Kablosuz Yerel Alan Ağlarına Sızma Uygulaması ve Temel Güvenlik Önerileri

M. Z. Gündüz ve R. Daş

***Özet*- Bilişim ağ sistemlerinde veri paylaşımı ve internet kullanım talepleri için kablosuz ağ sistemleri, yaygın olarak kullanılmaktadır. Ancak, bu ağlarda önemli birçok güvenlik açıklıkları bulunmakta ve bu ağlar zayıflıklardan dolayı saldırganlar tarafından sistem parolalarının elde edilmesine karşı savunmasız kalmaktadırlar. Bu ağların güvenliğini sağlamak için antivirüs yazılımları, güvenlik duvarları, saldırı tespit sistemleri, şifreleme, parola politikaları gibi teknolojiler ile bilinçli kullanıcılar önemli rol oynamaktadır.**
Bu makale çalışmasında, kablosuz ağ parolalarının elde edilmesi ve parola saldırıları üzerine bir uygulama gerçekleştirilmiş ve kablosuz ağ sistemlerinin güvenliğini artırmak için alınabilecek temel güvenlik önerileri belirtilmiştir.

***Anahtar Kelimeler*–Ağ Erişim Noktası, Kablosuz Ağ Güvenliği, Sızma, Parola Saldırıları**

***Abstr*act – Wireless network systems are widely used for data sharing and internet usage demands in information network systems. However, there are many important security gaps in these networks, and because of these weaknesses, networks remain vulnerable against the obtaining of the passwords by the attackers. To ensure the security of these networks, technologies such as antivirus software, firewalls, intrusion detection systems, encryption, password policies and conscious users play an important role.**
In this paper, basic security measures that can be taken to improve the reliability of wireless network systems have been focused on, and an application on obtaining the wireless network password and password attacks has been discussed.

***Keywords*–Network Access Point, Wireless Network Security, Penetration, Password Attacks**

I. GİRİŞ

Teknoloji alanındaki hızlı gelişmeler sayesinde insan yaşamındaki birçok işlem de kolaylaşmaktadır. Günlük iş süreçlerinin elektronik ortamlara taşınması, manyetik ortamdaki bilgilerin paylaşılması, e-devlet uygulamaları, veritabanlarının ortak kullanımı gelişen teknoloji sayesinde daha kolay ve hızlı bir şekilde gerçekleştirilmektedir. Özellikle bulut teknolojisi gibi ortak kullanım sağlayan sistemlerin ortaya çıkması ve geniş bir kullanım alanı bulması ile kurulan bu sistemler bilişim ağ güvenliğinin gerekliliğini ve önemini daha da artmıştır. Ağ erişimlerinin kolay olması, güvenlik açıklarını ve zaafiyetlerini kaçınılmaz bir hale getirmiştir. Bu bağlamda olası tehdit ve tehlikelerin araştırılıp, bunlara karşı her türlü gerekli önlemlerin alınması oldukça önem kazanmaktadır [1-2]. Bunlara paralel olarak dijital saldırganlar tarafından, sanal ortamlarda yapılan her türlü saldırılar da artmaktadır.

Bingöl Üniversitesi,Teknik Bilimler Meslek Yüksek Okulu, 12000, Bingöl / TÜRKİYE (e-mail: *zekeriyagunduz@gmail.com*)
Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, 23119 Elazığ / TÜRKİYE (e-mail*: resuldas@gmail.com*)

Bu saldırılar, kişisel veya kurumsal anlamda veri hırsızlıklarına veya veri kayıplarına sebep olmaktadır. Ağ sistemleri günümüz iletişim teknolojilerinin vazgeçilmez ana omurgasını oluşturmaktadır. Veriye ulaşma hızı ihtiyacının, eskiye nazaran daha önemli olduğu çağımızda kablosuz ağların gelişmesi kaçınılmaz olmuştur. Günümüzde insanoğlunun sosyal bir varlık olarak yaşadığı alanlarda kablosuz ağların bulunması neredeyse zorunluluk haline gelmiştir. Bilgisayar virüsleri, truva atları, arka kapı uygulamaları, ARP zehirlemeleri, parola saldırıları, sosyal mühendislik, son kullanıcıların bilinçsiz kullanımından kaynaklı saldırılar gibi durumlar bilgisayar ağları üzerinde büyük bir tehlike oluşturmaktadır[3].

