Bölüm 3

Dijitalleşen Lojistik İş Süreçlerinde Siber Güvenlik

Ömer Cengiz[1]

Özet

Lojistik yönetimi ihtiyaç duyulan mal ve hizmetlerin üretildikleri noktadan tüketim alanlarına hareketini amaçlayan ve tedarik zincirleri boyunca gerekli faaliyetlerin etkili ve verimli bir biçimde yerine getirilmesini sağlayan önemli bir süreçtir. Lojistik faaliyetler bilgi teknolojilerine önemli düzeyde ihtiyaç duymaktadır. Bu sebeple operasyonlar sırasında dijital teknolojilerin kullanımı vazgeçilmez bir gerekliliktir. Lojistik sektörünün yüksek düzeyde dijital bilgi teknolojilerine bağımlı olması siber güvenlik ihtiyacını ortaya çıkarmaktadır. Lojistik iş süreçleri ve operasyonel faaliyetlerin kesinti yaşamaması siber güvenlik uygulamalarının başarısı ile yakından ilişkili olacaktır. Bu sebeple, bu çalışma lojistik iş süreçlerinde yoğun bir şekilde kullanılan bilişim teknolojileri sonucu ihtiyaç duyulan siber güvenlik kavramına dikkat çekmeyi amaçlamaktadır.

1. Giriş

Yaşanan teknolojik gelişmeler dünyayı sürekli olarak yeniden şekillendirmekte ve tüketicilere ürünler ve hizmetlerle ilgili daha geniş bir seçenek yelpazesi sunmaktadır. Hızla gelişen ve büyümeye devam eden küresel ekonomide rekabetçi kalmak, değişen müşteri taleplerine zamanında yanıtlar vermek ve artan hizmet beklentilerini karşılamak için, işletmeler lojistik faaliyetleri ve tedarik zincirlerine bilgisayar tabanlı yönetim sistemlerini dâhil etmektedirler. Bu sayede birçok süreç otomatikleştirilerek tam zamanında üretim ve siparişe göre üretim sistemleri ile daha etkin envanter yönetimi sağlanmaktadır. Bilgi teknolojilerinin bu yaygın kullanımı ile birçok işletme dönüşerek tüm bilgi akışlarını dijital ortamlara ve veri tabanlarına aktarmaktadır (Boyes, 2015:28).

1 Dr. Öğr. Üyesi, Kafkas Üniversitesi, omercengiz99@gmail.com, 0000-0002-4645-3318

https://doi.org/10.58830/ozgur.pub688.c2903

Dördüncü sanayi devriminin getirdiği bilişim teknolojileri ile ortaya çıkan iyileştirilmiş iletişim ve bilgi akışı, tüm sektörlerdeki mal ve hizmet üreticilerinin müşterilerine sunduğu ürünlerin lojistik zinciri boyunca izlenmesini sağlamaktadır. Lojistik faaliyeti yürüten işletmeler süreç verimliliğini ve maliyet optimizasyonunu iyileştirmek için operasyonlarını dijitalleştirmektedirler. Bilgi teknolojisi araçlarının etkili bir şekilde uygulanması işletmelerin sürdürülebilir büyümesini sağlamaktadır. Özellikle Nesnelerin İnterneti, Siber Fiziksel Sistemler, Bulut Bilişim, Büyük Veri ve Yapay Zeka tedarik zincirlerinin uçtan uca gerçek zamanlı bilgiler ışığında yönetilmesini sağlamaktadır. Bu sayede geleneksel lojistik ve tedarik zinciri faaliyetleri büyük bir değişim yaşamakta ve zengin bilgiye sahip yeni ekosistemler oluşturulmaktadır (Pandey vd., 2020:104).

Kullanılan dijital teknolojiler sayesinde bilgi alışverişi, operasyon çevikliği ve süreç görünürlüğünün artması önemli bir sonuçtur. Bilişim sistemleri lojistik sektörünün daha hızlı, verimli ve etkili çalışmasını sağlamakla birlikte olumsuz sonuç ve endişeleri de beraberinde getirmektedir. Bu ağ yapıları ve teknolojik sistemleri kullanımına bağlı olarak tedarik zincirleri boyunca ortaya çıkan bazı tehditler ve riskler bulunmaktadır (Latif vd., 2021:50; Çelik, 2020:90). Bu risklerin en önemlisi siber güvenliğin sağlanamamasıdır. Lojistik sektörü hızla büyüyen siber uzaydan faydalanma düzeyini artırdıkça siber saldırılara maruz kalma riskini de artırmaktadır. Siber saldırılarla ve siber riskle mücadelede en önemli önlem, dijital lojistik ağındaki kritik varlıkların korumasıdır. Kritik varlıkları savunmak için gerekli önlemlerin proaktif bir şekilde alınması önem arz ederken lojistik ağının karmaşıklığı nedeniyle, siber güvenlik önlemlerinin etkinliği de zorlu bir sürece dönüşmektedir (Cheung ve Bell, 2021:481).

Dijital iletişim, otomasyon ve küresel ekonominin birbirine bağlılığına dayanan mevcut durum, siber güvenliği hem ulusal güvenlik, hem de küresel güvenlik sorunu haline getirmektedir. Yıkıcı kötü amaçlı yazılımlar, siber suçlar ve veri sızıntıları gibi ortaya çıkan birçok siber tehdit, hükümetleri, ekonomileri ve toplumları aynı şekilde etkilemektedir (Fitton vd., 2015:1).

Siber saldırılar için finans sektörü en büyük hedef iken ikinci sırada kamu hizmetleri, havacılık ve savunma sektörleri gelmektedir. Üretim, lojistik ve ulaştırma sektörlerinin orta düzey siber saldırılara maruz kaldığı bilinmektedir (Sarder ve Haschak, 2019:7). Yeni gelişmeler mevcut sisteme verimlilik getirdikçe, standart operasyonları bozan saldırıların ardından her düzeyde siber güvenliğe yönelik endişe de artmaktadır. Siber ve fiziksel sistemler arasındaki bağlantı ve etkileşim nedeniyle operasyonel siber

güvenlik, geleneksel bilgi teknolojisi güvenliği yaklaşımından farklı bir strateji gerektirmektedir (Parker vd., 2023:1).

Veri bütünlüğünü sağlamak için blok zinciri, uzaktan teslimatlar için dronlar ve depo operasyonları için robotlar gibi gelişmiş teknolojilerin benimsenmesi, lojistik süreçlerinde ve küresel tedarik zinciri ağlarında verimliliği artırmaktadır. Bu teknolojiler lojistik sektörü için fırsatlar yaratırken, siber suçluların istismar edebileceği potansiyel güvenlik açıkları da meydana gelmektedir (Bhattacharjya vd., 20121:14). Lojistik yönetiminde siber güvenliğin amacı, lojistik sektörü için güvenli bir siber alan oluşturmaktır. Bunu başarmanın kabul edilen yolu, dijital bir ağdaki siber riskleri (veya siber tehditleri) ortadan kaldırmak veya azaltmaktır. Siber risk, siber alanda bulunan bir risktir ve bu nedenle ortadan kaldırılması veya azaltılması gerekmektedir (Cheung ve Bell, 2021:472). Lojistik faaliyetlerin yürütüldüğü tedarik zincirlerindeki küçük kuruluşların siber saldırıların daha çok hedefi oldukları bilinmektedir. Bunun bir sonucu olarak aynı tedarik zinciri içerisinde yer alan ve küçük işletmeler ile sözleşmeleri olan daha büyük işletmeler belirli tehditlere maruz kalma riski altındadırlar. Bu sebeple tüm tedarik zinciri içindeki siber güvenliğin bir bütün olarak karşılanması adına güvenli ağ yapıları sağlanması gerekmektedir (Latif vd., 2021:50).

2. Lojistik Yönetimi ve Dijital Teknolojilerin Kullanımı

Lojistik, modern ekonomi ve güvenlik sistemleri için önemli bir temel unsurdur. İnsanları, yiyecekleri, malzemeleri ve makineleri konumlar arasında taşıma yeteneği, küresel ekonominin ve modern savaşın ölçeğini ve yoğunluğunu artırmaktadır. Lojistiğin etimolojisi, aritmetik hesaplama becerisine atıfta bulunurken, lojistik tüm üretim organizasyonları için hayati öneme sahiptir (Fitton vd., 2015:24; Alzahrani ve Asghar, 2024:1). Lojistik yönetimi, malların, hizmetlerin ve bilgilerin üretim noktasından tüketim alanlarına kadar hareketini entegre eden bir yönetim sürecidir (Cheung ve Bell, 2021:472). Lojistik yönetiminde doğru ürün, miktar, yer, kalite, zaman ve fiyat dâhil olmak üzere tüm faaliyetlerin, ortak dijital teknoloji özellikleri kümesiyle tam olarak desteklenmesi gerekmektedir (Golpira vd., 2021:2).

