Çevrimiçi Oyunlara İlişkin Güvenlik Riskleri

Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: iletisim@usom.gov.tr

Kasım 2014
UR.RHB.005

İÇİNDEKİLER

1.GİRİŞ 3

2. GÜVENLİK RİSKLERİ 3

2.1. TEKNOLOJİK RİSKLER 4

2.1.1. Virüsler ve Solucanlar 4

2.1.2. Zararlı Yazılımlar 4

2.1.3. Gizliliği İhlal Edilmiş Oyun Sunucuları 4

2.1.4. Güvenli Olmayan Oyun Kodlaması 5

2.2. SOSYAL RİSKLER 5

2.2.1. Sosyal Mühendislik ve Kimlik Hırsızlığı 5

2.2.3. Siber Fuhuş ve Mafya 6

2.2.4. Sanal Gasp ve Sömürü 6

3. KORUNMA YOLLARI 6

3.1. GENEL GÜVENLİK ÖNLEMLERİ 6

3.2. OYUNLARDA GÜVENLİK ÖNLEMLERİ 7

4. SONUÇ 8

5.KAYNAKLAR 9

1.GİRİŞ

Günümüzde, yeni teknolojiler ve internetin ulaştığı yüksek hızlar nedeniyle çevrimiçi oyunlar popüler eğlencelerden biri haline gelmiştir. Bir tarafta, oyun tutkunları, gelişmiş oyunlar için yüksek oranlarda zaman ve para harcarken, diğer tarafta güvenlik açıklıklarını kullanan siber saldırganlar oyunları ve ilgili platformları kendi emelleri için araç olarak kullanabilmektedir. Çevrimiçi oyunlar eğlenceli olsa da teknolojik ve sosyal risklerinin de farkında olunması gerekmektedir.

Bu riskler;

- Kişisel ve finansal bilgileri çalmak isteyen kişilerle iletişimde bulunmadan kaynaklanan riskler,
- Bilgisayar güvenlik açıklarından faydalanmak isteyenlerin sebep olduğu riskler,
- İnternet üzerinde ve gerçek dünyada kurban arayan suçluların sebep olduğu riskler,
- Truva atları, bilgisayar solucanları, casus yazılımlar ve virüslerin oluşturduğu riskler

olarak sıralanabilir. Buna ilave olarak son yıllarda çevrimiçi kumar oyunlarının popülaritesi de giderek artmaktadır. Genellikle kumarhane oyunlarının çevrimiçi ortama aktarılmış sürümleri, çeşitli piyango türleri ve bahis oyunları yaygın olarak oynanmaktadır. Kumar oyunları gerçek dünyada olduğu gibi sanal dünyada da bağımlılığa, zaman ve para kaybına sebep olmaktadır.

2. GÜVENLİK RİSKLERİ

Bugünün çevrimiçi oyun dünyasında tercih edilebilecek seçeneklerin sayısı büyük rakamlara ulaşmıştır. Bununla birlikte oyun dünyasının en popüler türlerinden biri Çok Oyunculu Çevrimiçi Rol Yapma Oyunlarıdır (Massive Multiplayer Online Role Playing Games - MMORPG). Bu tip oyunların çoğunluğunda, oyuncunun isteğine göre karakter oluşturma ve bu karakterlerle sanal maceralara atılma imkanı

sağlanmaktadır. Ancak kimi zaman bu durum sanallığı aşarak gerçek dünyaya sıçramaktadır. Örneğin oyuncular, oyunda kullandıkları sanal malzemeleri, alış veriş sitelerinde satışa sunmakta ya da oyundaki karakterleri geliştirmek amacıyla büyük paralar harcamaktadır. Bu durum sanal suçlara davetiye çıkarmaktadır. Çevrimiçi oyunlar genellikle hem sosyal hem de teknolojik riskler içermektedir.

2.1. TEKNOLOJİK RİSKLER

Çevrimiçi oyunlar, oyuncuların kullandığı sisteme veya oyuncuların etkileşim halinde olduğu diğer oyuncuların sistemlerine yönelik olarak aşağıda bahsedilen riskleri içermektedir.

2.1.1. Virüsler ve Solucanlar

Virüsler, anlık mesajlaşma programları veya e-posta eklentileri aracılığıyla bulaşabilmektedir ve zararlı programlar, internet üzerinden indirilen oyun dosyaları içerisine gizlenebilmektedir.

2.1.2. Zararlı Yazılımlar

Virüsler ve solucanlar, kullanıcı bilgisayarlarına zararlı yazılımlar yüklemek için kullanılabilmektedir. Ayrıca kötü niyetli kişiler, çevrimiçi sohbet, e-posta ve sesli iletişimi kullanan çevrimiçi oyunları barındıran sosyal ağları, kullanıcıyı sahte sitelere yönlendirmek, zararlı yazılım içeren e-posta eklerini açtırmak ve bu yazılımları sistem üzerine yüklemek için ikna edici olarak kullanabilmektedir. Daha sonra yüklenen bu yazılımlar, kötü amaçlı olarak kullanılabilmektedir.

