İNTERNET GÜVENLİĞİ FARKINDALIĞINDA OYUNLARIN ETKİSİ

By Fırat Yılmaz

WORD COUNT 3443
TIME SUBMITTED 04-NOV-2021 11:23PM
PAPER ID 78474813

İNTERNET GÜVENLİĞİ FARKINDALIĞINDA OYUNLARIN ETKİSİ

Fırat YILMAZ[1], 0000-0002-8751-7234, firat.yilmaz@meb.gov.tr
Dr. Öğr. Üyesi Aslıhan İSTANBULLU[2], 0000-0002-1778-859X,
aslihan.babur@amasya.edu.tr

[1] Amasya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar ve Öğretim Teknolojileri Eğitimi Anabilim Dalı [2] Amasya Üniversitesi

ÖZET

İnternet, kullanıcılarına farklı alanlarda, çeşitli olanaklar sunan siber bir dünyadır. Ekonomi ve teknolojinin gelişmesiyle birlikte internet hayatımızda çok önemli bir rol oynamaktadır. Yaşı ne olursa olsun tüm kullanıcılar internette zaman geçirirken çeşitli güvenlik risklerine maruz kalmaktadır. İnternet kullanıcılarının günlük yaşamlarında maruz kaldıkları bu riskleri ele almak için farklı terimler kullanılmaktadır. Siber güvenlik, çevrim içi güvenlik ve internet güvenliği, dijital dünyadaki güvenlik endişelerini gidermek için literatürde birbirinin yerine kullanılan kavramlardır. Kavramlar arasında siber güvenlik, internet güvenliği yerine yaygın olarak kullanılan bir terimdir. İnternet insanlara önemli kolaylıklar sağlasa da siber saldırılar da dâhil olmak üzere birçok güvenlik sorunu yaratır. Bu siber dünyanın imkânlarından zarar görmeden, "güvenli" biçimde faydalanmak için internet güvenliğinin sağlanması gereklidir.

İnsanların, özellikle de gençlerin çevrim dışı ortamdan çok çevrim içi ortamda yaşadığı bu dijital çağda, internet güvenliği alanında ilgiyi teşvik edecek daha iyi mekanizmalara ihtiyaç duyulmaktadır. Oyunlar internetteki mevcut ve ortaya çıkan güvenlik tehditleri hakkında farkındalığın oluşturulabileceği ideal bir araçtır. Yapılan araştırmalar siber güvenlik farkındalığı sağlamak amacıyla oyunların etkili olduğunu göstermiştir. Nitekim akademik kurum ve kuruluşlar, internet güvenlik farkındalığı kazandırmak amacıyla çeşitli oyunlar geliştirmektedir. Bu nedenle bu çalışmada, internet ya da siber güvenlik farkındalığında oyunların etkisini ortaya koymak amacıyla literatürde yer alan çalışmaların incelenmesi ve karşılaştırılması amaçlanmıştır. Bu kapsamda çalışmada, literatür taraması yöntemi kullanılarak derleme türünde bir araştırma yapılmıştır. Çalışmanın sonuçlarının internet güvenliği ve oyun alanında çalışma yapmak isteyen araştırmacılara katkı sağlayacağı düşünülmektedir.

Anahtar Kelimeler: *İnternet Güvenliği Farkındalığı, Siber Güvenlik, Oyun*

THE EFFECT OF GAMES ON INTERNET SAFETY AWARENESS

ABSTRACT

The internet is a cyber world that provides its users various opportunities in a different fields. While the development of the economy and technology, the Internet plays a very important role in our lives. All users, regardless of age, are exposed to various security risks while spending time on the internet. Different terms are used to address these risks that Internet users are exposed to in their daily lives. Cybersecurity, online security and internet security are interchangeable term in literature to addressed security concerns in digital world. Among the concepts, cyber security is a term commonly used instead of internet security. Although the Internet provides important conveniences to people, it creates many security problems, including cyber attacks. Internet security must be ensured in order to benefit from the opportunities of this cyber world "safely" without being harmed.

In this digital age where people, especially young people, live online rather than offline, better mechanisms are needed to stimulate interest in internet safety. Games are an ideal tool to raise awareness about current and emerging security threats on the Internet. Studies have shown that games are effective to provide cyber security awareness. As a matter of fact, academic institutions and organizations develop various games in order to raise awareness of internet security. Therefore, in this study, it is aimed to examine and compare the studies in the literature in order to reveal the effect of games on internet or cyber security awareness. In this context, a review type research was conducted using the literature review method. It is thought that the results of the study will contribute to researchers who want to work in the field of internet security and gaming.

