yön daha ekledi. Türkiye'nin spor sektöründe siber güvenlik açısından güçlü yönleri, uzmanlar tarafından belirlenen önem (öncelik) sırasına göre Çizelge 3.2'de verilmektedir. Bu sıralamaya aynı zamanda sosyal, teknolojik, ekolojik, politik, ekonomik, hukuki ve etik alt faktörlerine bağlı olarak dağıtıldı.

Çizelge 3.5. Spor sektöründe siber güvenlikte Türkiye’de Tehditleri.

No	Faktör	Tehditler
1.	Ekonomik	Ekonomik enflasyon ve darboğaz oluşması
2.	Politik	Ar-Ge’ye olması gerekenden daha az yatırım yapılması
3.	Ekonomik	Kamu ihale mevzuatı gereği, maliyetin kaliteden önce değerlendirilmesi
4.	Politik	Yetenekli mühendislerin beyin göçü
5.	Politik	Ar-Ge’ye olması gerekenden daha az yatırım yapılması
6.	Teknolojik	Bulut bilişime dayalı teknolojilerin yaygınlaşması ve bu alanda yabancı firmaların hâkimiyeti
7.	Hukuki	Gelişmiş siber güvenlik ürün ve teknolojilerinin satışına yönelik kısıtlamaların getirilmesi
8.	Ekonomik	Uluslararası rekabet
9.	Politik	Acil tedarik talepleri nedeniyle sistemlerin millî olarak geliştirilmesine yeterli önemin verilememesi
10.	Ekonomik	Yabancı ürünlerin pazarın büyük kısmına hâkim olması
11.	Ekonomik	Şirketler için ekonomik desteğin olmaması
12.	Ekolojik	Kripto para madenciliğinin tüketimi ve çevreye olumsuz etkisi, spor sektöründe yasal olmayan bahis ve pazarlamada kullanması
13.	Teknolojik	
14.	Ekonomik	Yabancı şirketlerin Türkiye'deki yatırımları ve ortaklıkları
15.	Ekolojik	Türkiye'nin içinde bulunduğu jeopolitik ortam
16.	Ekolojik	Türkeye’nin çevre ülkelerdeki istikrarsızlık potansiyeline sahip olması
17.	Ekonomik	Uluslararası Yarışma
18.	Sosyal	Kolay para kazanmaya hevesli bir kültürü yerleştirmeye başlayın
19.	Sosyal	Spor organizasyonları, sporcular ve taraftarlar tarafından oluşturulan büyük miktarda veri bulunması
20.	Teknolojik	Spor organizasyonlarına yönelik Dağıtık Hizmet Reddi (DDoS) saldırıları,
21.	Sosyal	Spor alanındaki siber casusluk, rakip takımların veya organizasyonların antrenman taktiklerini, transfer planlarını
22.	Sosyal	Kimlik avı saldırıları, sahte e-postalar, web siteleri veya iletişimle saldırılar
23.	Sosyal	Spor organizasyonları veya kulüpler, siber güvenlik önlemlerini yeterince uygulamamış olması
24.	Sosyal	Sporcular, kulüpler ve organizasyonlar, sosyal medyada geniş bir varlık gösterirmesi
25.	Hukuki	Hukuki cezaların az ve yetersiz olması
26.	Sosyal	Türkiye'deki spor sektörünün yaygın olması ve kitlesel yönlendirme gücünün fazla olması
27.	Sosyal	Yerli ürünlere olan güven eksikliği

3.2. Bulanık Delphi Analiz Sonuçları

Tasarlanan Delphi sürecinin nasıl uygulanacağı ve hangi araçların kullanılacağı ile ilgili çeşitli alternatifler üretilmiştir. Araştırmada sporda siber güvenlik teknolojisinin kendisinden faydalanılmasına özen gösterilmiştir. 2. fazda anketlerin elektronik mesaj ile bilgi verilmiştir ve geliştirilecek web tabanlı bir anket yazılımı ve tamamlayıcı olarak elektronik mesaj ile yapılması kararlaştırılmıştır. Analizlerde ise MS Excel ve MS Access veri tabanı/formları kullanılması, istatistiksel gelişmiş analizlerin ise SPSS programı ile yapılması öngörülmüştür. İstatistik araçlarından, katılımcı sayısına uygun şekilde istatistiksel anlamlılığının sınanmasında güvenilirlik ve geçerlilik için, tıp eğitimcileri, ölçme ve değerlendirmelerinin doğruluğunu artırmak için güvenilir ve geçerli testler ve soru formları oluşturmaya çalışırlar. Geçerlilik ve güvenilirlik, bir ölçme aracının değerlendirilmesinde iki temel unsurdur. Araçlar, geleneksel bilgi, beceri veya tutum testleri, klinik simülasyonlar veya anket anketleri olabilir. Araçlar kavramları, psikomotor becerileri veya duygusal değerleri ölçebilir. Geçerlilik, bir aracın ölçmeyi amaçladığı şeyi ne ölçüde ölçtüğü ile ilgilidir. Güvenilirlik, bir aracın tutarlı bir şekilde ölçme yeteneği ile ilgilidir (Tavakol, 2008).

Unutulmamalıdır ki, bir aracın güvenilirliği, geçerliliği ile yakından ilişkilidir. Bir araç güvenilir olmadıkça geçerli olamaz. Ancak, bir aracın güvenilirliği geçerliliğine bağlı değildir (Cohen, 2012). Bir aracın güvenilirliğini objektif olarak ölçmek mümkündür ve bu yazıda en yaygın kullanılan objektif güvenilirlik ölçüsü olan Cronbach'dır. Bu çalışmada delphi ifadelerin güvenilirliği ve geçerliği için Cronbach testi uygunlanmıştır. Bu oranın 0,70 ve üzerinde olması değişkenlerin güvenilir bir şekilde ölçüldüğünü göstermektedir (Ray, 2004). Aşağıdaki tablolardan da görülebileceği gibi faktörlerin Cronbach Alpha değerleri 0,70'den büyük olduğu için Delphi anketinde değişkenlerin güvenilir bir şekilde ölçüldüğü söylenebilir.

Çizelge 3.6. Delphi Anketinin Güvenilirliği.

Güvenirlik İstatisliği		
Cronbach's Alpha	Standart Maddelere Dayalı Cronbach Alfası	Madde Sayısı
0,979	0,980	25

Sporda siber güvenlik noktası konusunda yapılan ön araştırmalardan, siber güvenlik alanındaki teknoloji geliştiricilerin çok farklı kesimlerden, çok farklı geçmiş ve ilgi alanlarından, tam anlamıyla dağıtık bir demografik yapıda olduğu görülmüştür. Bu konuda, çalışmanın hedeflerine ve delphi esaslarına en uygun yöntemi belirleyebilmek için literatür araştırılması yapılmış ayrıca Çekirdek Uzman Grubu oluşturulmuş. Sonuç olarak optimum katılımcı sayısının her araştırma için farklı olabileceği belirlenmiştir. Türkiye'de meslek örgütlerine kayıtlı siber güvenlik çalışanı sayısı ile siber güvenlik işinde profesyonel olarak uğraşan kişi sayısı arasında çok ciddi farklılıklar bulunduğundan, toplam kütle belirlenememiştir.

Bağlam itibari ile disiplinler arası iş birliğini gerektiren bu çalışmada, sosyal bilimler içerisinde yer alan spor bilimleri ile bu alandan tamamen farklı olan siber güvenlik çalışan uzmanları belirlemek ve onlar ile iletişime geçmek ilk aşamada sorun teşkil etmiştir. Snow'un (2005) "İki Kültür" kitabında ifade ettiği doğa bilimleri ve insan bilimleri alanlarında çalışanlarının birbirlerine engel olan iletişim kopukluğu, kültür ve anlayış farklılığı bu aşamada derinden hissedilmiştir. Bunun yanı sıra spor alanının kendi içerisindeki dinamikleri ve siber güvenlik alanın daha sonra ayrılarak farklı bir alan ekolü oluşturması, tarım ve gıda alanındaki tartışmanın araştırmaya yansımalarını farklılaştırmıştır. Bir dereceye kadar bu tür problemler; araştırma ekibinin kişisel temasları, mevcut sosyal ağlar, temasa geçilen uzmanların yönlendirmesi ile çapraz alanlardan uzmanların bulunması, davet mektubu gönderilmeden önce yapılan profesyonel telefon görüşmeleri sürecin iyileştirilmesinde ve problemlerin çözümünde önemli rol oynamıştır. Bu grup, konuyla ilgili yüksek düzeyde uzmanlığı bulunan (siber güvenlik veya spor sektöründe deneyim ve unvan olarak sektörde belli bir düzeyin üzerinde görev yapan

kişiler veya en az Doktora öğretim üyesi unvanındaki akademisyenler) kişilerle 12 kişilik bir grup oluşturulmuştur.12 kişilik çekirdek uzman demografi özellikleri Çizelge 3.7'da gösterilmiştir.

Çizelge 3.7. Çekirdek Uzman Grubunun demografisi.

No	Çalışma Alanı	Kurum	Mesleki unvan	Kıdem (Yıl)
1.Uzman	Siber Güvenlik/IT	Özel Sektör	Kıdemli Siber Güvenlik Uzmanı	6-10 Yıl
2.Uzman	Spor	Akademi	Prof. Dr.	21 yıl ve üzeri
3. Uzman	Siber Güvenlik/IT	Kamu	Kıdemli Siber Güvenlik Uzmanı	6-10 Yıl
4. Uzman	Siber Güvenlik/IT	Kamu	Kıdemli Siber Güvenlik Uzmanı	21 yıl ve üzeri
5. Uzman	Siber Güvenlik/IT	Kamu	Kıdemli Siber Güvenlik Uzmanı	6-10 Yıl
6. Uzman	Spor	Akademi	Dr. Öğr.Üyesi.	6-10 Yıl
7. Uzman	Siber Güvenlik/IT	Akademi	Prof. Dr.	11-15 Yıl
8. Uzman	Siber Güvenlik/IT	Kamu	Kıdemli Netwrok Güvenlik Uzmanı	11-15 Yıl
9. Uzman	Spor	Kamu	Genel Sekreter	6-10 Yıl
10. Uzman	Spor	Özel Sektör	Yönetici	6-10 Yıl
11. Uzman	Siber Güvenlik/IT	Kamu	Kıdemli IT ve Sanallaştırma Yöneticisi	21 yıl ve üzeri
12. Uzman	Siber Güvenlik/IT	Özel Sektör	Kıdemli Sızma Testi Uzmanı	21 yıl ve üzeri

Bu araştırmada çekirdek araştırma grubuyla birebir görüşme üzerinden daha sonra delphi ifadeleri oluşturulmuştur. Uzmanlara spor sektöründe yaşanan siber güvenlik saldırıları üzerine yaşanmış olaylardan pilot örnekler verilmiştir. Bu görüşmelerde Delfi çalışması üzerine odaklanılmıştır. Katılımcılar Delfi ifadesini incelemiş ve gerekli değişiklik önerilerini dile getirmiştir. Katılımcılara, daha önce önemine göre listelenmiş olan teknolojilerin listesi dağıtılmış ve bunlar arasından ilave kabiliyet (yani Delfi ifadesi) yazmaları talep edilmiştir. Yapılan çekirdek uzmanı görüşmeler sonunda 35 adet delphi ifadesi belirlenmiş daha sonra bu 25 adet delphi ifadesi kararlaştırılmıştır. Delphi ifadeleri Çizelge 3.8 gösterilmektedir.

