Kablosuz Ağlarda Bilgi Güvenliği ve Farkındalık

Önder Şahinaslan[1] Ender Şahinaslan[2] Arzu Kantürk[3]

[1] Bilişim Bölümü, Maltepe Üniversitesi, İstanbul

[2]Bilgisayar Mühendisliği Bölümü, Trakya Üniversitesi, Edirne

[3]Bilgi Güvenliği Servisi, Bank Asya, İstanbul

[1]e-posta: onder@maltepe.edu.tr [2] e-posta: ender@bankasya.com.tr

[3] e-posta: arzu.kanturk@bankasya.com.tr

Özetçe

Günümüzde bilgiye her yerden kolayca erişebilme istek ve arzusu, kablosuz ağ teknolojilerinin kullanımda sağladığı pratik kullanımı gibi nedenler kablosuz ağ teknolojilerine olan talebi sürekli artırmakta, bu alanın sektörel olarak büyümesine, yaygınlaşmasına ve çeşitliliğine neden olmaktadır. Bu gelişmelerin bir sonucu olarak bilgiye her yerden erişim kolaylaşmakta bilgiler merkezi olmaktan çıkıp, daha kolay paylaşılabilir ve erişilebilir hale gelmektedir.

Bilginin bu denli kolay erişilebilir olması, sistemsel ya da insana dayalı pek çok zafiyeti beraberinde taşımaktadır. Bu zafiyetleri kullanan tehditler ise bilgi güvenliği açısından büyük riskleri doğurabilmektedir. Kablosuz ağ risklerinin yanında kablolu ağlar, e-posta ve web üzerinden gelebilecek tehditlerin de eklenmesi sonucu, bilgi güvenliği çok daha önemli hale gelmiştir. Bu riskleri önlemenin en etkin çözümlerinden biri kurumsal bilgi güvenliği politikalarını etkin işletmek yani sistemsel kontrol ve önlemleri almaktan diğeri ise bilgi güvenliği farkındalık çalışmalarını yürütmekten geçmektedir.

Bu çalışmanın ilk bölümlerinde her geçen gün hızla yaygınlaşan ve gelişen kablosuz ağ teknolojileri, türleri, standartları, bunları sağladığı yaşamsal kolaylıklar hakkında temel bilgilendirme sağlamayı amaçlamaktadır. Sonraki bölümlerde ise kablosuz ağlarda güvenlik, bilgi güvenliği riskleri, bu riskleri asgari seviyeye çekmede bilgi güvenliği farkındalığı önemi ve yöntemi hakkında bilgi vermektedir.

1.Giriş

Bilgi erişim ve kullanımına yönelik kablosuz erişim teknolojileri yaşamın birçok alanında kolaylıklar sağlamaktadır. Kablosuz erişim hızlarının kabul edilebilir seviyelere ulaşması ile internet üzerinden servis edilen e-ticaret, e-bankacılık, e-eğitim, e-devlet gibi kullanımlarla her geçen gün daha da artmaktadır. Bu durum kullanıcı alışkanlıklarında ve güvenlik algılamasında farkındalıklara neden olmuştur.

Kablosuz ağ teknolojisinin sunduğu hareket özgürlüğü, yapısal kablolama maliyetindeki tasarruf ve erişim kolaylılığı gibi etkenlerle kullanıcı alışkanlıkları bu yöne kaymaktadır. Bu teknoloji ürünlerinin belli standartlara uygun ve bilinçli kullanımı oldukça önemlidir. Üniversite kampüsleri, kütüphaneler, sosyal tesisler, fuarlar, toplantı salonları, hava alanları, tatil merkezleri, Wi-Fi erişimine açık toplumsal alanlar, işyerleri ve ev ortamları gibi daha birçok mekânda yaygın olarak kullanılmaktadır. Bu durum hizmeti alan ve kullanan kullanıcılar kadar saldırganlarında hareket alanını genişletmekte yeni güvenlik riskleri doğurmaktadır. Ağ üzerindeki yeterli güvenlik bilincine sahip olmayan kullanıcılar ile takipçisi niteliğindeki saldırganlar, bilgi güvenliğini tehdit eden en önemli iki unsur olarak karşımıza çıkmaktadır.

