

Güvenli Bir Toplum İçin Son Kullanıcı Siber Güvenliği

Önder Şahinaslan¹, Ender Şahinaslan², Emin Borandağ³, A.Mutalip Sahinaslan⁴

^{1,3} Maltepe Üniversitesi, İstanbul

² Bankasya, İstanbul

⁴ İnönü Üniversitesi, Malatya

Özet: İçinde bulunduğumuz dijital dünyada, internet bağlantı sayılarında benzeri görülmemiş bir artış söz konusudur. Bireysel yaşamdan, toplum ihtiyaçlarına kadar hayatın her alanında, pek çok kolaylığı beraberinde getirmiştir. Dünya da internet kullanıcı sayısı son 5 yılda yaklaşık iki katına ulaşmıştır. Yaşantımızda bu boyutta bir kullanıma sahip internet, göz korkutucu tehdit ve riskleri de beraberinde getirmektedir. Bireysel kullanıcılar kritik öneme sahip işlevlerini güvenli ortamlarda yapmalıdırlar. İnternet ve bilgi paylaşımı, güvenli olmayan son kullanıcı bilgisayarları ile çok daha büyük risk ve tehdit altındadır. Bu çalışma, daha güvenilir toplumlar için daha güvenli son kullanıcılar oluşturmak amacıyla alınması gereken tedbir ve önlemleri içermektedir.

Anahtar Sözcükler: Siber Tehdit, Son Kullanıcı Güvenliği, Siber Güvenlik ve Önlem

A Safe Community Cyber Security for the End User

Abstract: In the current digital world, there is an unprecedented rise in the number of Internet users. Individual life and every aspect of life as much as the needs of society has brought many ease. Number of Internet users in the world the last 5 years reached nearly doubled. Lives with the extent of this use the internet, brings an intimidating threats and risks. Individual users should perform critical functions of the secure operating environments. Through this personal data and privacy are protected against cyber threats. Internet and information-sharing non-secure end-user computers and threatened with a very big risk. In this study, more reliable, more secure for end users to create communities of measures and includes the measures to be taken.

Keywords: Cyber Threat, End User Security, Cyber Security and Prevention

1. Giriş

İnternet destekli yeni iletişim teknolojileri son kullanıcılar için sayısız fırsatlar sunmaktadır. Dünya da internet kullanıcı sayısı son 5 yılda 1.15 milyardan 2.27 milyara artarak yaklaşık iki katına ulaşmıştır[1]. Bu şekilde bir artış gösteren bilgisayar ve internet erişimi korunması gereken değerli varlıklardır. Siber tehdit ve risklerin önlenmesi sadece güvenlik yazılımlarına bırakılmamalıdır. Bilinçli kullanıcılar oluşturulmalıdır. İnternet veya taşınabilir aygıtlar üzerinden yayılan her türlü zararlılara karşı tedbirli olunmak için bu bildiride anlatılan basit ve önemli kullanım alışkanlıklarının yaygınlaştırılması gerekir[2].

Ciddi siber saldırıları önlemenin etkili ve kolay yolu basit son kullanıcı güvenlik tedbirlerinin alınması ile mümkün hale gelebilir.

Bu çalışmanın başlıca hedefi kişisel internet güvenliğinin sağlanması ile güvenli toplumların oluşmasına katkı sağlamaktır. Bunun için siber güvenlik risklerini doğru yönetebilmek için gerekli olan taktik ve tedbir amaçlı temel bilgiler anlatılmaktadır.

2. Siber Tehditlerin Son Kullanıcılar Açısından Önemi

İnternet olanakları ile birlikte çağımızın yaşam standartları ve alışkanlıkları da değişmiştir. Bilgi ve kaynağa hızlı, pratik, kolay, ucuz, zamandan ve

işgücünden tasarruflu şekilde yaygın bir kullanım aracı haline gelmiştir.