Küresel ekonomi içerisinde faaliyet gösteren bütün işletmeler gıda, enerji, mal ve teknolojinin ithalatını ve ihracatını mümkün kılan lojistik faaliyetlere bağımlıdırlar. Günümüz ekonomisinin aşırı rekabetçi yapısına bağlı olarak, lojistik iş süreçlerinin verimliliğine yönelik beklentiler her zamankinden daha fazladır. 21. yüzyılda lojistikten beklenen yenilik alanlarının başında dijitalleşme ve bilgi teknolojilerinin kullanımı gelmektedir. Bu sebeple lojistik faaliyetlere odaklanan tüm işletmeler, stratejik hedeflerini yalnızca yeni

teknolojiler kullanarak maliyetleri düşürmek üzerine değil, aynı zamanda alternatifler açısından hızlı ve verimli bir lojistik altyapısı oluşturmak üzerine kurmaktadırlar. Dijital inovasyon, dijital teknolojilere dayalı yeni ürünler, hizmetler veya iş modelleri yaratma yeteneğini ifade ederken (Heierhoff ve Hoffmann, 2022:6793). Dijitalleştirme ise üretim öncesi ve sonrası gerçekleştirilen tüm lojistik ve tedarik zinciri faaliyetlerinin sensörler, aktüatörler, ağlar, yazılımlar ve dijital donanımlar vasıtasıyla siber ortamlara aktarılmasını ifade etmektedir (Pan vd., 2021:4). Lojistik sektöründe 3D baskı, e-ticaret, nesnelerin interneti, siber fiziksel sistemler, bulut bilişim, yapay zeka, artırılmış gerçeklik gibi dijital teknolojiler ve trendler, dronlar ve robotlar gibi ekipmanlar, malların taşınmasını, depolanmasını, dağıtımını kolaylaştırmak ve müşteri hizmetlerini iyileştirmek için yaygın bir biçimde kullanılmaya başlamıştır. Gerçekleşen bu dijitalleşme süreci ile birlikte, veri bütünlüğü lojistik hizmetlerinin kalitesini sağlamada hayati bir rol üstlenmektedir (Bhattacharjya vd., 20121:2; Simon ve Omar, 2020:162).

Dördüncü sanayi devrimi ile ortaya çıkan yeni paradigma iş ve tedarik zinciri modellerini, iş süreçlerinin ayrıştırılmasını ve gerçek dünya görünürlüğünü geliştirmeye ve otomatikleştirmeye dönük önemli faydalar sunmaktadır. Gerçek zamanlı etkinleştirilmiş lojistik işletmeleri ve ilgili tedarik zinciri modelleri günümüz ekonomi sistemleri için çok önemlidir (Radanliev vd., 2020:1). Giderek daha karmaşık ve küresel hale gelen tedarik zincirlerinde etkinliği ve verimliliği artırmak ve tedarikçiler, üreticiler, dağıtımcılar ve hatta nakliye hizmeti sağlayıcıları ağı arasındaki iletişimi ve koordinasyonu desteklemek için bilgi teknolojilerine büyük ölçüde ihtiyaç duyulmaktadır (Colajanni vd., 2018:1444). Dijital tedarik zinciri terimi, planlama, kaynak sağlama, üretim, lojistik ve dağıtım aşamalarını kapsayan tüm tedarik zinciri sürecinde dijital teknolojilerin ve bilgi sistemlerinin entegrasyonunu ifade eder. Lojistik faaliyetler açısından dijital tedarik zinciri üreticiler, tedarikçiler, taşıyıcılar, distribütörler ve perakendeciler dâhil olmak üzere çeşitli paydaşlar arasında sorunsuz veri ve bilgi alışverişini içermektedir. Bu karşılıklı yoğun etkileşim ve koordinasyon yaklaşımı, tedarik zinciri boyunca gerçek zamanlı izleme, veri odaklı karar alma ve optimize edilmiş kaynak kullanımını mümkün kılarken, genel operasyonel performans düzeylerini iyileştirmektedir (Odimarha vd., 2024:26).

Lojistik faaliyetlerin yürütülmesi sırasındaki ana hedefler planlama sistemlerini iyileştirme, depo envanterini optimize etme, zamanında teslimat yapma, talebe uygun süreç tasarlama, maliyetleri düşürme ve işletme değerini artırma şeklindedir (Boiko vd., 2019:67). Lojistik planlama ve yürütmede faaliyetleri için bol miktarda veriye ihtiyaç duyulmaktadır. Teknolojinin kullanımı ile verilerin depolanması ve kullanılması kolaylaşırken, daha

basit ve hızlı lojistik operasyon planlamasının önü açılmış olur (Jagtap vd., 2020:8). Tüm bu dijitalleşme çabalarının önemli bir amacı süreç içerisindeki ürün ve hizmete ait tüm envanterin izlenebilirliğidir. İzlenebilirlik, bilgi ve iletişim teknolojilerinden yararlanarak ürünle ilgili bilgilerin ürünün üretim süreci dâhil yaşam ömrü boyunca erişilebilir olmasını sağlamaktır. Bu sayede işletmeler tedarik zincirinde herhangi bir noktadaki bir ürünün mevcut durumunu eş anlı olarak izleme yeteneğine sahip olmaktadır. Bu yetenek lojistik gibi müdahale gerektiren iş süreçleri için en önemli yeteneklerden biridir. Ürün ve hizmete ait izleme sonuçlarına dayanarak süreçlerde değiştirme, dönüştürme ve müdahale imkânları verimliliğin artmasını sağlamaktadır. Bu yetenekler tedarik zinciri paydaşlarına rekabet gücü, karlılık ve şeffaflık açısından önemli avantajlar sağlar (Syed vd., 2022:2). Lojistik süreçlerdeki izlenebilirliği artırmak için Radyo Frekansı Tanımlama (RFID), Kurumsal Kaynak Planlama (ERP), Elektronik Veri Değişimi (EDI) ve dijital bilgi teknolojilerinin koordinasyonu ve entegrasyonu artık vazgeçilmez bir gerekliliktir (Norman vd., 2020:2).

Dördüncü sanayi devrimini meydana getiren ve üretim sistemlerinde köklü değişimler yaşatan dijital teknolojiler lojistik süreçler ile yüksek düzeyde uyum göstermektedir. Taşıma sistemleri, depolama faaliyetleri, gümrükleme operasyonları, sigortalama işlemleri, envanter yönetimi ve diğer tüm lojistik faaliyetlerde dijitalleşme sayesinde verimlilik düzeylerinde önemli artışlar yaşanmaktadır. Lojistik bilişim sistemleri, dijitalleşme sürecinin önemli bir faktörü olan teknolojik gelişmeler ile ortaya çıkmış olup bu sistemlerin kullanılması sektöre önemli katkılar sağlamaktadır (Talih ve Dönmez, 2024:847).

3. Siber Güvelik Kavramı ve Siber Riskler

Son 20 yılın öncelikli güvenlik konularından biri siber güvenliktir. Kamusal faaliyetlerin de dijitalleşme sürecine girmesi ile birlikte devletlerin vatandaşlara ait bilgileri güvenli bir şekilde saklanması ve korunması için gerekli yöntemlere odaklanması gerekmektedir. Bu gereklilik neticesinde siber alanlarla ilgili güvenlik ve koruma kavramları detaylandırılmış ve konvansiyonel tehdit olguları dijital alanları da kapsayacak şekilde genişletilmiştir. Yeni güvenlik yaklaşımında toplumsal güvenlik kavramları verilerin korunmasını da içerecek bir yapıya dönüştürülmüş ve dijital güvensizliği ortadan kaldıracak adımlar atılmaya başlamıştır (Doğrul ve Erğurum, 2021:178). Gelecekte bilgisayar sistemleri insan varoluşunu daha iyiye doğru değiştirme potansiyeline sahiptir. Ancak öncelikli olarak siber uzayda güvenlik kavramı dikkate alınarak sistemler tasarlanmalı ve işletilmelidir. Siber güvenliğe yönelik çalışmaların bütünsel olması gerektiği

de açık bir şekilde görülmektedir. Dijital bir sistemin birbiriyle olan bağlantısını ve dayanıklılığını haritalamadan, sistemi oluşturan insanların ve bilgilerin detaylı bir resmi olmadan tehditleri etkili bir şekilde azaltmak mümkün görünmemektedir (Fitton vd., 2015:28).

