T.C.

BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

VERİ GÜVENLİĞİ ESASLI "KENDİ CİHAZINI GETİR" SİSTEM TASARIMI

(Yüksek Lisans Tezi)

Tezi Hazırlayan : **Volkan YILMAZ**

İstanbul, 2014

TC

BEYKENT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

BİLGİSAYAR MÜHENDİSLİĞİ BİLİM DALI

VERİ GÜVENLİĞİ ESASLI "KENDİ CİHAZINI GETİR" SİSTEM TASARIMI

(Yüksek Lisans Tezi)

Tezi Hazırlayan :

Volkan YILMAZ

Öğrenci No:

110820011

Danışman:

Yrd. Doç. Dr. Ediz ŞAYKOL

İstanbul, 2014

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum "Veri Güvenliği Esaslı "Kendi Cihazını Getir" Sistem Tasarımı " başlıklı bu çalışmanın, bilimsel ahlak ve geleneklere uygun şekilde tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmamın içinde kullanıldıkları her yerde bunlara atıf yapıldığını belirtir ve bunu onurumla doğrularım. **24/ 06/ 2014**

Volkan YILMAZ

T.C.
BEYKENT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZ SAVUNMA SINAVI SONUÇ TUTANAĞI

Beykent Üniversitesi
Fen Bilimleri Enstitüsü Müdürlüğü'ne,

Aşağıda tez adı belirtilen yüksek lisans öğrencisi...**110820011**....no'lu ...**Volkan YILMAZ**....'in **13/06/2014** tarihinde yapılan tez savunma sınavı[1] sonucunda 60 dakika süreyle sunduğu ve savunduğu tezi hakkında[2] oybirliğiyle, KABUL kararı verilmiştir.

Bilgilerinize saygılarımızla arz ederiz.

Anabilim Dalı : **BİLGİSAYAR MÜHENDİSLİĞİ**

Programı : **BİLGİSAYAR MÜHENDİSLİĞİ**

Tez Başlığı[3] : **VERİ GÜVENLİĞİ ESASLI "KENDİ CİHAZINI GETİR" SİSTEM TASARIMI**

Tez Sınav Jürisi		**Öğretim Üyesi**	**İmza**
Danışman	:	Yrd. Doç. Dr. Ediz ŞAYKOL	
Üye	:	Doç. Dr. Gökhan SİLAHTAROĞLU	
Üye	:	Doç. Dr. Kazım SARI	

[1] Jüri üyeleri söz konusu tezin kendilerine teslim edildiği tarihten itibaren en geç bir ay içinde toplanarak öğrenciyi tez savunma sınavına alır. Belirlenen günde yapılamayan jüri toplantısı, katılanların hazırladığı bir tutanakla enstitü yönetimine bildirilir. Bu durumda jüri en geç onbeş gün içinde toplanarak adayı tez savunma sınavına alır. Tez savunma sınav süresi en az 45 dakikadır. Yüksek lisans tez savunma sınavı, tez çalışmasının sunulması ve bunu izleyen soru-yanıt bölümlerinden oluşur ve dinleyiciye açıktır. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-3)

[2] Tez sınavının tamamlanmasından sonra jüri, tez hakkında "kabul", "düzeltme" veya "red" kararı verir. Jüri başkanı, jüri üyelerince imzalanmış sınav tutanağını, tez sınavını izleyen üç gün içinde ilgili enstitü yönetimine teslim eder. Tezi başarısız bulunan öğrencinin Enstitü ile ilişiği kesilir. Tezi hakkında düzeltme kararı verilen öğrenci en geç üç ay içinde gerekli düzeltmeleri yaparak ve yönetmelikte belirtilen usullere uygun olarak tezini aynı jüri önünde yeniden savunur. Bu savunma sınavında da tezi kabul edilmeyen öğrencinin enstitü ile ilişiği kesilir. (Beykent Lisansüstü eğitim ve Öğretim Yönetmeliği-Madde30-4)

[3] İleride doğabilecek aksaklıkların engellenmesi için tezin başlığının yazılması gerekmektedir.

Veri Güvenliği Esaslı "Kendi Cihazını Getir" Sistem Tasarımı

Tezi Hazırlayan: Volkan YILMAZ

ÖZET

Günümüzde basit işleri gerçekleştirmek için bile bilişim teknolojilerine ve teknolojik cihazlara kişisel bağımlılık mevcuttur. Bu durumun, toplum üzerinde yaratmış olduğu bağımlılık ve bilgi kaynaklarının gizliliği, bütünlük ve uygunluk durumu sürekli sorgulanmaktadır.

Kullanıcı sayısı arttırmasının bedeli olarak, mobil cihazların fonksiyonalite gelişimi azalmaktadır. Bu durumla beraber mobil cihazlar, bilgisayar korsanlarının ve kötü amaçlı yazılımların yardımı ile kişisel ve organizasyonel bilgileri ele geçirmek mümkündür. Bunlara rağmen, kullanıcılar mobil cihazları sadece arama yapmak, doküman okumak, e-postalarını cevaplamak ve takvimlerini kontrol etmek için kullanıldığını düşünmektedirler ve kişisel bilgilerini korumak için güvenlik önlemi almamışlardır. Gerçekte durum bu şekilde değildir. Mobil cihazlarda yukarıda sözü geçen durumlardan daha fazla şey olmaktadır. Kullanıcılar kişisel güvenlikle alakalı gerçekler hakkında eğitilmeli ve mevcut riskler hakkında kullanıcı bilinci arttırılarak farkındalık sağlanmalıdır.

Özetle, kişisel cihazların şirket ortamlarına veya halka açık alanlarda kablosuz ağlara erişmek için kullanıldığı vakit, potansiyel güvenlik açıklarını, şirket ağlarına taşıyacaklardır. Tez amacı bu potansiyel güvenlik açıkları hakkında farkındalık yaratıp, bu farkındalık üzerinde zafiyetleri anlamak ve açıklamaya yönelik çalışmalar yapılacaktır.

Anahtar Kelimeler: BYOD**,** Mobilite, Mobil Güvenlik, MDM, Şifreleme.

"Bring Your Own Device"System Design Based On Data Security

Presented by: Volkan YILMAZ

ABSTRACT

Today's world is characterised by a heavy dependence on information technology and technological devices to perform even the simplest of tasks. While this in itself is not a bad thing, our over dependence has put us in a situation where the confidentiality, integrity and availability of our information resources are continuously being questioned.

As the price of the mobile devices reduces and their functionality improves, the number of its users increases. This makes it a target for hackers and malware as they can exploit the device to gain personal and organizational data.

In spite of this, users still think that if only the mobile devices are used for making and receiving calls, reading and replying to emails and checking calendar schedules, then there is nothing much to protect. In reality this is not the case. Mobile devices have a lot more going on them than just the aforementioned. Users must be educated on the reality of the matter and be made aware of the current risks there are so as to increase their consciousness on this matter.

In summary, If personal devices using access wireless networks in the corporate environment or in public areas, all the potential security vulnerabilities, will be moves into the company network. The aim of this thesis create awareness about the potential security vulnerabilities, to understand weaknesses on this awareness and explain efforts are going to.

Key Words: BYOD**,** Mobility, Mobile Security, MDM, Encryption.

İÇİNDEKİLER

ŞEKİLLER LİSTESİ

Sayfa No.

KISALTMALAR

APP : Yazılım uygulamalarına verilen kısa isim.

B.Y.O.D. : Kendi Cihazını Getir (K.C.G.)

DMZ : Çevre Ağı

DATA : Veri

ENISA : Avrupa Ağ ve Enformasyon Güvenliği Ajansı

EXT : Harici

FW : Güvenlik Duvarı

GPS : Küresel Konumlandırma Sistemi

GSM : Mobil İletişim için Küresel Sistem

HOST : Sunucu

IBM : Uluslararası İş Makineleri

ICT : Bilgi ve İletişim Teknolojisi

IE : Internet Explorer- Web tarayıcısı

INT : Dahili

IOS : Apple, işletim Sistemi

IT : Bilgi Teknolojisi

LAN : Yerel Alan Ağı

MDM : Mobil Cihaz Yönetimi

MMS : Mobil Çoklu Ortam Mesajlaşma Hizmeti

NAT : Ağ Adresi Dönüştürme

NETWORK : Ağ

PDA : Kişisel Dijital Asistan

PIN : Kişisel Kimlik Numarası

POLICY : Politika

SATURE : Doygunluk

SESSION : Oturum

SLR : Sistematik Literatür İncelemesi

SMS : Kısa Mesajlaşma Servisi

TAM : Teknoloji Kabul Modeli

THIRD PARTY : Üçüncü Şahıslara Ait

VPN : Sanal Özel Ağ

Wi-Fi : Kablosuz Yerel Alan Ağı

1.GİRİŞ

Günümüzde basit rutin işleri gerçekleştirmek için "Bilgi Teknolojilerine" yüksek oranda bağımlılık mevcuttur.

Ev kullanıcılarından, endüstriyel kullanıcılara kadar herkese yönelik teknoloji çözümleri mevcuttur. Bugün, para transferleri akıllı telefonlar gibi kişisel cihazlar üzerinden saniyeler içerisinde yapılabilmektedir. Uçuş detaylarını kontrol etmek veya elektronik postalarımızı okumak için uzağa gitmemize gerek yoktur.

USA Today (2006) Dergisinin siber dünyanın geleceği ile ilgili olarak yapmış olduğu anket sonuçlarına göre, Bilişim Teknolojilerinin yaşamımızı 2025 yılına kadar, 92 farklı şekilde değiştireceğini bildirmektedir. Teknoloji insan yaşamını dramatik olarak değiştirmektedir ve bu değişim her zaman olumlu yönde olmamaktadır.