İster büyük ölçekli ister küçük ölçekli olsun bir ağ sisteminin istendiğinde üçüncü kişiler tarafından dinlenmesi artık basit araçlarla bile kolay bir şekilde yapılabilmektedir. Bu dinlemeler sadece ağı dinlemek şeklinde ise pasif saldırılar, ağ üzerindeki bilgilerin ya da şifrelerin değiştirilmesi veya cracklenmesi(kırmak) ise aktif saldırı olarak adlandırılmaktadır. Özellikle saldırganların parola çalma, paroların ele geçirildikten sonra değiştirilmesi ve sistemde istedikleri gibi dolaşmaları bir aktif saldırı türü olup ağ yöneticileri için istenmeyen durumlar olarak ortaya çıkmaktadır.

Bu makale çalışmasında, kablosuz yerel alan ağlarına izinsiz erişim sağlamak için kullanılan parola saldırı yöntemleri incelenerek, güvenlik zafiyetlerinin ortaya konulması için bir saldırı uygulaması gerçekleştirilmiştir. Bu saldırı uygulamasından elde edilen sonuçlar değerlendirilerek, kablosuz bir ağın parola güvenliğinin artırılabilmesine yönelik güvenlik önlemleri ortaya konulmuştur.

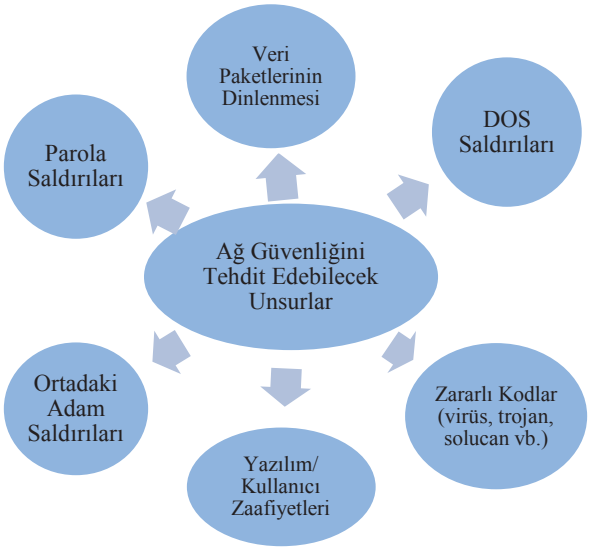
II. KABLOSUZ YEREL ALAN AĞ GÜVENLİĞİ

Kablosuz iletişim teknolojileri her geçen gün toplumsal yaşam içerisindeki yerini daha da belirginleştirmektedir. Günümüz şartlarında teknoloji ile ilişkili olan herkes her geçen gün önemi artan bu teknolojiler hakkında bilgi sahibi olmak ve temel ihtiyaçları için pratik uygulamalar yapabilmek zorundadır.

Kablosuz ağlar, RF (Radyo Frekansı) teknolojisini kullanarak havadan bilgi alış verişi yapan esnek bir iletişim sistemidir. Kablosuz yerel ağlar kablolu iletişime alternatif olarak uygulanan RF olup, 3Hz ile 300GHz aralığındaki frekanslara verilen genel isimdir [4]. Günümüz kablosuz küçük yerel ağların (*Wireless Local Area Network - WLAN*) kurulmasında temel ağ cihazı olarak *erişim noktası* (access point) elemanı kullanılmaktadır.

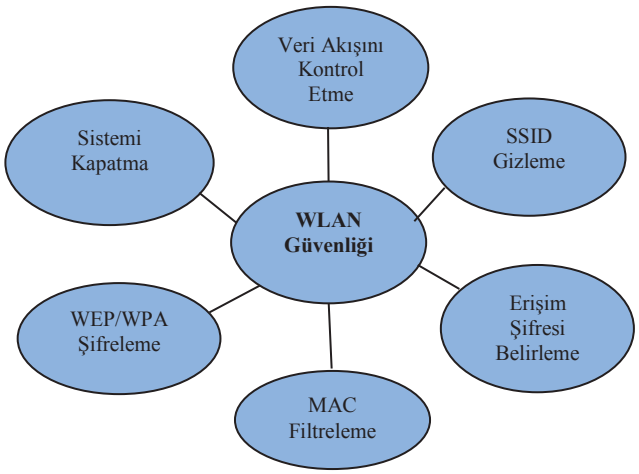
Bilişim ağ sistemlerinde, ağ güvenliğini tehdit edebilecek birçok unsur vardır. Bu unsurlar Şekil-1'de gösterildiği gibi ağdaki veri paketlerinin dinlenmesi, hizmet dışı bırakma saldırıları, ortadaki adam saldırıları, parola saldırıları, yazılımlardaki zafiyetlerin kötüye kullanımı, zararlı kodlar

(virüs, trojan, solucan vb.) ve sosyal mühendislik zaafiyetleri şeklinde sayılabilir.