3.1. Siber Güvenlik Kavramının Tanımı

Korunması gereken ve dijital veri ve argümanlardan oluşan siber uzay internet, bilgi sistemleri ve diğer iletişim ağları gibi dijital ağlardan meydana gelen insan yapımı bir alandır. Bu alan insanlar arasındaki mesafeyi kısaltan ve bilgi alışverişi için etkili bir platform sağlayan fiziksel dünyamızın sanal bir versiyonunu oluşturmaktadır (Gunaygunta, 2023:36; Kişman ve Güleç, 2021:6). İnsan hayatını önemli ölçüde kolaylaştıran yeni sanal dünyanın korunmasını amaçlayan kavram Siber güvenliktir. Siber güvenlik, verileri ve ağları saldırılardan, hasarlardan veya yetkisiz erişimden korumak için uygulanan birleşik teknolojiler, süreçler ve uygulamalar bütünü olarak tanımlanmaktadır (Simon ve Omar, 2020:161). Kötü niyetli taraflar sistemsel açıklardan yararlanarak hizmet kaybına, ekipmanların zarar görmesine ve potansiyel olarak kazalara neden olabilir (Tonn vd., 2019:105). Diğer bir tanımda siber güvenlik, saldırganların neden olduğu kesintileri önleme, savunma ve kurtarma yeteneğidir. Siber ihlaller her yıl artarak verilerin gizliliğini, bütünlüğünü ve kullanılabilirliğini etkilemektedir (Sarder ve Haschak, 2019:3).

Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansına göre ise siber güvenlik, kullanıcı varlıklarını, organizasyonu ve siber ortamı korumak amacıyla kullanılabilecek politikalar, güvenlik kavramları, araçlar, güvenlik önlemleri, eylemler, yönergeler, risk yönetimi yaklaşımları, eğitimler, teknolojiler ve en iyi uygulamaların bütünü olarak tanımlanmaktadır. Siber güvenlik aşağıda yer alan alt alanlardan oluşmaktadır (Cheung ve Bell, 2021:472):

- Ağ güvenliği
- Bulut güvenliği
- Kimlik Yönetimi ve Veri Güvenliği
- Mobil güvenlik
- Uygulama güvenliği
- Kullanıcı eğitimi

Siber güvenliğin önemli bir amacı sistemleri, ağları, programları, cihazları ve bilgileri korumak için teknolojik yöntem ve kontrollerin uygulanmasının yanı sıra bilgisayar sistemlerinin gizliliği, bütünlüğü ve erişilebilirliği için

siber saldırılara veya yetkisiz erişimlere karşı bir kalkan oluşturmaktır. Gelinen noktada siber güvenlik iş dünyasında çeşitli açılardan sıklıkla tartışılan önemli bir konuya dönüşmüştür. Çünkü yaşanan son ihlaller, tüm sektörlerin gerekli önlemler alınmadığında ne kadar savunmasız olabileceğini göstermektedir (Latif vd., 2021:49).

Siber güvenlik sadece doğrudan saldırılara karşı değil, aynı zamanda doğal afetler veya kazara meydana gelen olaylara karşı da bir korumadır. Siber saldırılar elektrik şebekesini, deniz limanı operasyonlarını, hava trafik kontrolünü veya ulaşım altyapısının diğer bileşenlerini ve hizmetlerini etkileyebilir. Küresel konumlandırma sistemlerine yönelik bir siber saldırı, ulaşım altyapısı da dâhil olmak üzere birçok altyapı sektörünü önemli ölçüde etkileyebilir. Ayrıca, hatalı sistem uygulamaları ve yapılandırmaları nedeniyle oluşan arızalar gibi saldırı şeklinde olmayan siber olaylar da bilgi altyapısının işlevselliğine zarar verebilir ve böylece beklenmeyen sonuçlara yol açabilir (Tonn vd., 2019:105).

Genel olarak siber güvenlik uygulama düzeyinde güvenlik, veri düzeyinde güvenlik, ağ düzeyinde güvenlik gibi birçok farklı düzeyi içermektedir (Colajanni vd., 2020:47). İyi siber güvenlik sistemi insanları, süreci, fiziksel ve teknolojik yönleri kapsayan bütünsel bir yaklaşıma odaklanmaktadır. Kapsamlı bir güvenlik anlayışına ulaşmak tamamen teknik çözümlerin, potansiyel tehditlerin ve güvenlik açıklarının genişliğini ele alarak güvenlik için bütünsel bir yaklaşım sağlamaktır (Boyes, 2015:29).

3.2. Siber Risk ve Siber Saldırı

Siber risk; devletlerin, işletmelerin ya da diğer dijital sistem kullanıcılarının bilgi sistemleri ve süreçlerindeki bir problemden kaynaklanan aksaklık yaşamaları sonucu finansal kayıp veya itibar kaybı yaşama ihtimali olarak tanımlanmaktadır. Yaşanacak operasyon kesintilerinin sürekliliği bozarak tüm süreçleri sekteye uğratabileceği unutulmamalıdır. Siber riski en aza indirmeye yönelik olağan yaklaşım, siber alandaki mümkün olan en çok sayıda güvenlik açığını ortadan kaldırmaktır (Cheung ve Bell, 2021:473). Siber güvenlik risk yönetimi inovasyon sürecinin merkezine konulmalıdır. Bu sayede kuruluşların entegrasyonu tam olarak sağlanmasının yanında ve mevcut ihlal ihtimallerinin azaltılması sağlanacaktır (Heierhoff ve Hoffmann, 2022:6800). Siber risk ve zafiyetlerin ortadan kaldırılması veya azaltılması, bir organizasyonda siber güvenliğin artırılmasına önemli katkılar sunmuş olacaktır (Bhattacharjya vd., 20121:2).

Siber riski yönetmeye yönelik yaklaşımlar arasında güvenlik yazılımı, sistem tasarımı ve operasyon iyileştirmeleri ve siber işgücüne yatırımlar gibi

önlemler yer almaktadır. Güvenlik duvarları, yazılım şifrelemesi, virüs tespiti ve sistem bölümlendirmesi gibi koruyucu önlemler de siber riski azaltmak için kullanılır. Siber riski yönetmek için kurumsal önlemler, teknolojik cihazları içeren yapısal önlemler, sistemlerin yönetimi ve işletimini içeren prosedürel önlemler ve olay tespitini yöneten duyarlılık önlemleridir. Bu koruyucu önlemlerin güvenlik faydaları, ilişkili maliyetler ve üretkenlik kayıplarıyla dengelenmelidir ve işletmelerin bu önlemlerin siber riski ortadan kaldıramayacağını fark etmeleri de önemlidir. Kalan riskin uygun şekilde yönetilmesi gerekir ve siber sigorta, riski üçüncü taraflara aktarmak için tamamlayıcı bir önlem olarak kullanılabilir (Tonn vd., 2019:104).

Dijital sistemlerdeki mevcut açıklar kullanılarak ya da çeşitli yazılım uygulamaları ile sistemlere yetkisiz giriş yapılması, bilgilerin alınması ya da değiştirilmesi siber saldırı olarak tanımlanmaktadır. Proses kontrol sistemleri ve tedarik zincirleri perspektifinden bakıldığında siber saldırılar, aktüatörleri, sensörleri, cihazlar arasındaki iletişim kanallarını ve operasyon kontrol sistemi algoritmalarını tehlikeye atabilen kötü amaçlı sinyallerdir (Parker vd., 2023:3). Siber saldırıların sıklığı ve siber saldırılarla ilişkili maliyetler yüksek bir hızla artmaktadır. Saldırıların tespiti, sınırlanması, kurtarma maliyetleri, iş kesintisi, gelir kaybı ve ekipman hasarı mali açıdan işletmelere büyük zararlar vermektedir. Bir siber ihlal ayrıca bir işletmenin veya müşterinin itibarını yok edebilir. Siber suçun maliyeti ülkeye, organizasyon büyüklüğüne, sektöre, siber saldırı türüne ve bir organizasyonun güvenlik durumunun olgunluğuna ve etkinliğine göre değişkenlik göstermektedir. Saldırıların sıklığı da siber suçun maliyetini belirleyen bir etkendir (Sarder ve Haschak, 2019:5).