Çizelge 3.8. Deplhi ifadeleri.

No	Delphi İfadesi
D-1	Dünyadaki bütün ülkeleri kapsayacak şekilde, spor alanında siber tehditlere yönelik istihbarat (tehdit yöntemleri, araçları, kaynakları, hedefleri vb.) toplamaya, analiz etmeye ve karar desteği vermeye yönelik altyapı, yazılım, donanım, teknik ve teknolojiler geliştirilmelidir.
D-2	Ülkemizdeki spor kulüpleri üst düzey siber saldırılara karşı teknik ve teknolojik sistemler geliştirmek ve güçlü bir siber savunma teknolojileri kurmalıdır.
D-3	Bir spor organizasyonu sırasında siber saldırılara karşı koruma sağlayabilecek ve her türlü elektronik devrenin (çipler, mikro-elektronik devreler vb.) güvenlik testlerini yapabilecek teknolojik seviyeye ulaşılmalıdır.
D-4	İnternet üzerinden her türlü canlı olarak yayınlanan spor karşılaşması sırasında kullanılan İletişim ağından gelecek trafiği analiz edip (deep packet inspection vb.) bunlara karşı otomatik önlemler alınmasını sağlayan sistemler (Firewall, Web Application Firewall, Intrusion Prevention System vb.) kullanılmalıdır.
D-5	Sporcu verileri bulut bilişimde saklanması tercih edilmektedir. Bulut bilişim güvenliğine yönelik teknik (encryption, access brokers vb.) gelişmiş teknolojiler başlanmalıdır.
D-6	Spor kulüplerinin veya spor müsabakalarının kullandığı teknolojik cihazların (bilgisayar, ağ cihazları, cep telefonları, kameralar vb. her türlü cihaz ve sistemler) siber güvenliğini sağlayacak teknolojiler geliştirilmesine önem verilmelidir.
D-7	Spor tesisleri ve stadyumlarda koltuk biletleri online bilet satışlarında güçlü bir siber savunma teknolojileri kurulmalıdır
D-8	Dijital (e-spor) turnuvalar ve spor organizasyonlarında güçlü bir siber savunma teknolojileri kurulmalıdır.
D-9	Sporda büyük veriler ve veri madenciliği yöntemleri kullanılmasında güçlü bir siber savunma teknolojileri kurulmalıdır.
D-10	Olimpik spor branşlarında kullanılan yazılım sistemlere güçlü bir siber savunma teknolojileri kurulmalıdır.
D-11	Birçok spor alanında nano teknoloji ile desteklenmiş olan ürünlerin kullanıldığı görülmektedir. Nano teknolojiden yararlanarak kullanılan ürünlerde (sporcuların antreman ve fiziki yeterlilik verilerinden bunların değiştirilmesi manupüle edilmesi karşı) siber güvenliği önem verilmelidir.
D-12	Spor işletmelerinde veya organizasyonlarında kullanılan sanal işletim sistemlerinin güvenliğini en üst düzeye çıkaracak teknik ve teknolojiler (virtualization security, hypervisor security) geliştirilmelidir.
D-13	Siber güvenlik araç ve mekanizmalarının (Ör.: firewall, security gateway, guard, router vb.) spor kulüp ve organizasyonlarda yazılım modülleriyle karşılandığı yazılım tanımlı güvenlik (software defined security) modül ve sistemleri geliştirerek ve bu ürünlerde spor pazarında kullanılmasına büyük önem verilmelidir.
D-14	Spor endüstrisinde büyük veri (big data) ve diğer veritabanı (database) sistemlerinin ve içindeki verilerin güvenliğini sağlamaya yönelik teknik (audit, encyption vb.), teknoloji, yazılım ve donanımlar geliştirilerek uluslararası boyutta önem kazanmaya başlanmalıdır.
D-15	Dünyadaki spor sektöründe üst düzey siber saldırı ve savunma kabiliyetine sahip ülkelerle (Ör.: ABD, Rusya, Çin) rekabet edecek düzeyde siber saldırı teknik, teknoloji ve sistemleri geliştirilmiş ve bu düzeyde güçlü bir siber savunmalar kurulmalıdır.
D-16	Uluslararası spor organizasyonlarında siber olaylara hızlı, etkin ve gerektiğinde otomatik bir şekilde karşılık verecek (incident response, automated response ve model-driven cyber defense dâhil) ve bu olayları yönetebilecek (incident management) yeni nesil teknoloji ve sistemler geliştirilmiş ve kullanılmaya başlanılmalıdır
D-17	Uluslararası spor organizasyonu düzenleyen kuruluş veya ülkeler siber saldırıları modelleyebilen, gerek test için gerekse gerçek anlamda otomatik saldırı kabiliyetine sahip, kendi kendine öğrenebilen (makine öğrenmesi, derin öğrenme vb. teknikleriyle) akıllı siber saldırı sistemleri geliştirilmelidir.
D-18	Spor dünyasında kulüp ve organizasyonlarda sistemlere (hakem/görevli) giriş ve yetki vermede kullanılan kullanıcı/nesne kimlik denetimini ve veri güvenliğini en üst seviyede sağlamak amacıyla blok zinciri (blockchain) ve yeni nesil uygulama ve teknikler geliştirilerek kullanıma açılmalıdır.
D-19	Spor Pazarlamasında Veri Madenciliğine yönelik tedbirleri alınarak yasal yayıncılık aktif hale getirilmelidir.
D-20	Spor sektöründe sponsor veya yasal bahis sitelerinde sporcuların verilerin önemler artırmalı Veri sızıntısı önleme (Data Loss Prevention -DLP) teknik ve sistemler kullanılarak veri sızması engellenmelidir.
D-21	Ulusal veya uluslar arası spor organizasyonları gerçekleştirmeden önce mutlaka sızma testleri yapılmalıdır.

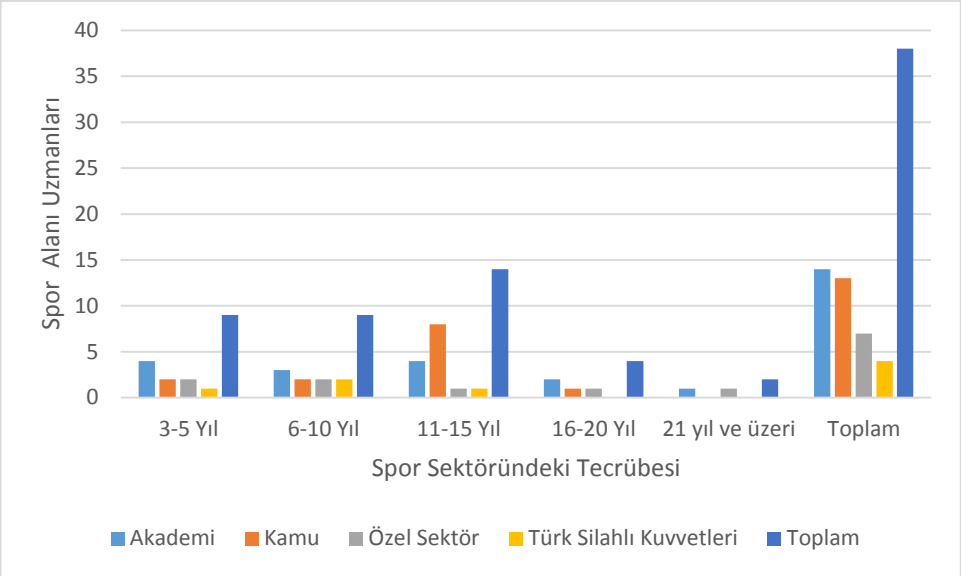
Çizelge 3.8. Devam. Deplhi ifadeleri.

D-22	Spor müsabakası anında ulusal yayın yapan kuruluşlarda insansız uçak sistemleri(drone vs.), yayın yapabilecek kamera sistemleri, yayın yapan skorboardlar ve siber güvenliğini sağlayabilecek, siber güvenlik protokol ve mimarileri geliştirilmeli ve kullanılmaya başlanmalıdır.
D-23	Sosyal medyada sporcu ve spor müsabakaları hakkında sosyal düzeni bozabilecek her türlü çevrimiçi yayını ve yanlış bilgilerin karşı tedbirler alınmalı bu konuda istihbarat yapabilecek yazılımlar geliştirilmelidir.
D-24	Spor sektöründeki unsurların arşivlenmesi, sahte ürünlerin engellenmesi, organizasyonların güncel veri kayıtlarının güvenilir bir şekilde tutulması gereklidir
D-25	Sporcularda giyilebilir nano teknolojilere (saat, gözlük, elbise, yapay organlar, muhtelif sensörler vb.) yönelik siber güvenlik teknoloji ve sistemleri geliştirilmeli ve giyilebilir nano teknolojik ürünlerin müsabaka anında rakip karşısında avantaj oluşturabilecek durumlara karşı tedbirler alınıp siber savunma yöntemleri kullanılmaya başlanmalıdır.

Çalışmanın 2. Fazında çekirdek uzman grubundan ayrı olarak çok sayıda uzmana delphi ifedesi sunulmuştur. Katılımcıların sektörlere göre eğitim ve deneyim düzeyleri Çizelge 3.9'dan Çizelge 3.10'a kadar verilmektedir. Spor alanında uzmanlarının çoğunun (14 kişi) akademi kökenli olduğu, uzmanlarının çoğunun 11 ile 15 yıl arası tecrübeye sahip olduğu (14 kişi) görülmektedir. Spor alanında 5 yıldan fazla deneyim ve katılımcıların çoğu (23 kişi) Master of Science (MS) derecesine sahiptir.

Çizelge 3.9. Delphi Turuna Katılan Spor Alanı Uzmanlarının Sektörlere Göre Tecrübesi.