2.1.3. Gizliliği İhlal Edilmiş Oyun Sunucuları

Oyun sunucuları üzerindeki yazılımın gizliliği ihlal edilmesi durumunda, bu sunuculara bağlı bütün bilgisayarların da gizliliği ve güvenliği ihlal edilmiş olabilmektedir. Ağ bağlantısı barındıran oyunlar, bilgisayar sistemlerinde güvenliği tehdit eden riskler taşımaktadır. Kötü amaçlı kişiler güvenlik açıklıkları kullanarak ele geçirdikleri bilgisayarları uzaktan kontrol edebilmekte ve bu bilgisayarları farklı sistemlere saldırı amacıyla kullanabilmektedir ya da kişisel bilgilere erişmek amacıyla bilgisayarlara

truva atı, casus yazılım gibi programlar yükleyebilmektedir. Örneğin bazı popüler çevrimiçi oyunlarda tespit edilen açıklıkları kullanan saldırganların oyuncunun bilgisayarındaki dosyaları okuyabildiği, oynanmakta olan oyunu kapatabildiği, hatta oyuncunun bilgisayarının kontrolünü tamamen eline geçirebildiği bilinmektedir.

Oyuncuların maruz kaldığı bu risklere ilave olarak oyun sunucularını yöneten tarafların karşılaştığı riskler de bulunmaktadır. Bir oyun uygulaması çalıştırmak için kullanılan bir sunucuyu yönetirken karşılaşılabilecek olası riskler ile başka herhangi bir uygulama için kullanılan sunucuyu yönetirken karşılaşılabilecek olası riskler aynıdır. Kötü amaçlı kişilerin, güvenlik seviyesi düşük olan sunuculara sızabilmesi veya zarar verebilmesi ihtimal dahilindedir.

2.1.4. Güvenli Olmayan Oyun Kodlaması

Oyun bilgilerinin iletişimi konusunda kullanılan bazı oyun protokolleri, diğer protokoller kadar güvenli hale getirilmemiştir. Ayrıca oyun kodları, popüler ticari yazılımlar kadar dikkatle incelenmemektedir. Bu nedenle oyun yazılımları, zararlı yazılım olarak çalışabilmekte veya sistem üzerinde güvenlik açıklıklarına sebep olabilmektedir.

2.2. SOSYAL RİSKLER

Önceleri bilgisayar oyunları yalnız başına oynanıyor olmasına rağmen, günümüzde çoğu oyun, mesajların, sesli iletişimin kullanıldığı ve topluluk halinde oynanan oyunlar haline gelmiş durumdadır. Kötü niyetli kişiler, yazılım güvenlik açıklıklarından faydalanabilmek için çevrimiçi oyunların sosyal iletişimini kullanabilmektedir. Bazıları da internete bağlı ve korumasız bilgisayarlara erişim sağlayabilmek için çaba sarf etmektedir. Kötü niyetli kişilerin amaçları genellikle, kişisel bilgilerin ele geçirilmesi, kimlik hırsızlığı, kredi kartı bilgilerinin çalınması veya çocuk istismarı olabilmektedir.

2.2.1. Sosyal Mühendislik ve Kimlik Hırsızlığı

Kötü niyetli kişiler, kullanıcıları aslında zararlı yazılım olan ancak oyun gibi görünen yazılımları internet üzerinden indirmeye yönlendirerek, bilgisayarlarını kontrol edebilecek, çevrimiçi hareketlerini takip edebilecek, başka bilgisayarlara atak

yapabilecek programlar yüklemeye ikna edebilmektedir. Kötü niyetli kişiler, kullanıcının oyunlarda oluşturduğu profillerden veya farklı kaynaklardan kişisel bilgiler elde edebildiği takdirde, kullanıcı bilgilerini satabilmekte veya banka hesap bilgilerine erişim için kullanabilmektedir.

2.2.3. Siber Fuhuş ve Mafya

Ülkemizde de yaygın olarak oynan bir oyunda 17 yaşında bir çocuk tarafından müşterilerin, siber seks için sanal para ödediği bir uygulama geliştirdiği, söz konusu oyun firması tarafından ilgili hesabın iptal edildiği ancak hiçbir yasal işlem yapılmadığı bilinmektedir. Ayrıca bazı ülkelerde zayıf oyuncuların, bir sanal suç şebekesi ile bağlantılı diğer kullanıcılar tarafından belirli bir "koruma parası" verilmemesi halinde negatif sonuçlarla karşılaşacakları belirtilerek tehdit edildiği olalar da görülmektedir.

2.2.4. Sanal Gasp ve Sömürü

Sanal gasp terimi, bir çevrimiçi oyunda bazı oyuncuların diğer oyuncuları yenmek ve onların malzemelerini almak için internet üzerinde çalışan uygulamaları kullanması olarak tanımlanabilmektedir. Üçüncü dünya ülkelerindeki insanların çok ucuz ücretler karşılığında çevrimiçi oyunlardaki kaynakları veya sanal paraları toplamak amacıyla çalıştırılması sanal sömürü kavramını doğurmuştur.