Bilişim teknolojisi çalışma verimini ve etkisini arttırırken (Walton, 1985; Manz & Stewart, 1997; Eason, 2001; Chen & Nath, 2011), bilgilerimizin bilmediğimiz ağlar ve farklı cihazlar aracılığıyla dolaşımına izin verdiğimiz sürece önemli ve hassas bilgilerimiz yetkisiz kişiler tarafından ele geçirilme riski taşımaktadır.
Sürekli lokasyon değiştiren ve bu lokasyonlardaki ağ bağlantılarını kullanarak çalışan, şirket veya şirket çalışanları adına bilgi güvenliği tehditi barındırmaktadır.

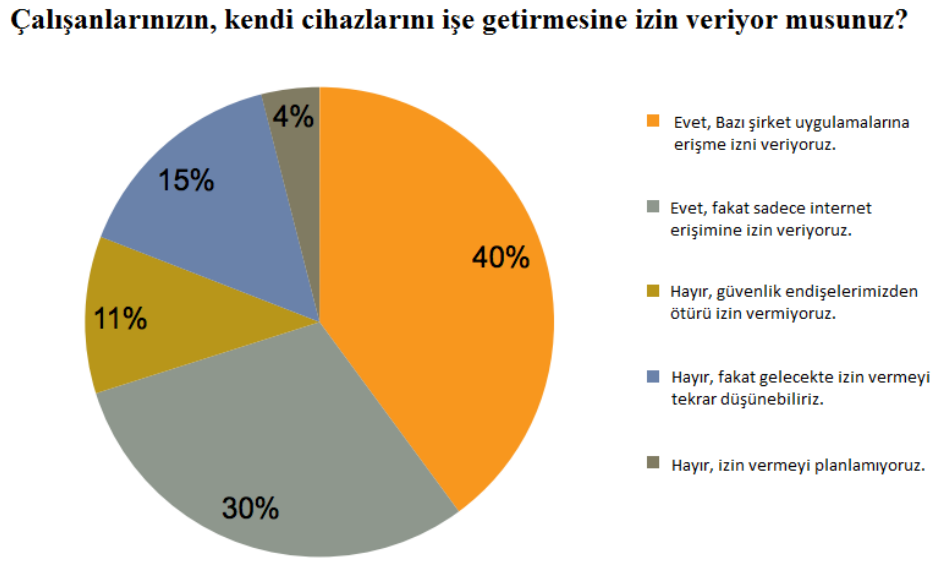
Bu çalışma gezici çalışanların ve taşınabilir cihazların organizasyonlar için yarattığı tehditler, riskler ve açıkları özetlemek amacıyla yazılmıştır. Bu çalışmada, taşınabilir cihazların kullanımı esnasındaki güvenlik açıklarını en aza indirgemek için K.C.G. teknoloji yöneliminin gelişmiş şifreleme standardının (AES) uygulanmasıyla önerilmiştir.

2. "KENDİ CİHAZINI GETİR" KAVRAMI

2.1. Genel K.C.G. Kavramı Ve Kullanım Alanları

Yapılan hesaplamalara göre önümüzdeki beş yıl içerisinde, dünyadaki taşınabilir cihazların sayısı 10 milyar'a ve her bir kadın, erkek ve çocuğa düşen mobil cihaz sayısının 1.5 oranında katlanacağı tahmin edilmektedir.

Mobil cihazların giderek kişisel hayatlarımızın her aşamasında yer almasıyla birlikte beraber çalışanlar, çalışmalarını yürütmek için organizasyonlardan kendi mobil cihazlarını kullanma isteğinde bulunuyorlar ve destek almak için şirketlerindeki bilgi işlem departmanlarına başvurmaktadırlar. İş verenler, çalışanların kendi mobil cihazlarını iş yaşamında kullanmalarını fiziksel olarak engellenemeyeceği sonucuna vardılar, fakat bu durumu güvenlik açısından kontrol edilmek için arayışlara yöneldiler.

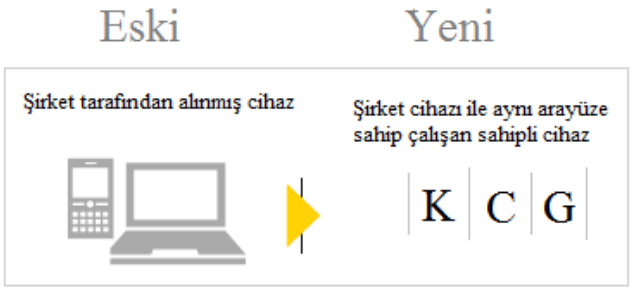


Şekil.1. Taşınabilir Cihazların Kişisel Kullanım Yüzdesi

Kaynak: Nusca A.(2012) "*BYOD inches along in Europe, Middle East, Africa"* içinde (Mayıs 2014) tarihinde http://www.zdnet.com/blog/btl/byod-inches-along-in-europe-middle-east-africa/77605'den alındı.

Kaspersky Lab ve B2B'nin (Kas 14,2013 - Yeşim Sarıer Aksu) ortak çalışmasıyla dünya çapında gerçekleştirilen araştırmada kurumların yalnızca yüzde 9'unun, çalışanlarının iş için kişisel akıllı telefonlarını kullanmalarının yasaklanabilir olduğunu düşündüğünü ortaya çıkarıyor.

Kurumların yüzde 29'u ise çalışanların taşınabilir cihazlar üzerinden kurumsal ağlardaki verilere ulaşımı için tam erişim izni de sağlıyor.
Şirketlerin yüzde 55'i, mobil cihaz yönetimiyle ilgili endişeye kapıldıklarını, yüzde 29'u ise daha şimdiden mobil cihaz çalınması ya da kaybolması nedeniyle sorun yaşadıklarını belirtiyor.



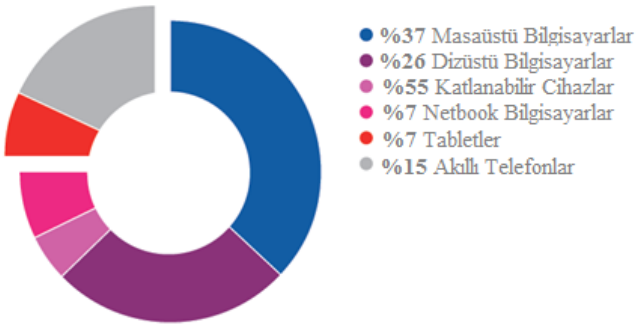
Şekil.2. "Kendi Cihazını Getir" Tanımı

Kaynak: Ernst & Young Global Limited (2013) "*Bring your own device Security and risk considerations for your mobile device program"* içinden (Mayıs 2014) tarihinde http://www.ey.com/Publication/vwLUAssets/EY_-_Bring_your_own_device:_mobile_security_and_risk/$FILE/Bring_your_own_device.pdf'den alındı.

K.C.G (Kendi Cihazını Getir), bilişim teknolojisi organizasyonlarındaki fiziksel lokasyon ve cihaz mülkiyeti gibi terimlerdeki temel tanımlamaları ve BT'de (Bilişim Teknolojisi) varolan geleneksel güvenlik modelini önemli ölçüde etkilemektedir. Personel cihazların kullanımı ile, resmi e-posta, takvim, uygulama ve şirket verilerine ulaşılmaktadır. Bu durumla beraber firmalar, şirket çalışanlarının ve kendi güvenlik ihtiyaçlarını birlikte karşılayacak dengeli modeller geliştirmekle, kabul edilebilir prosedürler ve kurallar ile güvenlik konusundaki tutumlarını belirlemeye çabalamaktadırlar.

Çalışanlar arasında gezici çalışma sisteminin (mobilite) ve akıllı cihazların kullanımının artmasıyla beraber uygulamalar ve depolama cihazlarındaki önemli verilerin ele geçirilme olasılığı artmaktadır ve bu durum güvenlik parametreleri arasında yerini almaktadır (Fitzgerald, 2009).

"Britannica" akademik versiyonunda "taşınabilir" kelimesini, kolaylıkla taşınma yetisi ve becerisi olan olarak tanımlanmıştır. Bu tanıma göre bizler taşınabilir cihazları, elde taşınabilecek boyut ve hafiflikte, ekstra bir yük ve enerji gerektirmeden taşınabilecek cihazlar olarak tanımlayabiliriz. Taşınabilir cihazlara en yaygın örnekler; Dizüstü bilgisayarlar, Kişisel Dijital Asistanlar (PDA), Akıllı Telefonlar (SmartPhone), Avuç- içi (hand-held) bilgisayarlar ve Tablet bilgisayarlar olarak verilebilir.



Şekil.3. En Çok Kullanılan Akıllı Cihazlar

Kaynak: Paganini P.(2013)" *Importance of a BYOD Policy for Companies"* içinden (Mayıs 2014) tarihinde http://resources.infosecinstitute.com/byod-policy-for-companies/ 'den alındı.

Flaş bellekler, akıllı telefonlar ve tabletler gibi taşınabilir cihazlar iş yaşamında veya kişisel yaşamda bilgilere erişimi her zaman ve her yerden kolaylıkla sağlamaktadır. Taşınabilir cihazların kullanışlı ve pratik olan özelliklerinin yanı sıra, çeşitli ağlar ve sunucularla olan fiziksel bağlantısı bu cihazları güvenlik açıklarına karşı savunmasız hale getirmektedir. Bu durum bilgi eksikliğinin artmasından kaynaklanmaktadır (Ernst &Young, 2011; Walters, 2012).

Giderek küçülen cihazlar ile kurumsal çalışanlar artık dünyanın her noktasından internete erişebildiği için, artık ofisler terkediliyor ve esnek çalışma yöntemleri sektöre yerleşiyor. Kurumlar bilgilerini sadece bilgisayarlarda bulundurmuyor, çalışanlarının her an kaybolmaya ya da çalınmaya müsait akıllı telefonlarında da çok önemli kurum bilgileri tutuyorlar.
Bu nedenle, büyük kurumsal işletmeler başta olmak üzere farklı ölçekteki işletmeler, bugün artık personellerinin iş amaçlı kullandığı ve ağa bağlanan, sayıları da gün geçtikçe artan internet erişimli cihazlar ile ilgilenmek durumundadır.