Şekil 1. Ağ güvenliğini tehdit edebilecek unsurlar

Kablosuz ağlara izinsiz erişim sağlamak isteyen kullanıcı profilleri genel olarak meraklı kullanıcılar, başkasının internetini kullanmak isteyenler ve hacker/crackerlar olabilir. Bu kullanıcıların saldırı ve izinsiz girişimlerini engellemek için birçok seçenek bulunmaktadır. Özellikle Şekil-2'de gösterilen bazı temel önlemler bunlara örnek verilebilir. İnternet erişimi için kurulan erişim noktası cihazlarının, varsayılan arayüz erişim şifrelerinin değiştirilmemesi de güvenlik zaafiyelerine sebep olabilmektedir. Tablo-1'de yaygın kullanılan bazı ADSL modemlere ait varsayılan erişim bilgileri verilmiştir. Saldırganlar bu erişim bilgilerini ele geçirebilmek için gerektiğinde her türlü yöntemi kullanmaktan çekinmezler.



Şekil 2. WLAN için temel güvenlik önlemleri

Saldırganlar pek çok yöntem ve farklı araçlar kullandıkları için yapılabilecek her türlü saldırılara karşı koyabilecek ve internet kullanıcılarını tamamen koruyacak bir savunma sisteminden veya yazılımından söz etmek mümkün değildir [5,6]. Ağ ve bilgi güvenliğinin sağlanabilmesi içim kullanıcıların sürekli farklı platformlarda eğitilmesi zorunlu hale gelmiştir.

İnsan zafiyetlerinden yola çıkılarak yapılan sosyal mühendislik yöntemleri ile de sistem şifrelerinin üçüncü kişilerin eline geçmesi mümkündür. İnsanların birileri tarafından yönlendirilerek, istenilenlerin yapılmasının sağlanması olarak da bilinen sosyal mühendislik sayesinde şifrelerin elde edilebileceği artık bilinen bir gerçektir. İlk hackerlardan olan Kevin Mitnick'e göre, bir sistemin güvenlik halkasındaki en zayıf halka, insandır [6]. Bu durumda sosyal mühendislik kullanılarak yapılan saldırılara karşı kullanıcıları bilgilendirmek ve bilgi güvenliği farkındalığının oluşturulmasını sağlamak çok önemlidir. Özellikle bilişim sistemlerinin her alanda aktif olarak kullanılması dikkate alındığında, bunun zorunluluk olduğu açıkça anlaşılır.

TABLO 1
BAZI ADSL MODEMLER İÇİN VARSAYILAN ERİŞİM BİLGİLERİ

Marka	ADSL Modem IP	Kullanıcı Adı	Parola
Asus	192.168.1.1	admin	admin
Aztech	10.0.0.2	admin	admin
Aztech	192.168.1.1	admin	admin
D-Link	192.168.1.1	admin	admin
Huawei	192.168.1.1	admin	admin
Huawei	192.168.1.1	admin	ttnet
Link SYS	192.168.1.1	admin	admin
TP-Link	192.168.1.1	admin	admin
TP-Link	192.168.1.1	admin	ttgalaksi
TP-Link	192.168.1.1	admin	ttnet
USB Robotics	10.0.0.2	admin	admin
ZyXEL	192.168.1.1	admin	1234
Airties	192.168.2.1	admin	ttnet

Özellikle büyük ağ sistemleri güvenliğini sağlamak için antivirüs yazılımları, güvenlik duvarları, saldırı tespit sistemleri, veri şifreleme teknolojilerinin etkili kullanımı ve güvenlik politikalarının iyi bir şekilde oluşturularak uygulanması gerekmektedir.

A. Kablosuz Yerel Ağ Üzerinde Parola Saldırıları

Verilerin ve sistemlerin gizliliğinin korunmasında parolaların kullanımı büyük önem taşımaktadır. Doğru kullanıldıklarında sistemin korunmasında en etkili yöntemlerden biri olurken bazen de ağ sistemlerinin en zayıf yönleri olmaktadırlar. Çünkü parolaların bir şekilde üçüncü kişiler tarafından öğrenilmesi onlara pek çok yetki sağlayabilir. Parolalara ilişkin belirli ilkelere uyulmamış ve bazı önlemler alınmamış ise, saldırganlar tarafından ele geçirilebilirler. Saldırganlar özel olarak hazırlanmış parola kırma yazılımlarıyla saniyede yüzlerce parolanın denenmesini sağlayabilirler [7-10]. Parola kırma yazılımları harf sayı kombinasyonlarını belli bir sırayla oluşturup deneyebildikleri gibi kendilerine verilen yüz binlerce kelimelik sözlüklerdeki kelimeleri de kullanabilmektedir. Bu yüzden akılda tutulması kolay şifrelerin genellikle elde edilmesi kolaydır. Bir kullanıcıya ait parola ya da şifrelerin ikinci şahısların eline geçmesi, sadece o kullanıcıya ait güvenlik zaafiyeti oluşturmaz. Bazen söz konusu şifre ya da parola aracılığı ile ağdaki diğer noktalara da erişim

sağlanabilir. Sadece bir kullanıcının bilgi güvenliği zaafiyeti oluşturması bile, farkında olmadan ağın ya da sistemi kullanan tüm kullanıcıların zarar görmesine sebep olabilir.