Bu amaçla öncelikle kullanıcı ve ağ yönetimi tarafında alınması gereken bir takım sistemsel kontrol ve önlemlerin alınması, bunların gelişen tehditler karşısında sürekli güncelleştirilmesi, bireysel ve/veya kurumsal bilgi güvenliği algısına özgü bilgi güvenliği politika veya yönergelerinin hazırlanması, kullanıcıların güvenlik bilincinin artırılması gerekmektedir. Sistemsel kontroller denilince; özellikle kullanıcıların ve cihazların ağa erişimini Active Directory veya benzer bir yazılımla merkezi yetkilendirme ve bunun denetiminin yapılmasıyla başlanmalıdır. Erişim yetkilendirme yazılımları sayesinde sunucu kimlik doğrulaması, 802.1x, Radius, NAC ve IAS sunucu yapılandırmaları gerçekleştirilmeli. Özellikle kapalı kampüslerde ve kritik uygulamaların bulunduğu ortamlarda bu tür bir güvenlik altyapısının kurulması ağ güvenliğini sağlamada ilk kontrol ve etkinliği sağlamış olacaktır.

Bilgi ve uygulamalara erişmeye çalışan kişilerin daha ağa bağlanmaya çalışırken tespiti, kayıt altına alınması ve erişim izini olmayan kişilerin ağ erişimlerinin durdurulması ileri seviye bilgi güvenliği için ilk adımdır. Tüm bu sistemsel kontrol ve zayıflıkları giderici önlemlerin yanında günümüzde bilgi güvenliğinin en zayıf halkası olarak kabul edilen, belirli bir güvenlik bilincine sahip olmayan kullanıcılardan kaynaklanabilecek riskler tespit edilmeli, gelişen teknoloji ve uygulamaların doğurabileceği riskleri de dikkate alan çeşitli farkındalık programları geliştirilmeli ve bu kullanıcılara sunulmalıdır. Bu sayede kişi ve kurumlar için değerli olan bilgiye kontrolsüz erişimlerin, kötü amaçlı saldırganların erişimlerinin önüne geçilerek bilgi koruma çemberi altına alınma ve güvenli kullanımı sağlanmalıdır.

2. Kablosuz Ağ Teknolojileri

Bu bölümde kablosuz ağ tanımı, türleri, standartları ve ağ güvenliği ile ilgili temel tanım ve bilgilendirmelere yer verilmiştir.

2.1. Kablosuz Ağ

Kablosuz ağ isminden de anlaşılacağı gibi bilgininin her hangi bir kablo kullanmadan radyo frekansları üzerinden iletilip alındığı ortamlardır. Bu yöntemde kablolama maliyetinin düşük, işletiminin pratik olmaması, bilgininin özgürce belirli bir alanda istenilen her ortamdan erişilebiliyor olması gibi nedenlerle kullanımı her geçen gün daha da yaygınlaşmaktadır. Özellikle üniversite yerleşkeleri, okullar, okuma salonları, kütüphane, fuar ve kongre merkezleri, oteller, tatil köyleri, topluma açık genel kullanım yerleri, hava limanı ve metro ulaşım istasyonları hatta artık evlerimizde de yaygın olarak kullanılmaktadır.

Kablosuz ağ teknolojilerinin günümüzde kullanıldığı bazı alanlara ilişkin örnekler Şekil-1'de gösterilmiştir.

Şekil 1: *Kablosuz ağ teknolojileri ve kullanım alanları*

2.2. Kablosuz Ağ Türleri

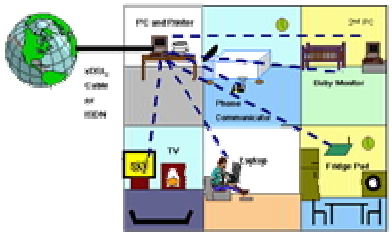
Belli başlı kullanılan kablosuz ağ türlerine ilişkin temel bilgilendirmeler bu bölümde ele alınmıştır.

Bluetooth: 2.4 GHz radyo frekans bandından telsiz iletişim protokolü ile bu protokolü destekleyen cihazlar arasında 10–100 metre kapsam alanında ses ve veri iletimi yapabilme yeteneği olan teknolojik aygıtlara denir.