Bu gözden gelinen güvenlik zafiyeti, taşınabilir cihaz kaybedildiğinde veya çalındığında birçok organizasyonun önemli bilgilerini kaybetmesine, bu bilgilerin ortaya çıkmasına veya izinsiz olarak üçüncü parti şahısların eline geçmesine sebep olabilir. Bu durum doğrudan ağ'a internet aracılığıyla bağlı olan cihazlar için, ağ bazlı saldırıların artmasına sebep olmaktadır (Heikkila, 2007; Fratto, (2009); Walters, 2012). Taşınabilir cihazlara her yerden her zaman bağlantı sağlamak, üretkenliği arttırmakla beraber, iş veya sosyalleşme amacıyla kişisel olarak gerekli olsa da bu cihazlar, güvenlik riskleri nedeniyle genel çevrelerde endişe yaratmaktadır. Dizüstü ve kişisel bilgisayarlar düzenli olarak güncellenen ve daha güvenli olmaları için ekstra ayarları olan çeşitli antivirüs yazılımı seçeneklerine sahiptirler, oysa akıllı telefon, Kişisel Dijital Asistanlar veya tabletler gibi taşınabilir cihazlar bu gibi dört dörtlük güvenlik yazılımlarına tam anlamıyla sahip değildirler.

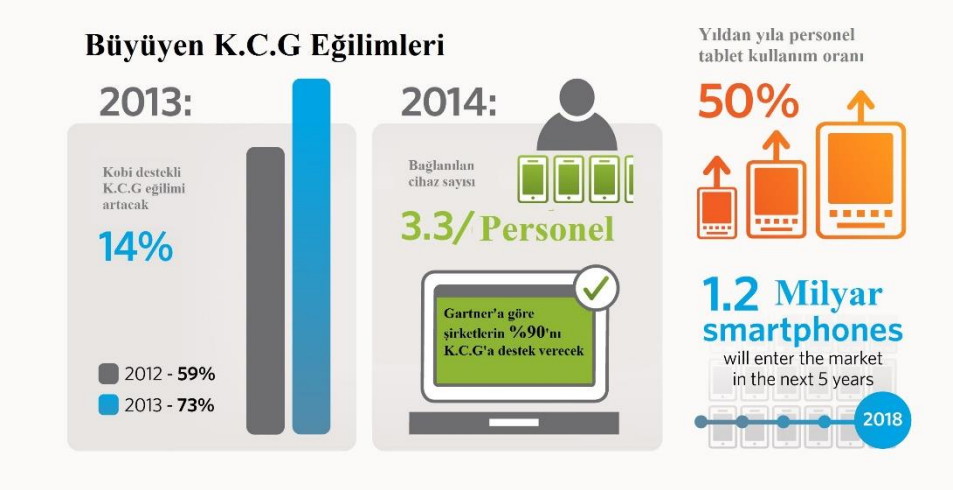
Araştırmaların Türkiye'ye özel bölümünde çalışanların taşınabilir cihazlarını çaldırmalarından kaynaklanan kazaların oranı, 2013'te yüzde 26'ya ulaşmış durumdadır. Yine şirketlerin yüzde 12'si, kritik derecede gizli bilgilerde yaşanan sızıntıların çalışanlardan kaynaklandığını açıklıyor. Türkiye'de taşınabilir cihazların hatalı kullanımı sonucu ortaya çıkan kazaların oranı ise yüzde 19'la yine dünya ortalamasının üstünde yer almaktadır.

Yukarıda değinilen zafiyetlere rağmen, dünya çapındaki şirketlerin sadece yüzde 28'i, kapsamlı "Taşınabilir Cihaz Yönetimi (MDM)" teknolojisini kullanmaya başladığı bilinmektedir.

Türkiye'de şirketlerin ise henüz sadece yüzde 16'sının tam kapsamlı bir taşınabilir güvenlik (Mobile security) çözümü bulunuyor. Yüzde 37'si ise taşınabilir güvenliğe önem verdiklerini, ancak bu konuda tam kapsamlı çözümlere henüz başvurmadıklarını açıklıyor. Yüzde 32'sinin ise taşınabilir güvenlik çözümü bulunmuyor.

Araştırmalar, ilerleyen yıllarda Kendi uygulamasının daha da yaygınlaşacağına dair ipuçları veriyor. Global şirketlerin yüzde 31'i önümüzdeki yıllarda daha çok çalışanın kendi cihazını işte de kullanacağını açıklıyor.

Türkiye'de ise bu oran yüzde 52 ile dünya ortalamasının da üstündedir. Bu konuda kısıtlama yapacağını ve izin vermeyeceğini açıklayan firma oranı ise dünya'da yüzde 10, Türkiye'de ise sadece yüzde 5 civarındadır.



Şekil.4. K.C.G. Eğilimleri

Kaynak: Jen C.(2013) "*Is a BYOD Policy Best for Your Business?"* içinden (Mayıs 2014) tarihinde http://truewirelessinc.com/byod/is-a-byod-policy-best-for-your-business/ 'den alındı.

Paul Ruggiero ve Jon Foote (2011)'a göre; geleneksel bilgisayarlardaki güvenlik, olgunlaşma çağını yaşarken tablet gibi taşınabilir cihazlarda ise güvenlik henüz emekleme çağını yaşamaktadır. Bazı taşınabilir cihazlarda ise güncellemeler, sadece sağlayıcılar bunu mümkün kıldığında yapılabilmektedir.
Tabi ki taşınabilir cihazlarda yapılan güncellemelerin sıklığı ile geleneksel bilgisayarlarda yapılanlar kıyaslanamaz. Bir çok durumda, taşınabilir cihazlar kısa vadeli, düzenli güncellemelere sahip değildir.

Botha, Furnell & Clarke (2009) açısından, taşınabilir cihaz güvenliği çoğu organizasyon tarafından göz ardı edilmektedir. İdeal güvenlik gereksinimlerine uygun olarak bilgisayarları yapılandıracak sistem yöneticisi mevcut olan organizasyonlarda dahi şirket tarafından çalışanlar için satın alınmış olmasına rağmen, akıllı telefon, tablet yada Kişisel Asistan (PDA) gibi taşınabilir cihazların yapılandırılması son kullanıcıların tercihine bırakılmaktadır. Bu yaklaşımdaki ana problem, tüm kullanıcıların taşınabilir cihazları, organizasyonun bilgi güvenliği gereksinimlerine uygun olarak yapılandıracak teknik bilgiye sahip olmamasından kaynaklanmaktadır. Bu durum organizasyon içerisinde bilgi sızıntısı olabilecek, güvenlik zafiyeti yaratan bir hat oluşturmaktadır.

Bunlara ek olarak, Cisco (2013) çalışanlar istediği zaman, istediği gibi sanaldoku (web) üzerinde tarama yapmanın ötesinde, özgürlük istemektedirler. Çalışanlar tarayıcı cihaz seçimi yapmak da istemektedirler. Bununla birlikte bu özgürlüklerinin ve mahremiyetlerinin iş verenleri tarafından ele geçirilmesini istememektedirler. Bu kullanıcılar, çalışanların aktivitelerinin işle alakalı olsa dahi, iş veren tarafından çevrimiçi olarak takip edilmesi konusunda iş verenler ile aynı fikirde değiller. Ve çalışanlar, iş verenlerin takip ve kayıt alma konusunda hakları olmadığına inanmaktadırlar.

Güvenlik personeline nerelerde iş düşmektedir? Eğer başarılı saldırı kaydı veya olası güvenlik saldırısı ile ilgili kayıtlar yok ise organizasyon için doğru güvenlik tekniğinin seçildiğinden nasıl emin olunabilir. Eğer organizasyonun olası saldırıları

düzenleyecek düşmanları hakkında bilgisi yok ise güvenlik ölçütleri belirlemek ve gelecekteki saldırıları önlemek mümkün olmayacaktır.

Doğru güvenlik tekniği olmaksızın, sanaldoku (web) üzerinde dolaşan bir çalışan aracılığıyla, organizasyonların bilgi kaynaklarına zarar verilmesini yada ulaşılmasını engellemek mümkün olmayacaktır. Çoğunlukla güvenlik yapılandırmalarının kullanışsız veya yanlış yapılandırılmış olduğu, bazı kullanıcıların bu güvenlik yapılandırmalarını atlatmak için verdikleri uğraşlar sayesinde ortaya çıkmaktadır ve bu durumun organizasyonların riske maruz kalmasına yol açmakta olduğu, Furnell, Jusoh & Katsabas (2006) tarafından ifade edilmiştir.

2.2. Problemin Tanımlanması

İyi bir güvenlik, bilgi ve iletişim cihazları kullanan tehditlere sınır getirmeye yardımcı olmalıdır ve "Derin Savunma" stratejisi olarak tanımlanmaktadır (McDonough, 2003). Bazı organizasyonlar, bu güvenlik stratejisine bağlı olarak gözükmelerine rağmen, taşınabilir cihazlar aracılığıyla oluşabilecek risklere karşı sistem açıklarını kapatmamaktadırlar. Bu ortamın güvenlik ve savunmasını sağlamak amacıyla, savunma ve sivil operasyonlar düzenli olarak incelenmelidir.

Akıllı telefonlar gibi taşınabilir cihazlar daha önceleri sadece geleneksel bilgisayarların desteklediği birçok uygulamayı destekleyebilecek güce erişmişlerdir. (Couture, 2010).

Taşınabilir cihazlar kullanılırken, iş için gereken bilgilere taşınabilir teknolojiler aracılığıyla, sorunsuz olarak ulaşılabilmelidir (Chen & Nath, 2003).
Bu durum son beş yılda taşınabilir cihazların kullanımının hızlı bir şekilde artmasını sağlamıştır (Ahmed et al., 2009; Neilson, 2010; Ruggiero & Foote, 2011; CISCO, 2013). Şirketlerdeki, elzem ve özel bilgilere beklenmedik müdahale ve kesinti gibi güvenlik sorunlarının kaynağı taşınabilir cihaz kullanımının artmasıdır.