İş yaşamındaki teknolojik uygulamaların yaygın kullanımına yönelik yaşanan artışlar siber saldırı oranlarını gün geçtikte artırmaktadır. Hemen her gün bilişim korsanları kritik verilere erişmeyi veya hizmetleri aksatmayı amaçlayarak büyük ve küçük işletmeleri hedef almaktadırlar. Saldırılar sonrasında işletmelerin hassas kullanıcı verileri yok edilmekte ve bu durum mali işlemler ve kuruluş itibarı açısından kalıcı hasarlar bırakmaktadır. Değişen teknolojik dünya, etkili bir siber güvenlik planının uygulanmasını zorunlu hale getirmektedir (Solfa, 2022:20). Günümüz iş dünyasında faaliyet gösteren çok sayıda işletme veya kuruluş artık siber güvenliğe yatırım yapmanın zorunlu olduğunu fark etmiş durumdadır. Özellikle tedarik zincirleri ve finansal ağlar aracılığıyla işletmelerin birbirine bağlılığı sonucu, bir paydaşın siber güvenlik yatırımları açısından aldığı kararlar diğer paydaşların siber güvenliğini etkileyebilmektedir (Colajanni vd., 2018:1444).

3.3. Siber Güvenlik Yatırımları

Siber güvenlik yatırımlarında amaç, uygulamada başarı sağlayacak alternatifleri değerlendirmek ve işletmeler, tedarik zincirleri veya finansal ağlar açısından en uygun seçenek kombinasyonunun uygulanmasıdır. Siber güvenlik alanının yeni gelişme göstermesi yapılacak yatırımların başarısını ve etkinliğini zorlaştırdığı bilinmektedir. Bu sebeple siber güvenlik sistemi alternatiflerinin ayrıntılı fizibilite çalışmaları önemli bir unsura dönüşmektedir (Melnyk vd., 2022:172). Yatırım kararlarını iyi bir şekilde belirlemek, siber güvenlikle ilgili önemli bir ilgi alanı olarak ortaya çıkmaktadır. Küresel ticaret ağlarının birbiri ile bağlantılı birçok işletmeden oluşması ve her paydaşın maruz kalacağı risklerin zincirin tamamını nasıl etkileyeceği önemli bir zorluk olarak görülmektedir. Dijital olarak kurulmuş olan ağlardaki paydaşların her birinin kendine ait güvenlik sistemlerine sahip olmaları yeterli olmayıp, zincirin tamamının bir bütün olarak güvenceye alınması beklenmektedir. Bu durum siber güvelik yatırımlarını koordinasyon gerektiren bütüncül bir hale taşımaktadır. Aksi durumda yetersiz ya da gereksiz yatırım yapma ihtimalleri ortaya çıkmaktadır. Siber güvenlik yatırımları için yönetimsel açıdan dikkate alınacak iç görüler aşağıdaki gibi özetlenebilir (Li ve Xu, 2021:1217).

(1) Risk yayılımı perspektifinden bakıldığında, bağlantılı tüm paydaşlar zincirin en zayıf halkası kadar güçlüdür, bu nedenle tüm paydaşların güvenlik açıkları dikkate alınmalıdır.

(2) Tedarik zincirlerini meydana getiren tüm paydaşlar, güvenlik açığı arttığında siber güvenlik yatırımlarını uygun şekilde artırmaları gerekmektedir. Ancak, çok daha büyük bir güvenlik açığı mevcut yatırımının yetersiz kalmasına yol açacaktır. Bu nedenle firmaların sistemlerin yapısını ve donanım yapılandırmasını yeniden tasarlamaları gerekir.

(3) Perakendeci ve tedarikçiler arasındaki karşılıklı bağımlı ilişki ne kadar yakınsa, paydaşların birbirine bağımlılığı ve bilgi paylaşım miktarı o düzeyde artış göstermektedir. Bu durum paydaşların sistemlerine giriş miktarlarının artıracağı için koordinasyon mekanizmalarının tasarlanması önemlidir.

(4) Ortak karar ve güvenlik riski telafisi, olumsuz dış müdahaleleri etkili bir şekilde azaltabilir ve tedarik zincirinin güvenlik seviyesini iyileştirebilir. Ancak, birbirine bağımlı firmalar arasındaki güvenlik bilgisi paylaşımı, paydaşların bedavacı davranışlarını artırabilir. Bu nedenle yatırımların dikkatli bir şekilde planlanması gerekmektedir.

Siber güvenlik sorunları artık sadece bilgi teknolojisi sorunları değildir. Geleneksel güvenlik uygulamalarıyla karşılaştırıldığında, varlıkları izleme ve güvence altına alma yeteneği manuel kontrollerin ötesindedir. Bu durum

artık organizasyonun en üst seviyesinde dikkatlice ele alınması gereken bir iş riskine dönüşmüş durumdadır (Hemanand ve Vallem, 2023:64). Siber risk ve saldırılara karşı sağlam stratejiler geliştirme ihtiyacı, tüm dünyada dijital dönüşüm süreciyle birlikte oldukça belirgin hale gelmiştir. Bu nedenle hem ekonomik büyüme hem de dijital dönüşüm açısından büyük potansiyele sahip ülkelerde endüstriyel tesislerin siber tehditlere karşı korunmasına yönelik strateji ve çözümlerin geliştirilmesine öncelik verilmelidir (Duran, 2024:758).

4. Lojistik Faaliyetlerde Siber Güvenlik

Lojistik yönetimi, malların, hizmetlerin ve bilgilerin üretim noktasından tüketim alanlarına kadar hareketini entegre eden yönetim sürecidir (Cheung ve Bell, 2021:473). Lojistik bir faaliyetler bütünü olarak bilgi, teknoloji ve insanların kesiştiği noktadadır. Lojistik iş süreçlerinin geleceği bilişim teknolojilerindeki gelişmelerle yakından ilişkilidir. Aynı zamanda bu süreçlerin bilişim dünyası ve siber uzaydaki güvenlik alanındaki gelişmelere yakından bağımlı olduğu söylenmelidir. Küresel ekonomik düzenin beklentilerini karşılayacak daha güçlü ve güvenilir bir lojistik sektörü yaratmak için, ortaya çıkabilecek teknoloji kaynaklı tehditleri azaltmak adına önlemlerin alınması gerekmektedir (Fitton vd., 2015:27).

Günümüzde lojistik faaliyetlerin yürütüldüğü tedarik zincirleri daha karmaşık ve küresel hale gelmiştir. Gerçekleştirilen iş süreçlerinin verimliliğini artırmak ve ağ içindeki tedarikçiler, üreticiler, dağıtımcılar ve hatta ulaşım hizmeti sağlayıcıları arasındaki iletişimi ve koordinasyonu desteklemek için artık giderek daha fazla bilgi teknolojisine ihtiyaç duyulmaktadır. Bu artan talep karşısında geliştirilen ve sistemlere entegre edilen bilişim teknolojileri uygun şekilde güvence altına alınmazsa, kuruluşların siber saldırılara karşı savunmasızlığı artacaktır (Latif vd., 2021:74). Lojistik yönetiminde siber güvenlik endişesi, hem siber alanı koruyabilecek hem de bir lojistik ağındaki tüm üyeler için lojistik performans artırabilecek kabiliyetlere sahip olunmasıdır (Cheung ve Bell, 2021:472).

Lojistik faaliyetlerin gerçekleştirildiği tedarik zincirleri, kuruluşlar için kritik öneme sahiptir ve temel prosedürler ile lojistik gereksinimlerinin karşılanmasını sağlamaktadır (Sobb vd., 2020:1). Tedarik zinciri içerisindeki tüm üyeler paylaşılan bilgi ve güvenlik düzenlemeleri açısından en zayıf paydaş kadar güçlü sayılmaktadırlar. Tedarik zinciri içinde eşgüdümle yürütülen faaliyetlere ilişkin siber saldırılar veya yazılım hataları, zincirdeki bilgi alışverişi yoluyla herhangi bir paydaşta bulunan güvenlik açıkları gibi birçok nedenden dolayı diğer ortak sistemlerini etkileyebilir. Zincir

içerisinde faaliyet gösteren kuruluşların geniş bir teknoloji yelpazesini koruması gerekirken, saldırganların yalnızca en zayıf halkayı belirlemesi yeterli olmaktadır. Ortaya çıkan bu yeni riskler etkili bir şekilde yönetilmeli ve azaltılmalıdır (Pandey vd., 2020:105).

Tedarik zincirindeki risk ihtiyaçları hakkında daha olgun bir anlayış edinmek için, dijital sistemlere ait risk eğilimlerinin sağlam bir temelinin geliştirilmesine ve bunların nasıl düzgün bir şekilde ölçülüp modellenebileceğine yönelik araştırmalar önem arz etmektedir. Zincirlerde yüksek düzeydeki belirsizlik nedeniyle her süreç ve karar incelenmeli ve hasar açısından sürekli olarak izlenmelidir (Barron vd., 2016:20). Tedarik zincirlerine yönelik siber saldırılar mevcut ekonomik hareketliliğin kesintiye uğraması ihtimalinden dolayı ciddi bir endişe konusudur. Bu saldırılar yıllar içinde önemli ölçüde artmış göstermiş ve yeni yöntemler ile gelişim sağlamıştır. Hâlihazırda kullanılan siber güvenlik stratejilerinin sınırlı düzeyde etkin olması, politika yapıcıların tedarik zincirlerindeki kesintileri sınırlamak için siber suçların artan tehdidini ele almak için yenilikçi yaklaşımlara yönelmesini zorunlu hale getirir (Afenyo ve Caesar, 2023:1).