Günümüzde pek çok teknolojik cihaz 'bluetooth' özelliği taşımaktadır. Bunlardan bazılarına; PC, dizüstü bilgisayarlar, cep telefonları, blackberry, PDA, USB, kamera, fotoğraf makinesi örnek olarak verilebilir.

Bluetooth teknolojileri 128 bit veri şifreleme kullanabilmekte ve kimlik doğrulama kontrolleriyle güvenli teknolojiler sınıfında da yer almaktadır. Aynı zamanda düşük enerji tüketmesi nedeniyle çevreci olma özelliği öne çıkmakta. Bu nedenlerle önümüzdeki dönemde yeni kullanım alanlarıyla birlikte daha çok tercih edileceği öngörülebilmektedir.

HomeRF: 1–2 Mbps hızında çalışabilen, 23–38 metre kapsam alanında 120 cihazı destekleyebilen ve veriyi şifreli olarak iletebilme yeteneğine sahiptir. HomeRF türünü destekleyen teknolojik cihazlardan oluşan örnek bir ağ ortamı Şekil-2'de gösterilmektedir



Şekil 2*: HomeRF [1]*

IRDA: Uzun dalga boyuna sahip, gözle görülmeyen kısa menzilli kızılötesi ışınlardır. Veri transferi; Birkaç metrede doğrudan bir birini görebilen cihazlar arasında maksimum 4 Mpbs'e kadar gerçekleştirilebilir.

Wi-Fi(Wireless **Fi**delity**):** IEEE 802.11x telsiz teknolojilerini kullanan, farklı telsiz cihazların birlikte çalışabilmesi için oluşturulmuş akreditasyon standardı ve bu teknolojideki telsiz iletişim ağı [2]

802.11b/802.11g standartlarında geliştirilen Wi-Fi kablosuz ağ bağlantılarında yaygın olarak kullanılmaktadır. Günümüzde normal şartlarda 50–100 metre mesafede 54 Mbps hızında kullanılabilmektedir. Erişimin zayıflaması durumunda veri transfer hızını 1Mbps'e kadar düşürerek hat kalitesini koruyabilmektedir.

ViMax: Wi-Fi teknolojisinin daha geniş kapsam alanına(56 Km) sahip çok daha güçlü bir versiyonu olarak adlandırılabilir. Genellikle yüksek bir vericiden

iletilen güçlü sinyallerin geniş bir alanda küçük alıcılara ulaştırılmasına dayalı internet ve ağ bağlantısı kurulur. Bir nevi kablosuz televizyon vericilerine benzetebiliriz. Henüz yaygın bir kulanı yaygınlaşmamıştır.

2.3 Kablosuz Ağ Standartları

Uluslararası kabul görmüş ve yaygın kullanıma sahip kablosuz ağlara yönelik IEEE(*The Institute of Electrical and Electronics Engineers*) 802.11 standardı kullanılmaktadır. Cihazların üretim ve birbiri ile sorunsuz çalışmasını sağlayan bu standartlar IEEE tarafından belirlenmekte ve denetlenmektedir.

Teknolojik gelişmeler ve kullanıcı gereksinimlerini dikkate alarak temelde 802.11 ağ iletişim protokollerini destekleyen yeni kablosuz ağ standartları türetilmiştir. Bunlar arasında en önemli fark yeni türetilen standardın bir öncekine göre daha güvenilir ve/veya daha geniş alana ulaşabilme özelliği sayılabilir.

Değişen ve gelişen yeniliklere rağmen 802.11x ailesi aynı temel iletişim kurallarını korumaktadır. Standartlara ait temel özellikler Tablo-1'de özetlenmiştir.

Tablo 1: *802.11x standart ailesi temel nitelik tablosu*

802.11x standart ailesi	802.11a	802.11b	802.11g	802.11i	802.11n
Frekans Aralığı	5 GHz	2.4 GHz	2.4 GHz	Şifreli iletişim	2.5–5 GHz
Veri iletim hızı	54Mbps	11Mbps	54Mbps		600Mbps
Yayın kapsam mesafesi (iç-dış)	15m-30m	45m-90m	45m-90m		91m-182m

Standartlar arasında temelde frekans aralığı, veri iletim hızları veya kapsam alanı bakımından farklılıklar gösterilmekle birlikte kablosuz ağ güvenliğini sağlamaya yönelik IEEE tarafından 802.11 standardına WPA(*Wi-Fi Protected Access*) güvenlik modelinin eklenmesiyle 802.11i modeli geliştirilmiştir. Böylece kablosuz ağ iletişiminde gelişmiş şifreleme ve kimlik denetim özelliğinin de yer alması sağlanmış oldu.