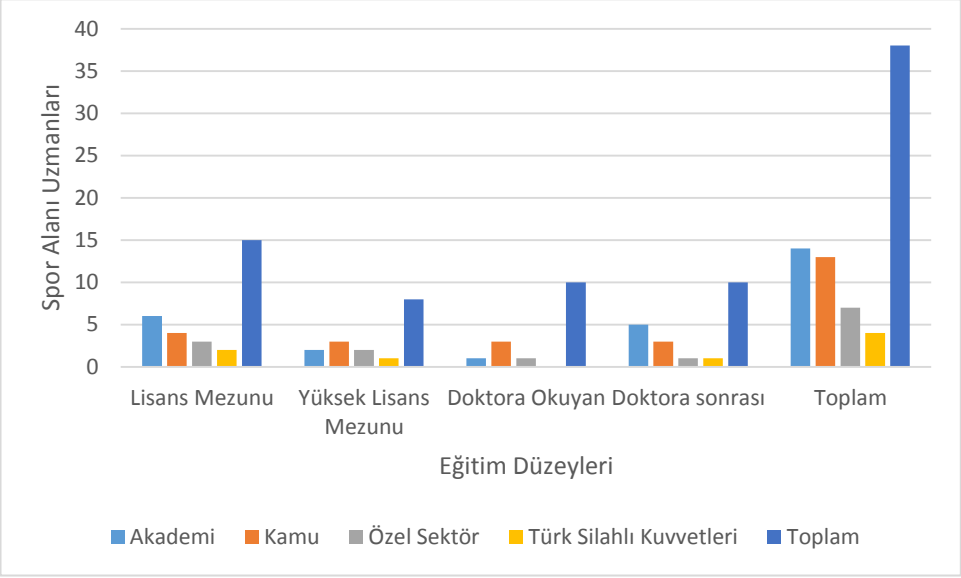
Sektör	3-5 Yıl	6-10 Yıl	11-15 Yıl	16-20 Yıl	21 yıl ve üzeri	Toplam
Akademi	4	3	4	2	1	14
Kamu	2	2	8	1	0	13
Özel Sektör	2	2	1	1	1	7
Türk Silahlı Kuvvetleri	1	2	1	0	0	4
Toplam	9	9	14	4	2	38



Şekil 3.1. Delphi Turuna Katılan Spor Alanı Uzmanlarının Sektörlere Göre Tecrübesi.

Çizelge 3.10. Delphi Turuna Katılan Spor Alanı Uzmanlarının Eğitim Düzeyleri.

Sektör	Lisans Mezunu	Yüksek Lisans Mezunu	Doktora Okuyan	Doktora sonrası	Toplam
Akademi	6	2	1	5	14
Kamu	4	3	3	3	13
Özel Sektör	3	2	1	1	7
Türk Silahlı Kuvvetleri	2	1	0	1	4
Toplam	15	8	5	10	38

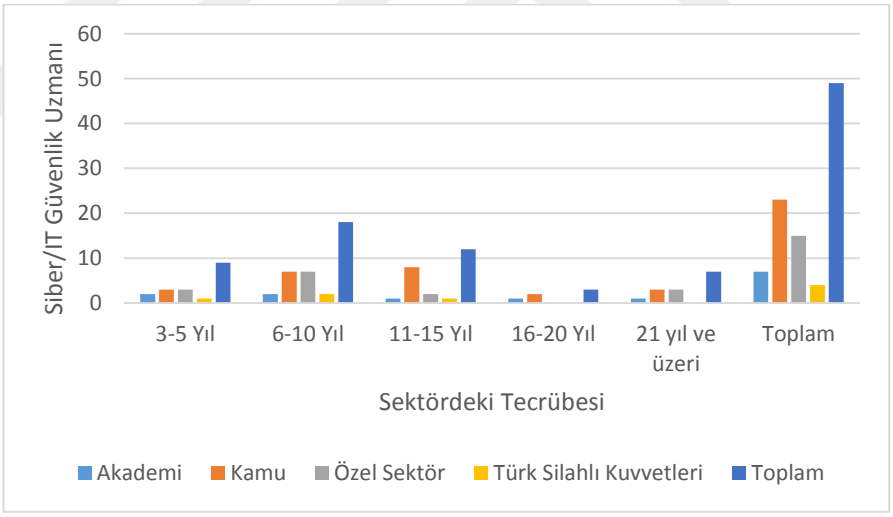


Şekil 3.2. Delphi Turuna Katılan Spor Alanı Uzmanlarının Eğitim Düzeyleri.

Çalışmanın 2. Fazına katılan siber güvenlik sektöründe tecrübeli uzmanlarına göre eğitim ve deneyim düzeyleri Çizelge 3.11'den Çizelge 3.12'ye kadar verilmektedir. Spor alanında uzmanlarının çoğunun (14 kişi) akademi kökenli olduğu, uzmanlarının çoğunun 11 ile 15 yıl arası tecrübeye sahip olduğu (14 kişi) görülmektedir. Spor alanında 5 yıldan fazla deneyim ve katılımcıların çoğu (23 kişi) Master of Science (MS) derecesine sahiptir.

Çizelge 3.9. Delphi Turuna Katılan Siber/IT Güvenlik Alanı Uzmanlarının Sektörlere Göre Tecrübesi.

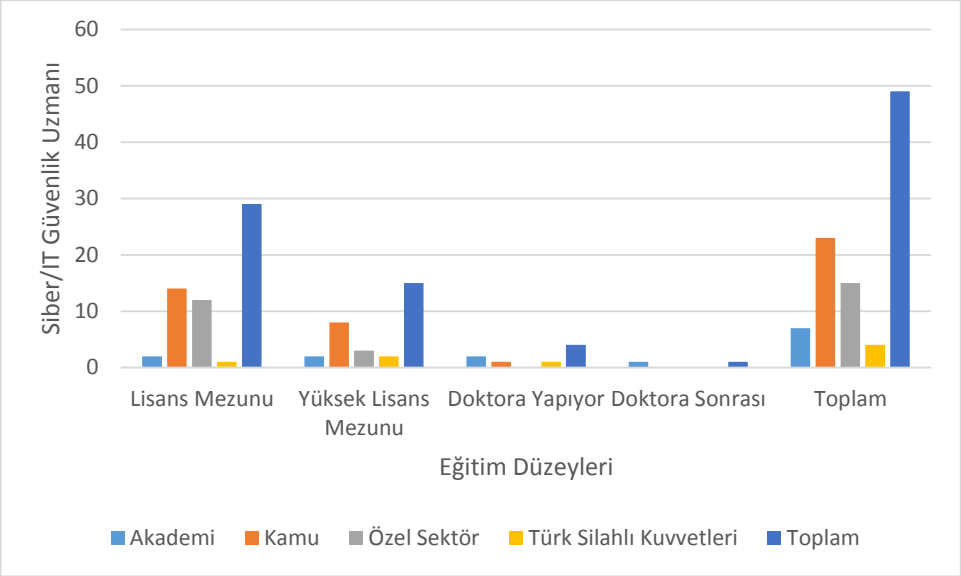
Sektör	3-5 Yıl	6-10 Yıl	11-15 Yıl	16-20 Yıl	21 yıl ve üzeri	Toplam
Akademi	2	2	1	2	1	7
Kamu	3	7	8	1	3	23
Özel Sektör	3	7	2	0	3	15
Türk Silahlı Kuvvetleri	1	2	1	0	0	4
Toplam	9	18	12	3	7	49



Şekil 3.3. Delphi Turuna Katılan Siber/IT Güvenlik Alanı Uzmanlarının Sektörlere Göre Tecrübesi.

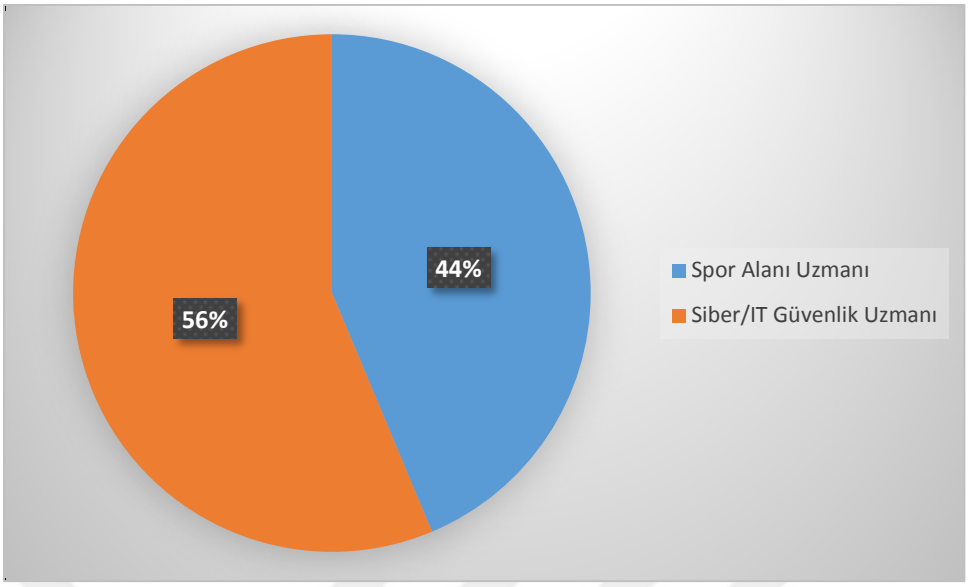
Çizelge 3.10. Delphi Turuna Katılan Siber/IT Güvenlik Alanı Uzmanlarının Eğitim Düzeyleri.

Sektör	Lisans Mezunu	Yüksek Lisans Mezunu	Doktora Okuyan	Doktora sonrası	Toplam
Akademi	2	2	2	1	7
Kamu	14	8	1	0	23
Özel Sektör	12	3	0	0	15
Türk Silahlı Kuvvetleri	1	2	1	0	4
Toplam	29	15	4	1	49



Şekil 3.4. Delphi Turuna Katılan Siber/IT Güvenlik Alanı Uzmanlarının Eğitim Düzeyleri.

Araştırmada bulanık delphinin 2. Aşamasında siber/IT güvenlik ve spor alanlarında toplamda 87 uzman katılmıştır. Bunun büyük bir çoğunluğunu siber güvenlik uzmanları oluşturmuştur. Uzmanların alanlarına göre dağılımını Şekil 3.5'de gösterilmiştir.



Şekil 3.5. Bulanık Delphi Turuna Katılan Uzmanlarının Alanlarına Göre Dağılımı.

Bu kısımda çalışmamıza sektöründe sunduğumuz sporda siber güvenlik nedenlerinden biri olan "Spor sektöründe sponsor veya yasal bahis sitelerinde sporcuların verilerin önemler artırmalı Veri sızıntısı önleme (Data Loss Prevention - DLP) teknik ve sistemler kullanılarak veri sızması engellenmelidir." başlıklı 20. maddesine ilişkin cevaplar Çizelge 3.12'te verilmiştir. İlk olarak, Likert ölçeği değerleri Çizelge 2.1 verildiği gibi üçgen bulanık değerlere dönüştürülmüştür.

Daha sonra Denklem (1) kullanılarak 20. madde için 87 uzmanın üçgensel bulanık ortalamaları şu şekilde hesaplanmıştır:

Çizelge 3.11. Madde 20'in örnek hesaplaması.