Bu araç kullanıcılar kadar hırsızlarında işini bir o kadar kolaylaştırmıştır. Fiziksel güç kullanmadan, vize, ulaşım, zaman ve mekân kısıtı olmaksızın, çok fazla hayati risk taşımayan her yaşta yapılabilen bir saldırı yöntemine dönüşmüştür.

Siber suçlular çeşitli aldatmaca yöntemler kullanarak pek çok kişiyi mağdur etmektedir. Uzaktan yazılımlar kurarak veya masum sosyal mühendislik yöntemleri ile insanların önemli kişisel bilgilerini ele geçirmektedirler. Örneğin önemli kişi ve kuruluş isimleri taklit edilerek sahte LinkedIn, Facebook, Twitter hesapları açılmaktadır. Bu profiller üzerinden son kullanıcılar sahte tuzak olarak hazırlanmış dolandırıcı sitelere yönlendirilmektedir. O siteden indirdikleri müzik, film, resim ve programlar bazı zararlı eklentileri de beraberinde bilgisayar kurdukmaktadırlar. Bu sayede son kullanıcının bilgisayarını veya kritik bilgi ve iletişim trafiği ele geçirilmiş olmaktadır.

Sahte anti-virüs yazılımlarını güvenlik amaçlı kurdurarak aslında o bilgisayarları daha güvensiz ve uzaktan yönetilebilir duruma getirilebiliyor.

İnternet üzerinde çok fazla virüs, trojan, malware, spam türü zararlı yazılımların elden ele değiştirmektedir. Bunların varlık nedeni çoğu son kullanıcıların tedbirsiz ve güvensiz bilgisayar kullanımını nedeniyledir.

Hizmet veren bir sunucunun ilgili servisini engellemede zombi olarak nitelendirilen zehirlenmiş bilgisayar(zararlı yazılım kurularak bir çeşit yönetimi başkalarının eline geçmiş bilgisayar) kullanılmaktadır. Denial-of-service saldırıları olarak algılanan bu yöntemde ağırlıklı olarak son kullanıcı bilgisayarları kullanılmaktadır.

Kısaca el terminalerinden bilgisayara, son kullanıcıların kullanmış oldukları tüm internet kullanım araçları güvensiz ve tedbirsiz kullanılmamalı. Aksi takdirde kötü amaçlı zararlı kodlar enjekte edilerek anında kişisel veya kurumsal bir saldırı ve sızıntı aracına dönüşebilmektedir.

3. Önlem Alma ve Korunma

Kişisel bilgilerimizi internette gelebilecek saldırılara karşı korumak için kullanılan tüm araçlar ve bağlantı yöntemleri asgari güvenli hale getirilme ile mümkündür. Son kullanıcılar açısından siber önlemlerin nasıl gerçekleşeceği, beş ana eylem planı altında özetlenmiştir.

3.1 Masaüstü Sistem Güvenliği

Günlük yaşamda kişisel ve dizüstü bilgisayarların kullanımı oldukça yaygındır. Siber saldırılara karşı güvenli bir kullanıcı topluluğu oluşturmak için masaüstü güvenliği kesinlikle gereklidir. Bunu sağlayabilmek için internet bağlantısı olan her bir cihazın asgari şu güvenlik standartları sağlaması gerekir[2].

1. Cihaz üzerinde kurulu olan yazılımların güncel sürümlerini yada kullanılan sürümün en son yaması yüklenmiş olmalıdır.
2. Bu cihazlarda güncel bir anti-virüs ve anti-spyware yazılımının çalışıyor olması son derece önemlidir.
3. Sistemi başlatma kullanıcı adı ve şifre kontrollü olmalıdır. Birden fazla kullanıcı paylaşıyorsa kendi içinde yetkilendirme yapılmalıdır. Kullanılan şifreler belli uzunlukta ve karmaşık karakter yapıda olmalıdır. Varsayılan olarak atanmış kullanıcı adları ve şifreler mutlaka değiştirilmelidir.
4. Cihazın risk düzeyine göre fiziki erişim güvenliği sağlanmalıdır. Potansiyel hırsızlık veya doğrudan bilgiye erişim gibi tehlikeli olabilecek ortamlarda dikkatli olunmalıdır. Bilgisayar başından kısa süreli ayrılma durumlarında şifre korumalı ekran koruyucu aktif hale getirilmelidir. Unutulması durumunda 5-10 dakika içerisinde kendiliğinden etkin hale gelecek duruma getirilmelidir.
5. Daha çok sunucu servislerinde kullanılan FTP, SNMP, Telnet, IIS, IMAP, POP gibi hizmet portları kapatılmalıdır. Bu servisler ihtiyaç olmadığı sürece