3. KORUNMA YOLLARI

Yukarıda açıklanan risklere rağmen, internet üzerinden oynanan oyunlar, kullanıcının bilgisayar güvenliği konusunda dikkatli davranması halinde güvenli ve zevkli bir aktivite haline gelebilmektedir.

3.1. GENEL GÜVENLİK ÖNLEMLERİ

Kişisel bir bilgisayarda geçerli olan aşağıda belirtilen temel güvenlik uygulamaları, çevrimiçi oyun amacıyla kullanılan bilgisayarlarda da güvenliği sağlamak için tavsiye edilmektedir.

- Antivirüs ve anti casus yazılım programlarının kullanılması.

- E-posta ve anlık iletilerde gelen ek dosyalarını açarken dikkatli olunması.
- İnternetten dosya ve yazılım indirilmesinde güvenlik konusunda emin olunması.
- Kullanılan internet tarayıcısının güvenli olacak şekilde ayarlanması.
- Güvenlik duvarı kullanılması.
- Kişisel ve finansal bilgilerin güvenliğinin sağlanarak ve yedeklerinin alınması.
- Güçlü şifreler kullanılması.
- Kullanılan yazılımları güncelliğinin sağlanması.

3.2. OYUNLARDA GÜVENLİK ÖNLEMLERİ

Bazı oyunlar, kullanıcının bilgisayarı, sınırlı yetkiye sahip kullanıcı hesapları yerine, tam yetkiye sahip yönetici olarak kullanmasını istemektedir. Bu gibi durumlarda oyun satıcısının veya oyunun indirildiği sitenin güvenilirliğinden emin olmak büyük önem taşımaktadır. Özellikle bedava indirilen oyunlar genellikle zararlı yazılım barındırmaktadır. Yönetici oturumuyla çevrimiçi oyun oynanması sırasında bu gibi yazılımların aktive edilmesi, kullanılan bilgisayarının tüm yetkilerinin siber saldırganlar tarafından ele geçirilmesi riskini doğurmaktadır. Bu nedenle yönetici oturumunda güvenilirliğinden emin olunmayan yazılımlar veya oyunların çalıştırılmaması gerekmektedir.

Bazı çevrimiçi oyunlar internet tarayıcısı üzerinden oynanabilmektedir. Bu tip oyunlar genelde ActiveX ya da JavaScript uygulamalarının aktif hale gelmesini istemektedir. ActiveX ve JavaScript'in aktif hale getirilmesi, bazı güvenlik açıklıklarını da beraberinde getirmektedir. Konuyla ilgili risklerden kaçınmak amacıyla internet tarayıcısının güvenlik ayarları dikkatli bir şekilde yapılandırılmalıdır. dikkat edilmelidir.

Ayrıca, uyun oynanırken, oyun sitesinde oynamak ve daha sonrasında internet taramasını kaydetmek en iyisidir. Bu yolla, oyun oynama işi bittikten sonra, internette gezinti yapmak için tekrar kullanıcı hesabına dönülebilmektedir. Bu da kullanıcıyı zararlı internet sitelerinden korumaktadır.

Ev kullanıcıları genellikle, bilgisayarlarını korumaya yardım etmesi için güvenlik duvarı kullanmaktadır. Ancak çok oyunculu çevrimiçi oyunların bazıları, bilgi alışverişini sağlamak için güvenlik duvarında bir istisna açıklık istemektedir. Verilen her açıklık, bilgisayarın güvenliğini daha da fazla tehdit etmektedir. Bu nedenle güvenlik duvarında birbirini tanıyan oyucular için IP adresine göre ayrıcalık tanınması, kötü amaçlı kişilerden sakınılması açasından faydalı olacaktır.

4. SONUÇ

Günümüzde, çevrimiçi oyunlar eğlencenin en önemli kaynaklarından biri haline gelmiş, yeni gelir kaynakları oluşturmuş ve milyonlarca insanın hayal gücü sınırlarını aşmasını sağlamıştır. Bununla birlikte oyunların güvenli hale getirebilmesi amacıyla, mevcut riskler hakkında bilgi sahibi olunması ve bu risklere karşı tedbirli olunması büyük önem taşımaktadır.

5.KAYNAKLAR

[1] Dormann, W. & Rafail, J. 2006. *Securing Your Web Browser.* US-CERT.

http://www.us-cert.gov/publications/securing-your-web-browser

[2] Hayes, E.J. 2008. *Playing It Safe: Avoiding Online Gaming Risks.* US-CERT.

http://www.us-cert.gov/sites/default/files/publications/gaming.pdf

[3] Microsoft, Güvenlik Merkezi.

http://www.microsoft.com/security/default.asp

[4] U.S. Department of Justice Federal Bureau of Investigation. 2014. *A Parent's Guide to Internet Safety.* FBI Publications.

http://www.fbi.gov/publications/pguide/pguidee.htm