	Likert Ölçeği		Bulanık Ölçeği		mesafe (d)
1. Uzman	5	0,6	0,8	1	0,1
2. Uzman	5	0,6	0,8	1	0,1
3. Uzman	4	0,4	0,6	0,8	0,2
4. Uzman	5	0,6	0,8	1	0,1
5. Uzman	5	0,6	0,8	1	0,1
6. Uzman	5	0,6	0,8	1	0,1
7. Uzman	5	0,6	0,8	1	0,1
8. Uzman	5	0,6	0,8	1	0,1
9. Uzman	5	0,6	0,8	1	0,1
10. Uzman	5	0,6	0,8	1	0,1
11. Uzman	5	0,6	0,8	1	0,1
12. Uzman	5	0,6	0,8	1	0,1
13. Uzman	4	0,4	0,6	0,8	0,2
14. Uzman	5	0,6	0,8	1	0,1
15. Uzman	3	0,2	0,4	0,6	0,3
16. Uzman	3	0,2	0,4	0,6	0,3
17. Uzman	5	0,6	0,8	1	0,1
18. Uzman	5	0,6	0,8	1	0,1
19. Uzman	4	0,4	0,6	0,8	0,2
20. Uzman	3	0,2	0,4	0,6	0,3
21. Uzman	5	0,6	0,8	1	0,1
22. Uzman	4	0,4	0,6	0,8	0,2
23.Uzman	5	0,6	0,8	1	0,1
24.Uzman	5	0,6	0,8	1	0,1
25.Uzman	4	0,4	0,6	0,8	0,2
26.Uzman	1	0	0	0,2	0,5
27.Uzman	5	0,6	0,8	1	0,1
28.Uzman	2	0	0,2	0,4	0,4
29.Uzman	4	0,4	0,6	0,8	0,2
30.Uzman	5	0,6	0,8	1	0,1
31.Uzman	4	0,4	0,6	0,8	0,2
32.Uzman	4	0,4	0,6	0,8	0,2
33.Uzman	4	0,4	0,6	0,8	0,2
34.Uzman	5	0,6	0,8	1	0,1
35.Uzman	5	0,6	0,8	1	0,1
36.Uzman	5	0,6	0,8	1	0,1
37.Uzman	3	0,6	0,8	1	0,3
38. Uzman	5	0,6	0,8	1	0,1
39. Uzman	5	0,6	0,8	1	0,1
40. Uzman	5	0,6	0,8	1	0,1
41 Uzman	5	0,6	0,8	1	0,1
42. Uzman	5	0,6	0,8	1	0,1
43. Uzman	5	0,6	0,8	1	0,1
44. Uzman	4	0,4	0,6	0,8	0,2
45. Uzman	5	0,6	0,8	1	0,1
46. Uzman	4	0,4	0,6	0,8	0,2
47. Uzman	5	0,6	0,8	1	0,1
48. Uzman	4	0,4	0,6	0,8	0,2
49. Uzman	5	0,6	0,8	1	0,1
50. Uzman	5	0,6	0,8	1	0,1
51. Uzman	5	0,6	0,8	1	0,1
52. Uzman	5	0,6	0,8	1	0,1
53. Uzman	4	0,4	0,6	0,8	0,2

Çizelge 3.12. Devam. Madde 20'in örnek hesaplaması.

54. Uzman	5	0,6	0,8	1	0,1
55. Uzman	5	0,6	0,8	1	0,1
56. Uzman	5	0,6	0,8	1	0,1
57. Uzman	5	0,6	0,8	1	0,1
58. Uzman	5	0,6	0,8	1	0,1
59. Uzman	5	0,6	0,8	1	0,1
60.Uzman	5	0,6	0,8	1	0,1
61.Uzman	5	0,6	0,8	1	0,1
62.Uzman	5	0,6	0,8	1	0,1
63.Uzman	4	0,4	0,6	0,8	0,2
64.Uzman	5	0,6	0,8	1	0,1
65.Uzman	3	0,2	0,4	0,6	0,3
66.Uzman	3	0,2	0,4	0,6	0,3
67.Uzman	5	0,6	0,8	1	0,1
68.Uzman	5	0,6	0,8	1	0,1
69.Uzman	4	0,4	0,6	0,8	0,2
70.Uzman	3	0,2	0,4	0,6	0,3
71.Uzman	5	0,6	0,8	1	0,1
72.Uzman	4	0,4	0,6	0,8	0,2
73.Uzman	5	0,6	0,8	1	0,1
74.Uzman	5	0,6	0,8	1	0,1
75.Uzman	4	0,4	0,6	0,8	0,2
76.Uzman	1	0	0	0,2	0,5
77.Uzman	5	0,6	0,8	1	0,1
78.Uzman	2	0	0,2	0,4	0,4
79.Uzman	4	0,4	0,6	0,8	0,2
80.Uzman	5	0,6	0,8	1	0,1
81.Uzman	4	0,4	0,6	0,8	0,2
82.Uzman	4	0,4	0,6	0,8	0,2
83.Uzman	4	0,4	0,6	0,8	0,2
84.Uzman	5	0,6	0,8	1	0,1
85.Uzman	4	0,4	0,6	0,8	0,2
86.Uzman	5	0,6	0,8	1	0,1
87.Uzman	5	0,6	0,8	1	0,1
Ortalama (Denklem 1)	4.46	0,494	0,689	0,889	
Defuzzification (Denklem 4)			0,690		

Bu sayı, 20. öğenin öncelik değerini temsil eder. Değer ne kadar yüksek olursa, öncelik de o kadar yüksek olur. 0,690 değeri ile 20. madde en önemlisidir.

Analiz sonucunda, üçgen bulanık ortalamalar r_{25} ile her bir uzmanın değerlendirme verileri arasındaki mesafe r_{25}^{87} = 0,184 < 0,2 olması nedeniyle tüm uzmanların fikir birliği oluşturduğu belirlenmiştir.

Ayrıca, grup anlaşması yüzdesi %87 olup, bu oran %75'in üzerindedir. Yani ilk turda uzmanlar arasında uzlaşma sağlanmış ve yeni bir tura gerek kalmamıştır.

Çizelge 3.13. Spor sektöründe siber güvenlik Türkiye'de Delphi İfadesi Puanları.

Delphi No	Ortalama	**Derecesi**
D-20	4,46	1.
D-4	4,46	2.
D-21	4,42	3.
D-9	4,38	4.
D-10	4,34	5.
D-24	4,34	6.
D-3	4,32	7.
D-6	4,32	8.
D-15	4,32	9.
D-22	4,32	10.
D-5	4,3	11.
D-8	4,3	12.
D-11	4,28	13.
D-12	4,28	14.
D-1	4,26	15.
D-14	4,26	16.
D-17	4,26	17.
D-18	4,26	18.
D-7	4,24	19.
D-25	4,24	20.
D-19	4,2	21.
D-13	4,18	22.
D-2	4,16	23.
D-16	4,16	24.
D-23	4,14	25.

Çizelge 3.14. Spor sektöründe siber güvenlik Türkiye'de Delphi İfadesi İstatisliği.

Delphi No	Ortalama	SS	**Variance**	**Range**	**Minimum**	**Maximum**
D-1	4,26	1,065	1,135	4	1	5
D-2	4,16	1,113	1,239	4	1	5
D-3	4,32	1,096	1,202	4	1	5
D-4	4,46	1,073	1,151	4	1	5
D-5	4,3	0,974	0,949	4	1	5
D-6	4,32	0,999	0,998	4	1	5
D-7	4,24	1,098	1,207	4	1	5
D-8	4,3	1,111	1,235	4	1	5
D-9	4,38	0,753	0,567	3	2	5
D-10	4,34	0,939	0,882	4	1	5
D-11	4,28	0,948	0,900	4	1	5
D-12	4,28	1,011	1,022	4	1	5
D-13	4,18	0,896	0,804	3	2	5
D-14	4,26	1,006	1,013	4	1	5
D-15	4,32	0,999	0,998	4	1	5
D-16	4,16	1,037	1,076	4	1	5
D-17	4,26	0,965	0,931	4	1	5
D-18	4,26	1,046	1,094	4	1	5
D-19	4,2	1,01	1,020	4	1	5
D-20	4,46	0,885	0,784	4	1	5
D-21	4,42	0,883	0,779	4	1	5
D-22	4,32	0,935	0,875	4	1	5
D-23	4,14	1,107	1,225	4	1	5
D-24	4,34	0,848	0,719	3	2	5
D-25	4,24	1,041	1,084	4	1	5

Ek olarak, soru başına konsensüs şu şekilde formüle edilmiştir: En yüksek puan alan seçeneğin yüzdesi, toplam puanların ortalama yüzdesinden büyükse ve en yüksek puan alan seçenek ile en yüksek puan alan ikinci seçeneğin toplamı %50'den büyükse, uzlaşma sağlanmıştır. En çok puan alan iki seçeneğin toplam yüzdesi, "orta" %50 - %70, "yüksek" %70 - %90 ve "çok yüksek" %90 - %100 arasında olmak üzere fikir birliği derecesini gösterir. Sonuçlar, 25 delphi ifadesi için 15 ifadenin uzlaşı derecesinin "çok yüksek", 10 ifadenin "yüksek" derece olduğunu göstermektedir (bkz. Çizelge 3.15).

Çizelge 3.15. Spor sektöründe siber güvenlik Türkiye'de Delphi İfadesi Uzmanların Tercihindeki Fikir Birliği Derecesi.

Delphi No	En Çok Puan Alan Seçeneğin %	En Çok Puan Alan İkinci Seçeneğin %	**En Çok Puan Alınan İki Seçeneğin Toplam %**	**Uzlaşma**
D-1	68.15	18,80	86,95	Yüksek
D-2	64,80	21,60	86,40	Yüksek
D-3	73,92	14,80	88,72	Yüksek
D-4	80,64	16,56	97,20	Çok Yüksek
D-5	62,91	27,9	90,81	Çok Yüksek
D-6	66,99	24,5	91,49	Çok Yüksek
D-7	70,8	13,23	84,03	Yüksek
D-8	72,23	18,6	90,83	Çok Yüksek
D-9	59,28	32,94	92,22	Çok Yüksek
D-10	64,4	27,6	92,00	Çok Yüksek
D-11	60,84	29,94	90,78	Çok Yüksek
D-12	63,18	28,05	91,23	Çok Yüksek
D-13	50,19	40,11	90,30	Çok Yüksek
D-14	61,1	30,8	91,90	Çok Yüksek
D-15	66,99	22,2	89,19	Yüksek
D-16	60,0	28,8	88,80	Yüksek
D-17	58,75	33,84	92,59	Çok Yüksek
D-18	63,45	28,2	91,65	Çok Yüksek
D-19	59,5	26,6	86,10	Yüksek
D-20	71,68	21,48	93,16	Çok Yüksek
D-21	67,8	25,4	93,14	Çok Yüksek
D-22	64,68	24,05	88,73	Yüksek
D-23	60,5	27,02	87,52	Yüksek
D-24	62,1	27,4	89,70	Yüksek
D-25	61,36	30,24	91,60	Çok Yüksek

4. TARTIŞMA

Bu tez çalışması kapsamında yapılan sporda siber güvenlik teknolojisi öngörüsü uygulaması sonucunda aşağıdaki sonuçlara ulaşılmıştır:

Sporcuların ve spor organizasyonlarının karşı karşıya olduğu siber güvenlik sorunları, sporcuların mahremiyetine ve hayatlarının güvenliğine yönelik büyük riskler oluşturma potansiyeline sahiptir ve bu organizasyonların kazançlarının yanı sıra profesyonel spor kurumlarına halkın güvenini de etkileyebilir.