bilgisayarlara kurulmamalıdır. Telnet bağlantılar yerine SSH şifreli bağlantılar tercih edilmelidir.

6. Bilgisayardaki paylaşılmış klasörler, servisler kontrol edilmelidir. Paylaşım gerekli ise şifre koruması mutlaka sağlanmalıdır. İnternet çıkış ayarları, IP, DNS, Proxy sunucu tanımları doğru yapılandırılmalıdır[3].

7. Cihaz üzerine doğrudan veya istem dışı kurulmuş yazılımlar denetim altında tutulmalıdır. Kurulu yazılımlar belli aralıklarda gözden geçirilmeli kullanılmayan veya güncelliğini kaybetmiş yazılımlar kaldırılmalıdır.

8. E-posta yolu ile talep edilen kimlik kartı, kredi kart, üyelik bilgileri vb. ile her türlü şifre bilgileri istenildiğinde kesinlikle gönderilmemelidir.

9. Cihazların depolama aygıtlarında veya taşınabilir belleklerde tutulan hassas veriler siber tehditlere karşı korunmalıdır. Ele geçirilme durumlarına karşı, kişisel veya kurumsal kritik verilerin tutulduğu belgeler veya klasörler şifreli şekilde saklanmalıdır.

10. Cihaz üzerindeki verilere olası bir siber tehdit in verebileceği yıkıma karşı, özellikle sabitlikteki önemli kritik varlıklar belli aralıklarda yedeklenerek kopyaları oluşturulmalı[4].

11. Yedek kopyalar şifre korumalı şekilde alınmalı ve fiziksel olarak cihazdan uzak güvenli yerde korunmalıdır.

12. Tanımadığımız kişi ve kuruluşlardan gelen e-posta ekleri asla açılmamalıdır. Bildiğimiz yerlerden gelen e-posta ekleri de mutlaka güvenlik yazılımları ile taratılarak açılmalıdır.

13. Güvenilir ücretsiz anti-virüs yazılımı adı ile gelen bir e-posta veya web sayfası linkine kesinlikle itibar edilmemelidir. İhtiyaç varsa doğrudan belli firmaların adresleri ziyaret edilerek doğrudan güvenli kurulumlar yapılmalıdır[5].

14. İçeriğinden çok emin olmadığımız masum gibi görünen bir e-postayı virüs veya kötü amaçlı yazılım içerme riskine karşı başkasına veya bir gruba göndermeyiniz.

15. Ücretsiz veya deneme amaçlı reklam edilen yazılımları doğrudan kurmadan önce kaynağı iyi araştırılmalıdır. Belli kurumsal veya ticari kimliği olmayan yazılımlar her zaman risklidir. Cihazınızı amaçları doğrultusunda uzaktan yönetebilir, açık kapılar oluşturur, kanunsuz işlerde siber saldırı aracı olarak rahatlıkla kullanabilir.

3.2 Zararlı Yazılımlım Güvenliği

Virüsler; bir bilgisayarın sistemine, yazılımına veya performansına zarar verirler. Kendini çoğaltma şeklinde tasarlanmıştır.