Bu duruma rağmen, akıllı cihaz kullanıcıların büyük çoğunluğu cihazlarının ve kullanımlarının şirketlere getirmiş olduğu güvenlik zafiyetlerinin farkında değildirler. Bu durum, birincil önceliği güvenlik olan organizasyonlar için fırsat yaratmaktadır.

Akıllı cihazların satışlarındaki artışa bağlı olarak bu cihazlara yapılan saldırıların da arttığını bildirmektedir (Ruggiero & Foote (2011). Bu cihazlardaki güvenliği kırabilmek için mevcut eski tekniklerle ek olarak akıllı cihaz kullanıcılarının yardımlarıyla saldırı sahipleri için yeni tekniklerde geliştirilmektedir.
İş siber saldırıya geldiğinde, hangi yöntem seçilirse seçilsin, saldırı başarıyla tamamlandığı sürece yöntem seçiminin önemi yoktur (Cisco, 2013, p. 51).

Mobil Çoklu Ortam Mesajlaşma Hizmeti (MMS) gönderiliyormuş gibi yapılarak, kullanıcıların bilgisi dışında taşınabilir cihazların güvenliğinin kırılması en tipik durumlardan biridir.

Ruggiero & Foote (2011)' a göre, 2009 ve 2010 yılları arasında Android, IOS, Symbian ve windows mobil gibi mobil işletim sistemleri tarafından %42 oranında zafiyet sayısı artışı rapor edilmiştir. Bu uyarı verici durum endişe sebebidir. Bu zafiyetler yüksek derecede sofistike olmakla beraber, durum ve karakter değiştirebilirler ve tarama esnasında gözden kaçabilirler. Ölçütlere ve uyarı oranlarının artışına rağmen, akıllı cihazların bu zafiyetlere tepkimesi eş zamanlı olarak ilerlememektedir.

Takesue (2007) ve Ernst & Young (2012)'a göre taşınabilir cihazlar, iş verenler tarafından organizasyon içerisinde ve dışarısındaki dijital servetlerini ne derece riske attıklarını bilmeden, iş aracı olarak kullanılmaktadır.
Siber suçlular bugünün hızla gelişen teknoloji dünyasında saldırı sayılarını ve hızlarını arttırarak, dağıtık bulut servislerinden iş uygulamalarına erişen ağdaki cihazlara, kullanıcıların yetersizliğinden faydalanarak erişmektedirler(Cisco, 2013).

Price waterhouse Coopers (2012), organizasyonların sadece %44'ünün taşınabilir güvenlik stratejisine sahip olduğuna dikkat çekmektedir. 2012'de gerçekleştirilen anket sonuçlarına göre, cihazlarını iş ortamında kullanan katılımcıların %45'inin sadece taşınabilir güvenlik stratejisine sahip olduğunu ve bunların %37'sinin taşınabilir cihazlarını kötü amaçlı yazılımlara karşı korunma sağladığına dikkat çekmektedir.

Organizasyonlardaki taşınabilir (mobile) iletişim güvenliği ve güvenlik politikalarına adaptasyonun giderek artışta olduğu görünmesine karşılık, taşınabilir teknolojilerin hızla gelişimine kıyasla hala bu gelişim düşük seviyede kalmaktadır (PricewaterhouseCoopers, 2012).

2.3. Güvenlikte Tanımlanan Amaçlar

Araştırmaların asıl amacı, bilinmeyen gerçekler ile ilgili kanıt toplamaktır (Taflinger, 1996). Bu çalışma, taşınabilir cihazları iş ortamında kullanan gezici çalışanların, organizasyonlara bilgi güvenliğini sağlamak için düşen zorluklar ve etkileri çözümleme amacıyla yazılmıştır.

Bu çalışmada amaçlanan konular aşağıdaki gibidir;

i. Organizasyon içerisinde, çalışanların akıllı cihazların kullanımı sonucu ortaya çıkabilecek bilgi güvenliği ilgili açıların algılanması ve potansiyel saldırıların negatif sonuçlarının ortaya çıkarılması,

ii. Organizasyon içerisinde, taşınabilir cihazların kullanılması sonucunda oluşabilecek en belirgin tehdit ve risk alanlarının analiz edilmesi,

iii. Çalışan ortamlardaki akıllı cihazlar için uygun ve ücretsiz karşı önlemlerin belirlenmesine katkı sağlamak,

iv. Mobilite'nin Bilgi Güvenliğine getirmiş olduğu zorlukların analiz edilmesi,

2.4. Araştırma'nın Ana Soruları

Aşağıda listelenmiş olan sorular, bu çalışmanın amaç ve kapsamını detaylandırmak ve yardımcı olmak amacıyla oluşturulmuştur.

1. Çalışma aracı olarak mobil cihazların kullanılmasının yaratacağı riskler, tehdit veya zafiyetler nelerdir?

2. Çalışma aracı olarak mobil cihazların kullanılmasının yaratacağı riskler, tehdit veya zafiyetler nasıl kontrol edilebilir?

3. Mobilite bilgi güvenliğini ne ölçüde zorlamaktadır ve taşınabilirlik sayesinde yaşanan bilgi güvenliği problemlerini adreslemek için sosyo-teknik teoriler nasıl kullanılabilir?

2.5. "Kendi Cihazını Getir" Kapsamı, Kısıtlamalar ve Kullanım Alanları

Bu çalışma iş aracı olarak taşınabilir cihazların kullanılmasından kaynaklı riskler, tehdit veya zafiyetlerin altını çizmektedir. Ayrıca bilgi güvenliği açısından taşınabilir cihaz kullanıcılarının algısını özetlemektedir. Son olarak da taşınabilirlik ve akıllı cihaz kullanımının organizasyonların bilgi güvenliğine olan etkisini analiz etmektedir. Organizasyon içerisindeki çalışanların IOS, Android, Symbian veya Windows mobil gibi farklı işletim sistemlerine sahip farklı akıllı cihazları kullanmasıyla birlikte araştırmaların hedefi herhangi bir işletim sistemi olarak belirlenememektedir.

Cihazların arama, tarama, görev atama, uygulama çalıştırma gibi özelliklerini ve "kablosuz kişisel alan ağ" (Bluetooth-WPAN) cihazları, kulaklıklar gibi aparatların cihazlar tarafından kullanılabilmesini sağlayan yazılımların tümü işletim sistemi içerisinde ele alınmaktadır.

Şekil.5. K.C.G. Cihazlarının Kullanım Oranları

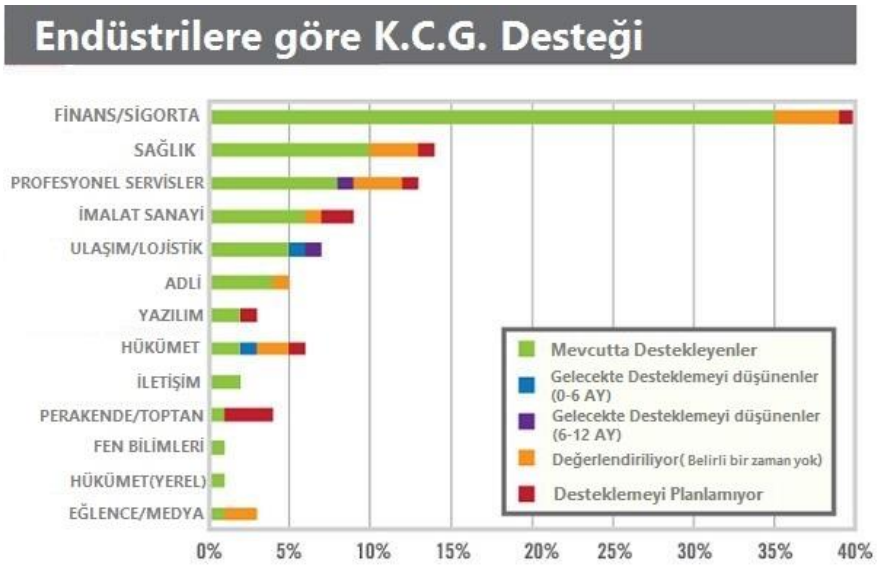
Kaynak: Editorial Team (2013) "*Bring Your Own Device: Pros and Cons"* içinden (Mayıs 2014) tarihinde http://edtechreview.in/e-learning/334-byod-pros-cons 'den alındı.

Bu cihazlar; taşınabilir medya cihazları, dijital kameralar, video kameralar, doküman okumayı destekleyen, dokunmatik ekrana sahip, sanaldoku (web) tarayıcısı olan Küresel Konumlama Sistemi (GPS), kablosuz bağlantı alanı (Wi-Fi) ve taşınabilir geniş bant bağlantı (mobile broadband) teknolojileri aracılığıyla ağlara bağlanabilen ve üzerinde Android, IOS, windows ya da Symbian işletim sistemi olan taşınabilir cihazlar olarak düşünülebilir.

Sektör açısından; Tüm kurumsal firmalar, finans şirketleri, kamu teşkilatları, üniversiteler, özel kuruluşlar ve hatta günümüzde gönüllü çalışan sivil toplum örgütleri ve organizasyonlar K.C.G.'yi desteklemektedir.

Teknik açıdan K.C.G. genel kapsamı itibariyle akıllı telefon, tablet ve dizüstü bilgisayarları destekleyecek şekilde tasarlanmıştır. Bu doğrultuda Android, IOS ve Windows işletim sistemleri açısından incelenmeli ve bu doğrultuda güvenlik saptamaları yapılmalıdır.

Bu alan özellikle güvenlik protokolleri düşünüldüğünde K.C.G. projesinin işletim sistemi seviyesinde incelenmesi açısından önemlidir. IOS işletim sistemini kullanan mobil cihazların üzerine uygulanacak şifreleme yöntemleri ve kontrolü açısından önemlidir.