Keywords: Internet Security Awareness, Cyber Security, Gaming

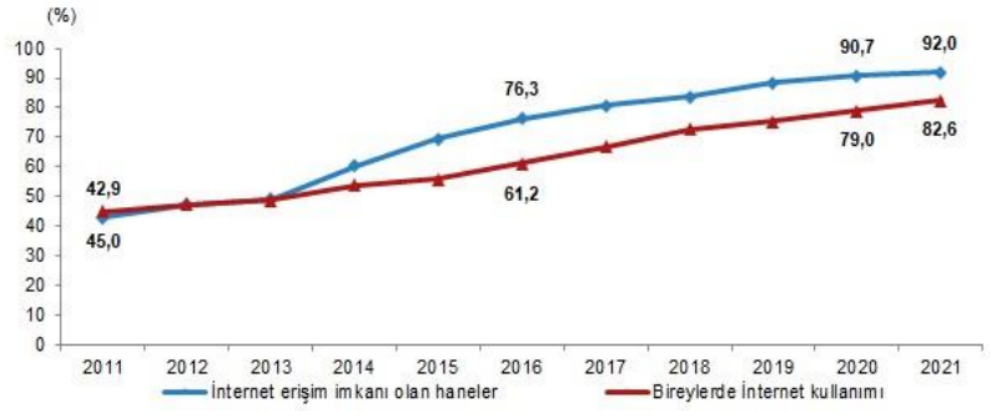
GİRİŞ

Nesnelerin interneti ile (Internet of Things) bilgisayar ve telefonların haricinde televizyonlardan, buzdolaplarına, çevrimiçi banka hesaplarımızın elektronik sağlık kayıtlarımızın hatta robot süpürgelerin internet ortamında birbirleriyle haberleşmeleri son kullanıcılar için kolaylık sağlarken, birbirine bağlı bu büyüyen dijital ayak izi, bir siber saldırı için uygun bir ortam oluşturmaktadır. Birbirine ne kadar çok cihaz bağlarsak, yaşanacak bir siber güvenlik tehdidinin boyutu da artmaktadır. Türkiye İstatistik Kurumu'nun (TÜİK) 2021 yılı verilerine göre Türkiye'de 2011 yılında %45 olan internet erişimi olan hane sayısı on yılda %47 artışla %92 seviyesine ulaşırken, 2011 yılında %42,9 olan bireylerde internet kullanımı yaklaşık %40 artış göstererek %82,6 seviyesine ulaşmış dünyada ve ülkemizde artan bu kullanıcı ve cihaz sayısı siber güvenlik tehditlerinin artmasına sebep olmaktadır (Türkiye İstatistik Kurumu [TÜİK], 2021). Burada dikkat edilmesi gereken en önemli husus gerekli kişisel internet güvenliği farkındalığı oluşturulmaması ve önlemlerin alınmaması sonucunda bu cihazların tehdidin ana kaynağı haline gelebilmesi, sadece cihaz sahibine değil internetin kendisine de tehdit haline gelmesidir. İnternet güvenliği (siber güvenlik

veya çevrim içi güvenlik) son yıllarda birçok araştırmanın konusu haline gelmiştir (Aslanyürek, 2016).

Şekil 1

2011-2021arasında İnternet erişim imkânı olan haneler ve bireylerde İnternet kullanımı



İnternet güvenliği (siber güvenlik) kapsamında ülkeler arasında küresel bir ilgi ve önem konusu haline gelmiştir. 50' den fazla ülke, siber uzayda, siber suçlarda ve siber güvenlikte olası saldırılara önlem almak amacıyla strateji belgeleri yayınlamıştır. Bu ihtiyaçtan ortaya çıkan siber güvenlik, küresel siber tehdit ortamını yönetmek için alanlar arası çözümler gerektiren, gelişmekte olan bir bilimsel disiplindir. Pandeminin de etkisiyle internet kullanıcı sayısındaki artış, sadece teknik personelin değil, tüm kullanıcıların internet güvenliğinden haberdar olması gerekliliğini ortaya koymaktadır. Literatürde sadece teknik personelin teknik güvenlik eğitiminin değil, aynı zamanda internet güvenliği farkındalık eğitimlerinin ve diğer farkındalık kampanyalarının herkes için "zorunluluk" haline geldiğini belirtmektedir. İnsanların siber güvenlik ihlallerinin çoğunun nihai kaynağı olduğu ve bu nedenle siber güvenlik zincirindeki en zayıf halka olduğu göz önüne alındığında, internet güvenliği hakkında farkındalık yaratılması gereklidir(Vaczi vd., 2020).