Çalışmanın ilk kısmında uzmanlar tarafından belirtilen "Spor sektöründe sponsor veya yasal bahis sitelerinde sporcuların verilerin önemler artırmalı Veri sızıntısı önleme (Data Loss Prevention -DLP) teknik ve sistemler kullanılarak veri sızması engellenmelidir." görüşü ikinci turda öngörü yönteminde en yüksek puanı alıp ortak görüş haline gelmiştir. Bu da gösteriyor ki spor alanında veri sızıntısına karşı önlemlerin artırılması gerektiğidir. Veri sızıntıları çeşitli şekilde yer alabilir. Bunlar kullanılan yazılım kısmına ve bilişim alt yapısına göre değişebilir. Spordaki büyük kurum, kulüp ve şirketlerin ürettiği kurumsal verileri kurumların ürettiği ve işlediği verilerdir. Bu verilerin bilinçli/kasti ya da bilinçsiz şekilde değişik yöntemlerle kurum dışına çıkarılabilir. Sporda büyük veri sızıntılarına rastlanabiliyor günümüzde yakın zamanda yaşanan örneklerden biride Türkiye'nin önemli spor kulüplerden biri olan Trabzonspor, sunucularının uğradığı siber saldırı sonucunda bazı bilgilerin ele geçirilmesinden dolayı Kişisel Verileri Koruma Kurumuna (KVKK) veri ihlaliyle ilgili bildirimde bulundu. Bu tür durumlar kulüplere zora sokmakta ayrıca büyük maddi kayıplara neden olmaktadır.

Bulgularda bahsedilen uzmanlarında yüksek görüşte belirtiği "Dünyadaki bütün ülkeleri kapsayacak şekilde, spor alanında siber tehditlere yönelik istihbarat (tehdit yöntemleri, araçları, kaynakları, hedefleri vb.) toplamaya, analiz etmeye ve karar desteği vermeye yönelik altyapı, yazılım, donanım, teknik ve teknolojiler geliştirilmelidir." Maddesinde bahsedilen spor endüstiriyi gelişmek ve geniş bir

kitleye hitap etmektedir. Bu yüzden araştırmada gösteriyor ki siber tehditlere yönelik çalışmaların sadece savunma sanayisinde değil aynı zamanda spor alanında kurumsal firmalarda da kullanılması gerektiğidir. Bu tür savunma sistemlerini kullanan spor organizasyonu kurum veya kuruluşlar güvenilebilir bir alt yapı oluşturduğu için taraftarlarından ve kamuoyundan saygınlık kazanacaktır.

Giyilebilir cihazlar her zamankinden daha yaygın hale geldikçe ve büyük veriler sporcuların başarısı için giderek daha hayati hale geldikçe, güvenlik açıkları insanların temel mahremiyetine yönelik bir tehdit oluşturmaktadır.Bu konuların farkında olmak ve insanları siber güvenlik tehditleriyle mücadelede bir araya getirmek her zamankinden daha önemli hale gelmiştir. Çalışmada spor ve bilişim uzmanların ortak görüşünde "Sporcularda giyilebilir nano teknolojilere (saat, gözlük, elbise, yapay organlar, muhtelif sensörler vb.) yönelik siber güvenlik teknoloji ve sistemleri geliştirilmeli ve giyilebilir nano teknolojik ürünlerin müsabaka anında rakip karşısında avantaj oluşturabilecek durumlara karşı tedbirler alınıp siber savunma yöntemleri kullanılmaya başlanmalıdır" maddesi çok yüksek oranda uzmanların ortak görüşü haline gelmiştir. Buda gösteriyor ki sporcuların giydiği nano teknolojiler hem denetlenmeli hem de bilgi yaymaması konusunda bağlantıları da kontrol edilip başka saldırgan kullanıcıların ellerine geçmemelidir.

Spor giderek daha fazla teknoloji kullanmaya devam edecek olması aslında önemli ve güzel gelişmelerden biridir ancak, güvenlik ve performans açısından rekabeti ilerletmeye devam edecek. Ancak, bu teknolojileri veya bireylerin mahremiyetini hafife almamalıyız ve gelecekteki kullanımlarında tutarlılık ve en iyi uygulamalar için çaba göstermeliyiz.

Spor organizasyonları, ofis işlevlerini ve giderek artan bir şekilde sahalardaki güvenlik sistemlerini yönetmek için BT ve teknolojiye güvenmektedir. Bu araştırmada detaylandırıldığı üzere, siber saldırıların çok çeşitli etkileri olabilir; multi-milyon sterlinlik dolandırıcılıktan hassas kişisel verilerin kaybına kadar sonuçları olabilir.

Türkiye'nin sporda siber güvenlikteki önemi, diğer ülkelerde olduğu gibi oldukça yüksektir. Türkiye'nin sporda siber güvenlikteki önemine dair bazı noktalar:

Spor Organizasyonları: Türkiye, birçok ulusal ve uluslararası spor organizasyonuna ev sahipliği yapmaktadır. Bu organizasyonlar, büyük bir kitleye hitap eden etkinliklerdir ve siber saldırılara karşı hassas bir konumdadır. Spor organizasyonlarının altyapılarının, web sitelerinin ve diğer dijital varlıklarının güvenliği büyük önem taşır.

Sporcuların Veri Güvenliği: Türk sporcuları, performans analizi, sağlık takibi ve diğer kişisel verileri içeren dijital platformları kullanmaktadır. Bu verilerin güvenliği, sporcuların gizliliğini ve performanslarını korumak için kritik bir faktördür.

Lisanslı Yayıncılar ve Medya Kuruluşları: Spor etkinliklerinin yayın haklarına sahip lisanslı yayıncılar ve medya kuruluşları, siber saldırılara karşı önemli bir hedef olabilir. Bu kuruluşlar, yayın hizmetlerinin kesintisiz ve güvenli bir şekilde sunulmasını sağlamak zorundadır.

Taraftar ve İnteraktif Platformlar: Spor organizasyonları, taraftarlarına yönelik interaktif platformlar ve dijital deneyimler sunmaktadır. Bu platformlar, taraftarların kişisel verilerini ve finansal bilgilerini içermektedir. Dolayısıyla, siber güvenlik önlemleri, taraftarların güvenliğini ve gizliliğini sağlamak için önemlidir.

Tüm bu faktörler göz önüne alındığında, Türkiye'nin sporda siber güvenliğe yatırım yapması ve gerekli önlemleri alması büyük önem taşımaktadır. Bu sayede, spor organizasyonları, sporcular ve taraftarlar güvende olacak ve dijital ortamda sorunsuz bir deneyim yaşayabilecektir.

Jenkins ve Evens 2020 yılında spordaki verilerin büyümesinin siber güvenlik etkisi sistem entegrasyonu, verilerin kullanılabilirliğini ve teknolojilerin

güvenilirliğini sağlamaya odaklanma eğilimindedir, ancak verilerin gizliliğine (mahremiyetine) ve bütünlüğüne yönelik riskler getirebilceğine değinmiştir. Potansiyel risklerin tanınması, gözden geçirme ve değerlendirmeyi gerektiğini, verilerin çoğu, hayranlara açık bir şekilde bilgi sağlamak için toplanıp, bu nedenle gizliliğe yönelik tehditler daha az risk oluşturur. En büyük risk, özel bir performans testi gibi oyuncuların mahremiyetini ihlal etmek veya rekabet avantajı elde etmek için teknolojiyi kullanmak olduğu belirtmiştir. Aslında temas ettiği özelliği ile çalışmamıza paralellik göstermektedir. Çalışmamızda sporcu verileri bulut bilişimde saklanması tercih edilmektedir. Bulut bilişim güvenliğine yönelik teknik (encryption, access brokers vb.) gelişmiş teknolojiler başlanması gerektiğini ayrıca sporda büyük veriler ve veri madenciliği yöntemleri kullanılmasında güçlü bir siber savunma teknolojileri kurulmalısı konuları katılan uzmanların ortak görüşüdür.

Andjelic ve ark. (2022) yapmış olduğu "Cybersecurity Risk with Wearable Technology in Sports: Why Should We Care?" çalışmasında, giyilebilir spor sistemleri üzerindeki güvenlik endişesi devam etmekte olduğunu ve araştırma ve geliştirme etkili güvenlik algoritmaları geliştirilmrsi gerektiğini vurguluyor. Bilişim ve spor pazarın katlanarak büyümesiyle birlikte, spor dünyasında yüksek düzeyde olumlu etkiye izin verebilecek güvenli giyilebilir teknolojilerin araştırılması ve geliştirilmesi için daha fazla yatırım yapılması gerekiğin, bununla birlikte, spor endüstrisindeki liderler temkinli olmazsa ve siber güvenliğin temel ilke ve uygulamalarını takip etmezlerse, yeterince güvenli olmayan ürünler kullanan sporculardan yararlanan bilgisayar korsanları ile gelecek zor geçeceğini araştırmada belirtiyor. Siber güvenlik, uzun vadeli başarı için bir ürün veya hizmet geliştirmenin ayrılmaz bir parçası olduğunu, eğer insanlar sporda giyilebilir teknolojinin gelişmesini istiyorsa, liderlerin siber güvenliğin en iyi ilkelerini ve uygulamalarını uyguladıklarını ummuş olmalarını ki bu daha fazla araştırmaya ihtiyaç gerektiğini belirtiyor. Belirli kurallar ve düzenlemeler çerçevesinde spor alanında güvenlik ve mahremiyet düzeyini artırmak için siber güvenlik konusundaki öneriler ve iyileştirmeler dikkate alınaması gerektiği konusunda çalışmamıza paralellik göstermektedir.

Oconner ve arkadaşlarının 2023 yılında yapmış olduğu “Compete to Learn: Toward Cybersecurity as a Sport” isimli makalesinde nitelikli siber güvenlik profesyonellerinin iş gücü açığını desteklemek için, siber güvenliği öğretmek için oyunlaştırılmış pedagojik yaklaşımlar son yirmi yılda katlanarak arttığını, aynı dönemde, e-spor multi-milyar dolarlık bir endüstri haline geldiğini ve bu konuda üniversite kampüslerinde temel bir unsur haline geldiğini belirtmiştir. Bu çalışmada, e-sporları ve oyunlaştırılmış siber güvenlik yaklaşımlarını ilk ABD Siber Oyunlar Ekibine entegre etme fırsatını araştırıldığı çalışmada, görev süresi boyunca siber güvenlik ekiplerinin işe alınması, değerlendirilmesi ve eğitilmesi hakkında e-spor yaklamışı kullanılmasında birçok ders çok yönde pozitif gelişme yaşandığı belirtilmiştir. Yaklaşımlarının, materyallerin ve öğrendiğinilen dersleri, amatör siber güvenlik ekiplerinin gelecekteki rekabet için sahaya çıkarılmasına bir model teşkil etmesi için belilirtildi. Aslında konu olarak spor bakış rekabet gücünün siber güvenlik yönelik pozitif etkisi görülmüş çalışmada bu aynı zamanda e-spor konusunda veya spor kulüplerinde aranan güvenlik personelleri belirlenirken kullanılabilir.