4.1. Lojistik Faaliyetlere Yönelik Siber Saldırı Yöntemleri

Teknolojik entegrasyon iş süreçlerini, imalat üretkenliğini artırmaya ve hatta dağıtım maliyetlerini düşürmeye yardımcı olan en önemli unsurdur. Ancak, çeşitli tedarik zinciri paydaşları arasındaki artan karşılıklı bağımlılık, üçüncü taraf denetim mekanizmalarının eksikliği ve siber tehditler de dâhil olmak üzere birçok zorluk ortaya çıkarmaktadır. Bu nedenle, güvenlik duvarları ve saldırı tespit sistemleri aracılığıyla dikkatli izleme yapılması gerekmektedir (Latif vd., 2021:50). Lojistik faaliyetlerin yürütülmesi sırasında dijitalleştirilmiş tedarik zincirlerine yönelik en yaygın siber saldırı yöntemleri aşağıdaki gibi özetlenebilir (Pandey vd., 2020:110):

1. Parola koklama veya kırma: Kullanıcı adlarını ya da şifrelerini ele geçirmek amacıyla kullanılan en basit ve en yaygın saldırı yöntemlerinden biridir. Geliştirilmiş yazılım paketleri aracılığıyla gerçekleştirilir. Yazılım veya hizmetler, bilgisayar korsanları tarafından parolaları elde etmek, sistemlere veya daha fazla kullanım için verilere erişmek için kullanılır.

2. Sahtecilik saldırıları: Bir kişi ya da yazılımın yasa dışı bir şekilde fayda elde etmek amacıyla, verileri çarpıtması sonucu başka bir kimlik olarak kendini tanımladığı durumdur. Web sahteciliği, bir saldırgan tarafından sahte bir web sitesinin kurulduğu başka bir sahtecilik türüdür.

3. Hizmet reddi saldırıları: Bu saldırılar başka bir kullanıcı tarafından gerçekleştirilen kötü niyetli bir eylem nedeniyle bir bilgisayara veya ağ

kaynağına erişimin kasıtlı olarak engellenmesi olarak tanımlanmaktadır. Veriler doğrudan veya kalıcı olarak zarar görmez ancak kaynakların kullanılabilirliği tehlikeye girer.

4. Doğrudan saldırı: Bilgisayar sisteminin direk ele geçirilerek bilgiler doğrudan bir saldırı sonucu yeniden yazılır veya çalınır. Bu saldırılarda genelde çevrimiçi hizmet sunan kuruluşlar hedef alınır. Saldırıya uğrayan kuruluş saldırıyı belirleyemezse doğrudan saldırılar tekrarlanır.

5. Kötü niyetli kurcalama: Verilerin kötü niyetli bir şeklide düzenlenmesi veya değiştirilmesi olarak tanımlanmaktadır. Tedarik zincirleri içerinde yer alan çok paydaşlı teknolojik iş süreçlerinin sahip olduğu daha az güvenlik kontrolü, saldırganların hassas verilere erişim elde etmesini kolaylaştırmaktadır.

6. İçeriden gelen tehdit: Bir organizasyon içerisinde siber güvenlik riski oluşturan kişiler içerden gelen tehdit olarak tanımlanmaktadır. Lojistik iş süreçlerinde istihdam edilen çalışanlardan kaynaklanan içeriden gelen tehditler, dijitalleşme ve küreselleşme olguları nedeniyle artış göstermektedir. Ayrıca bu tehditlerin harici tehditlere nazaran denetlenmesi daha zor hale gelmiştir.

Son yıllarda lojistik sektörüne yönelik üst düzey siber saldırılarda artan bir eğilim olduğu bilinmektedir. Yaşanan birçok siber müdahale sektörün bu saldırılara karşı savunmasızlığını ortaya koymaktadır (Bhattacharjya vd., 20121:2). Lojistik iş ve işlemlerinin yürütüldüğü operasyonel sistemlere yönelik siber saldırılar sonucu fiziksel demiryolu sistemlerinin kesintiye uğraması veya kullanılamaması, yük ve yolcu bilgi kontrollerinin yapıldığı veri tabanlarının bloke edilmesi gibi kısıtlamalar meydana gelmektedir. Denizyolu taşımacılığını etkileyen siber olaylar navigasyon, kargo kontrolü ve diğer endüstriyel süreçleri etkileyebilmektedir. Bunun sonucunda insanların hayatları, çevre ve ticarete konu mülkler tehdit altına girerek, ticari faaliyetlerde önemli aksaklıklar yaşanmaktadır. Ulaşım sistemlerindeki kesintiler, soğutmalı konteynerler ve acil durum sistemleri için sıcaklık kontrolünü etkileyebilmektedir. Bir çekme köprüyü kaldırma, trafik ışıklarını kontrol etme ve gemilere yakıt ve sıvı kargo teslimatı için pompaları, vanaları ve boru hatlarını kontrol etme gibi müdahaleler lojistik operasyonları sekteye uğratmaktadır. Kara, hava, demir yolu, transit ve deniz ulaşım altyapı sistemlerinin tümü, sistem operasyonlarını ve veri gizliliğini etkileme potansiyeline sahip çeşitli siber risklerle karşı karşıyadır (Tonn vd., 2019:112). Bu tür ihlaller dakikalar veya saatler içinde gerçekleştirilebilir, ancak tespit edilmesi ve kontrol altına alınması aylar veya yıllar alabilir. Saldırılar, lojistik, üretim ve operasyonlarda büyük kesintilere ve veri kaybına

neden olabilir. Operasyonlarda kesinti, tedarik zincirindeki birkaç şirket için orijinal operasyon durumuna dönmek için ek maliyetlere yol açmaktadır. Tedarikçilere yönelik saldırılar, operasyonları kesintiye uğratarak tüm tedarik zinciri üzerinde kademeli olumsuz bir etkiye neden olabilir. Siber saldırılar gecikmelere ek olarak, mevcut envanter eksikliğine ve kesintiyi karşılamak için hızlandırılmış nakliye ihtiyaçlarından kaynaklanan maliyetlere yol açabilir. Bir tedarik zinciri düğümüne yapılan saldırı, bir şirket için fikri mülkiyet kaybına veya son müşterilere yönelik hizmet seviyelerinde bir azalmaya da neden olabilir (Simon ve Omar, 2020:162).

4.2. Lojistik İş Süreçlerine Yönelik Siber Tehditler

İşletmeler tedarik zinciri operasyonlarını kolaylaştırmak için giderek daha fazla dijital teknolojiye güvendikçe, dijital tedarik zincirinin birbirine bağlı yapısı, siber tehditler tarafından istismar edilebilecek çok sayıda güvenlik açığı ortaya çıkarmaktadır. Dijital tedarik zincirini güvence altına almak, hassas bilgilerin bütünlüğünü ve gizliliğini korumak, operasyonların sürekliliğini sağlamak ve tedarik zinciri ekosisteminin genel dayanıklılığını korumak için çok önemlidir. Siber saldırıların artan sıklığı ve karmaşıklığıyla, lojistik sektöründeki kuruluşlar dijital varlıklarını korumak ve modern iş ortamında rekabet avantajını sürdürmek için proaktif olarak sağlam siber güvenlik önlemleri uygulamalıdır. Lojistik sektörü, operasyonlarının karmaşık ve dinamik yapısı nedeniyle benzersiz siber güvenlik zorluklarıyla karşı karşıyadır (Odimarha vd., 2024:27). Geniş ve birbirine bağlı dijital tedarik zinciri içerisinde faaliyet gösteren lojistik sektörü, çok etkili sonuçları olabilecek bir dizi siber güvenlik tehdidine karşı savunmasız kalabilmektedir. Bu tehditleri anlamak, etkili güvenlik önlemleri geliştirmek olmazsa olmazdır. Lojistik şirketlerinin bilgi yönetimi için kullandığı dijital uygulamalar ve uygulamaların getirdiği siber tehditler aşağıda özetlenmiştir.

4.2.1. Lojistikte Kullanılan Dijital Teknolojilere Yönelik Tehditler

Dördüncü sanayi devrimi ile birlikte iş ve sosyal hayatın kolaylaşmasına büyük katkılar sunan dijital teknolojiler, lojistik yönetimi iş süreçlerine büyük faydalar sunmuş ve bir paradigma değişimi meydana getirmiştir. Bu faydalarının yanında güvenlik konusunda bazı yeni tehditlerin oluşması doğal bir sonuç olarak ortaya çıkmaktadır. Lojistik sektöründe kullanılan ve siber tehditlere maruz kalabilecek teknolojiler aşağıda kısaca açıklanmıştır.