Bir solucan; ağ üzerinden diğer bilgisayarlara kendini yayarak güvenlik açıklarını o bilgisayarlarda uzaktan erişim için port açıklıkları oluşturur. Truva atı; zararlı program taşıyan ve yükleyen yazılımlardır. Bunlar virüs ve solucanlar gibi kendi başına kopyalanmazlar. Bir takım ilginç ve masum yazılımların içerisinde, paylaşım ortamlarında kullanıcıların faydalı yazılım diye kurdukları kodlar içerisinde gizlenirler. Faydalı denilen program çalıştırıldığında arka planda bunlar üstlendikleri zararlı görevleri icra ederler.

Spyware; virüs özelliği olup bilgisayarın etkinliği hakkında şifre ve ekran görüntüleri şeklinde bilgi toplar karşıya gönderir. Rootkits, adware, scareware gibi virüs özellikli zararlı yazılımlarda benzer şekilde son kullanıcılar üzerinde siber tehditler oluştururlar[6,11].

Kısaca Virüsler ve zararlı yazılımların şu sakıncaları vardır;

1. Kimlik hırsızlığı
2. Sahtekârlık
3. Silme, hırsızlık ve veri bozulması
4. Yavaş ve kullanılmaz hale gelen bilgisayar ve ağlar.

Bu zararlılara karşı güvenlik şu şekilde sağlanmalıdır;

1. Öncelikle siber tehdit içeren bu zararlı yazılımların sistemlere bulaşma teknikleri kullanıcılar tarafından çok iyi bilinmelidir.
2. Hiç bir trojan siz izin vermediğiniz takdirde sizin bilgisayarınızda çalışamaz.
3. Tanımadığınız kişilerden gelen hiç bir dosyayı açmayın böylece zararlı yazılım bulaşma riski azalır.
4. Herhangi bir programın içerisinde siz farkında olmadan zararlı yüklemeyi engellemek için öncesinde mutlaka otomatik anti virüs taraması yaptırılmalı.
5. Bilgi ve bilgisayar güvenliğini sağlamada en önemli tedbirlerin başında gelen, bilgisayar sisteminin, yama ve güncellemelerle sürekli güncel tutulmalıdır.
6. İnternet üzerinde bilinmeyen programların indirilip, çalıştırılmaması zararlı yazılımlara karşı etkin korunma sağlayacaktır.
7. Virüs korunma yazılımı tek başına bütün kötücül zararlılara karşı koruma sağlayamaz. Kullanılan bilgisayarın güvenlik risk seviyesine göre antispyware türü koruma araçlarda kullanılmalıdır.

Algılanan öge	Uyarı düzeyi	Tarih
Worm:Win32/Rimecud.B	Ciddi	28.11.2012 19:53
Worm:Win32/Rimecud.B	Ciddi	28.11.2012 19:53
Worm:Win32/Rimecud.B	Ciddi	28.11.2012 19:53

Kategori: Solucan

Açıklama: Bu program tehlikelidir ve ağ bağlantısı üzerinden kendi kendine yayılır.

Önerilen eylem: Bu yazılımı hemen kaldır.

Şekil: Örnek bir son kullanıcı virüs tehdidi

3.3 Kişisel Güvenlik Duvarı

Güvenlik duvarı, üzerinde güvenli-güvensiz pek çok bilgi ve kullanıcı barındıran internet üzerinden gelebilecek yetkisiz kaynak erişimlerini engeller. Son kullanıcı ve sistemleri korumada bir süzgeç görevi görür. Ağ trafiği üzerinde bilgi güvenlik riskine karşı izin kontrolü gerçekleştirilen ilk savunma hattıdır. Bu şekilde kullanıcının erişim yapacağı sitelere olan istekler kontrol altında tutularak veri akış yönetimi sağlanır. Giriş/çıkış servis portlarının ve olası atakların takibi ve yönetimi için masaüstü güvenlik duvarı sürekli etkin olmalıdır. Bir kampüs veya şirket ağında merkezi güvenlik duvarının olması son kullanıcının korunma ihtiyacını ortadan kaldırmaz.

Son kullanıcı siber tehditlerini önlemede güvenlik duvarının katkısı şu şekilde özetleyebiliriz.