Çiftçi 2019 siber güvenlik öngörüsü 2019 çalışmasında; Çalışma sonuçlarına göre, siber güvenlik teknolojileri, eğitimi, ürün ve hizmetleri konusunda ve araştırma ve geliştirmeye yatırım yapma konusunda ülkemizin kat etmesi gereken uzun bir mesafe olduğu görülmektedir. Çalışma kapsamında tanımlanan vizyona erişmek için, belirlenen işlem maddelerinin kararlı bir şekilde gerçekleştirilmesi ve senaryolarda yer alan yol haritalarındaki kabiliyet ve teknolojilere yönelik çalışma ve yatırımların gerçekleştirilmesi gerektiği, ayrıca, siber güvenliğe yönelik teknoloji öngörüsü çalışmalarının düzenli olarak tekrar edilmesi ve yapılan çalışmaların sonuçlarının değerlendirilerek gerekli düzeltme ve geliştirmelerin yapılması hayati önem taşımakta olduğu belirtilmiş olup çalışmamıza paralellik göstermektedir.

5. SONUÇ VE ÖNERİLER

Çalışma sonucunda sporda siber güvenlik anlamında aşağıda belirtilen tedbirlerin daha sıkı bir şekilde alınması önemlidir:

-Bilinçlendirme ve Eğitim: Spor organizasyonları, sporcular ve diğer ilgili taraflar için siber güvenlik konusunda farkındalık ve eğitim programları düzenlemelidir. Bu programlar, temel güvenlik uygulamaları, güçlü şifre kullanımı, phishing saldırılarından korunma, güvenli dosya paylaşımı gibi konuları kapsamalıdır.

-Güçlü Şifre Politikaları: Sporcular, antrenörler, yöneticiler ve diğer ilgili kişiler için güçlü şifre politikaları benimsenmeli ve uygulanmalıdır. Şifreler düzenli olarak güncellenmeli, karmaşık olmalı ve çok faktörlü kimlik doğrulama gibi ek güvenlik önlemleri kullanılmalıdır.

-Veri Güvenliği ve Şifreleme: Sporcuların kişisel verileri, performans verileri ve sağlık bilgileri gibi hassas bilgiler, güvenli bir şekilde saklanmalı ve iletilmelidir. Veri şifreleme teknolojileri kullanılmalı ve erişim kontrolleri sıkı bir şekilde uygulanmalıdır.

-Ağ Güvenliği: Spor organizasyonlarının ve sporcuların kullandığı ağ altyapıları, güvenlik duvarları, ağ izleme ve tehdit tespit sistemleri gibi güvenlik önlemleriyle korunmalıdır. Ağlara yetkisiz erişim girişimleri izlenmeli ve engellenmelidir.

-Yazılım Güncellemeleri: Spor organizasyonları ve sporcular tarafından kullanılan yazılımların güvenlik güncellemeleri düzenli olarak yapılmalıdır. Bu, bilinen güvenlik açıklarının kapatılmasını ve potansiyel saldırı vektörlerinin azaltılmasını sağlar.

-Saldırı Önleme ve İzleme: Siber saldırıları tespit etmek ve önlemek için güvenlik olaylarına tepki verebilecek bir olay yönetimi sistemi kurulmalıdır. Saldırı girişimleri izlenmeli, tehditler analiz edilmeli ve hızlı yanıt önlemleri alınmalıdır.

-Dış Kaynaklı Güvenlik Denetimi: Spor organizasyonları, siber güvenlik uzmanları veya dış kaynaklı güvenlik hizmet sağlayıcılarıyla işbirliği yaparak düzenli olarak güvenlik denetimleri gerçekleştirmelidir. Bu, mevcut güvenlik zayıflıklarını tespit etmek ve düzeltici önlemler almak için önemlidir.

Bu tedbirler, sporda siber güvenliği güçlendirmeye yönelik genel yaklaşımlardır. Her spor organizasyonu veya sporcu, kendi özel gereksinimlerine ve risk profilimize uygun tedbirleri almalı ve sürekli olarak güncellemelidir. Ayrıca, teknolojik gelişmeleri takip etmek, yeni tehditlere karşı bilinçli olmak ve güvenlik önlemlerini sürekli olarak güncellemek de önemlidir.

Çalışmada spor ve siber güvenlik uzmanlarının nitel araştırma sonucunda elde edilen her bir delphi ifadesi tekrardan bir uzmanlar tarafında değerlendirilen nicel öngörü yöntemine göre her bir ifade yüksek veya çok yüksek düzeyde ortak görüş olarak belirlenmiştir. Her bir ifade aslında bu çalışmanın sonucunu yansıtır. Politikaları belirlerken yol gösterici niteliğindedir.

Sporun siber güvenliğin önemini belirten çalışmamızda, sporun bilişimde kullanımı konusunun yanında bilgi güvenliğine yönelik konu ile ilgili akademik araştırmalar artırılabilir.

Öngörü yöntemleri düşüldüğünde çalışmaya etki edebilir trend analizi veya senaryo yöntemleri gibi öngörü yöntemi kullanılarak çalışma genişletebileceği ve ilerleyen araştırmalarda farklı bilişimle ilgili uzman grupları ile bir araya gelip ile arasındaki ilişkiler araştırılabilir

ÖZET

Sporda Siber Güvenliğin Önemi

Spor, ülkeleri birleştiren en büyük organizasyon faaliyetleri bütünüdür. Ancak bu organizasyonların başarılı ve etkili olmasında temel olarak seyirci ve sporcuların güvenliği ön plana çıkmaktadır. Ülkelerin sağladığı güvenlik ölçüsünde değerlendirilen faaliyet raporu güvenliğin ne derece etkin rol oynadığını göstermektedir. Gündemiz hayatıda en önemli noktalarından biride, spor organizasyonları, alanların veya ofis işlevlerinin giderek artan bir şekilde mekânlardaki güvenlik sistemlerini yönetmek için bilgi teknolojilerine güveniyor olmasıdır. Bilgi teknolojilerin etkisinde gerçekleşen siber saldırıların çok çeşitli etkileri olabilir; multi-milyon pound dolandırıcılıktan hassas kişisel verilerin kaybına kadar. Siber güvenlik, kişisel verileri veri tabanlarında tutan kulüplerinden, büyük uluslararası spor etkinliklerine ev sahipliği yapanlara ve bunlara katılan ulusal kuruluşlara kadar spor organizasyonları ve spor alanlarında çalışan kuruluşlar için giderek artan bir önem kazanmaktadır. Bu konuda herhangi bir zafiyet veya saldırı, bilgi teknolojileri veya teknolojiye erişimin kaybedilmesi, spor organizasyonları üzerinde veri ihlallerine, dolandırıcılık amaçlı fon kaybına ve spor alanında etkinlik veya sunumunun aksamasına neden olan önemli bir etkiye sahip olabilir. Spor sektöründe siber güvenliğin iyileştirilmesi kritik öneme sahiptir. Araştırmanın sonucunda spor alanında siber güvenliğin önemini araştırmak, ülkemizin içinde bulunduğu özel ve stratejik durumundan dolayı daha sonra düzenlenecek yarış organizasyonların güvenliğinde önemli bir rol oynamak ve bu organizasyonlarda güvenlik önlemlerine kaynak oluşturmak, spor alanında bilişim konusunda güvenlikle ilgili riskler neler, tehditler neler, bu konuda oluşturulması gereken politika ve stratejiler neler ve spor bilimlerinde yeni olan bu alana literatür açısından katkıda bulunmayı amaçlamaktadır.

Anahtar Sözcükler: Bilgi teknolojileri, riskler, spor bilimleri, siber güvenlik, tehdit

SUMMARY

The Importance of Cyber Security in Sports

Sport is the largest organizational activity that unites countries.However, the safety of the spectators and athletes comes to the fore as the basis for the success and effectiveness of these organizations.The annual report, which is evaluated in terms of the security provided by the countries, shows how effectively security plays a role.One of the most important aspects in our day-to-day life is that sports organizations, spaces or office functions are increasingly relying on information technologies to manage security systems in spaces.Cyber attacks under the influence of information technologies can have a wide variety of effects; from multi-million pound fraud to the loss of sensitive personal data.Cybersecurity is becoming increasingly important to sports organizations and organizations working in the field of sports, from clubs that keep personal data in their databases to those that host major international sporting events and national organizations that participate in them.Any vulnerability or attack in this regard, information technology or loss of access to technology can have a significant impact on sports organizations causing data breaches, fraudulent loss of funds, and disruption of sports activity or presentation.Improving cybersecurity in the sports industry is critical. As a result of the research, to investigate the importance of cyber security in the field of sports, to play an important role in the security of the race organizations to be held later due to the special and strategic situation in our country and to create resources for security measures in these organizations, what are the risks related to security in informatics in the field of sports, what are the threats, and how to create them. What are the necessary policies and strategies and it aims to contribute to this field, which is new in sports sciences, in terms of literature.

Keywords: Cyber security, information technologies, risks, sports science, Threat

KAYNAKLAR

ADAMSKY, D. (2017). The israeli odyssey toward its national cyber security strategy. The Washington Quarterly, **40**(2)**:** 113-127.

AKKUŞ, B. (2013). Özgürlük ve Güven (siz) lik İkileminde Siber Uzay (Doctoral dissertation, Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler ABD).

AKYILDIZ, Z., & YILDIZ, M. (2020). Polar Team Pro Mikro Elektro-Mekanik Sisteminin Gerçek Zamanlı ve Müsabaka Sonrası Verilerinin Karşılaştırılması. Turkiye Klinikleri Journal of Sports Sciences, **12**(3).

ANDRADE, E. R., SİMPLİCİO, M. A., BARRETO, P. S., & DOS SANTOS, P. C. (2016). Lyra2: Efficient password hashing with high security against time-memory trade-offs. IEEE Transactions on Computers, **65**(10)**:** 3096-3108.

APPELQVİST, P., CHAVEZ-DEMOULİN, V., HAMERİ, A. P., HEİKKİLÄ, J., & WAUTERS, V. (2013). Turnaround across diverse global supply chains using shared metrics and change methodology: The case of Amer Sports Corporation. International Journal of Operations & Production Management, **33**(5)**:** 622-647.

ARIKAN, Y. ve ÇELİK, O. (2007). Futbolda Şiddet ve Polis. Polis Bilimleri Dergisi, **9**(4)**:** 109-132.

AUSTİN, G. (2018). Cybersecurity in China: The next wave. Springer International Publishing.

BAKIR, İ. Y., & MÜNİROĞLU, (2007). Türkiye süper liginde mücadele eden bir futbol takımın iç saha ve dış sahalarda yaptığı maçların analiz sonuçlarının karşılaştırılması (Doctoral dissertation, Ankara Üniversitesi Sağlık Bilimleri Enstitüsü Beden Eğitimi ve Spor Anabilim Dalı).

BARNEY, J. (1991). Firm Resources and Sustained Competitive Advantage. Journal of Management, **17**(1)**:** 99–120. https://doi.org/10.1177/014920639101700108

BAŞLAR, K. (2012). Uluslararası Kuruluşlar ve Uluslararası Hukuk Kişiliği. Uluslararası Hukuk ve Politika, (30), 1-23.

BAYKAN, E. (2022). Dünya Taekwondo şampiyonasının teknik ve taktik analizi (Master's thesis, Hitit Üniversitesi).