İnternet güvenliği eğitiminin amacı, teknoloji kullanıcılarının sosyal medya, sohbet, çevrimiçi oyun, e-posta ve anlık mesajlaşma gibi internet iletişim araçlarını kullanırken karşılaşabilecekleri potansiyel riskler konusunda eğitmektir (Rahman vd., 2020). Yaşanan güvenlik zafiyetlerinden sadece saldırıya uğrayan kullanıcılar değil internet ortamının yapısı ve işlevselliği de zarar görmektedir. Örneğin zararlı bir botnet yazılımı olan Mirai, 2016 yılından önce 100.000 IoT cihazını ele geçirerek bu cihazların işlem gücünü bir araya getirmeyi başarmıştır. Saldırganlar bilgi işlem gücü olarak zayıf bu 100.000 cihazın sayı avantajı sayesinde alan adı kayıt hizmetleri sağlayıcısı Dyn'i çökerten bir DDoS saldırısı başlattı. Cihaz sahiplerinin varsayılan fabrika kullanıcı adlarını ve parolalarını değiştirmemesi klasik bir güvenlik açığına sebep olmuş ve cihazların ele geçirilmesini kolaylaştırmıştır. Nihayetinde Mirai' nin esas yaratıcıları takibe alınarak hapse atıldı. Ancak Mirai hâlâ mutasyon geçirip tehdit olmaya devam etmektedir (Kaspersky, 2021).

Dünya genelinde internet güvenliğine yönelik yapılan yüksek harcama ve alınan önlemler siber saldırıları engellemede yetersiz kalmaktadır. Güvenlik teknolojilerinden ziyade sıradan kullanıcıların siber güvenlik ihlallerinin çoğunun nihai kaynağı olduğu tespit edilmiştir (Tuğal vd., 2021). Ciddi oyunlar ve oyun tabanlı öğrenme yaklaşımları, internet güvenliğini öğrenme ve eğitim için umut verici bir fırsat oluşturmaktadır. Oyunlar, stratejileri ve seçimleri analiz ederek çeşitli varlıklar arasındaki etkileşimlerle ilgilenen matematiksel modellerdir (Kakkad vd., 2019). Günümüz dünyasında oyunlar, çok yönlü doğası ve sayısız çatışma ve problemdeki uygulamaları nedeniyle eğitim, askeri, sağlık, ekonomi, sosyoloji, siyaset bilimi vb. alanlarda yaygın olarak kullanılmaktadır. Bu

makalede oyunların internet güvenliği ve siber güvenlik alanlarındaki uygulamaları tartışılmıştır.

YÖNTEM

Bu çalışmada literatür taraması yöntemi kullanılarak derleme türünde bir araştırma yapılmıştır. Literatür taraması belirli bir konudaki bilimsel kaynakların araştırılmasıdır. araştırmacılar tarafından daha önceden tamamlanan ve kayıt altına alınan tanımlanmış, değerlendirilmiş ve sentezi yapılmış verilerin incelenmesidir (Fink, 2009). Mevcut araştırmalardaki ilgili teorileri, yöntemleri ve boşlukları belirlemenize izin vererek mevcut bilgilere genel bir bakış sağlar. İyi bir literatür taraması sadece kaynakları özetlemek yerine konuyla ilgili bilgi durumunun net bir resmini vermek için analiz edilmesi, sentezlenmesi ve eleştirel olarak değerlendirilmesidir.

İNTERNET GÜVENLİĞİ VE SİBER GÜVENLİK

Siber güvenliği, bilgi güvenliğinin, özellikle dijital bilgi varlıklarının "Gizlilik" (confidentiality), "Bütünlük" (integrity) ve "Kullanılabilirlik" (availability), kapsamında bu tür varlıkların güvenliğinin ihlal edilmesinden kaynaklanabilecek herhangi bir tehdide karşı korumaya odaklanan bir parçası olarak tanımlanmaktadır. Siber güvenliğin uygulandığı ana alan olarak interneti kapsaması nedeniyle bazı tanımlar "internet bağlantılı bilgi sistemlerine" atıfta bulunmakta ve birbirlerinin yerine kullanılmaktadır (Von Solms ve von Solms, 2018). Bu yaklaşım internet ağındaki güvenlik açıklarının ve güvenlik tehditlerinin türlerinin tam olarak belirlenmesi, uygun karşı önlemlerin ve saldırılara karşı mücadelenin tanımlanmasını sağlar (Lopez vd., 2015).

Gizlilik, bilgilere izin verilen kişilerin erişebilmesi, Bütünlük, bilginin hâlihazırda var olan düzeninin ve içeriğinin herhangi bir etkiye bağlı olmaksızın korunması, tahrifata uğramadan saklanması şeklinde ifade edilirken, Erişilebilirlik ise bilginin erişim hakkı olan kişiler tarafından istenildiğinde erişilebilir durumda olması anlamını taşımaktadır. Sözü edilen üç özellik internet güvenliğinden bahsedilebilmesi için temel özellikler olarak kabul edilmektedir (Yiğit ve Seferoğlu, 2019).