4.2.1.1. Nesnelerin İnterneti

Nesnelerin İnterneti alanındaki gelişmeler, ağ ekonomisinin gelişimini büyük ölçüde desteklemenin yanında benzeri görülmemiş siber güvenlik

sorunlarının da önünü açmıştır (Li ve Xu, 2021:1216). Diğer bir deyişle, Nesnelerin İnterneti siber saldırılar için olası müdahale noktalarını daha da genişletmiştir (Colajanni vd., 2018:1444). Nesnelerin İnterneti sayesinde cihazlar ve nesneler dijital ortamlara daha fazla bağlandıkça, lojistik sektörü saldırılara daha fazla maruz kalmaya başlamıştır. Saldırganlar, hassas verilere yetkisiz erişim elde etmek, operasyonları aksatmak veya fiziksel hasar vermek için lojistik tabanlı veri alışverişindeki siber güvenlik açıklarından yararlanabilmektedir (Alzahrani ve Asghar, 2024:2). Nesnelerin İnterneti kullanımı sırasında oluşan zorluklar arasında standardizasyonlar, güvenlik sorunları ve veri sızıntısı riskleri yer almaktadır. Bağlantıların güvenlik kısıtlamaları, taktiksel değerlendirmeler ve ağ kesintileri gibi her yerde bulunan internet bağlantılarına yönelik engeller, operasyonların yürütülmesini ciddi şekilde aksatma potansiyeline sahiptir. Bilgilerin gizliliği ve bilgilerin yetkisiz bir şekilde ele geçirilmesi potansiyeli önemli bir risk meydana getirmektedir (Sobb vd., 2020:16).

Nesnelerin İnterneti ile birlikte birçok cihazın ve nesnenin birbiriyle etkileşim sağlaması ve korunması gereken hassas veriler toplaması, tüm cihaz ve nesneler arasındaki iletişim ve toplanan verilerin güvence altına alınması gerekliliğini ortaya çıkarmaktadır. Bu gerekliliğin önemi her geçen gün artmaktadır (Karaarslan ve Akbaş, 2017:19). Lojistik sektörü, verileri toplamak, siparişleri işlemek ve malzemeleri ve/veya ürünleri teslim etmek için giderek daha fazla Nesnelerin İnterneti'ni, sensörleri ve aktüatörleri kullanmaktadır. Bu dijital otomasyon ekipmanları, siparişleri işlemedeki insan hatalarını azaltmakta ve sipariş teslimatlarındaki verimliliği artırmaktadır. Ancak bu durum siber uzay ve internet üzerinden gelen kötü niyetli saldırılar tarafından kullanılamaz hale getirilerek kesintiye uğratılabilir. Bunun sonucunda siber uzaydan gelen kötü niyetli saldırılara karşı varlıkların korunması konusunda endişe yaratmaktadır (Cheung ve Bell, 2021:472).

4.2.1.2. Siber Fiziksel Sistemler

Siber Fiziksel Sistemler fiziksel bileşenler, ağ sistemleri, gömülü bilgisayarlar, yazılımlar ve bilgi paylaşımı amacıyla cihazların ve sensörlerin birbirine bağlanması gibi eksiksiz bir sistemi oluşturan dijital ve fiziksel süreçlerin entegrasyonudur. Siber Fiziksel Sistemler akıllı, otonom teknolojileri kullanarak üretim ve tedarik zinciri süreçleri boyunca dijital yetenekleri geliştirmeyi ve bağlı cihazlarda devrim niteliğinde değişiklikler yapmayı planlamaktadır. Bu gelişimlerin yanında sektörün hazırlıksız olduğu yeni siber riskler de süreçle birlikte ortaya çıkmaktadır. Bu riskler arasında var olan tehditlere ilişkin bilgi, üçüncü parti işletmelerin denetiminde

yaşanan başarısızlıklar ve güvenlik kontrollerinin yetersizliği olarak ortaya çıkmaktadır (Pandey vd., 2020:105).

Lojistik ve tedarik zinciri iş süreçlerinde Siber Fiziksel Sistemler, fiziksel bileşenler, ağ sistemleri, gömülü bilgisayarlar, yazılımlar ve bilgi paylaşımı için cihazların ve sensörlerin birbirine bağlanması ile fiziksel sistemin dijital ortamda takibini mümkün kılan önemli bir teknolojidir. Siber fiziksel sistemler siber saldırılar, yazılım hataları veya herhangi bir zincir ortağındaki güvenlik açıkları gibi birçok nedenden dolayı tehditlere maruz kalmaktadırlar (Ofori ve İslam, 2019:2).

Siber Fiziksel Sistemlerin kritik altyapı ve operasyonel uygulamalarla ilgili bütün siber-fiziksel bağlantıları bünyesinde barındırması siber güvenlik açısından çok sayıda dezavantaja sebep olmaktadır. Özellikle güncelleme yapma süreçlerinin zorluğu, iş akış sistemlerinde değişim yapmanın zorluğu ve bu sistemlerin kritik doğasından kaynaklı saldırı etkisini potansiyel olarak artırma dezavantajları öncelikli zorluklar olarak karşımıza çıkmaktadır. Lojistik ve tedarik zinciri iş süreçlerindeki Siber Fiziksel Sistemlere yönelik tehditlere örnek ulaşım ağlarına yönelik solucan saldırılar, izleme sinyallerinin engellenmesi ve üretim sırasında yazılım bütünlüğünün tehlikeye atılması verilebilir. Saldırıların özellikle lojistik ve tedarik zinciri yönetimi alanlarında faaliyet gösteren sistemler üzerinde önemli düzeyde etkiye sahip olduğu bilinmektedir. İnsansız hava araçları ve yarı otonom sistemler siber saldırı için saldırı yüzeyleri sunabilmekte ve gelecekteki depoların büyük ölçüde robotik olması sebebiyle siber tehditlerle daha çok karşı karşıya kalabileceği düşünülmektedir. Artmaya devam eden siber tehditler ve saldırılar sonucu yarı veya tam otomatik tedarik zinciri sistemlerinde meydana gelen aksamaların maliyetli olacağı ve onarımlarının önemli ölçüde zaman alacağı unutulmamalıdır (Sobb vd., 2020:17).

4.2.1.3. Bulut Bilişim Teknolojileri

Bulut Bilişim Sistemleri tüm verilerin istenilen zamanda ve istenilen yerde internet bağlantısı kullanılarak depolanmasını ve erişime sunulmasını sağlayan teknolojilerdir. Lojistik sektöründe Bulut Bilişim Teknolojilerinin kullanılmasıyla birlikte üretim, bilgi, süreç optimizasyonu, envanter yönetimi, navigasyon, akıllı depolama sistemleri ve performans değerlendirme faaliyetlerinde önemli düzeyde maliyet tasarrufları sağlanmıştır (Cengiz, 2021: 124). Bulut Bilişim Teknolojileri, tedarik zincirlerinin doğasına uygun bir uygulama olması nedeniyle lojistik iş süreçlerinde artan şekilde talep görmekte ve benimsenmektedir. Küresel iletişim ve ağ hizmetlerinin sorunsuz çalışmasına önemli katkılar sunan bu teknolojiler dijital çağın

önemli sistemlerinden biridir. Bulut Bilişimin sektörel kullanımları hızla artmakta ve bazı riskleri de beraberinde getirmektedir (Boyes, 2015:33).

Birçok web tedarik yönetimi için hayati önem taşıdığı bilinen Bulut Bilişim Sistemlerine yetkisiz girilebilmesi, diğer kurumsal sistemlere daha hızlı giriş imkanı sunacak bilgilere erişim sağlamayı kolaylaştırmaktadır. Modern dinamik ağlar, yeni güvenlik riskleri yaratan ve kontrol olasılığını azaltan daha fazla saldırı fırsatı sunmaktadır. Sayılan bu risklerin ana kaynağı bulut teknolojisidir (Boiko vd., 2019:69). Bulut bilişim sistemlerinde risk oluşturan güvenlik açıkları vardır; bunlar arasında; hizmet kararlılığı sorunları, bellek ayırma hataları, ağ bağlantı sorunları, sunucu yönetim sorunları, kimlik doğrulama sorunları ve hizmet reddi saldırılarıdır. Bulut sistemleri, son derece sanallaştırılmış bir ortamda birden fazla ana bilgisayardan önemli veri rezervlerinin birleştirilmesini içerdiğinden, kimlik yönetimi sağlayıcılar için önemli bir sorumluluk haline gelmektedir. Bulutlar, kaynak paylaşımını etkili bir şekilde yapmak için çok kullanıcılı sistemlere dayanmaktadır. Bu da farklı kullanıcıların donanım düzeyinde ayrılmadığı anlamına gelmektedir. Çoklu kiracılık, kaynak paylaşım tahsisleri değiştiğinde veri kalıcılığı yoluyla bilgi ihlal edilebileceği ve ifşa edilebileceği için gizlilik tehditleri doğurabilmektedir. Bulut hizmetleri, değişen kaynak gereksinimleri için bir miktar esnekliğe sahip olsa da hizmet reddi saldırılarına karşı bağışıklık sağlamamaktadır (Sobb vd., 2020:15).