1. Bir zararlı yazılımın bilgisayara bulaşmasıyla dosyalarınıza uzaktan erişme, görüntüleme veya cihazınızı kontrol altına almak isteyen saldırganlara karşı uyarır.
2. Yeterli ve güncel anti-güvenlik yazılımı olmayan bilgisayarlar bir spam yayma aracı haline getirilmiş olabilir. Güvenlik duvarı yoğun e-posta trafiğini algılayarak uyarı verir.
3. Bazı yazılım ve cihazlara uzaktan varsayılan olarak erişilebilen port veya servisler vardır. Bu kanallardan sızma isteyen davetsiz saldırganlara karşı alarm verir.
4. İstem dışı yazılımlar kurularak, bir bilgisayar sürekli karşı tarafa trafik gönderebilir. Hedef sunucu bir zaman sonra yeni bağlantılara cevap veremez duruma gelir. Son kullanıcı bilgisayarlarının hizmet engelleme şeklinde kullanılmasına ve aşırı kota kullanımını önlemeye yardımcı olur.

Güvenlik duvarı siber saldırılara karşı düzgün yapılandırılmalıdır, eksik ve yanlış tanımlama güvenlik riski oluşturur. Ekranı gelen güvenlik uyarısını dikkate almadan izin verilirse güvenlik duvarının bir koruyuculuğu kalmaz. Yazılım tabanlı güvenlik duvarı; işletim sistemleri üzerine kurulur ve daha fonksiyonel ve etkin kullanımı vardır. Donanımsal güvenlik duvarı ise; ya modeme entegre şekilde yada ayrı cihaz olarak ağı dinler. Bu tür güvenlik duvarı genelde geniş kullanıcı ağılarda kullanıcıların genelini izleme veya kısıtlamalarda mutlaka kullanılır.

3.4 Erişim Güvenliğinin Sağlanması

Erişim güvenliğinde esas olan prensipler;

- **Gizlilik:** Bilgi ya da kaynakların gizlenmesi
- **Orijinallik:** Bilginin kaynağından emin olmaktır.
- **Güvenilirlik:** Veri ya da kaynağın uygunsuz ya da yetkisizce değiştirilmediğinden emin olmaktır.
- **Kullanılabilirlik:** İstenildiği zaman veri ve kaynakların ulaşılabilir durumda olmasıdır.

Kullanıcı girişi güvenlik doğrulaması gerektirmeden yapılan erişimlerden kaçınılmalıdır. Veri iletimini açık okunabilir düzende gönderilmemelidir. Erişim trafiğinin şifreli yani her iki tarafta kodlama ve kod çözme şeklinde bilginin orijinal formuna getirilmesidir. Şifreleme işlemlerinde simetrik ve asimetrik yöntemler kullanılabilir.

Güvenilir bir son kullanıcı erişimi şu şekilde sağlanmalıdır;

1. Eğer bir şirket ağına bağlanılıyorsa arada mutlaka VPN türü sanal şifreli bağlantılar oluşturulmalıdır.
2. Finansal, online alışveriş, bankacılık, e-devlet vb. bağlantılarda mutlaka ssl şifreli https bağlantılar üzerinden gerçekleştirilmelidir.
3. Kablosuz erişimlerde ağ erişim şifresi periyodik olarak değişim yapılmalı.
4. Kablosuz bağlantılarda WEP, WPA ve WPA2 şifreleme seviyesi vardır. Bunlardan yüksek güvenlik seviyesi olan WPA2 dir.
5. İnternete bilinen servis sağlayıcılar üzerinden çıkmak daha güvenilirdir.
6. Cihazları kablosuz erişim sinyali aldığı anda otomatik bağlantı konumunda tutmak tuzak erişimler nedeniyle risklidir.
7. Belli yaşın altındaki çocuklar tuzak sahte, korsan siteleri ayırt edememesi nedeniyle erişim ebeveynlerinin kontrolü altında gerçekleşmelidir.
8. Sitelere erişim şifrelerini çoğu tarayıcılar tutmak ve doğrudan hatırlatılabilir durumda olması siber suçluların işine oldukça yarar[7].