İNTTERNET GÜVENLİK FARKINDALIĞI

İnternet güvenlik farkındalığı terimi, Shaw ve diğerleri, (2009) hali hazırda tanımlanmış olup şöyledir: "Kullanıcıların bilgi güvenliğinin önemi ve sorumlulukları hakkındaki anlayış derecesi ve kuruluşun verilerini ve ağlarını korumak için yeterli düzeyde bilgi güvenliği kontrolü uygulamak için hareket eder". Farkındalığın artırılmasında amaçlanan kişilerin tehditler ve güvenlik açıkları hakkında doğru bilgilerle donatılması, olası bir siber tehdit anında önemli ipuçlarının anlamını teşhis edebilmesi ve açıklayabilmesi, belirli tehditlerin sonuçlarını ve risklerini tahmin edebilmesi, oluşabilecek hasarı nasıl sınırlayacağını ve sorunları nasıl çözeceğini bilmesidir (Quayyum, 2020). Zayıf, orta veya yüksek olarak tanımlanabilen bireysel internet güvenlik farkındalığı, düşük farkındalık davranışlarda, mobil cihazlar ve dizüstü bilgisayarlar ile ücretsiz açık ağlara (Wi-Fi gibi) erişirken olduğu gibi çoğu durumda uygulamalar tarafından otomatik olarak sağlanan dikkat etmemeyi veya güvenlik uyarılarını ihmal etmeyi içerir. Orta düzeyde bir farkındalık düzeyi, uygun olmayan teknoloji işletiminde ifade edilen ihmal ile karakterize edilebilir. Son olarak, yüksek farkındalık, siber tehditler hakkında bilgi sahibi olmayı ve bunların önlenmesi için alınan yeterli eylemleri içerir (Zwilling vd., 2020).

Bilişim teknolojileri sistemlerinin güvenliği ve siber dünyada giderek artan tehditler, internet güvenlik bilincinin hem bireyler hem de kurumlar için önemini artırmıştır. Ancak internet güvenlik konusunda bilinçli olmaya yeterince önem verilmemekte ve özellikle iş yerlerinde sıklıkla ihmal edilmektedir. Herhangi bir kuruluş için, güvenlik ihlali olaylarını potansiyel olarak azaltabileceğinden, çalışanların siber güvenlik tehditlerinden haberdar olmaları ve güncel olmaları önemlidir. Ancak İngiltere İnternet Güvenlik İhlalleri Araştırması'na göre kuruluşların sadece %30'unun bu konuda farkındalık sağladığı gözlemlendi (Klahr vd., 2017).

Son kullanıcılar hakkında yapılan çalışmalar sonucunda, genellikle "Koruma var, bu yüzden güvendeyim" şeklinde özetlenebilecek bir düşünceye sahip olmaları bir kişinin emniyet kemeri taktığı için daha az dikkatli bir şekilde araba kullanmanın güvenli olduğunu önermekle bir bakıma benzerdir. Bu bağlamda online olarak koruma ancak bir noktaya kadar etkilidir. Bununla birlikte, daha az güvenlikli İnternet sitelerinde dikkatsizce dolaşarak kendi risklerini artıran ve maruz kalabilecekleri tehlikeleri düşünmeden şüpheli yazılımları cihazlarına yükleyen kullanıcılar olduğu tespit edilmiştir (Furnell, 2008).

OYUNLAR'IN İNTERNET GÜVENLİK FARKINDALIĞINA ETKİSİ

Kullanıcıların siber güvenlik konusunda bilinçli olmaları için eğitilmeleri önemlidir. Bunu başarmak için etkili bir yaklaşım, oyuncuları eğlendirmekle birlikte bir amaca ulaşmak için tasarlanmış ciddi oyunları kullanmaktır. Oyun tabanlı öğrenme yönteminin önemli bir özelliği, seçilen konu hakkında kullanıcıları eğitmek ve eğitmek için etkileşimli bir yaklaşım sağlamasıdır. Oyunlar, oyuncuların hedef becerilerini eğlenceli ve ilgi çekici bir şekilde aktarabilir veya geliştirebilir. Oyunların tasarımı esnektir ve eğitimle ilgili hemen hemen her konunun gereksinimlerini karşılayacak şekilde uyarlanabilir. İyi bir oyun, oyuncuyu sanal bir dünyaya götürür ve oyuncuları gerçek dünyada ortaya çıkabilecek durumlara ve sonuçlarına bağlamak için gerçek dünya senaryolarını simüle eder. Oyuncu sonuçlara tanık olur ve ayrıca oyunda kullanabileceği araçlar verilir (Alotaibi vd., 2018).