2.4. Kablosuz Ağ Güvenliği

Kablosuz ağ teknolojilerinin doğurabileceği bilgi güvenlik risklerinin önüne geçmenin ilk ve temel yolu sistemlerin beraberinde getirdikleri teknolojik güvenlik açıklarını takip etmek ve bunlara karşı kontrol ve sistemsel önlemleri almaktan geçmektedir.

Bilginin gizliliği ve bütünlüğüne yönelik kötü niyetli saldırı önlemek için aşağıdaki temel güvenlik önlemlerinin alınması pek çok güvenlik riskinin oluşmasını önleyecektir.

- Kablosuz ağ cihazları üzerinde yer alan 'default' kullanıcı ad ve parolaları, SSID yerel ağ ismi değiştirilmeli.
- Şifreli bilgi iletimi için WPA/WEP gibi şifre algoritmalarını etkin hale getirilmeli.
- Erişimine izin verilecek cihazların MAC adresleri önceden tanımlanmalı, tanımlı olmayanların erişimi engellenmeli.
- Kablosuz ağ ortamında cihazların belirli aralıklarla sürekli SSID yayınlaması engellenmeli,
- Tuzak olarak kurulmuş dağıtıcılara doğrudan bağlanma olmaması için "otomatik bağlan" özelliği pasif hale getirilmeli.
- Cihazlardaki otomatik IP set etme yerine sabit IP verme yöntemi seçilmeli.
- Dağıtıcıların tuzak amaçlı değişimlerine karşı cihaza kontrolsüz fiziksel erişimler engellenmelidir.

Yukarıda sıralanan ön kontrol ve düzenlemeleri yanısıra iletişim ağıda virüs, trojan, keylogger, solucan türü zararlı yazılımlar ve port açıklarına karşı ek önlemler alınmalıdır.

3. Kablosuz Ağlarda Bilgi Güvenliği

Kablosuz ağ ve bunu destekleyen cihazların kullanımının yaygınlaşmaya başlamasıyla birlikte daha önce sistem yöneticileri tarafından iletişim öncesi alınan pek çok kontrol ve tedbirlerin kablosuz ağ kullanımıyla birlikte elinde bulunduğu cihazın temel güvenlik ayarlarını tedbirlerini yerine getirmesi beklenen kullanıcılarda yeterli bilincin olmaması, bu alanın kontrolsüz ve hızlı gelişmesi pek çok zaafiyetleri, bu zaafiyetleri kullanabilen tehditler ise çeşitli bilgi güvenlik risklerini doğurmaktadır.

3.1. Tehdit

Bilginin korunması gereken niteliklerini bozmaya yönelik mevcut ya da olabilecek her türlü algıya tehdit denir

İstenmeyen kişiler('hacker' vb) kablosuz erişim yöntemi ile kişi ya da kurumlara ait bilgi ve değerlere izinsiz erişebilir ve ilgililere maddi ve/veya manevi zarar verilebilirler. Bu kişiler haksız kazanç sağlamak, kendilerine ün/itibar sağlamak niyetiyle saldırılar düzenleyebilir, çeşitli tehditleri oluşturabilirler.

Bu tür tehditlere karşı olası kablosuz güvenlik açıkları önceden tespit edilmeli, tespit edilen tehdit ve zafiyetleri belirlenerek zamanında gerekli kontrol ve önlemler alınmalıdır. Bunların yanında önceden kestirilemeyen ya da bilinmeyen tehditlerin de olabileceği veya zamanla oluşabileceği unutulmamalı güvenlik faaliyetlerinin sürekliliği sağlanmalıdır.