Şekil.6. K.C.G.'nin Desteklendiği Endüstriler

Kaynak: Ravindran, S. , Sadana, R. , Baranwal, D.(Ağustos 2013) "*BYOD in the Enterprise—A Holistic Approach"* içinden (Mayıs 2014) tarihinde http://www.isaca.org/Journal/Past-Issues/2013/Volume-1/Pages/BYOD-in-the-Enterprise-A-Holistic-Approach.aspx 'den alındı.

Örneğin; "Samsung Mobile" taşınabilir cihazlarını gelişmekte olan K.C.G. kurumsal alan içinde kullanılabilmesi için "KNOX" teknolojisi yaratmış ve üzerinde çalışmaya devam etmektedir. "Knox" sayesinde güvenlik açıklarının olduğunu düşündüğümüz android işletim sistemi için Samsung firması farklı bir boyut kazandırmıştır.

Bu araştırmada kullanılan taşınabilir cihazlar organizasyonlar tarafından çalışanın iş esnasında kullanımı için yada çalışanların kendileri tarafından temin edilmiş olabilir. Aktarımı esnasında bu çalışma bazı kısıtlamalar içermektedir. Bu çalışmada taşınabilir cihazlarla ilgili ele alınan güvenlik senaryoları, araştırmacıların ilgili tutum ve deneyimlerine rağmen gizli dataları yoğunlukta olan kurumlar için referans oluşturmamaktadır.

2.6. K.C.G. 'in Güvenlik Açısından İncelenmesi

K.C.G. kullanımı öncesi birçok firma ve BT (IT) liderinin sorguladığı ilk konu veri güvenliğidir. Özellikle finans şirketlerinde veri güvenliği hassasiyeti en üst seviyededir. Bu noktada şirket verilerinin çalışanların kendi cihazlarından monitör edilmesi noktasında ortaya çıkabilecek olası riskler değerlendirilmelidir.

K.C.G. hazırlayacağınız yazılım yada üçüncü şahsa ait (third party) uygulamalar ile belli bir güvenli bağlantı ile kullanıcı cihazı üzerinde çalıştırmayı amaçlar. Tıpkı kişinin bir internet sayfasını kendi cihazında açması gibi. Veriler sağlayıcılar tarafından ağırlanır. Farklı noktası ise kişinin K.C.G'e konu olan servisin monitör edilmesi için kullanılan uygulamanın ve içerisinde monitör edilen verinin güvenliğini sağlamak için oluşturulacak şifreleme yöntemleri ve protokollerdir.

Bizim çalışmamızdaki inceleme alanımız da tam olarak bu noktadır. Kullanıcının cihazında çalıştıracağınız uygulama üzerinde izlenilen şirket verisi, içinde bulunduğu servisin şifreleme yapılması ile korunur. Fakat günümüzde akıllı cihazların ve işletim sistemlerinin yaygınlaşması ve kullanım alanlarının artması bu nokta da güvenlik açıklarının oluşmasına ve sosyal mühendislik açıklarına yada bilgi hırsızlığına yol açmıştır. Bu noktada bizim önerimiz oturum şifreleme (session encryption) dışında verinin de şifrelenmesidir. Oluşturulacak bu şifreleme yöntemi ile Rastlantısal Erişim Hafızası (RAM) üzerinde görüntülenen verinin korunması sağlanmış olunacaktır.

Bilgi riskinin ulaşabileceği noktalar;

- Mobil cihazın çalınma ihtimali,
- İşletim sisteminin kırılma ihtimali,
- Cihaza virüs girmesi yada kötü amaçlı yazılım (malware) bulaşması ihtimali,
- Uygulama bazlı sorun yaşanma ihtimali,
- Oturumun uzaktan ele geçirilme (hack) ihtimali,

2.7. K.C.G. Ağlarındaki Güvenlik Açıkları

"CNBC" ye göre , 258 üst düzey yönetici arasında yapılan bir ankette, yöneticilerin %85'i organizasyonlarına gerçekleştirilebilecek potansiyel siber saldırılar hakkında endişelerini dile getirdi. Raporlara göre ağ güvenliği ihlallerinden etkilenen şirketlerin haberleri istisnadan çok standart hale gelmiştir. 2011 yılında, Federal İletişim Komisyonu (FCC) bir BT güvenlik ihlali keşfetti ve hızla virüslü iş istasyonlarını belirlemek, kaldırmak için gelişmiş güvenlik ağı üzerinde acil müdahale planı oluşturarak harekete geçti.

2013 Şubat ayı içerisinde, "US Federal Reserve" sunucusu, çalışanların kişisel ve hesap bilgilerini çalan anonim bir grup tarafından ele geçirildi (hack'lendi). Sunucu sonrasında hızla tamir edilebilen bir açık sayesinde ele geçirildi (hack'lendi). Federal Rezerv güvenlik ihlali ufak gibi görünüyor olsa da herhangi bir devlet kurumu bilgilerinin sızması ihtimali çok önemli bir durumdur. Tüm organizasyonlar harici bir kaynaktan gelebilecek bir güvenlik tehditleri için risk altındadır. Güvenlik ihlallerinin ve hassas verilerin ele geçirilmesini önlemek amacıyla güçlü politikalar oluşturulmalı ve uygulanmalıdır.

2.8. K.C.G. Ağ (Network) Güvenlik Açıklarının Giderilmesi Çalışması

Şu ana kadar ki kısımlarda K.C.G.'nin ne olduğu, K.C.G.'yi oluşturan temel noktaları ve bu noktaların çalışma mantığı temel düzeyde anlatılmıştır.

K.C.G. sisteminin çalışmasında dikkat çektiğimiz güvenlik açıklarının başında şirketin içerideki bilgilerine erişilmesi durumu mevcuttur. Bu noktada Cihaz güvenliği, bağlantı güvenliği ve uygulama güvenliği dışında veririnin de şifrelenmesi gerektiği bu tezin konusunu oluşturmaktadır.

İş dünyası giderek gezici çalışma sistemine yönelmektedir. K.C.G. programlarındaki güvenlik ihlallerini ve açıkları gidermek için önlemler alınmalıdır

Veri şifreleme: Verilerin yetkisiz kişilerce okunmasını engellemek amacıyla verinin şifrelenerek tutulmasıdır. Uygulanması diğer yöntemlere nispeten daha ucuz ve basittir. Veri şifreleme, taşınabilir cihazlarda güvenlik ihlallerini önlemek için etkili bir çözümdür.

Yönetim sistemleri : Özellikle K.C.G. sistemini uygulayan şirketlerin, yazılan politika ve kuralları çalışanlarına uygulayabilmesi için sistemlerini yönetmeleri gereklidir. Bu sistemler, şirket ağında çalışanlar tarafından kullanılan şifrelenmemiş cihazları ağ dışarısında bırakmak için kullanılabilir. Güvenli veri transferi için onaylanmış cihazların kullanımı, organizasyonları güvenlik ihlallerinden korur. Ayrıca, tüm çalışanların bilgisayarlarına konulacak güçlü parolalar ve düzenli olarak güncellenen anti-virüs yazılımları güvenlik ihlali şansını azaltacaktır.

Teknoloji: Teknoloji bazı hayati fonksiyonlar üzerinde personeli eğitmeyi gerektirmektedir. Anti-virüs yazılımı, güvenlik duvarları ve WPA2(Kablosuz Korumalı Erişim) desteklenen kablosuz yönlendiriciler gibi teknolojiler doğru ve etkin kullanıldığı zaman çalışanların işlerini daha güvenli olarak yapabilmelerine olanak sağlar.

Kurumsal veri kontrolü : K.C.G. sisteminde taşınabilir cihazlar üzerindeki kurumsal bilgileri ve uygulamaları izlemek yeni teknoloji ile daha kolay hale gelmiştir. Örneğin, BlackBerry 10, K.C.G. için özel olarak yapılmış bir işletim sistemine sahiptir. BT departmanları kurumsal veri kontrolü cihazın çalınması durumunda şirket bilgileri ile birlikte kişisel verilerin açığa çıkmasını engellemektedir.

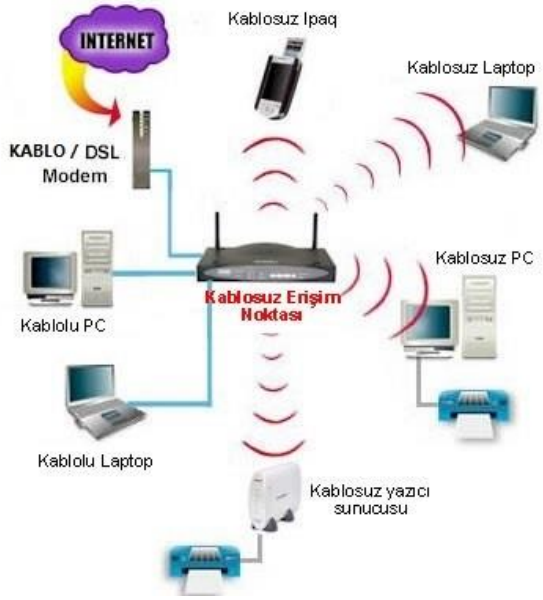
Şirketler, gelişmekte olan K.C.G trendinden, ölçülü davranarak yararlanmaktadırlar. K.C.G şirket verilerinin güvenliklerinin ihlal edilebilmesi için fırsatlar sağlar. En küçük güvenlik ihlali için bile uygun önlemler alınmalıdır.

2.9. Kablosuz Ağlar ve Güvenlik

2.9.1. Kablosuz Ağ Nedir ve Çalışma Mantığı Nasıldır?

Kablosuz Ağlar, kablosuz haberleşme yeteneğine sahip (802.11, GSM, Bluetooth) cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır. Örnek; Yerel Alan Ağları (802.11 gibi..), Kişisel Alan Ağları (bluetooth gibi..), Geniş Alan Ağları (GSM gibi..)