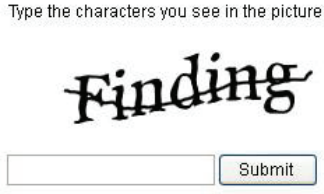
B. Kriptografik Parola Saldırıları

Şifrelenmiş bilgilerin şifresini çözmek için yapılan saldırılardır. Bu saldırılar, kriptoanaliz yöntemleri ile gerçekleştirilmektedir. Literatürde, kriptografik saldırılar ile ilgili bilinen birçok saldırı türü vardır. Bunlar kaba kuvvet saldırısı (brute force attack), sözlük saldırısı (dictionary attack), ortadaki adam saldırısı (man in the middle attack), sadece şifreli metin (chipertext only), bilinen düz metin (known plaintext), seçilen düz metin veya şifreli metin (chosen plaintext, chipertext), uyarlanır seçili düz metin (adaptive chosen plaintext) ve ilişkili anahtar saldırısı (related key attack) gibi saldırı türü örnekleri verilebilir [9]. Bu saldırılar aktif saldırı grubuna girerler. Saldırılar veya saldırılarda kullanılan araçlar, teknik açıdan gittikçe karmaşıklaşırken, bu saldırıyı yürütecek saldırganın sistem üzerinde ihtiyaç duyduğu bilginin seviyesi de o derecede azalmaktadır [7].

C. Ağ Güvenliği İçin Parola Politikaları Oluşturma

Ağ sistemlerindeki parolaların saldırganların eline geçmesini engellemek için güvenli parola politikaları oluşturulmalıdır. Ağ kullanıcıları tahmin edilmesi veya kırılması zor olan parolalar kullanmaya teşvik edilmeli gerekirse zorlanmalıdır. 4-5 karakterden oluşan şifreler çok kısa sürelerde kırılabileceğinden güvenli sayılmazlar [11]. Günümüz sistemlerinde güvenli sayılabilecek bir parola en az 8 karakterden oluşmalıdır. İçerisinde farklı karakterlerin ve sayıların bulunduğu parolaların kırılma sürelerinin yıllar alacağından dolayı daha güvenli olduğu bilinmelidir.

Sistem parolalarını ele geçirmek için yapılan parola saldırıları, genellikle özel yazılımların veritabanlarındaki parola kombinasyonlarının hızlıca denenmesi ile yapılır. Bu yazılımlar parolaları elde etseler bile sistemlere sızmalarını engellemek için CAPTCHA (Completly Automated Public Turing Test To Tell Computers And Humans Apart) resimleri kullanılabilir. Şekil-3'de görüldüğü gibi CAPTCHA resimleri genellikle üzerinde karmaşık halde bulunan ve metin okuma yazılımları tarafından zor okunabilen karakter kombinasyonları bulundururlar. Bu karakterler karakter tanıma yazılımlarıyla bile zor tanınabilecek şekilde oluşturulurlar. Bu karakterler bilgisayar veya robotlar tarafından tanınmamalıdır. Ancak insan beyninin algılayabileceği karakterlerin tespit edilebileceği karmaşık şekildedirler. CAPTCHA aracılığı ile otomatik parola deneme yazılımlarının işlevsiz kalması sağlanabilir [4].



Şekil 3. CAPTCHA örneği

Şifrelerin güçlü olması, içerdiği karakterlerin karmaşıklığıyla doğru orantılıdır. Artık bazı kamu kuruluşlarının bile şifre alırken kullanıcılara basit şifreler vermeyeceği yönünde çalışmaları vardır [12]. Bazı sistemlerde ise belli bir sayıda yapılan başarısız giriş sonunda gizli soru uygulaması yapıldığı görülmektedir.

III. KABLOSUZ AĞ ERİŞİM NOKTASINA İZİNSİZ SIZMA UYGULAMASI

Bu bölümde, bir kablosuz yerel ağına giriş parolasının nasıl elde edilebileceği adım adım anlatılmaktadır.