3.2. Açıklık-Zafiyet

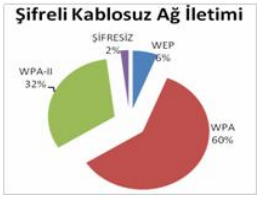
Açıklık ya da zafiyet korunmaya muhtaç bilginin tehditler karşısında korunmasını sağlayan önlemlerin yeterli seviyede olmaması durumuna denir.

Kablosuz ağların kendisine özgü yapısı nedeniyle merkezi denetimin yapılamadığı durumlarda sistem açıklarını kullanabilen kullanıcıların saldırılarına açık hale gelerek en büyük zafiyeti oluşturmaktadır.

Kablosuz ağlar, merkezi **fiziksel erişimli** ağlara göre yeni güvenlik zayıflıkları oluşturmaktadır. Kablosuz erişime açık bir yerde yeterli güvenlik önlemleri almadan ağa dahil olduğunuzda yanı başınızda ağa dahil olan bir başka tanımadığınız beklide sevimli afacan bir çocuk sizin makinenize erişip sizin için hayati önem taşıyabilecek bilgilerinize rahatlıkla dokunabilir!, onu kendi emelleri için kullanabilir, değiştirebilir sizi telafisi mümkün olmayabilecek bir durumla karşı karsıya bırakabilir.

En yaygın olarak karşılaşılan bilgi güvenliği zafiyeti kullanıcıların karşılaşabilecekleri tehditler ve doğurabileceği zararları hakkında yeterli bilgiye sahip olmamaları, dikkatsiz davranmaları ve şifrelerin yeterli komplekslikte olmaması ve onları koruyamamaları gösterilebilir.

Bu alanda yapılan yeni bir çalışma sonucu Şekil-3'de gösterilmektedir.



Şekil–3: *Türkiye'deki Güvenli Kablosuz Ağ Erişimi* [3]

Şekil–3'de yer alan çalışmada kablosuz ağa şifresiz bağlanma oranı %2 gibi küçük bir oran gözükmesine rağmen bu oran doğurabileceği kayıplar ve riskler açısından oldukça yeterli olabilir.

3.3. Risk

Risk, sözlük anlamı olarak zarara uğrama tehlikesidir; öngörülebilir tehlikeleri ifade eder.[4]

Kablosuz cihazlar ve üzerindeki uygulamalar yeterli güvenlik önemi ve bilinci oluşturulmadan kullanıldığında kullanıcılara kolaylıkları sunmandan öte çeşitli bilgi güvenlik riskleriyle karşı karşıya bırakabilmektedir.

Bireysel veya kurumsal bilgiler, kablosuz cihazlarda, bu cihazlara rahatlıkla takılabilecek, çıkarılabilecek ve değiştirilebilecek harici hafıza kartlarında taşınmaya başlamasıyla bilgi 'on-line' ya da 'off-line' hareket kabiliyetine daha kolay kavuşmuştur. Bilgininin bu denli hareketliliği kontrollerin yeterli seviyede uygulanmasında aksaklıklar doğurabilmekte yeni güvenlik risklerini beraberinde getirmektedir.

3.3. Tehdit, Zafiyet, Risk ve Risk Önleme

Kablosuz ağlarda da bilgi güvenliği tehditleri, var olan sistemsel ya da diğer açıklıklar önceden belirlenmeli, bunların doğuracağı riskler ve bu riskleri önleyici risk önleme planları oluşturulmalı, bunlar belirli bir önceliğe tutulmalıdır. Böylece riskler bir olaya dönüşmeden giderilmeli ya da kabul edilebilir seviyeye çekilmelidir. Buna ait bir örnek tablo Tablo-2'de gösterilmektedir.

Tablo 2: *Bilgi güvenliği tehdit, zafiyet, risk tablosu*

Tehdit	Zafiyet	BG Riski	Risk Önleme
• İstenmeyen kişi saldırılar, davetsiz misafir • Saldırgan	• Bilginin havada şifresi erişime açık olması • Sistem ilk kurulum ayarlarının değiştirilmemesi	• Bilgi mahremiyetinin sağlanamaması, 'gizlilik', 'bütünlük' nitelikleri, • Maddi kayıp, • İtibar, • Yasal sorumluluklar vb	• Ağ erişim noktası(AP)'nın gizlenmesi, • Erişimin önceden tanımlı MAC üzerinden yapılması • Sistem kurulumunda tanımlı 'default' kullanıcı şifrelerin değiştirilmesi vb

4. Bilgi Güvenlik Politikası ve Farkındalık Yaklaşımı

Bilgi, günümüzde haberleşme kanalları olan kablolu ve kablosuz olarak ağlar üzerinden paylaşılabilmekte ve iletilebilmektedir. Kablosuz iletişim kanallarının kullanımı oldukça yaygınlaşmakla birlikte bilginin istenilmeyen kişiler tarafından kötü amaçlı kullanımı da yaygınlaşmakta, güvenlik zafiyetleri ise artmaktadır.