4.2.1.4. Blok Zinciri Teknolojileri

Blok zinciri, verilerin kalıcı kayıtlarını tutabilen dağıtılmış bir defter olarak düşünülebilir. Saklanan veri kümeleri, ilgili üyelerin çoğunluğunun izni olmadan silinemediği veya değiştirilemediği için blok zinciri güvenli bir teknolojidir. Lojistik operasyon yönetiminde blok zinciri teknolojilerinin kullanımı iş süreçlerinin şeffaflığı ve ürün izlenebilirliği konularında önemli katkılar sunmaktadır (Choi vd., 2019:179). Dijitalleşen lojistik iş süreçlerindeki kurcalamaya dayanıklı kimlik doğrulama hizmetleri ve işlemlerin doğrulanmasını sağlamak amacıyla blok zinciri ve şifreleme şemaları konsepti benimsenmektedir (Bhattacharjya vd., 20121:6). Blok zinciri teknolojilerinin lojistik ve tedarik zinciri süreçleri için büyük değere sahip olduğu ve siber güvenlikle ilgili kurulacak sistemlerde faydalanılması gereken önemli bir teknoloji olduğu bilinmektedir (Markov ve Vitliemov, 2020:6). Blok zincir teknolojilerinin uygulanmasında, veri gizliliği, operasyonel dayanıklılık ve sistemlerin yönetimi gibi bazı zorluklar vardır. Eski sistemlerden blok zincirlere uygulama geçişi yapmak, organizasyonel tembelliğe yol açabilmektedir. Bu durumlarda maliyet-fayda analizi fayda sağlayabilecek bir araç olarak görülmektedir. Blok zincirin merkezi olmayan

yapısı, operasyon yüküyle birleştiğinde, tüm kullanım durumlarına uygun değildir. Ek olarak, blok zincirin bazı kötü amaçlı saldırılara karşı savunma tasarımı bulunmaktadır ancak her zaman siber risklerin var olabileceği unutulmamalıdır. Kimlik hırsızlığı ve programlama kodlarının hacklenmesi gibi saldırılar, blok zincir süreçlerinin bütünlüğü için risk oluşturmaktadır (Sobb vd., 2020:18).

4.2.1.5. Yapay Zeka Teknolojileri

Lojistik ve tedarik zinciri süreçlerinde sinir ağlarının doğrulanması ve incelenmesiyle ilgili makine öğrenimi uygulamalarına yönelik güvenlik açıkları bulunmaktadır. Doğrulama ve onaylama, yapay sinir ağlarında doğruluk ve güvenilirliği sağlamak için kullanılan birincil araçları temsil etmektedir. Karmaşık yapay zekâ sistemleri ile çalışmak, kullanıcıların uygulamayı tam olarak anlayamadığı ve güven sorunları ortaya çıkaran süreçlere sebep olmaktadır. Siber güvenlik sistemlerinin kurulması ve işletilmesi süreçlerinde yapay zeka hem güvenceye alınması gereken bir uygulama iken hem de siber saldırılarla mücadelede etkin kullanılması gereken bir teknoloji olarak karşımıza çıkmaktadır (Sobb vd., 2020:22).

4.3. Siber Saldırılara Yönelik Önlemler

Lojistik şirketlerinin siber saldırı riskini azaltmak için değerlendirebilecekleri birçok adım vardır. Operasyonlarına herhangi bir yeni teknoloji uygulamadan önce, güvenlik özelliklerini değerlendirebilir ve risklerini göz önünde bulundurabilirler. Teknoloji sağlayıcıları, şirketlere belirli sistemler için gereken güvenlik önlemleri konusunda tavsiyelerde bulunabilir. Siber güvenliğin yerinde olduğundan emin olmak için personel eğitimi yapılması da güvenli operasyonlar için etkilidir. Bununla birlikte, alınan güvenlik önlemlerinin güvenlik ihlallerini önlemek için yeterli olduğunun garantisi olmadığından bir geri dönüş planı da hazırlanmış olmalıdır. Siber saldırı risk değerlendirmesi ve güvenlik planlarının eksikliği sistemleri savunmasız hale getirerek lojistik operasyonlarını daha da tehlikeye atacağı kesinlikle unutulmamalıdır (Jagtap vd., 2020:8).

Lojistik ve tedarik zincirlerini yönetmede siber güvenliği artırmak için, ulaştırma ve lojistik sektöründeki uygulayıcılar üç aşamalı bir yaklaşım benimseyebilir. Bunlar önleyici planlama aşaması, gerçek zamanlı kurtarma planlama aşaması ve süreç sonrasına yönelik planlama aşaması. Her aşamada, uygulayıcılar güvenlik kurulunun kararlarıyla uyumlu güvenlik önlemlerini seçebilirler. Siber saldırılarla ilgili olarak önlemlerin niteliğine göre üç kategoriye ayrılmıştır (Bhattacharjya vd., 20121:5):

1. Proaktif önlemler: Bir siber saldırının meydana gelmesinden önce uygulanan savunma eylem planlarıdır. Bu planlar siber uzaydan gelecek bilinen saldırılara karşı bir koruma duvarı görevi görecektir.

2. Gerçek zamanlı kurtarma önlemleri: Bir siber saldırı sırasında uygulanan savunma eylem planlarıdır. Gerçek zamanlı kurtarma önlemleri, ilk adımla önlenemeyen saldırılardan kaynaklanan hasarı hafifletir. Gerçek zamanlı kurtarma önlemlerinin uygulanması, tehlikeye atılmış bir ağı/sistemi kabul edilebilir bir işlevsel duruma getirmeyi amaçlamaktadır.

3. Sonrasına yönelik önlemler: Bir siber saldırıdan sonra uygulanan eylem planlarıdır. Üçüncü kategori yalnızca kurtarma önlemlerini değil, aynı zamanda bir saldırıdan sonra ağın/sistemin dayanıklılığını artıran önlemleri ve tüm sistemi siber saldırılara karşı daha dirençli hale getiren iyileştirme önlemlerini de içermektedir.

5. Sonuç

Lojistik iş süreçlerinin başarısı, tedarik zinciri içindeki tüm paydaşların birlikte hareketi ve amaç bütünlüğüne dayalı bir operasyon yönetimine bağlıdır. Bunun sağlanabilmesi için tüm sistemin görünürlüğünü sağlayacak bilgi ve iletişim ağlarının kurulması önemli bir gerekliliktir. Bu sebeple bilgi yönetimi, lojistiğin en önemli unsurlarından birine dönüşmektedir. Bilginin daha etkin kullanılmasına yönelik çabalar devam ederken geliştirilen yeni dijital teknolojiler sektör için birçok iş sürecine çok önemli katkılar sunmuştur. Tüm zincir içerisinde bilgiye anlık ulaşım ve süreçlere insansız müdahale imkânları sağlayan dijital teknolojiler lojistikte dijitalleşmenin önünü açmıştır. Bu önemli faydaların yanında süreçlerin dijitalleşmesi ile birlikte, sistemlerin dışarıdan müdahalelere açık hale gelmesi ise sürecin doğal bir sonucu olarak karşımıza çıkmaktadır. Bu müdahalelere karşı alınacak önlemler ve sistemin korunması amacı, siber güvenliğin ortaya çıkmasını sağlamıştır. Yeni ekonomi düzeni içerisinde ortaya çıkan bu kavram süreçlerin devamlılığı ve işlerin istenen başarı düzeylerine ulaşmasını sağlayacak gereksinimler arasına girmiştir. Lojistik ve tedarik zinciri faaliyetlerinde bugün ve gelecekte sürekli olarak gündemde tutulması gereken ve gerekli önlemlerin göz ardı edilmeden yerine getirilmesi beklenen ana unsurlardan biri artık siber güvenliktir. İş süreçlerinin iyileştirilmesi, operasyonların yüksek verimlilikle gerçekleştirilmesi ve hata, kayıp, hasar oranlarının düşürülmesi lojistik sektörü için ne kadar önemli ise siber güvenlikte o düzeyde önemlidir. Bu sebeple lojistik faaliyet gösteren işletmelerde siber güvenlik ihlallerine yönelik alınması gereken önlemlerin dikkatli bir şekilde belirlenmesi, kurulu bilgi sistemlerinin güvenliğini sağlayacak sistemlerin kurulması ve tüm kurum içerisinde siber güvenlik farkındalığının artırılması önem arz etmektedir.