Son yıllarda özellikle Bakışımsız Sayısal Abone Hattı (ADSL) hizmetinin genişlemesi ile birlikte kablosuz ağ destekli modemlerin kullanımı da artmıştır. Bu tip modemlerdeki kablosuz ağ özelliğinin sağladığı esneklikler ve kolay kullanımı sayesinde artık her evde bir kablosuz ağ oluşmaya başladığını görüyoruz. Özellikle fiyat/kullanım özelliği oranındaki başarım kablosuz ağların yaygınlaşmasında önemli rol oynamıştır. Teknolojiye uyum sağlamak ve avantajlarından "zarar görmeden" maksimum seviyede yararlanmak gerekmektedir fakat bunun için önce kullandığınız sistemi tanımanız şarttır.



Şekil.7. Kablosuz Ağ Grafiği

Kaynak: Emre A. (Ocak 2014) "Kablosuz ağ" içinden (Mayıs 2014) tarihinde http://turkkod.org/?p=2052 'den alındı.

2.9.2. Kablosuz Ağlarda Güvenlik Açıkları Ve Riskler

Bu kadar kolaylıklar sağlayan her teknolojide kaçınılmaz bazı tasarım eksiklikleri, güvenlik açıkları olacaktır. Kablosuz ağlardaki en temel güvenlik problemi verilerin havada uçuşmasıdır. Normal kablolu ağlarda anahtar ya da hub kullanarak güvenliğimizi fiziksel olarak sağlayabiliyor iken, anahtar'a/hub'a fiziksel olarak bağlı olmayan makinelerden korunma sağlanabiliyordu. Oysaki kablosuz ağlarda tüm iletişim hava üzerinden kuruluyor ve veriler gelişigüzel ortalıkta dolaşıyor.

Erişim Noktasını görünmez kılma

Kablosuz ağlarda erişim noktasının adını (SSID) saklamak alınabilecek ilk temel güvenlik önlemi olarak gözüküyor. Fakat bu tip ağların çalışma yöntemlerine bakacak olursak bu adın (SSID) sadece belirli seviyedeki kullanıcılardan saklanabileceğini görmüş oluruz. Erişim noktaları ortamdaki kablosuz cihazların kendisini bulabilmesi için kendilerini devamlı anons ederler. Teknik olarak bu durulara "beacon frame"(yol gösterici/yönetici yapı) denir. Güvenlik önlemi olarak bu anonsları yaptırmayabiliriz ve sadece erişim noktasının adını bilen cihazlar kablosuz ağa dahil olabilir. Böylece Windows, Linux da dahil olmak üzere birçok işletim sistemi etraftaki kablosuz ağ cihazlarını ararken bizim cihazımızı göremeyecektir.

Diğer bir sorun da erişim noktasının Kabloya Eşdeğer Gizlilik (WEP) ya da Kablosuz Korumalı Erişim (WPA) protokollerini kullanması durumunda bile SSID'lerini (Hizmet Seti Tanımlayıcısı) şifrelemeden göndermesidir. Bu da ortamdaki kötü niyetli birinin özel araçlar kullanarak bizim erişim noktamızın adını her durumda öğrenebilmesini sağlayacaktır.

Erişim Kontrolü

Standart kablosuz ağ güvenlik protokollerinde ağa giriş anahtarını bilen herkes kablosuz ağa dahil olabilir. Kullanıcılarınızdan birinin WEP (Kabloya Eşdeğer Gizlilik) anahtarını birine vermesi/çaldırması sonucunda WEP (Kabloya Eşdeğer Gizlilik) kullanarak güvence altına aldığımız kablosuz ağımızda güvenlikten eser kalmayacaktır. Zira herkeste aynı anahtar olduğu için kimin ağa dahil olacağını bilemeyiz.

Medya Erişim Kontrolü (MAC) tabanlı erişim kontrolü

Piyasada yaygın kullanılan erişim noktası (AP) cihazlarında güvenlik amaçlı konulmuş bir özellik de Medya Erişim Kontrolü (MAC) adresine göre ağa dahil olmadır. Burada yapılan kablosuz ağa dahil olmasını istediğimiz cihazların Medya Erişim Kontrolü adreslerinin belirlenerek erişim noktasına bildirilmesidir. Böylece tanımlanmamış Medya Erişim Kontrolü adresine sahip cihazlar kablosuz ağımıza bağlanamayacaktır. Yine kablosuz ağların doğal çalışma yapısında verilerin havada uçuştuğunu göz önüne alırsak ağa bağlı cihazların Medya Erişim Kontrolü adresleri de havadan geçecektir, burnu kuvvetli koku alan bir bilgisayar korsanı bu paketleri yakalayarak izin verilmiş Medya Erişim Kontrolü adreslerini alabilir ve kendi Medya Erişim Kontrolü adresini kokladığı Medya Erişim Kontrolü adresi ile değiştirebilir. Medya Erişim Kontrolü adresleri cihazlar üzerinde tanımlı gelir ve değiştirilemez ama biz cihazı kullanan işletim sistemine vereceğimiz komutlarla Medya Erişim Kontrolü adresini farklı gösterebiliriz.

Sonuç olarak; Erişim Noktası (AP) ile İstemci arasındaki Medya Erişim Kontrolü (MAC) adresleri açık bir şekilde gideceği ve Medya Erişim Kontrolü (MAC) adreslerini değiştirmek oldukça kolay olduğu için bu yöntemde kesin bir güvenlik sağlamayacaktır.

2.10. Kablosuz Ağlarda Güvenlik Hiyerarşisi

Kablosuz Ağ hiyerarşisinin anlaşılabilmesi için kablosuz ağın ne olduğunun, çalışma mantığının ve yöntemlerinin iyi anlaşılması önemlidir.

2.10.1. Kablosuz Ağ Standartları

Kablosuz ağ standartları 1997 yılından itibaren Elektrik-Elektronik Mühendisleri Enstitüsü (IEEE), tarafından geliştirilmeye başlanmıştır. Geliştirilen bu standardın genel adı IEEE 802.11'dir. 802.11 standardı kablosuz yerel ağ, üzerinden iletişim kurarken kullanılan kuralları temsil eder. IEEE 2,4 GHz frekansında çalışan, maksimum 75 metreyi kapsayan, 1-2 Mbps aralığında veri iletimi hızı sunan bu standardın teknolojik gelişmeler sonucunda yetersiz hale gelmesiyle, 802.11x adı verilen standartlar serisini geliştirmeye başlamıştır.

Arada farklar olmasına rağmen temel olarak 802.11 ailesi aynı iletişim kurallarını kullanır. 802.11a, 802.11b, 802.11g ve yeni geliştirilen 802.11n bu standartlardan en çok kullanılanlardır.

802.11a

802.11 standardının yetersiz hale gelmesiyle, 1999 yılında ortaya çıkan ilk geliştirilmiş sürümdür. Bu standart temelde 802.11 ile benzer olmasına karşın 5 gHz frekansında çalışmaktadır. 54 Mbps veri iletim hızı sunan bu standart, açık alanlarda maksimum 100 metreyi kapsayacak şekilde çalışabilmektedir.

802.11a'yı diğer kablosuz ağ standartlarından ayıran temel avantajı daha fazla kapasiteye (throughput) destek vermesi ve daha fazla kanal kapasitesi olmasıdır, böylelikle daha fazla bant genişliği kullanımına olanak sağlamaktadır.

Diğer standartların aksine 802.11a'nın 5GHz frekansında çalışması bu standarda çeşitli avantajlar ve dezavantajlar sağlamıştır. Bu frekansta yayın yapmanın olumlu yanı, kablosuz kişisel alan ağ (bluetooth), mikrodalga fırın ve kablosuz telefon gibi diğer elektronik cihazlarının farklı frekans aralığını kullanmasından dolayı kanal

kapasitesi artar ve veri iletim hızı daha yüksek olur. Bununla birlikte 5GHz frekansında yapılan yayınların, duvar gibi engeller tarafından daha fazla emilmesi nedeniyle 802.11a'nın kapalı alanlardaki kapsama alanı diğer standartlara göre daha düşüktür.

Son olarak, bu teknoloji yüksek veri iletim hızına ihtiyaç duyan kullanıcılar ve video dağılım sistemlerinde aktif olarak kullanılmaktadır. Daha pahalı cihazlarda bulunmasına rağmen iş hayatında kurumsal kullanıcılar tarafından tercih edilmektedir.

802.11b

802.11b standardı 802.11a ile beraber 1999 yılında piyasaya sürülmüştür. Ancak 802.11a'ya göre çok daha kısa bir sürede yaygınlaşarak bütün dünyada kullanılmaya başlanmıştır. 802.11b, 802.11 gibi 2.4 GHz frekans bandında çalışmakta ve 11 Mbps veri iletimi hızına çıkabilmektedir.
İlk çıktığında 802.11b erişebildiği veri iletim hızının etkisiyle yerel ağ (ethernet) teknolojisine rakip hale gelmiş ve kablosuz ağ kullanımının yaygınlaşmasında büyük rol oynamıştır.

802.11b'nin sağladığı en önemli avantaj kapsama alanı mesafesinin fazla olmasıdır. 2.4 GHz frekansında yayın yapmasından dolayı kapalı alanlarda yaklaşık olarak 38 metre, açık alanlarda ise 150 metreyi aşacak şekilde alanı kapsayabilmektedir. Ayrıca maliyet açısından da diğer standartlara göre oldukça uygundur. Bununla birlikte kablosuz kişisel alan ağ (bluetooth), mikrodalga fırın ve kablosuz telefon gibi farklı elektronik cihazlar ile aynı frekansta çalışmasından dolayı işaretler birbiriyle karışmaktadır. Bunun sonucunda veri iletim hızı ve bant genişliği 802.11a'ya göre daha düşüktür.

Sonuç olarak, 802.11b genellikle ofis ortamları, hastaneler, depolar ve fabrikalar gibi ortamlarda kullanılmaya oldukça uygundur. Özellikle konferans salonları, çalışma alanları ve kablo çekmenin tehlikeli olduğu noktalarda ağ bağlantısı sağlanması için uygun bir teknolojidir. Kısaca 802.11b, taşınabilirliğin gerekli olduğu ve orta hızlı ağ bağlantılarına ihtiyaç duyulan alanlarda kullanılır.