Kablosuz ağlar yapıları itibariyle kablolu ağlara göre daha güvensiz olup çeşitli zafiyetleri de beraberinde taşımaktadır. Kablolu ağlarda ise bilgiler kablolar vasıtasıyla iletildiğinden daha güvenli iletilebilmektedir. Kullanımda ise kablosuz ağlarda verilerin erişim noktasından aktarılıyor olması nedeniyle bilgiye erişimi kolaylaşır. Kablosuz ağların kullanımın kolay ve yaygın olması bununla birlikte barındırdığı zafiyetlerin çeşitli bilgi güvenliği tehditleri ile karşı karşıya kalması kaçınılmazdır. Kurum ve bireyler için önemli ve sürekli korunması gereken varlık olan bilgi ise olası kötü amaçlı saldırılar karşısında savunmaya muhtaç hale gelir.

Kablosuz ağlarda, bilgi güvenliğinin üç temel prensibi olan gizliğin, bütünlüğün ve erişilebilirliğin sağlanması noktasında öncelikle; SSID kullanımı, kimlik doğrulama mekanizmaları, MAC adres filtreleme ve kablosuz

şifreleme teknolojileri gibi sistemsel özel güvenlik kontrolleri uygulanmalıdır.

Bu güvenlik tedbirlerine paralel olarak güvenlik en zayıf halkasını oluşturan insan faktörü hiçbir zaman unutulmamalı ve bireyler üzerinde belirli bir bilgi güvenliği farkındalığı sağlanmalıdır.

Her ne kadar sistemler üzerinde gerekli güvenlik önlemleri alınsa bile kullanıcılar bu konuda bilinçlendirilmedikçe gerçek anlamda güvenlik hiçbir zaman sağlanmayacaktır.

TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsünün Türkiye'de kablosuz internet ağı kullanan 30 bin bilgisayar üzerinde yaptığı araştırmaya göre, kullanıcıların yüzde 5'nin şifre kullanmadığı ve bilgisayarların yarısında ADSL modemlerin yönetim ara yüzüne dışarıdan ulaşılabildiği görülmüştür.[5]

Bu tür araştırmalar ya da günümüzde her geçen gün artan bilgi güvenlik olayları kullanıcılarda farkındalık oluşturulmasının gerekliliği gösterir.

Bu doğrultuda, kurumlar öncelikli olarak kurumsal bilgi güvenlik politikalarını oluşturmalı, kurumun en üst düzey yönetiminin onayından geçirmeli, güvenlik kural ya da yönergelerini hazırlamalı, bilgi güvenliği farkındalığını arttırmaya yönelik belirli aralıklarla eğitimler, seminerler düzenlemeli ve işleyişi gözlemleyerek sürekli iyileştirmeler yapmalıdır.

Düzenlenen bu farkındalık eğitimlerde; bilgi güvenliği temel kavramları, kurum beklentileri, yaşanılmış ya da yaşanması muhtemel tehditler, riskler ve bu riskleri önleyici kontroller, bilgi güvenliği olayları ve bunların kurumlara ya da bireylere verebileceği zararlar hakkında güncel örneklerle örneklendirilerek anlatılmalı ve sürekli farkındalık seviyesi yükseltilmelidir.

Bireyler uğrayabilecekleri bilgi güvenlik saldırıları hakkında da bilgilendirilmelidir.

Kablosuz ağları da kapsayan temel bir bilgi güvenlik kuralları ya da yönergesinde aşağıdaki temel yaklaşım yada tavsiyeleri dikkate almalı, bu kuralların gerekliliği, ne tür risklere karşı alındığı ve uymaları gereken kurallar iyice anlatılmalı, anlaşılabilirliği sağlanmalıdır.