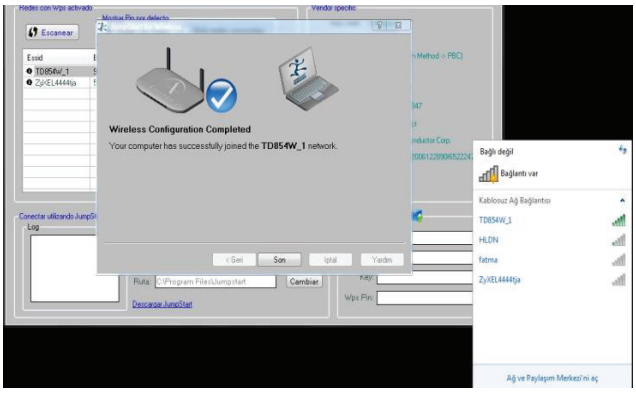
A. Kablosuz Yerel Ağların Tespit Edilmesi

Ortamda mevcut olan kablosuz yerel alan ağ erişim noktaları, Windows işletim sistemlerinin ağ yönetiminden yararlanılarak, Şekil-4' de görüldüğü gibi kolayca kablosuz yayın yapan cihazın yayın adı olan SSID özellikleri rahatlıkla görülebilmektedir. Bu çalışmada Şekil-1 de görülen ve çekim gücü en yüksek olduğu için TD854W_1 isimli ağ erişim noktasının bağlantı şifresi elde edilmiştir.

Şekil 4. Ortamda bulunan kablosuz ağ erişim noktaları

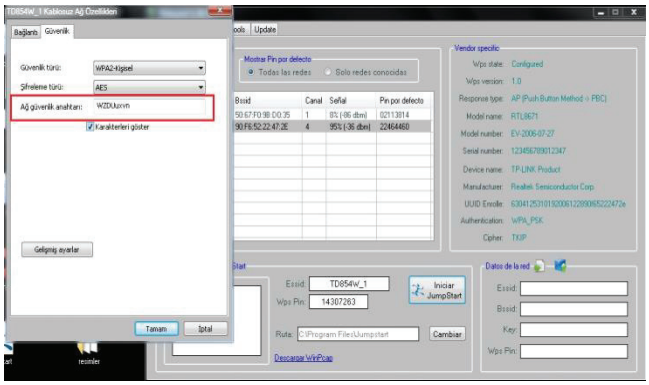
B. Kablosuz Ağ Erişim Noktasına Saldırının Yapılması

Ağ erişim ortamında tespit edilen *TD854W_1* isimli ağ erişim cihazının *giriş* şifresini elde etmek için saldırı gerçekleştirilmiştir. Bu saldırı için Brute Force saldırıları için kullanılan *Jumpstar* ve *Dumpper* araçları birlikte kullanılmıştır [13]. Bu araçlar sayesinde yapılan şifre kırma saldırısının başarılı bir şekilde gerçekleştiği Şekil 5'de gösterilmektedir.



Şekil 5. Kablosuz ağ cihazına izinsiz sızmanın başarılması

Gerçekleştirilen bağlantının ardından *TD854W_1* isimli cihaz şifresinin Şekil-6'daki gibi olduğu ağ özelliklerinden görülmektedir.



Şekil 6. *TD854W_1* isimli cihaz şifresinin açık hali

C. Kablosuz Ağa Sızma Uygulaması Sonuçları

Gerçek zamanlı olarak gerçekleştirilen uygulamada ağ güvenliğindeki parola zafiyetlerinin görülebilmesi için bir farkındalık oluşturulmuştur. Çünkü bir saldırının nereden ve ne şekilde geleceğini bilmek, güvenlik önlemlerinde dikkate alınması gereken en öncelikli savunmadır.

Uygulama sonucunda elde edilen bulgulara göre aşağıda belirtilen önemli çıkarımlar elde edilmiştir:

1) Farklı kablosuz ağ erişim noktalarının güvenliklerinin genellikle doğru yapılandırılmadığı tespit edilmiştir. Eğer gerekli güvenlik önlemleri alınmadı ise; basit bazı işlemler ile bu erişim noktalarının ağlarına dâhil olunarak istenilen kullanıcılar izlenebilmekte, yönetim paneli ele geçirilebilmekte ve hatta ağ yöneticisinin haberi olmadan sistem şifreleri değiştirilebilmektedir.
2) Güçlü kriptolama teknikleri ile oluşturulmuş şifrelerin kırılması neredeyse imkânsızdır. Teorik olarak kırılması mümkün olsa bile, uygulamada kriptolu şifrelerin elde edilmesi uzun süre ve yüksek maliyet gerektireceğinden dolayı neredeyse mümkün değildir.
3) Parola kırma yazılımları ile ağ üzerinden kablosuz ağ erişim elemanlarına aşırı yüklenilmesinden dolayı bu cihazların zarar görebileceği sonucu gözlemlenmiştir. Bu tür cihazlar; işlemci güçleri çok fazla olmadığı için aşırı ısınma neticesinde zarar görebilmektedir. Bu makale çalışmamız için gerçekleştirilen şifre kırma deneme uygulamalarında işlem yoğunluğundan dolayı, cihazın aşırı ısınmaya bağlı olarak zarar görüp çalışmadığı gözlemlenmiştir.
4) Şifre kırma saldırılarını gerçekleştiren kişilerin kullandıkları bilgisayarların işlemci güçleri de şifrenin elde etme sürecini etkilemektedir. Özellikle güçlü işlemcilerde işlemlerin daha hızlı gerçekleştiği ve şifre tespitinde zaman kazanıldığı ortaya konulmuştur.
5) 12345, abcd, 123abc gibi basit şifrelerin şifre kırma için kullanılan araçların veritabanlarında yaygın olarak bulunmasından dolayı, bu şifrelerin çok daha kolay elde edildiği gözlemlenmiştir.
6) Tablo-1'de verilen ve varsayılan olarak çalışan cihazların arayüzlerine, şifre kırma yazılımlarına ihtiyaç kalmadan kolaylıkla erişim sağlanabildiği görülmüştür.
7) Ağ şifresini kırma yazılımlarının ağa saldırı sırasında modemlere aşırı yüklenmesinden dolayı saldırıdan habersiz şekilde web ortamında dolaşan kullanıcıların internet hızının fark edilebilir seviyede düştüğü görülmüştür.
8) MAC filtremelerinin WLAN güvenliğini sağlaması açısından etkili oldukları gözlemlenmiştir.
9) Kampüs ağlarında kullanılan kablosuz erişim noktalarında kullanıcı sayısı çok fazla ise bu ortamlarda kablosuz ağ ayarlarının daha yönetilebilir olarak tasarlanması gerekmektedir.
10) Güvenlik açısından özellikle tüm ağ aktif cihazlarında günlüklerin tutulması sağlanmalı ve önem durumuna göre, gerekirse yedekleme yapılması sağlanmalıdır. Böylece kütüklerde kayıtlı bulunan saldırı ve saldırganlara ait bilgilere erişilebilir.

IV. SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin yaygınlaşması ile günlük hayatımızdaki iş ve işlemler elektronik ortamlarda artık daha hızlı yapılmaktadır. Bu durum, bilgi güvenliğinin sağlanmasını zorunlu hale getirmektedir. Bu nedenle kullanıcılar yaptıkları iş ve işlemlerde bilginin öneminin farkında olup, bu konuda güvenlik unsurlarını, politikalarını ve güvenlik süreçlerini uygulamak zorundadırlar. Böylece belli oranda, karşılaşılabilecek sorunlar ve tehlikeler azaltılabilecek, işgücü, zaman ve parasal kayıplar önlenebilecektir. Aynı zamanda, internet üzerinden gelebilecek zararlı yazılımlara veya program parçacıklarına karşı kişisel ve kurumsal bilgi güvenliğinin arttırılmasına katkılar sağlanacaktır [5, 14-15,17].

Bilgi güvenliği konusunda güvenlik açıklarının önlenebilmesi için kişi ve kurumların en basitten, çok daha karmaşık güvenlik yöntemlerine kadar bir dizi önlemler almaları gerekmektedir [16-17]. Ancak, tüm önlemler alınmış olsa da, sürekli geliştirilen saldırı teknikleri yüzünden, hiç kimse ve hiç bir kuruluşun kendini tam olarak güvende hissetmesi mümkün değildir. Buna paralel olarak saldırıların her geçen gün farklı türlerde ve kendini geliştirerek ortaya çıkmasından dolayı güvenliğin statik değil, dinamik bir sürece sahip olması gerektiği unutulmamalıdır.

Yapılan çalışma ve uygulamalar sonucunda elde edilen bulgular doğrultusunda hem son kullanıcılar hem de ağ yöneticileri için, genelde tüm ağlar özelde ise kablosuz yerel alan ağları üzerinde ağ şifrelerinin elde edilmesine karşı alınabilecek güvenlik önlemlerin en önemlileri şu şekilde belirtilebilir:

1) Ağ sistemi üzerinde bulunan güvenlik duvarı üzerindeki parola politikaları analiz edilerek, detaylıca belirlenmelidir.
2) Ağ sisteminde sniffing işlemlerinin tespiti için wireshark [18] gibi ağ dinleme araçları kullanılmalıdır.
3) Ağ aktif cihazları arayüz bağlantı şifreleri, belirli periyotlarda değiştirilmelidir. Bunun için de bir parola /şifre politası belirlenmeli, bunların uygulanması ve takibinin yapılması sağlanmalıdır.
4) Ağ ve bilgi güvenliği ile ilgili güncel konu ve bilgiler takip edilmelidir.
5) Yönlendiricilerin erişim hakları, erişim protokolleri güvenliği, şifrelerin güvenliğinin sağlanması, gereksiz

servislerin kapatılması gibi yapılandırma ayarlamaları yapılmalıdır.