802.11g

2003 yılında Elektrik-Elektronik Mühendisleri Enstitüsü (IEEE) tarafından kablosuz ağ standartlarında geliştirilen üçüncü nesil teknolojidir. 802.11b'de olduğu gibi 2.4 GHz frekansında çalışmaktadır. 802.11g standardı temel olarak 802.11b standardının bir uzantısıdır, fakat veri iletim hızı ve kullanılan bant genişliğinde önemli ölçüde gelişme sağlanmıştır. Bu açıdan bakılırsa 802.11g için 802.11a ve 802.11b'nin daha etkin olduğu özelliklerinin birleştirilmiş hali olduğu söylenebilir.

802.11g'nin sahip olduğu en önemli özellik 802.11b ile ulaşılan kapsama alanını koruyarak, (açık alanlarda 38 metre, kapalı alanlarda 150 metre) veri iletim hızını ortalama 22 Mbps'a ulaştırmasıdır. Bu hız 802.11a'da olduğu gibi maksimum 54 Mbps'a ulaşabilmektedir.

Bu standardın zaman zaman 802.11b ile çalışan cihazlarla uyum sorunu yaşamasından dolayı kullanımı çok fazla yaygınlaşmamıştır. Bununla birlikte fiyatının 802.11b'den yüksek olması da tercih edilebilirliğini azaltmaktadır.

Son olarak, yüksek hız gerektiren video ve çoklu ortam uygulamalarında hızı ve kapsadığı alanın genişliği nedeniyle 802.11g standardı oldukça uygundur.

802.11n

Zaman içerisinde kullanıcı sayısının artması ve kullanıcıların farklı uygulamaları kullanmak istemesi daha fazla bant genişliği, daha fazla süreklilik ve daha geniş kapsama alanı gibi talepleri artırmıştır. Bu amaçla Elektrik-Elektronik Mühendisleri Enstitüsü (IEEE) 2003 yılından beri 802.11n standardını geliştirmek üzere çalışmaya başlamıştır.

802.11n, Çoklu Giriş / Çoklu Çıkış, MIMO (Multiple Input / Multiple Output), adı verilen bir protokol sayesinde 2,4 GHz ve 5 GHz frekanslarının her ikisini de aynı anda kullanabilmektedir. MIMO teknolojisi, iletilecek bir bilginin parçalara ayrılıp farklı antenler üzerinden karşı tarafa gönderilmesini sağlar. Diğer standartlarla çalışan cihazlar bir anten üzerinden bir yayın yaparken, 802.11n teknolojisine sahip ağ

cihazları gönderi tarafında 2 veya daha fazla yayın yaparken, alım tarafında birden fazla anten kullanırlar ve birden fazla alınan/gönderilen yayınları birleştirirler. Gönderilen veriler duvarlardan, kapılardan ve diğer eşyalardan yansıyarak ve farklı rotalar takip ederek alıcı antene farklı zamanlarda ve birden fazla kere varır. MIMO teknolojisi bu durumu kendi lehine kullanarak işaretin güçlenmesini ve daha uzaklara iletilmesini sağlar.

802.11n standardına göre veri iletim hızı ortalama 130 Mbps seviyelerinde olacaktır. Hatta teorik olarak bu hız 600 Mbps'ye kadar ulaşabilir ve kapsama alanı kapalı alanlarda 70 metre, açık alanlarda ise 250 metre kadar olabilir. Bu teknolojinin en önemli özelliklerinden birisi de eski standartlarla uyumlu bir şekilde çalışabilmesidir.

Sonuç olarak, 802.11n henüz tam olarak tamamlanmamış bir standart olmasına rağmen vadettiği veri hızı, güvenilirlik ve olması beklenen yüksek fiyatı ile İnternet telefonu, müzik ve video yayını, IPTV gibi daha fazla bant genişliği isteyen uygulamalar için oldukça yeterli olacaktır.

2.10.2. Açık ve Paylaşılan Ağ Kimlik Doğrulaması

802.11 iki tipte ağ kimlik doğrulama yöntemini destekler: Açık sistem ve paylaşılan anahtar kimlik doğrulaması.

Açık kimlik doğrulama yöntemi kullanıldığında her kablosuz istasyon kimlik doğrulama talebinde bulunabilir. Başka bir kablosuz istasyonla kimlik doğrulaması yapması gereken istasyon, gönderen istasyonun kimliğini içeren bir kimlik doğrulama yönetim isteği gönderir.
Alıcı istasyon ya da erişim noktası her kimlik doğrulama isteğini kabul eder. Açık kimlik doğrulama yöntemi her aygıta ağa erişim izni verir. Ağda şifreleme etkinleştirilmediyse erişim noktasının Hizmet Seti Tanımlayıcısını (SSID) bilen her kablosuz aygıt ağa erişebilir.

Paylaşılan anahtar kimlik doğrulaması kullanılırken, her kablosuz istasyonun, 802.11 kablosuz ağ iletişim kanalından bağımsız güvenli bir kanal üzerinden gizli bir paylaşılan anahtar aldığı varsayılır. Bu gizli anahtarı, kablolu bir yerel ağ(ethernet) bağlantısı aracılığıyla ya da bir Evrensel Seri Veriyolu(USB) bellek kartı ya da Yoğun Disk(CD) yardımıyla fiziksel olarak paylaşabilirsiniz. Paylaşılan anahtar kimlik doğrulaması, istemcinin statik bir Kabloya Eşdeğer Gizlilik(WEP) anahtarı yapılandırmasını gerektirir. İstemci yalnızca, sorgulama tabanlı bir kimlik doğrulamasından geçerse erişim izni alır.

Kabloya Eşdeğer Gizlilik (WEP)

Kabloya Eşdeğer Gizlilik (WEP), kablosuz verilerin yetkisiz biçimde alınmasını önlemeye yardımcı olmak için şifreleme kullanır. Kabloya Eşdeğer Gizlilik (WEP), verileri göndermeden önce şifrelemek için bir şifreleme anahtarı kullanır. Yalnızca aynı şifreleme anahtarını kullanan bilgisayarlar ağa erişebilir ve başka bilgisayarlar tarafından gönderilen verilerin şifresini çözebilir. Kabloya Eşdeğer Gizlilik (WEP), şifrelemesi 64-bit anahtar (bazen 40-bit olarak anılır) ya da 128-bit anahtar (104-bit olarak da bilinir) kullanan iki güvenlik düzeyi sağlar. Daha iyi güvenlik için 128-bit anahtar kullanmalısınız. Şifreleme kullanıyorsanız, kablosuz ağınızdaki tüm kablosuz aygıtlar aynı şifreleme anahtarını kullanmak zorundadır.

Kabloya Eşdeğer Gizlilik (WEP), veri şifreleme ile bir kablosuz istasyon, en çok dört anahtar içerecek biçimde yapılandırılabilir (anahtar dizini 1, 2, 3 ve 4'tür). Bir erişim noktası ya da kablosuz istasyon belirli bir anahtar dizininde saklanan bir anahtarı kullanan şifrelenmiş bir ileti gönderdiğinde, iletilen mesajda mesaj gövdesini şifrelemek için hangi anahtar dizininin kullanıldığı belirtilir. Alıcı erişim noktası ya da kablosuz istasyon, belirtilen anahtar dizinindeki anahtarı alarak şifrelenmiş ileti gövdesinin şifresini çözebilir. Kabloya Eşdeğer Gizlilik (WEP) şifreleme algoritması, ağ saldırılarına açık olduğundan, Kablosuz Korumalı Erişim-Bireysel (WPA-Bireysel) ya da Kablosuz Korumalı Erişim2-Bireysel (WPA2-Bireysel) güvenlik yönteminin kullanımı dikkate alınmalıdır.

Kablosuz Korumalı Erişim-Bireysel (WPA-Bireysel)

WPA-Bireysel Modu, ev ve küçük işletme ortamları için tasarlanmıştır. WPA Bireysel için erişim noktalarında ve istemcilerde bir ön paylaşımlı anahtarın (PSK) el ile yapılandırılması gerekir. Kimlik doğrulama sunucusu gerekmez. Bu bilgisayarda ve kablosuz ağa erişen tüm bilgisayarlarda erişim noktasına girilen parola kullanılmalıdır.

Güvenlik, parolanın gücüne ve gizliliğine bağlıdır. Uzun parolalar kısa bir parolaya oranla daha fazla ağ güvenliği sağlar. Kablosuz erişim noktanız ya da yönlendiriciniz WPA-Bireysel ve WPA2-Bireysel özelliğini destekliyorsa, erişim noktasında bu özelliği etkinleştirip uzun, sağlam bir parola girmelisiniz. WPA-Bireysel, Geçici Anahtar Doğruluğu Protokolü (TKIP) ve Gelişmiş Şifreleme Standardı-CCMP(AES- Counter Mode with Cipher Block Chaining Message Authentication Code Protocol) veri şifreleme algoritmalarını kullanılabilir kılar.

Kablosuz Korumalı Erişim2-Bireysel (WPA2-Bireysel)

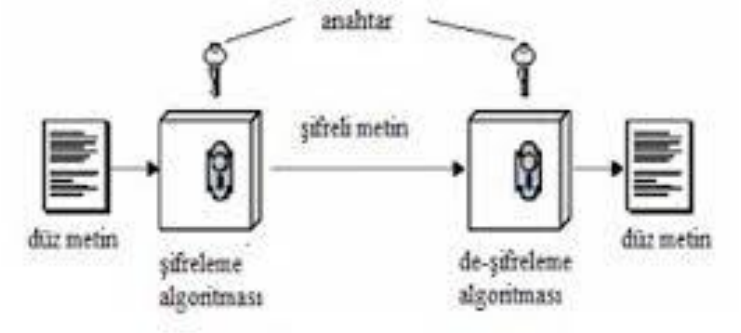
WPA2-Bireysel için erişim noktalarında ve istemcilerde bir ön paylaşımlı anahtarın (PSK) el ile yapılandırılması gerekir. Kimlik doğrulama sunucusu gerekmez. Bu bilgisayarda ve kablosuz ağa erişen tüm bilgisayarlarda erişim noktasına girilen parola kullanılmalıdır.