Şekil 2

Eğitsel Dijital Oyunların Kullanılma Gerekçeleri

Çeşitli alanlarda çeşitli etkinlikler hakkında farkındalık yaratmada Oyun Tabanlı Öğrenmenin etkisini analiz etmek için araştırmalar yapılmış ve yapılmaya devam etmektedir. Oyun Tabanlı Öğrenmenin bazı durumlarda daha iyi performansla sonuçlanmasa da, genel olarak daha kötü performansla sonuçlanmadığı ve oyun tabanlı öğrenme konusuna karşı daha olumlu bir tutumun ek faydaları olabileceği öne sürülmüştür (Oblinger, 2006). Ciddi oyunların, kullanıcılar arasında etkili eğitim ve davranış değişikliği sağlamada etkili olduğu düşünülmektedir. Oyunları eğitim amaçlı kullanma yaklaşımı oyun temelli öğrenme yaklaşımı olarak adlandırılmaktadır. Bu oyunlar okul eğitiminde yaygın olarak kullanılmaktadır. Daha yakın zamanlarda, sağlık hizmetleri, reklamcılık, davranış değişikliği ve siber güvenlik eğitimi için de benimsenmiştir. Alışkanlık, insan davranışlarını motive eden önemli bir faktördür. İnternet güvenlik davranış alışkanlıklarının oluşum mekanizması üzerine yapılan çalışmalar, bilgi güvenliği davranışına ilişkin araştırmaların sınırlarını genişletebilir ve bilgi güvenliği davranışlarının oluşum mekanizmalarının daha kapsamlı tanımlarının yapılabileceği yeni bakış açıları sağlayabilir (Hong ve Furnell, 2021).

İNTERNET GÜVENLİK FARKINDALIĞINA YÖNELİK GELİŞTİRİLEN OYUNLAR

Yapılan literatür taramasında internet güvenlik eğitimlerinin oyunlaştırma yoluyla öğretimine yönelik birçok çalışma bulunmaktadır. Etkileşimli ortamında CyberCIEGE, bilgisayar ve ağ güvenliği ve savunmasının önemli yönlerini kapsar. Bu video oyununda oyuncular, iş istasyonlarını, sunucuları, işletim sistemlerini, uygulamaları ve ağ cihazlarını satın alır ve yapılandırır. Bütçe, üretkenlik ve güvenlik arasında bir denge sağlamaya çalışırken ödünler verirler. Daha uzun senaryolarda, kullanıcılar bir dizi aşamada ilerler ve giderek daha değerli hale gelen kurumsal varlıkları artan saldırılara karşı korumalıdırlar. Oyun, yüksek uyarlanabilirlik ve oynanan senaryoların kontrolünü sunar, ancak takım oyununun olmaması, masa üstü oyunlarının sunabileceği teknik ve karar verme becerilerinin akran öğrenmesini engeller. Riskio' dan farklı olarak, savunma kontrollerine özel odaklanma, oyuncuların güvenlik farkındalıklarını düşmanca davranışlar konusunda geliştirmelerini engeller. Benzer şekilde, bilgisayar oyunu PERSUADED (Aladawy ve diğerleri, 2018), oyuncuların en yaygın sosyal mühendislik saldırılarına karşı savunma kontrollerinin etkinliğini öğrenmesine izin verir, ancak saldırganların yararlanabileceği gerçek saldırı vektörleri hakkında farkındalık yaratmaz.

Chothia ve diğerleri (2017), öğrencilerin giriş seviyesindeki bir internet güvenlik dersine katılımını artırmak için bayrağı ele geçirme tarzı bir VM önerdiler. VM, oyunlaştırmayı hikâye anlatımı ve karakter geliştirme şeklinde kullanır. Öğrenciler hayali bir şirkette yeni bir BT güvenlik çalışanı rolünü oynarlar ve bayrak aldıkları farklı alıştırmaları çözmeleri gerekir. Öğrenciler bayrakları bir dizi farklı karaktere göndermeye karar verebilir ve seçimleri hikâyenin akışını değiştirir. Riskio, oyuncuların tahtada tasvir edilen karakterleri ve varlıkları içeren bir saldırı senaryosu icat etmelerini sağlayan oyun tahtası aracılığıyla hikâye anlatımını destekler.

Haggman (2019), internet güvenlik eğitimi için Birleşik Krallık Ulusal İnternet Güvenlik Stratejisini temel alan bir masa üstü savaş oyunu önermektedir. Oyun tahtası, İngiltere ve Rusya arasındaki siber savaşı simüle eder ve iki düşman ülkede siber güvenlik stratejisinin uygulanmasına dâhil olan ana varlıkları temsil eder: hükümet, ulusal kritik alt yapılar, insanlar, akıllı ajanslar ve işletmeler. Her kurumun, sınırlı kaynakları kullanarak ulaşmaları gereken bir dizi stratejik hedefi vardır. Her varlığa, bir saldırı gerçekleştirmek veya ona karşı savunmak için varlık satın almak için kullanabilecekleri bir dizi kaynak atanır. Riskio' ya benzer şekilde, bu savaş oyunu oyuncuları çeşitli siber saldırılara ve savunma dinamiklerine maruz bırakmayı amaçlıyor.