6) Özellikle web ortamında kullanılan şifreler dikkatli kullanılmalıdır ve sadece kişiye ait olmalıdır.
7) Web ortamında güvenliğin hiçbir zaman tam olarak sağlanamayacağı unutulmamalıdır.
8) Sosyal mühendislik yöntemleriyle bile ağ şifrelerinin yakın çevredeki insanlar tarafından elde edilebileceği unutulmamalıdır.
9) Ağ şifresinin belli aralıklarla değiştirilmesinin faydalı olabileceği unutulmamalıdır.
10) Sazan avlama türündeki saldırılarda çoğunlukla insanların bilgisizliğinden, tecrübesizliğinden ve zaaflarından yararlanıldığı unutulmamalıdır [7].
11) İşletim sistemlerine ait güncellemeler düzenli olarak yapılmalıdır.
12) Ağ erişim noktasının SSID yayın adı kapatılmalıdır.
13) WEP şifrelemede en az 128 bir şifreleme tercih edilmelidir.
14) Kullanılacak olan şifrelerin tahmininin ve kırılmasının zor olacak şekilde belirlenmesi gerekmektedir.
15) Kullanılmadığı zaman kablosuz internet erişimi kapatılmalıdır.
16) İşletim sistemi ve programlara ait güvenlik ve sistem güncellemeleri ve yamalarının düzenli olarak yapılması ve bunların en güncel olanlarının kullanılması sağlanmalıdır.
17) Wireshark gibi ağ dinleme programları aracılığı ile ağ küçük bile olsa ağ veri akışı arasıra ağ yöneticisi tarafından denetlenmelidir.
18) Son kullanıcılar varsayılan olarak verilen modem arayüzüne bağlanma şifrelerini güvenli bir şekilde değiştirme konusunda bilgilendirilmelidir.
19) Kablosuz ağlar dâhil her türlü ağ sistemine izinsiz erişimin hukuki yaptırımının olduğu bilinmelidir.

Yukarıda ortaya konulan öneriler dikkate alındığında kablosuz yayın yapan ağ erişim noktaları büyük ölçüde şifre kırma saldırılarından korunacaktır. Bunlara ek olarak güçlü şifreleme algoritmalarının tercih edilmesi ve bu algoritmaların güçlendirilmesi şifre kırma saldırılarının zorlaştırılmasında büyük rol oynayacaktır. CAPTCHA gibi sadece insanlar tarafından okunabilen karakterlerin ağ şifrelemelerinde güvenlik kodu olarak kullanılmaları parola kırma saldırılarının tamamen engellenmesini sağlayabileceği düşünülmektedir.

Bu makale çalışmasında, gerçekleştirilen uygulamalar sonucunda kullanıcıların çoğunlukla kablosuz alan ağlarına yönelik parola saldırı ve tehditlerinden haberdar olmadığı anlaşılmıştır. Kurum veya kullanıcıların ciddi bir saldırıya uğramaması ve bu anlamda çeşitli güvenlik zafiyetleri ile karşılaşılmaması için konuya gereken önem verilmelidir. Bilgi birikiminin arttırılması, ağ parola güvenliğine yönelik hassasiyet gösterilerek gerekli tüm önlemlerin alınması ve bilgi güvenliği farkındalığının oluşturulması gerekmektedir. Ağ ve internet hizmeti sunan ve alan her kurum, kuruluş ve kullanıcının ağ güvenliği konusunda yeterli bilgilere sahip olması ve bu bilinçle uygulamaların gerçekleştirilmesi gerekmektedir.