- Kullanıcıların ağ ayarları değiştirebilme yetkileri belli ölçülerde kısıtlanmalı, mümkünse merkezi güvenlik politikası uygulanmalıdır.
- Kablosuz ağlarda kullanıcı şifrelerinin kompleks güçlü şifreler(H@rf, S@y1, Özel karakter, en az 8 uzunlukta) kullanılması zorunlu yapılmalı, güvenlik politikalarıyla desteklenmeli, kullanıcılar kolay tahmin edilebilir basit şifrelerin getirebileceği riskler hakkında bilgilendirilmelidir.
- İşletim sistemlerde özellikle Windows işletim sisteminde yer alan güvenlik açıklarına dikkat edilmeli. İşletim sistemleri güvenlik yama(patch)'leri otomatik yüklenecek şekilde konfigüre edilmelidir. Sunucu hizmeti kaldırılmalı, bu işlemin DOS komut satırından "net share" yazılarak gerçekleştirmesi önlenmelidir.
- Kurumların çevrelerinde güçlü antenler kullanılarak kablosuz ağın dinlenmesine karşı önlemler alınmalı ve bu noktada kullanıcılar bilgilendirilmelidir.
- Dizüstü bilgisayarlarda taşınan hassas verilerin şifrelenmiş bir şekilde korunmasının gerekliliği kullanıcılara anlatılmalı bilginin hareket halinde şifreli taşınmasına yönelik yatırımlar yapılmalıdır.
- Kayıp dizüstü bilgisayarlarının yetkili mercilere hemen bildirilmesi gerekliliği bireylere açıklanmalı, bilgi güvenlik müdahale süreci önceden belirlenerek derhal işletilmelidir.
- Kullanıcılara yapmaları gereken güvenlik ayarları konusunda bilgilendirme yapılmalı ve sistemlerinde mevcut olan güvenlik ayarlarını kapatmaları engellenmelidir.[6,7]
- Bilgisayar sisteminin belirli bir süre kullanılmaması durumunda sistemsel olarak erişime kapatılması(*Log Off*) sağlanmalı.
- Her türlü haberleşmede kullanılan cihazlar (telefon, faks, fotokopi makineleri) başı boş yetkisiz erişimlere açık bir şekilde konumlandırılmamalı, bu cihazlar üzerinde bilgi ve belge bırakılmamalıdır. [8]
- Her türlü bilgiler, şifreler, anahtarlar ve bilginin sunulduğu sistemler, ana makineler(server), pc'ler vb. cihazlar yetkisiz kişilerin erişebileceği şifresiz ve korumasız bir şekilde başıboş bırakılmamalı[8]
- Kullanıcılar resmen tanımadıkları özellikle güvenilirliği konusunda bilgi sahibi olmadıkları internet adreslerinden her hangi bir kod çalıştırma (Cross-Site Scripting) açıklarının doğurabileceği riskler hakkında bilgilendirilmeli zararlı olduğu belirlenmiş internet adreslerine girişler merkezi sistemsel olarak engellenmeli, kurum politikalarında buna yer verilmeli.
- Bilgi iletişimini yalnızca kablosuz ağlar üzerinden kurgulayan bir kurumun ağda oluşabilecek haberleşme zayıflıklarını da dikkate alması olası iş sürekliliği ya da bilgiye erişememe problemlerine karşı ilgili tarafları önceden bilgilendirmesi gerekmektedir. İlgili tarafların buna tahammülü yok ise kablosuz ağ çözümlerinin yanında diğer kablolu erişim gibi alternatif planları geliştirmesi gerekmektedir.
- Kurumlarda bireylerin yapabilecekleri küçük hatalar tüm teknik anlamda alınan tüm güvenlik

önlemlerini boşa çıkarabileceği unutulmamalı, çalışanlar çeşitli bilgi güvenliği farkındalık programlarına tabi tutulmalı.