Play2Prepare (Graffer vd., 2015), asıl amacı oyuncuları Dağıtım Sistemi Operatörleri (DSO) organizasyonlarında BT güvenlik olaylarının nasıl ele alınacağı konusunda eğitmek olan bir masa oyunudur. Oyun, oyuncuların saldırıyı azaltmak için birlikte çalışması gereken endüstriyel kontrol sistemlerine yönelik gerçek saldırılara ilham veren beş farklı saldırı senaryosunu destekler. Oyuncular, bir saldırıyı hafifletmek için kullanılabilecek bir dizi beceriyle ilişkilendirilen oyunda belirli bir rol oynarlar. Her saldırı senaryosu, oyuncular arasında tartışmalar yaratmak ve güvenlik kavramlarını anlamalarını artırmak için tasarlanmış bir dizi soru ile birlikte gelir. Oyun ayrıca, oyunda dinamikler ve çeşitlilik yaratmayı ve oyuncunun düşünmesini teşvik etmeyi amaçlayan kısa girdiler olan "biliyor muydunuz" gerçeklerini de kullanır.

İnternet Güvenlik-Gereksinim Farkındalık Oyunu (Yasin ve diğerleri, 2019), hastane ile ilgili senaryolarda güvenlik riskleri konusunda eğitim vermek için geliştirilmiş bir masa üstü kart oyunudur. Oyuncular, senaryolardaki güvenlik açıklarını belirlemeli ve içeriden veya dışarıdan saldırılar gerçekleştirmek için bunları kullanmalıdır. Oyuncular arasındaki tartışmalar, saldırı senaryolarını değerlendirmek ve puanlamak için kullanılır. Oyun, oyuncuların birden fazla güvenlik açığını ve saldırıyı öğrenmesine izin verir, ancak standart bir tehdit sınıflandırmasını takip etmediği için Riskio'dan önemli ölçüde farklıdır, örneğin oyunun kolayca uyarlanmasını ve farklı senaryolarda kullanılmasını engelleyen STRIDE; hepsinden önemlisi bir savunma aşamasından yoksundur.

Decision & Disruption (Frey vd., 2019), korunması gereken endüstriyel bir siber fiziksel sistemi temsil eden bir Lego™ oyun tahtası aracılığıyla tasarlanmış bir masa üstü kart oyunudur. Oyun, sistemi korumak için dağıtılacak mevcut bir bütçe savunma önlemlerine dayalı olarak oyuncuların öncelik vermesi gereken turlar halinde düzenlenmiştir. Her turun sonunda, oyun yöneticisi, oyuncular tarafından bilinmeyen sabit saldırı profillerine dayalı olarak seçilen savunmaların etkinliğini değerlendirir. Oyuncular, savunmacıların rolünü ve sınırlı ölçüde güvenlik yönetimi stratejilerini öğrenirler. Riskio' dan farklı olarak, siber tehdit farkındalığına ve ilgili saldırılara odaklanmaz: oyuncular, saldırıları tanımlamaya veya bilinen bir saldırıya dayalı savunma seçmeye zorlanmaz.

[d0x3d!] (Gondree ve Peterson, 2013), K-12 CS ve STEM olmayan öğrencilere ağ güvenliği kavramlarını öğretmek için tasarlanmış bir masa üstü kart oyunudur. Oyuncular, bir ağa giren ve yeteneklerini kullanarak ve ağ güvenlik açıklarından yararlanarak değerli dijital varlıkları alan bir grup beyaz şapkalı bilgisayar korsanının kimliğine bürünür. Her fırsatta, oyuncuların dijital varlıkları almasını zorlaştıran bir ağ yöneticisinin eylemlerini simüle etmek için ağ yamalı. Buna karşılık Riskio, oyuncunun en son güvenlik raporlarından alınan daha geniş bir güvenlik tehdidi yelpazesini öğrenmesini sağlar.

Control-Alt-Hack (Denning vd., 2013), bilgisayar güvenliği kavramlarının farkındalığını ve anlaşılmasını artırmak için tasarlanmış bir masa üstü kart oyunudur. Oyunun birincil izleyici kitlesi bilgisayar ve mühendislik lisans öğrencileri ve lise öğrencileridir. [d0x3d!]'ye benzer şekilde, oyuncular güvenlik denetimleri yapan ve danışmanlık hizmetleri sunan bir güvenlik şirketi için çalışan beyaz şapkalı bilgisayar korsanları rolünü oynarlar. Oyuncular, bilgisayar korsanlarının becerilerini kullanarak farklı görevleri tamamlamak zorundadır. Riskio'nun ana hedefi oyuncuları bir saldırgan olarak nasıl düşünecekleri konusunda eğitmek ve ardından saldırıları nasıl caydıracaklarını öğrenmek iken, Control-Alt-Hack'in ana odak noktası saldırı ve güvenlik açığından yararlanmadır.