Kaynaklar

Afenyo, M., & Caesar, L. D. (2023). Maritime cybersecurity threats: Gaps and directions for future research. *Ocean & Coastal Management*, *236*, 106493.

Alzahrani, A., & Asghar, M. Z. (2024). Cyber vulnerabilities detection system in logistics-based IoT data exchange. *Egyptian Informatics Journal*, *25*, 100448.

Barron, S., Cho, Y. M., Hua, A., Norcross, W., Voigt, J., & Haimes, Y. (2016, April). Systems-based cyber security in the supply chain. In *2016 IEEE systems and information engineering design symposium (SIEDS)* (pp. 20-25). IEEE.

Bhattacharjya, J., Cheung, K. F., & Bell, M. G. (2021). Cybersecurity in logistics and supply chain management: An overview and future research directions. *Transportation Research Part E: Logistics and Transportation Review*, *146*, 102217.

Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia computer science*, *149*, 65-70.

Boyes, H. (2015). Cybersecurity and cyber-resilient supply chains. *Technology Innovation Management Review*, *5*(4), 28.

Cengiz, Ö. (2021). *Lojistik 4.0 Türkiye Lojistik Sektörü Durum Analizi*. Siyasal Kitabevi: Ankara.

Cheung, K. F., & Bell, M. G. (2021). Attacker–defender model against quantal response adversaries for cyber security in logistics management: An introductory study. *European Journal of Operational Research*, *291*(2), 471-481.

Choi, T. M., Wen, X., Sun, X., & Chung, S. H. (2019). The mean-variance approach for global supply chain risk analysis with air logistics in the blockchain technology era. *Transportation Research Part E: Logistics and Transportation Review*, *127*, 178-191.

Colajanni, G., Daniele, P., & Sciacca, D. (2020). A projected dynamic system associated with a cybersecurity investment model with budget constraints and fixed demands. *J. Nonlinear Var. Anal*, *4*(1), 45-61.

Colajanni, G., Daniele, P., Giuffrè, S., & Nagurney, A. (2018). Cybersecurity investments with nonlinear budget constraints and conservation laws: variational equilibrium, marginal expected utilities, and lagrange multipliers. *International Transactions in Operational Research*, *25*(5), 1443-1464.

Çelik, R. (2020). Lojistik sektöründe kullanılan yeni bilişim sistemleri: Lojistik 4.0 örneği. *Balkan & Near Eastern Journal of Social Sciences (BNEJSS)*, *6*(4).

Doğrul, M., & Erğurum, A. (2021). Blok zincirinin (blockchaın) literatür büyümesi ışığında yeni siber güvenlik arayışları. *Güvenlik Bilimleri Dergisi*, *10*(3), 175-194.

Duran, Z. (2024). Endüstri 5.0'a geçişte siber güvenlik: Yeni sanayileşen ülkeler üzerine bir inceleme. *Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Dergisi*, *25*(3), 745-760.

Fitton, O., Prince, D., Germond, B., & Lacy, M. (2015). The future of maritime cyber security. *Lancaster University*, 8.

Golpîra, H., Khan, S. A. R., & Safaeipour, S. (2021). A review of logistics internet-of-things: Current trends and scope for future research. *Journal of Industrial Information Integration*, *22*, 100194.

Gonaygunta, H. (2023). Machine learning algorithms for detection of cyber threats using logistic regression. *International Journal of Smart Sensor and Adhoc Network. Department of Information Technology, University of the Cumberlands*. 36–42.

Heierhoff, S., Hoffmann, N. (2022). Cyber Security vs. Digital Innovation: A Trade-off for Logistics Companies?. In Proceedings of the 55th Hawaii International Conference on System Sciences.

Hemanand, D., & Vallem, R. R. (2023). Cyber security system based on machine learning using logistic decision support vector. *Mesopotamian Journal of CyberSecurity*, *2023*, 64-72.

Jagtap, S., Bader, F., Garcia-Garcia, G., Trollman, H., Fadiji, T., & Salonitis, K. (2020). Food logistics 4.0: Opportunities and challenges. *Logistics*, *5*(1), 2.

Karaarslan, E., & Akbaş, M. F. (2017). Blokzinciri tabanli siber güvenlik sistemleri. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *3*(2), 16-21.

Kişman, Z. A., & Güleç, Ö. (2021). Uluslararası ilişkiler açısından siber güvenlik ve NATO'nun siber güvenlik stratejileri. *Akademik Açı*, *1*(1), 127-154.

Latif, M. N. A., Aziz, N. A. A., Hussin, N. S. N., & Aziz, Z. A. (2021). Cyber security in supply chain management: A systematic review. *LogForum*, *17*(1), 49-57.

Li, Y., & Xu, L. (2021). Cybersecurity investments in a two-echelon supply chain with third-party risk propagation. *International Journal of Production Research*, *59*(4), 1216-1238.

Markov, K., & Vitliemov, P. (2020). Logistics 4.0 and supply chain 4.0 in the automotive industry. In *IOP conference series: Materials Science and Engineering*,Vol. 878, No. 1, p. 012047).

Melnyk, S. A., Schoenherr, T., Speier-Pero, C., Peters, C., Chang, J. F., & Friday, D. (2022). New challenges in supply chain management: cybersecurity across the supply chain. *International Journal of Production Research*, *60*(1), 162-183.

Norman, D., Bhargava, N., Harmon, M., Wright, J., Springs, D., & Dawson, M. (2020). Supply chain and logistics management and an open door policy concerning cyber security introduction. *International Journal of Management*, *9*(1), 1-10.

Odimarha, A. C., Ayodeji, S. A., & Abaku, E. A. (2024). Securing the digital supply chain: Cybersecurity best practices for logistics and shipping companies,'. *World Journal of Advanced Science and Technology*, *5*(1), 026-030.

Pan, S., Trentesaux, D., McFarlane, D., Montreuil, B., Ballot, E., & Huang, G. Q. (2021). Digital interoperability in logistics and supply chain management: state-of-the-art and research avenues towards Physical Internet. *Computers in industry*, *128*, 103435.

Pandey, S., Singh, R. K., Gunasekaran, A., & Kaushik, A. (2020). Cyber security risks in globalized supply chains: conceptual framework. *Journal of Global Operations and Strategic Sourcing*, *13*(1), 103-128.

Parker, S., Wu, Z., & Christofides, P. D. (2023). Cybersecurity in process control, operations, and supply chain. *Computers & Chemical Engineering*, *171*, 108169.

Radanliev, P., De Roure, D., Page, K., Nurse, J. R., Mantilla Montalvo, R., Santos, O., & Burnap, P. (2020). Cyber risk at the edge: current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains. *Cybersecurity*, *3*, 1-21.

Sarder, M. D., & Haschak, M. (2019). Cyber security and its implication on material handling and logistics. *College-Industry Council on Material Handling Education*, *1*(1), 1-18.

Simon, J., & Omar, A. (2020). Cybersecurity investments in the supply chain: Coordination and a strategic attacker. *European Journal of Operational Research*, *282*(1), 161-171.

Sobb, T., Turnbull, B., & Moustafa, N. (2020). Supply chain 4.0: A survey of cyber security challenges, solutions and future directions. *Electronics*, *9*(11), 1864.

Solfa, F. D. G. (2022). Impacts of cyber security and supply chain risk on digital operations: evidence from the pharmaceutical industry. *International Journal of Technology Innovation and Management (IJTIM)*, *2*(2), 18-32.

Syed, N. F., Shah, S. W., Trujillo-Rasua, R., & Doss, R. (2022). Traceability in supply chains: A Cyber security analysis. *Computers & Security*, *112*, 102536.

Talih, Ö., & Dönmez, E. (2024). Tedarik zincirine genel bakış: Akıllı tedarik zincirinde risk ve güvenlik. *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, *11*(2), 836-854.

Tonn, G., Kesan, J. P., Zhang, L., & Czajkowski, J. (2019). Cyber risk and insurance for transportation infrastructure. *Transport policy*, *79*, 103-114.

Yeboah-Ofori, A., & Islam, S. (2019). Cyber security threat modeling for supply chain organizational environments. *Future internet*, *11*(3), 63.