KAYNAKLAR

[1] Bıçakcı, K., "Kullanışlı Güvenlik İçin Temel Prensipler", 4. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (4th International Conference on Information Security and Cryptology), 06-08 Mayıs 2010, Ankara.
[2] Daş, R., Kara, Ş., Gündüz, M.Z., "Casus Yazılımların Bilgisayar Sistemlerine Bulaşma Belirtileri ve Çözüm Önerileri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[3] Burlu, K., 2010. "Bilişimin Karanlık Yüzü", Nirvana Yayıncılık, Ankara.
[4] Kuzu, A., 2009. Bilgisayar Ağları ve İletişim, Nobel Yayın Dağıtım, Ankara
[5] Gündüz, M.Z., 2013. "Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti", Yüksek Lisans Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü, Elazığ.
[6] Şenol, A., Karacan, H., "Sazan Avlama(Phishing):Kullanılan Teknikler ve Bunlardan Korunma Yöntemleri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[7] Canbek, G., Sağıroğlu, Ş., Bilgi,Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme, Politeknik Dergisi, Cilt 9, sayı:3, 2007, Ankara, Türkiye.
[8] Elbahadır, H., 2011. Hacking Interface, Kodlab Yayıncılık, İstanbul.
[9] Canbek, G., Sağıroğlu, Ş., Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri:Bir İnceleme, Erciyes Üniversitesi Fen Bilimleri Dergisi, sayı:23, 2007.
[10] Baykara, M., Daş, R., Karadogan, İ., "Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi", 1st International Symposium on Digital Forensics and Security (1. Uluslararası Adli Bilişim ve Güvenlik Sempozyumu)", 20-21 Mayıs 2013, Elazığ.
[11] Özseven,T., Bilgisayar Ağları, Murathan Yayınevi,Trabzon, 2012.
[12] *İnternet*:http://www.haberjet.net/teknoloji/internet/3456-ile-baslayan-sifreler-artik-olmayacak!-h883.html, Erişim Tarihi: 05.07.2014
[13] *İnternet*:http://www.webdeneyim.com/wpapsk-wpa2psk-ile-korunan-modemlerin-sifresini-kirma, Erişim Tarihi: 08/09/2014.
[14] Yıldırım Okay, F., Özdemir , S., "Kablosuz Algılayıcı Ağlarda Güvenli Ortam Erişim Protokkolleri", 5. Uluslararası Bilgi Güvenliği ve Kriptoloji Konf. (5th International Conference on Information Security and Cryptology), 17-18 Mayıs 2012, ODTÜ, Ankara.
[15] Gündüz, M.Z., Daş, R., "Yerel Alan Ağları İçin IP Tabanlı Saldırı Tespit Uygulaması ve Güvenlik Önerileri", 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı (6th International Conference on Information Security and Cryptology), pp.302-307, 20-21 Eylül 2013, ODTÜ, Ankara.
[16] Sağıroğlu, Ş., Ersoy, E., Alkan, M., "Bilgi Güvenliğinin Kurumsal Bazda Uygulanması", 2. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı (II. Information Security and Cryptology Conference with International Participation), pp.200-207, 13-14 Aralık 2007, Ankara.
[17] Vural, Y., Sağıroğlu, Ş., "Kurumsal Bilgi Güvenliğinde Güvenlik Testleri ve Öneriler", Gazi Üniv. Müh.Mim.Fak.Dergisi, 26(1), pp. 89-103, 2011.
[18] *Internet:* www.wireshark.org, Erişim Tarihi: 07/07/2014.

M. Zekeriya GÜNDÜZ, 1983 yılında Bakırköy'de doğdu. 2006 yılında Süleyman Demirel Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Sistemleri Öğretmenliği bölümünü bitirdi. 2006-2010 yılları arasında Milli Eğitim Bakanlığına bağlı Endüsri Meslek Liselerinde Bilişim Teknolojileri öğretmeni olarak görev yaptı. Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik ve Bilgisayar Eğitimi Anabilim dalında Ağ güvenliği konusunda " Bilişim Suçlarına Yönelik IP Tabanlı Delil Tespiti" adlı yüksek lisans çalışmasını tamamladı. Halen Bingöl Üniversitesi Teknik Bilimler Meslek Yüksek Okulu, Bilgisayar Programcılığı bölümünde öğretim görevlisi olarak çalışmaktadır.

Resul DAŞ, 1975 yılında Elazığ'da doğdu. 1999 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğr. bölümünü, 2002 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Sistemleri alanında yüksek lisansını tamamladı. 2008 yılında aynı üniversitenin Elektrik-Elektronik Mühendisliği bölümünde doktora eğitimini tamamlayarak, bu alanda Doktor ünvanını aldı. 2000–2011 yılları arasında Fırat Üniversitesi Enformatik bölümünde öğretim elemanı olarak çalıştı. Kasım 2011 yılından beri Fırat Üniversitesi Teknoloji Fakültesi, Yazılım Mühendisliği

bölümünde öğretim üyesi olarak görev yapmaktadır. Bilgisayar Ağları, Ağ Güvenliği, Web ve Veri Madenciliği, Bilgi Keşfi, Adli Bilişim ve Güvenlik araştırma konularında çalışmalar yapmaktadır.