- Bilgi güvenliği farkındalığını oluşturmanın ana yolu kurumda en üst seviyedeki yönetimden en alt seviyedeki çalışana hatta tedarikçilere kadar çalışanların görev ve pozisyonları da dikkate alınarak ihtiyaç ve beklentilere göre farklı eğitim ve farkındalık programları hazırlanmalı ve eğitimler düzenlenmelidir.[9]

5. Sonuç

Günümüzde özgür iletişim kanalı olarak da algılanan kablosuz ağ teknolojileri, kolay ve yaygın kullanımının yanında bir takım bilgi güvenlik risklerini de beraberinde taşımakta ve önlemler alınmadığı takdirde bu risklerin bilgi güvenliği olaylarına dönüşmesi kaçınılmaz hale gelecektir. Bilgi güvenlik risklerin olaya dönüşmesi halinde kişi ve kurumlar maddi ve manevi-itibar kayıpların yanında yasal pek çok yaptırımlarla ya da cezai müeyyide ve yaptırımölarla karşı karşıya kalabilirler. Bilişim suçları kanunu ve 5651 sayılı internet suçlarını önlemeye yönelik kanun ilk akla gelen kanunlara örnek olarak verilebilir.

Teknolojik yenilikler birçok noktada kurumlara, ya da bireylere bilgiye kolay erişim ve kullanım imkanı sağlamaktadır. Hızla gelişen teknoloji, kullanıcı taleplerini karşılamada pazar rekabeti ve liderlik kaygısı da eklenince bu teknolojiyi kullanacak birey ya da kurumları çeşitli güvenlik riskleriyle yüz yüze bırakabilmektedir.

Bu teknolojileri kullanacak kurumlar artan güvenlik risklerine karşı varlıklarını devam ettirebilmek için öncelikle sistemlerini en ileri teknolojilerle ve sistemsel kontrollerle güvenli hale getirmeli ve güvenlik noktasında kullanıcı farkındalığını arttırmalıdır.

Bir kurumu rakipleri karşısında ilerletecek asıl nokta sistemsel önlemlerden çok güvenlik noktasında yeterli farkındalığa sahip çalışanlarıdır.

Sonuç olarak; günümüzde kablolu, kablosuz ağlar, mobil teknolojiler günlük yaşantımızın vazgeçilmez bir parçası haline gelmiştir. Gelişen yeni teknolojilere karşı bireyler ya da kurumlar içten ya da dıştan gelebilecek her türlü güvenlik riskine karşı yeterli bilinçte olmalı ve ona göre davranmalıdır. Aksi takdirde kurumlar ya da bireyler telefisi mümkün olmayan pek çok maddi ve/veya çok büyük zararlarla karşı karşıya kalabilirler.

Bu çalışmada, kablosuz ağ teknolojileri ve bu teknolojilerin sağladığı avantajların karşısında oluşabilecek bilgi güvenlik risklerlerine dikkat çekilmiş, riskleri önelemeye ilişkin farkındalığın önemi vurgulanarak temel bir bilgi güvenliği farkındalığı oluşturulması hedeflenmiştir.

6. Kaynakça

[1] www.palowireless.com/homerf/images/homerf2.gif , *Ekim 2009*

[2] http://en.wikipedia.org/wiki/WiFi

[3] http://www.cozumpark.com/mklresim/KablosuzAlarVeGvenlik_18F1/clip_image012_thumb.jpg , *Ekim 2009*

[4] TBD Kamu BİB VIII, Bilişim Teknolojilerinde Risk Yönetimi – II. Çalışma Grubu, S.4.

[5] http://www.teknoport.com.tr/2009/05/27/kablosuz-aglarda-guvenlik-problemi/ , *Kasım 2009*

[6] Kablosuz Yerel Ağ Güvenliği Kılavuzu*, Kasım 2009*

[7] A-Z' ye Kablosuz Ağ Hakkında Herşey*, Chip Dergisi Eki, Kasım 2009*

[8] Bilgi Güvenliği Farkındalık Eğitim Örneği, E.Şahinaslan, A.Kantürk, Ö.Şahinaslan, E.Borandağ, *Ab2009 Akademik Bilişim Konferansı*, , *Şubat 2009*

[9] Kurumlarda Bilgi Güvenliği Farkındalığı, Önemi ve Oluşturma Yöntemleri, E.Şahinaslan, R.Kandemir, Ö.Şahinaslan, *Ab2009 Akademik Bilişim Konferansı*, *Şubat 2009*