Güvenlik Kartları (Tamara vd.,2013), oyuncuları bilgisayar güvenliği tehditleri hakkında geniş ve yaratıcı düşünmeye teşvik eden bir kart destesidir. Kart destesi 4 kategoride düzenlenmiş 42 kart içerir: 1) Düşmanın Motivasyonları, 2) Düşmanın Kaynakları, 3) Düşmanın Yöntemleri ve 4) İnsan Etkisi. Kartlar, akademik ve endüstri ortamlarında farklı türdeki eğitim faaliyetlerini desteklemek için kullanılabilir: örneğin, güvenlik tehditleri hakkında bilgi edinmek veya yazılım tasarımındaki tehditleri ortaya çıkarmak için kullanılabilirler. Riskio ile karşılaştırıldığında, Güvenlik Kartları destesi, güvenlik tehditlerini caydırmak için olası savunmalar konusunda eğitim veren kartlar içermez.

Sherlocked (Jaffray vd., 2021), İngiltere'de Kent Üniversitesi'nde ikinci ve son sınıf öğrencilerine sunulan siber güvenliğe giriş modülü müfredatına bağlı olarak hazırlanmış bir 2D tabanlı oyundur. Oyunda amaçlanan müfredata bağlı olarak konuların anlaşılmasına yardımcı olmaktır. 112 bilgisayar lisans öğrencisi tarafından oynanan oyunun daha çekici bir etkileşim biçimi sağlamada başarılı olduğu ve aynı zamanda ders içeriğinin anlaşılması, öğrencinin anlama ve özgüveninin artmasına yardımcı olduğu sonucunda ulaşılmıştır. Ancak müfredat temelli olması diğer diğer kullanıcıların ya da aynı müfredat da eğitim almamış bir kullanıcının istenen farkındalık düzeyine erişmesine yeterli katkıyı sağlamayabilir.

Elevation of Privilege: Drawing Developers into Threat Modeling (Hart vd., 2019), isimli kart oyunu her yaştan kullanıcıya hitap ederken öğrenci ve personellerin kendilerini geliştirmeleri amacıyla okullar ve küçük ölçekli işletmeler tarafından rağbet görmektedir. Oyunculardan biri Minecraft hesabını nasıl hacklemeye çalıştığını ve bu fikrin Elevation of Privilege kartlarıyla oynamaktan geldiğinden bahsederken bir devlet kurumu yetkilisi, ellerinde oyun ortaya çıktıklarında daha önce yüzlerine kapatılan kapıların açıldığını belirtti. Ulusal bir hükümet, ulusal sembolleri ve saldırının ayrıntılarını içeren sekiz özel kartla tamamlanan "Ayrıcalıklı Vahiy" adı altında bir saldırı belgelemesi oyuncuların daha sonra siyah şapkalı birer hackera dönüşmesine neden olabildiğini göstermektedir.

CybAR (Alqahtani ve Kavakli-Thorne, 2020) siber tehditler hakkında hem kavramsal hem de prosedürel bilgi sağlamak amacıyla sistem yazılımının ayrıntılı teknik bilgisinden ziyade üst düzey kullanıcı davranışlarına odaklanan rekabetçi ve bir Mobil Artırılmış Gerçeklik tabanlı bir oyundur. CybAR, gerçek hayattaki bir siber güvenlik sorununu eğlenceli ve anlaşılır bir şekilde taklit eder. Oyuncuların CybAR hakkında düzenlenen ankete verdikleri cevaplarda oyuncuları gelecekte internet güvenliği ile ilgili kavramlar hakkında daha fazla bilgi edinmeye motive ettiği ve siber güvenlikle ilgili kavramları öğrenmenin etkili ve eğlenceli bir yolu olabileceğini gösterdi. CYBAR tek kullanıcılı bir oyun olduğundan grup aktivitesi bulunmamaktadır. Katılımcılar yer yer oyunun karmaşıklaştığını ve daha fazla oyunlaştırma öğesi eklenmesi gerektiğini belirtmişlerdir.