BELTON, I., MACDONALD, A., WRİGHT, G., HAMLİN, I., 2019. Improving the practical application of the Delphi method in group-based judgment: a six-step prescription for a well-founded and defensible process. Technol. Forecast. Soc. Change 147.

BLAŽİČ, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. Education and information technologies, **27**(3)**:** 3011-3036.

BOWEN, B. M., HERSHKOP, S., KEROMYTİS, A. D., & STOLFO, S. J. (2009). Baiting inside attackers using decoy documents. In Security and Privacy in Communication Networks: 5th International ICST Conference, SecureComm 2009, Athens, Greece, September 14-18, 2009, Revised Selected Papers 5 (pp. 51-70). Springer Berlin Heidelberg.

BRODİE, J. F. (2011). Learning Secrecy in the Early Cold War: The RAND Corporation. Diplomatic History, **35**(4)**:** 643-670.

BUDAK, E. (2019). Türk medyasında dijital spor yayıncılığı üzerine bir araştırma. TRT akademi, **4**(8)**:** 226-245.

CAN, H., LU, M., AND GAN, L. (2011). The research on application of information technology in sports stadiums. Physics Procedia, **22:** 604-609

CHANG, P.-L., HSU, C.-W., CHANG, P.-C., 2011. Fuzzy Delphi method for evaluating hydrogen production technologies. Int. J. Hydrogen Energy **36**(21)**:** 14172–14179. https://doi.org/10.1016/j.ijhydene.2011.05.045.

CHEN, C.T., 2000. Extensions of the TOPSIS for group decision-making under fuzzy environment. Fuzzy Set Syst. **114**(1)**:** 1–9. https://doi.org/10.1016/S0165-0114 (97)00377-1.

CHENG, C.H., LİN, Y., 2002. Evaluating the best main battle tank using fuzzy decision theory with linguistic criteria evaluation. Eur. J. Oper. Res. **142**(1)**:** 174–186. https://doi.org/10.1016/S0377-2217(01)00280-6.

CLARK, D. (2014). The role of trust in cyberspace. Trust, computing, and society, 17-37.

COHEN, R. J., SWERDLİK, M., & STURMAN, E. (2012). EBOOK: Psychological Testing and Assessment. McGraw Hill.

CUHLS, K. (2008). Foresight in Germany. The Handbook of Technology Foresight: concepts and practice, 131-153.

CYBER SECURİTY COUNCİL. (2016). European Foresight Cyber Security Meeting.

ÇİFCİ, H. (2017). Her Yönüyle Siber Savaş (2'nd Ed.). Ankara: TÜBİTAK.

DEMİREL, Özcan. (1993). Eğitim Terimleri Sözlüğü. Usem Yayınları, Ankara

DEMİRKAYA, Y., & ÇELİK, F. (2021). Uluslararası İlişkilerde Kamu Ve Sivil Toplum Kuruluşlarının Stratejik İşbirliği: Tika Faaliyetleri Analizİ. Oğuzhan Sosyal Bilimler Dergisi, **3**(2)**:** 125-149.

Dİ ZİO, S., & MARETTİ, M. (2014). Acceptability of energy sources using an integration of the Delphi method and the analytic hierarchy process. Quality & Quantity, **48:** 2973-2991.

ECKERT, S. (2005). Protecting critical infrastructure: the role of the private sector. Guns and Butter: The Political Economy of International Security, in: P. Dombrowski (Ed.), Lynne Rienner Publishers, Boulder, Colorado.

EMANS, B. (1986). Interviewen: theorie, techniek en training. Groningen: Wolters-Noordhoff, 1986.

EVANS, R., MCNAMEE, M., & GUY, O. (2017). Ethics, nanobiosensors and elite sport: The need for a new governance framework. Science and engineering ethics, **23:** 1487-1505.

FİŞEK, K. (1985). 100 soruda Türkiye spor tarihi (Vol. 53). Gerçek Yayınevi.

GREENWALD, M. (2017). Cybersecurity in sports. Questions of Privacy and Ethics. Tufts University Department of Computer Science. Recuperado de http://www. cs. tufts. edu/comp/116/archive/fall2017/mgreenwald. pdf.

GÜVEN, Ö. (1992). Türklerde Spor Kültürü/Sport Culture in Turks.

HAEGEMAN, K., MARİNELLİ, E., SCAPOLO, F., RİCCİ, A., & SOKOLOV, A. (2013). Quantitative and qualitative approaches in Future-oriented Technology Analysis (FTA): From combination to integration? Technological Forecasting and Social Change, **80**(3)**:** 386–397.

HAN, X., Kheir, N., & BALZAROTTİ, D. (2017, October). Evaluation of deception-based web attacks detection. In Proceedings of the 2017 Workshop on Moving Target Defense (pp. 65-73).

HANSMAN, S., & HUNT, R. (2005). A taxonomy of network and computer attacks. Computers & Security, **24**(1)**:** 31-43.

HİSCOCKS, E. S. (1960). Organization and Methods. Nature, **186**(4718)**:** 62-62.

IBM. (2018). IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses. https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses Erişim Tarihi: 15/3/2023

IBM. (2022). IBM Study: Cost of a Data Breach Report 2021 Erişim Tarihi: 21/3/2023 https://www.ibm.com/downloads/cas/OJDVQGRY.

İÇTEN, T., & GÜNGÖR, B. (2017). Artırılmış gerçeklik üzerine son gelişmelerin ve uygulamaların incelenmesi. Gazi University Journal of Science Part C: Design and Technology, **5**(2)**:** 111-136.

JENKİNS, S., & EVANS, N. (2020, April). Cybersecurity impact of the growth of data in sports. In Cyber Sensing 2020 (Vol. 11417, pp. 84-100). SPIE.

KAPIR, B. (2022). Yapay Zekâ Eksenli Gelişen Algoritmik Toplum ve Medya (Doctoral dissertation, Marmara Universitesi (Turkey)).

KARAMAN, M. (2022). Bir Politika Belirleme Aracı Olarak Öngörü. Balkan & Near Eastern Journal of Social Sciences (BNEJSS), **8**(2).

KARA, İ. (2019). Kaba Kuvvet Saldırı Tespiti ve Teknik Analizi. Sakarya University Journal of Computer and Information Sciences, **2**(2)**:** 61-69.

KİM, S., PARK, J., LEE, K., YOU, I., & YİM, K. (2012). A Brief Survey on Rootkit Techniques in Malicious Codes. J. Internet Serv. Inf. Secur., **2**(3/4)**:** 134-147.

KOCAKULAH, M. C., & UPSON, J. (2004). Lean manufacturing: Selected financial performance of recognized lean manufacturers. International Business & Economics Research Journal (IBER), **3**(12).

KORKUT, C. (2022). Dijital Spor Teknolojilerinin Spor Televizyonculuğunda Kullanımı. EKEV Akademi Dergisi, (90), 79-92.

KUBAT, A. (2021). Futbol Altyapı Antrenörlerinin Altyapı Eğitiminde Karşılaştıkları Sorunlar ve Çözüm Önerileri (Master's thesis).

KUO, Y. F., & CHEN, P. C. (2008). Constructing performance appraisal indicators for mobility of the service industries using Fuzzy Delphi Method. Expert systems with applications, **35**(4)**:** 1930-1939.

KUŞ, A. A. & BİÇER, T. (2022). Büyük Spor Organizasyonlarındaki Güvenlik Uygulamalarının Güvenirliği: İstanbul Maratonu Örneği . Çanakkale Onsekiz Mart Üniversitesi Spor Bilimleri Dergisi, **5**(2)**:** 40-45. Retrieved from https://dergipark.org.tr/tr/pub/comusbd/issue/72541/1162271

LİU, W., & ZOU, X. (2021, August). Learning and Content Management System in the Process of Sports and Training. In 2021 International Conference on Diversified Education and Social Development (DESD 2021) (pp. 126-131). Atlantis Press.

MARTİN, B. R. (1995). Foresight in science and technology. Technology Analysis and Strategic Management, **7**(2)**:** 139–168.

MCAFEE, 2006 "Rootkits, Part 1 of 3: The Growing Threat" (PDF). 2006-04-17. Erişim tarihi: 20/4/2023 https://web.archive.org/web/20060823090948/http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_akapoor_rootkits1_en.pdf

MEREDİTH, J. R., & Mantel, S. J. (1995). Technological Forecasting.

MİLES, I. (2010). The development of technology foresight: A review. Technological Forecasting and Social Change, **77**(9)**:** 1448-1456.

MİLLETLER, B. (2005). BM Ülke İçinde Göç Ettirme Konusunda Yol Gösterici İlkeler.

MİTNİCK, K.D., SİMON, W.L., 2013. "Aldatma Sanatı", Odtü Yayıncılık, Ankara

MOLAS-GALLART, J. (1997). Which way to go? Defence technology and the diversity of 'dual-use'' technology transfer.' Research Policy, **26**: 367–385. https://doi.org/10.1016/S0048-7333(97)00023-1

NAZLI, M. 2009. Bilgi Güvenliği Açısından Erişim Kontrolü, Ulusal Bilgi Güvenliği Kapısı.

NOVAK, M. (1993). Joy of sports, Revised: Endzones, bases, baskets, balls, and the consecration of the American spirit. Madison Books.

OGASAWARA, A. (2015). 1st Preliminary Report on The 10th Science and Technology Foresight Survey, 1–40. Retrieved from http://www.nistep.go.jp/wp/wp-content/uploads/2-1_Ogasawara.pdf

OCONNOR, T. J., BROWN, D., JACKSON, J., PAYNE, B., & SCHMEELK, S. (2023). Compete to Learn: Toward Cybersecurity as a Sport. Journal of Cybersecurity Education, Research and Practice, 2023(1)**:** 6.

ÖZDENGÜL, A. G., & AYDIN, M. (2022). Pazarlanan Sporun Dijital Dönüşümü. Birey Toplum ve Dijitalleşme Bağlamında Tüketimin Yeni Formları, 131.

ÖZDOĞAN, O. (2017). Endüstri 4.0: dördüncü sanayi devrimi ve endüstriyel dönüşümün anahtarları. Pusula.

PHAAL, R., FARRUKH, C. J. P., & PROBERT, D. R. (2001). Technology Roadmapping: linking technology resources to business objectives. International Journal of Technology Management. https://doi.org/10.1504/IJTM.2003.003140

POPPER, R., & TEİCHLER, T. (2011). 1st EFP Mapping report: Practical guide to mapping forward-looking activities (FLA) practices, players and outcomes. European Foresight Platform, 1-83.

PORTER, A. L., ASHTON, W. B., CLAR, G., COATES, J. F., CUHLS, K., CUNNİNGHAM, S.W., … THİSSEN, W. (2004). Technology futures analysis: Toward integration of the field and new methods. Technological Forecasting and Social Change, **71**(3)**:** 287–303.

RABAİOTTİ, J. R., & HARGREAVES, C. J. (2010). Using a software exploit to image RAM on an embedded system. Digital Investigation, **6**(3-4)**:** 95-103.