3.5 Sosyal Ağların Kullanım Güvenliği

Siber tehditler açısından günümüz sosyal ağlar, hassas ve kritik bilgilerin elde edilmesi için yaygın kullanılan bilgi toplama kaynağıdır. Saldırı öncesinde seçilen kurbanı ait, bu sitelerden edinilen bilgiler yol göstericidir. Elde edilen her bir bilgi saldırganı yardımcı olur ve çok değerlidir. En değerli bilgi varlıklarından bazıları şunlardır[9]:

- Nüfuz cüzdan bilgileri

- e-devlet bilgileri
- Sağlık güvenlik bilgileri
- Ehliyet, pasaport bilgileri
- İnteraktif banka hesap bilgileri
- Kredi kart bilgileri
- Kurum ve maaş bilgileri
- En önemlisi de her türlü kullanıcı adı ve şifre bilgileri

Bunlardan bir veya birkaçının ele geçirilmesi ile kişisel siber saldırı kapısı aralanmış olur. BFacebook, Twitter, MySpace, Friendster, Xanga ve Blogspot gibi 300 e yakın sosyal ağ içerikli web siteleri vardır[8]. Bu tür siteler genellikle kullanıcı profillerini, kişisel bilgilerini, hobilerini, yerleşim yeri ve çalışma alanlarını, çocuk ve aile bilgilerini, üyeliklerini, alışkanlıkları gibi pek çok detay bilginin profilden takip edilebildiği veri paylaşım siteleridir. Bu kadar geniş kapsamlı paylaşımlar, saldırganların kaçırılmayacağı, tam bir sosyal mühendislik alan haline gelmiştir. Son kullanıcıdan, çalışana, öğrenciden, akademisyene her grup insan bu paylaşımları sıklıkla çekinmeden saatlerce kullanmaktadır.

Güvenli bir sosyal ağın kullanımı için, son kullanıcı aşağıda belirtilen bilinç ve duyarlılıkla hareket etmelidir.

1. Sosyal ağlar üzerinden gerçek kimlikler maalesef gizlenmektedir.
2. Farklı kimliklerle hile, şantaj, rüşvet, korku gibi sosyal saldırı tehditlerini kullanarak kritik bilgileri elde edebilirler.
3. Yanıltıcı maskeler kullanılarak teknik bilgi adı altında yanıltıcı, tuzak yönlendirmeler yapabilirler.
4. İyi niyetli olarak yayımlanan bir haber linkinin veya yazılımın kaynağı mutlaka sorgulanmalıdır. Maalesef sosyal dolandırıcılık olarak ta nitelendirilen bu yöntemle sıklıkla virüs, worm, spam dağıtmaktadırlar.
5. Günümüzün yaygın iz sürme ve bilgi toplama aracı sosyal mühendislik(dostum, arkadaşım) yaklaşımları sorgulanmalıdır.
6. Kişisel bilgilerinizi korumak için atabileceğiniz eylemlerin farkında olun. Bu eylemler şunlardır: Uygun şifre kullanımı, veri yedekleme, uygun anti virüs koruması, herhangi bir şüpheli vakaların veya ihlallerin izlenmesi için program rapor çıktıları belli periyotlarda incelenmelidir.
7. Paylaşım sitelerinde çalıştığınız kurum, aileniz ya da bir arkadaşınızın hesap bilgileri kullanılmamalıdır.

8. Her türlü şifre işlemleri girilirken azami gizlilik sağlanmalıdır. İnternet kafe, otel ve halka açık erişim yerlerinden üyelik girişi ve şifre işlemi yapılmamalıdır[10].