AWATO Corp' ta (Ferro ve Sapio, 2020) insan hatasının neden olduğu siber güvenlik sorunlarını belirlemesi gereken, yakın zamanda işe alınan bir güvenlik analistinin rolünü oynadığınız ciddi bir oyundur ve oyunun adıyla uygun bir şekilde adlandırılmıştır. Kullanıcıların yalnızca tehditlerden ziyade kullanıcıların davranışlarını dikkate almalarına olanak tanıyan bir güvenlik oyununun ilk türüdür. Kullanıcıları ve/veya güvenlik analistlerinin insan faktörüyle ilgili tehditleri belirlemelerine yardımcı olmak için tehdit modelleme konusunda kullanıcıları eğitmeyi amaçlar. Genel kullanıcıların aksine daha üst düzey kullanıcılara yönelik olması diğer oyunlara göre daha küçük bir kitleye hitap etmesine neden olmaktadır.

PROTECT (Goeke vd., 2019) sosyal mühendislik konusunda bir eğitim uygulayan ciddi bir kart oyunudur. Birincil amacı, insanları sosyal mühendislik saldırılarına karşı farkındalık oluşturmaktır. Bu farkındalık, uygun bir tepkiyi tetiklemek için insanların tekrar tekrar sosyal mühendislik senaryolarıyla karşı karşıya gelmesiyle sağlanacaktır. Protect toplum mühendisliğine yönelik farkındalığın arttırılmasının yanı sıra iknaya karşı eğitim direnci ve genel nüfusa hitap eden özelleşmiş bir oyun türüdür.

A Serious Game for Eliciting Social Engineering Security Requirements yine sosyal mühendisliğe karşı (Beckers ve Pape, 2016) geliştirilmiş bir kart oyunudur. Temel amacımız, sosyal mühendislik güvenlik gereksinimlerini ortaya çıkarmak ve önceliklendirmek için yapılandırılmış araçlar sağlamaktır. İlk olarak, saldırının oyuncuların zihninde sezgisel olarak işe yarayıp yaramadığını veya makul şüphelerin olup olmadığını belirlenir. Eğer şüpheler o kadar güçlüyse ki hiçbir oyuncu bu saldırının işe yarayacağına inanmıyorsa, oyunda bir ceza mevcut (0 puan ve tur sonu). Daha sonra oyuncuları kartlarındaki davranışlar ve saldırı senaryoları ile iç ve dış saldırganların farklı yaklaşımları hakkında düşünmeleri için ödüllendirme sistemi mevcuttur.

SONUÇ

Siber güvenlik tehditleri her geçen arttığı, kötü niyetli saldırıların sürekli şekil değiştirdiği ve her geçen gün karmaşıklaştığı dünyamızda son kullanıcıların istenen farkındalığa ulaşmalarına ve beklenen davranışları sergilemelerine yönelik oyunlaştırmanın etkili bir yöntem olduğu aşikârdır. Yapılan çalışmalar incelendiğinde oyunlar ister video ister masa oyunları (kart ve benzeri) siber güvenlik farkındalığının artırılmasına olumlu yönde etki ettikleri, öğrenenlerden beklenen yüksek motivasyonu sağlamaları, karmaşık bilgiler arasında ilişki kurmalarına yardımcı oldukları tespit edilmiştir. Oyun temelli yaklaşım, oyuncuları uygun eylemleri kullanarak hedefe doğru ilerlemeye motive eder ve gerçek yaşam maliyetlerine maruz kalmadan bunu yapmamanın sonuçlarını gözlemlemelerini sağlar. Geleneksel eğitim yöntemleriyle karşılaştırıldığında, oyun temelli yaklaşımlar daha ilgi çekici, nispeten uygun maliyetli, çok sayıda kursiyere kolayca aktarılabilir ve her oyuncuya göre özelleştirilebilir. Her yaştan insanın oyun oynadığı göz önüne alındığında, internet farkındalığı ya da siber güvenlik farkındalığı kazandırmak amacıyla oyunların kullanılması önerilmektedir.

İNTERNET GÜVENLİĞİ FARKINDALIĞINDA OYUNLARIN ETKİSİ

ORIGINALITY REPORT

6%
SIMILARITY INDEX

PRIMARY SOURCES

1	Farzana Quayyum, Daniela S. Cruzes, Letizia Jaccheri. "Cybersecurity awareness for children: A systematic literature review", International Journal of Child-Computer Interaction, 2021 Crossref	47 words — 1%
2	dergipark.gov.tr Internet	44 words — 1%
3	www.kaspersky.com.tr Internet	38 words — 1%
4	fmgtegitimikongresi.com Internet	24 words — 1%
5	www.amasya.edu.tr Internet	13 words — < 1%
6	etd.lib.nsysu.edu.tw Internet	10 words — < 1%
7	mediatum.ub.tum.de Internet	9 words — < 1%
8	ulead2018.ulead.org.tr Internet	9 words — < 1%
9	www.ismsitconf.org Internet	

9 words — < 1%

10 www.ices-uebk.org
Internet

8 words — < 1%

EXCLUDE QUOTES	OFF	EXCLUDE MATCHES	OFF
EXCLUDE BIBLIOGRAPHY	OFF		