RÁTHONYİ, G., MÜLLER, A., & RATHONYİ-ODOR, K. (2018). How digital technologies are changing sport?. APSTRACT: Applied Studies in Agribusiness and Commerce, **12**(1033-2019-3296)**:** 89-96.

RAY, G., BARNEY, J. B., & MUHANNA, W. A. (2004). Capabilities, business processes, and competitive advantage: choosing the dependent variable in empirical tests of the resource based view. Strategic management journal, **25**(1)**:** 23-37.

SABİLLON, R., CAVALLER, V., & CANO, J. (2016). National cyber security strategies: global trends in cyberspace. International Journal of Computer Science and Software Engineering, **5**(5)**:** 67.

SANDERSON, J. (2009). Professional athletes' shrinking privacy boundaries: Fans, information and communication technologies, and athlete monitoring. International Journal of Sport Communication, **2**(2)**:** 240-256.

SANG, M. S. (2010). Penyelidikan dalam Pendidikan - Perancangan dan Pelaksanaan Penyelidikan Tindakan. Kuala Lumpur: Penerbitan Multimedia Sdn. Bhd

SANGAL, S., NİGAM, A., & BHUTANİ, C. (2022). Conceptualizing the role of blockchain in omnichannel healthcare: a Delphi study. Aslib Journal of Information Management, **74**(5)**:** 782-800.

SAVAŞ, B. Ç. (2023). METAVERSE VE SPOR. Efe Akademi Yayınları.

SAVAŞ, İ. (1989). Spor Sözlüğü, İstanbul: Remzi Kitabevi.

SERTÇELİK, A. (2015). Siber olaylar ekseninde siber güvenliği anlamak. Medeniyet Araştırmaları Dergisi, **2**(3)**:** 25-42.

SEZGİN, Ş., & SEZGİN, S. (2018). Dünya'da Ve Türkiye'de Savunma Sanayi: Genel Bir Bakiş. Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi, **5**(12)**:** 1-19.

ŞİMŞEK, A. ve DEVECİ, S. (2018). Spor endüstrisinde yeni teknolojilerin görünümü. Uluslararası Beden Eğitimi Spor Rekreasyon ve Dans Dergisi, **1**(1)**:** 20-36

SLAUGHTER, R. A. (1997). Developing and applying strategic foresight. ABN Report, **5:** 13–27.

SLİPACHUK, L., TOLİUPA, S., & NAKONECHNYİ, V. (2019, July). The Process of the Critical Infrastructure Cyber Security Management using the Integrated System of the National Cyber Security Sector Management in Ukraine. In 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT) (pp. 451-454). IEEE.

ŞENTÜRK, H., ÇİL, C. Z., & SAĞIROĞLU, Ş. (2012). Cyber Security Analysis of Turkey. International Journal of Information Security Science, **1**(4)**:** 112–125. Retrieved from http://ijiss.org/ijiss/index.php/ijiss/article/download/18/112-125

SMİTH MCGLOİN, R., & WYNNE, C. (2022). Structures and strategy in doctoral education in the UK and Ireland.

SOYSAL, M., & ÖMÜRGÖNÜLŞEN, M. (2010). Türk turizm sektöründe talep tahmini üzerine bir uygulama. Anatolia: Turizm Araştırmaları Dergisi, **21**(1)**:** 128-136.

TAVAKOL, M., MOHAGHEGHİ, M. A., & DENNİCK, R. (2008). Assessing the skills of surgical residents using simulation. Journal of surgical education, **65**(2)**:** 77-83.

TAYLOR, T. (1986). Sport and International Relations: A Case of Mutual Neglect. L. Allison içinde, Politics of Sport (s. 27-48). Manchester: Manchester University Press.

TOLAN, S. (2014). Spor endüstrisinde etkinlik pazarlaması: Galatasaray spor kulübü örneği (Master's thesis, Maltepe Üniversitesi, Sosyal Bilimler Enstitüsü).

TOZKOPARAN, K. E., & KARADUMAN, Ö. (2022). Spor Biyomekaniğinde Performans Analizi için Hareket Yakalama Teknolojisi Uygulamaları. Fırat Üniversitesi Fen Bilimleri Dergisi, **34**(2)**:** 95-111.

TRENDMİCRO, (2015) Cybercrime in Sports: Scoring Against Sports-themed Scams Erişim Tarihi: 22/4/2023 https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/cybercrime-in-sports-scoring-against-sports-themed-scams

TRTSPOR, 2019. TRT'den Dev Adım Erişim tarihi: 20/5/2023 https://www.trtspor.com.tr/haber/diger-sporlar/trtden-dev-adim-192214.html

TUNCA, S. (2019). MODERN ÇAĞDA SİBER GÜVENLİK KAVRAMI . Dumlupınar Üniversitesi İİBF Dergisi, (3-4), 1-7. Retrieved from https://dergipark.org.tr/tr/pub/dpuiibf/issue/68606/1076685

TÜMER, T. 2002. TÜBİTAK Teknoloji Öngörüsü Projesi Sunumu, TÜBİTAK MAM, 17/06/2002, Gebze

ULAŞTIRMA VE ALTYAPI BAKANLIĞI. (2012). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, Ankara. https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf . Erişim Tarihi: 15/2/2023

ULAŞTIRMA VE ALTYAPI BAKANLIĞI. (2016). U Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2016-2019, Ankara. https://hgm.uab.gov.tr/strateji-eylem-planlari Erişim Tarihi: 15/2/2023.

ULMER, K. (2021). Cyber risks and cybersecurity: risk communication and regulation strategies in the United States and Germany.

USLU, T. (2007). İnternet güvenliği ve risk yönetimi (Doctoral dissertation, İstanbul Kültür Üniversitesi/Fen Bilimleri Enstitüsü/Bilgisayar Mühendisliği Anabilim Dalı).

VAN DER SLIKKE, R. M., SINDALL, P., GOOSEY, V. L., & MASON, B. S. (2023). Load and performance monitoring in wheelchair court sports: a narrative review of the use of technology and practical recommendations. European Journal of Sport Science, **23**(2)**:** 189-200.

WATSON, G., MASON, A., & ACKROYD, R. (2014). Social engineering penetration testing: executing social engineering pen tests, assessments and defense. Syngress.

WEBSTER, F. (2014). Theories of the information society. Routledge.

WEHREMEYER, W., CLAYTON, A. ve LUM K., 2002. Foresighting For Development, Greener Management International, **37:** 24-31.

WİLLETTS, D. (2013). Eight great technologies.

YILDIRIM, E. Y., & ADALI, E. (2017, October). The threats and risks in personal data security. In 2017 International Conference on Computer Science and Engineering (UBMK) (pp. 610-615). IEEE.

YILDIRIM, N. (2006). Türkiye'de yazılım teknolojisi için teknoloji öngörüsü (Doctoral dissertation, Sosyal Bilimler Enstitüsü).

YILDIZ, A. B. & ALGÜN DOĞU, G. (2022). Sporda Teknoloji Kullanımı: Bir Metafor Çalışması . Ahi Evran Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, **8**(1)**:** 67-80. DOI: 10.31592/aeusbed.980957

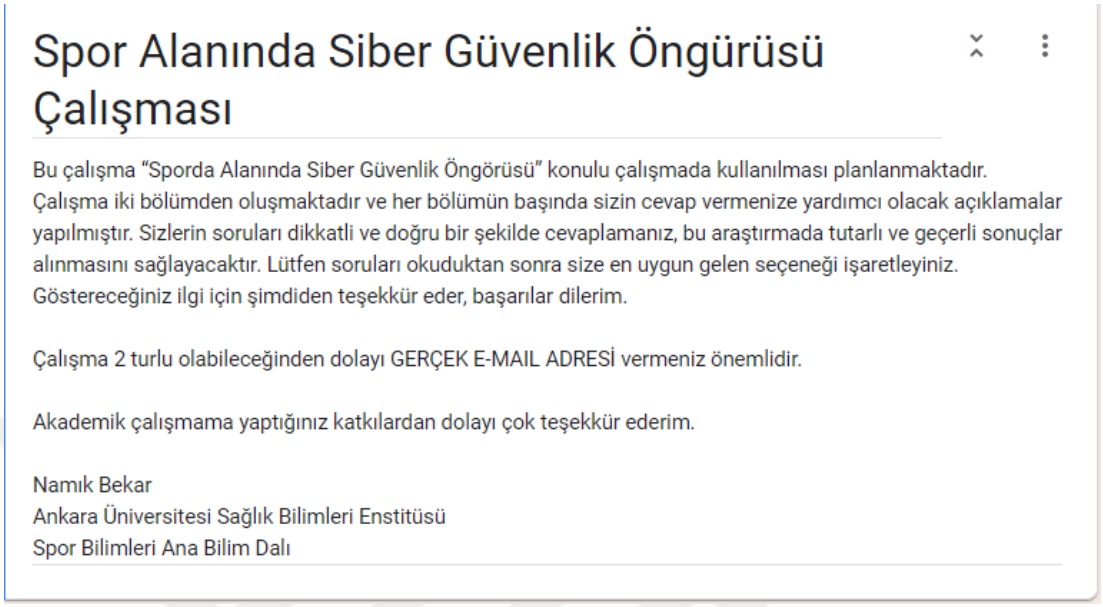
YILMAZ, M., & BALLI, S. (2016). Veri Şifreleme Algoritmalarının Kullanımı İçin Akıllı Bir Seçim Sistemi Geliştirilmesi. Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, **2**(2)**:** 18-28.

YOUNG, S. J., & ROSS, C. M. (2000). Recreational sports trends for the 21st century: Results of a Delphi study. Recreational Sports Journal, **24**(2)**:** 24-37.

YÜKÇÜ, S., & KAPLANOĞLU, E. (2018). UİK e-Spor endüstrisi. Uluslararası İktisadi ve İdari İncelemeler Dergisi, 533-550.

ZHANG, J. J., BREEDLOVE, J., KİM, A., Bo, H. H., ANDERSON, D. J., ZHAO, T. T., & PİTTS, B. G. (2021). Issues and new ideas in international sport management. International sport business management: Issues and New ideas, 1.

EKLER



Spor Alanında Siber Güvenlik Öngürüsü Çalışması

Bu çalışma "Sporda Alanında Siber Güvenlik Öngörüsü" konulu çalışmada kullanılması planlanmaktadır. Çalışma iki bölümden oluşmaktadır ve her bölümün başında sizin cevap vermenize yardımcı olacak açıklamalar yapılmıştır. Sizlerin soruları dikkatli ve doğru bir şekilde cevaplamanız, bu araştırmada tutarlı ve geçerli sonuçlar alınmasını sağlayacaktır. Lütfen soruları okuduktan sonra size en uygun gelen seçeneği işaretleyiniz. Göstereceğiniz ilgi için şimdiden teşekkür eder, başarılar dilerim.

Çalışma 2 turlu olabileceğinden dolayı GERÇEK E-MAIL ADRESİ vermeniz önemlidir.

Akademik çalışmama yaptığınız katkılardan dolayı çok teşekkür ederim.

Namık Bekar
Ankara Üniversitesi Sağlık Bilimleri Enstitüsü
Spor Bilimleri Ana Bilim Dalı