4. Sonuç

Bu çalışma ile son kullanıcı siber güvenliği sorunu işlenmiştir. Geniş halk kitlelerinin kişisel internet kullanımında alması gereken politikalar ve teknik yaklaşımlar sunulmuştur. Sonuç olarak siber güvenliği bir kullanıcı bilgisayarından üzerinden özetlenecek olunursa. İnternet erişimi olan kişisel bir bilgisayar; normalden daha yavaş çalışıyorsa, tarayıcınız açık olmadığı halde sürekli bir ağ hareketliliği varsa, güvenlik yazılımları veya uygulama yazılımları beklenilmeden tepkiler veriyorsa, disk üzerinde istem dışı dosya artışı oluyorsa, sizin yüklediğiniz ve bilmediğiniz yeni program artışları olmuşsa bilgisayarınız siber tehditlere karşı risk taşımaktadır. Bu ve benzer güvenlik zafiyetlerinin olduğu düşünüldüğünde derhal bu güvenlik zafiyeti açıklığının kaynağı tespit edilmelidir. İlk olarak işletim sistemi ve güvenlik yazılımlarının güncelliği ve doğruluğu kontrol edilmeli. Kurulu programlar gözden geçirilmeli varsa kullanılmayan şüpheli bir yazılım derhal kaldırılmalı. Halen güvenlik riskinin devam ettiği düşünülüyorsa cihazdaki kişisel belge ve bilgilerin önceki ve son yedekleri güvenli bir makineden taratılarak ayrı bir kayıt ortamına aktarılır. Bilgisayarın yeniden kurulumu sağlanır. Öncelikle disk biçimlendirilerek olası zararlı yazılımlardan temizlenir sonra; işletim sistemi, anti-virüs, kişisel güvenlik duvarı ve diğer ihtiyaç programları yüklenerek tüm yazılım güncelleme işlemleri gerçekleştirilir. Özellikle internet uygulamalarında kullanılan önceki şifrelerin tamamı değiştirilir[12].

Bilgisayarı kullanan bireyler güncel siber tehditlere karşı, sosyal paylaşım siteleri başta olmak üzere olası siber tehditler konusunda bilinçlendirilir. Neredeyse hemen her gün medyada yeni bir siber saldırı yaşanmışlığı ve mağdur örneklerini duymaktayız. İnternet erişimi ile çok her an kapımızda bekleyen bu tür siber tehditlere karşı bu bildiride belirtilen en asgari düzeyde önlem ve tedbirlerin alınması kaçınılmaz bir zorunluluk olmuştur.

5. Kaynaklar

[1] International Telecommunications Union World Internet Usage And Population Statistics, Dünyada İnternet Nüfus Artışı, <http://csrc.nist.gov/publications/nistir/>

[2] University of California, Riverside University Ave <http://cnc.ucr.edu/>.(2012)

[3] Canbek, G., Sağiroğlu, Ş., “Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri,” Aralık 2006, ISBN 975-6355-26-3

[4] Vorobiev, A., & Bekmamedova, N. (2007). An ontological approach applied to information security and trust. Information Systems, 865–874.

[5] Siber Güvenlik ve Gizlilik Koruması Carnegie Mellon Yazılım Mühendisliği Enstitüsü'nün CERT Coordination Center: www.cert.org/ [2011]

[6] Online güvenlik kontrolleri: <http://www.staysafeonline.org/tools-resources/free-security-check-ups/> [2011]

[7] Küçük İşletmeler Ev Kullanıcıları için National Cyber Security Alliance: <http://www.staysafeonline.info/> [2012]

[8] Fake Profiles On Fakebook /Facebook. <http://www.Pc1news.com/> [2012]

[9] SANS (SysAdmin, Denetim, Network, Güvenlik) En Kritik İnternet Güvenlik Açıkları: www.sans.org/top20/ [2011]

[10] Siber Güvenlik Tehdit Merkezleri Open Web Application Security Project: www.owasp.org/ [2012]

[11] Şahinaslan, Ö., Şahinaslan, E., Borandağ, E., Can, E., “Güvenlik Tehdidi Oluşturan Spam Saldırılarına Karşı Önlemler”, ABGS 2010 – Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2010.