Güvenlik, parolanın gücüne ve gizliliğine bağlıdır. Uzun parolalar kısa bir parolaya oranla daha fazla ağ güvenliği sağlar. WPA2, WPA'nın geliştirilmiş bir şeklidir ve IEEE 802.11i standardına tam olarak uygundur. WPA2, Kablosuz Korumalı Erişim (WPA) ile geriye dönük uyumludur. WPA2-Bireysel, TKIP (Geçici Anahtar Doğruluğu Protokolü) ve AES-CCMP (Gelişmiş Şifreleme Standardı - CCMP) veri şifreleme algoritmalarını kullanılabilir kılar.

2.11. Geçmişten Günümüze Şifreleme ve Kimlik Doğrulama Yöntemleri

2.11.1. Veri Şifreleme

Veriler, çeşitli şifreleme yöntemleri kullanılarak şifrelenir (encryption) ve okunamaz hâle getirilir. Gönderildiği yerde de yine çeşitli yöntemlerle şifresi çözülür (decryption). Verinin gönderildiği sistemde, kaynakta kullanılan şifreleme tekniği ile aynı mantıkta çalışan şifre çözme programı bulunmak zorundadır. Çünkü şifrelerin çözülebilmesi için kaynakta kullanılan algoritmaların hedefte de kullanılması gereklidir. Eğer kaynakta kullanılan algoritmalar hedefte yoksa şifrenin çözülmesi imkânsız hâle gelebilir.



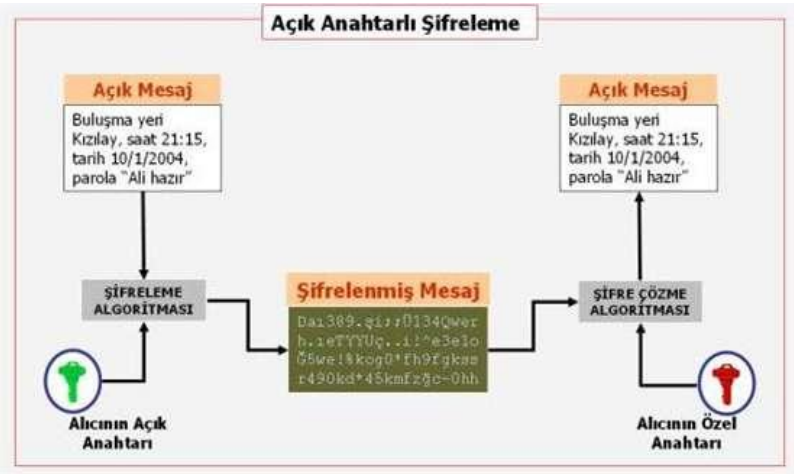
Şekil.8. Şifreleme

Kaynak: Deveci M.S.(Haziran 2011) "*DES ile Veri Şifreleme -1"* içinden (Mayıs 2014) tarihinde http://mehmetsalihdeveci.net/2011/06/12/des-ile-veri-sifreleme-1/ 'den alındı

2.11.2. Açık Anahtarlı Şifreleme

Açık Anahtarlı Kriptografi, Asimetrik Anahtarlı Kriptografi olarak da adlandırılır. Açık Anahtarlı Kriptografi tek anahtar kullanan simetrik şifreleme algoritmalarının yerine iki ayrı anahtarın asimetrik kullanımını öngörür. Bu sistemde her bir kişi iki ayrı anahtar edinir. Bu anahtarlardan bir kamusal anahtar (public key), diğeri ise, özel anahtar (private key) olarak adlandırılır.

Açık anahtar kişinin şifreli iletişim kuracağı kişilere iletilir yani herkesin erişimine açıktır, gizli anahtar ise sadece sahibinin erişebileceği şekilde saklanmalıdır. Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır, fakat anahtarlardan birini kullanarak diğerini bulmak çok zor hatta imkânsızdır.



Şekil.9. Açık Anahtarlı Kriptografi

Kaynak: Seyir Defteri(Temmuz 2013)"*Şifreleme Yöntemleri"* içinden (Nisan2014)tarihinde,http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri 'den alındı.

Şifreleme deyince akla iki temel tehditin ortadan kaldırılması gelmektedir. Bunlardan bir tanesi ağ üzerinden gönderilen mesajın şifreli olarak gitmesi, bu şekilde mesajı sadece alıcı ve gönderenin görebilmesidir (şifreleme/deşifreleme).

Diğeri ise alıcının mesajı gönderen kişinin gönderdiğinden emin olması, yani alıcının mesajın yolda değiştirilmediğinden ve gönderen kişinin sahte olmadığından emin olmasıdır.Gizli Anahtarlı şifreleme yönteminde güvenli anahtar yönetimi sağlamada problem yaşanır. Bunda şifreleme ve deşifreleme için gizli anahtarı, iletişim kuracak kişiler ya birbirlerine güvenli olduğuna inandıklarına bir iletim kanalıyla alacaklar ya da bir anahtar dağıtım merkezinden faydalanmak zorunda kalacaklar.

Açık Anahtarlı şifreleme sisteminde bu gizli anahtarı tutma durumu ortadan kalkmıştır. Bütün iletişim sadece açık anahtarları gerektirir, gizli anahtarlar ne iletilir ne de paylaşılır, sadece şifrelenmiş veriyi çözme işinde kullanılır. Bu sistemde kaygı duyulucak tek nokta açık anahtarı kullanacak kişinin ve anahtar sahibinin doğru şekilde eşleştirilmesidir. Açık anahtarlı kriptografi sadece şifreleme ve deşifreleme işinde değil, kimlik denetimi (sayısal imza) ve daha birçok teknik için kullanılır.

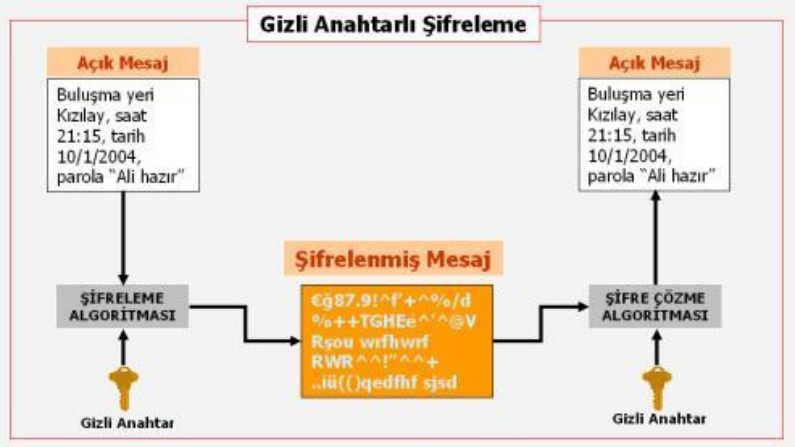
Yukarıda anlattığımız Simetrik şifrelemede oluşan anahtar yönetimi problemini çözmek amacıyla, Whitfield Diffie ve Martin Hellman, 1976 yılında Açık Anahtarlı Kriptografi yöntemini geliştirdiler. Bu yöntem ile şifre yazımda yeni bir dönem başlamış oldu. Böylece iletişimde %100 güvenliği yerine getiremeyen bir anahtar dağıtım merkezi gerekliliğini ortadan kaldırdı. Çünkü güvenli iletişim kurmak isteyen kişilerin kullanacakları gizli anahtarları bir anahtar dağıtım merkezinden almaları üçüncü bir kişinin iletişimi anlaşılır kılabileceği durumunu doğuruyordu. Bu da hiç istenmeyen bir durumdu. Diffie ve Hellman herhangi bir açık anahtarlı algoritmanın varlığını göstermeksizin bu sistemi varsaymışlardır.

Açık Anahtarlı kriptografinin dayanak noktası tek yönlü fonksiyondur. Bu fonksiyonda, fonksiyonun bire bir olduğu bir aralıkta, tersini hesaplamak imkansız kabul edilirken, fonksiyonun kendisinin hesaplanması kolaydır.

2.11.3. Gizli Anahtarlı Şifreleme

Gizli anahtarlı kriptografi, simetrik kriptografi ya da tek anahtarlı kriptografi olarak da adlandırılır. Tek bir anahtarın hem şifreleme hem de şifre çözme amacıyla kullanıldığı daha geleneksel bir yöntemdir. Simetrik anahtarlamada genel olarak basit şifreleme algoritmaları kullanılmaktadır.

Bu tip anahtarlamada, aynı anahtar hem gönderen kişide, hem de alan kişide bulunmalıdır. Bu şekilde şifrelenmiş veri ağdan geçerken bir başkası tarafından elde edilip okunmak istendiğinde, kişi anahtara sahip değilse anlaşılamaz.



Şekil.10. Gizli Anahtarlı Şifreleme

Kaynak: Seyir Defteri(Temmuz 2013)"*Şifreleme Yöntemleri"* içinden (Nisan2014)tarihinde,http://bidb.itu.edu.tr/seyirdefteri/blog/2013/09/07/%C5%9Fifreleme-y%C3%B6ntemleri 'den alındı.

Gizli anahtarlı kriptografi sadece şifreleme değil, kimlik denetimiyle de ilgilenir. Kimlik denetiminde kullanılan yöntemlerden biri Medya Erişim Kontrolüdür (MAC). Medya Erişim Kontrolü, sayısal imza ile benzer amaçlarla kullanılır. Ancak burada kimlik denetimi için çift anahtarlı kriptografi yerine tek anahtarlı kriptografi, yani sadece üzerinde anlaşılan ortak anahtar kullanılır. Yani

bu şekilde kimlik denetimini sadece istenilen kullanıcı yapabilir; sayısal imzada olduğu gibi gönderenin açık anahtarına sahip herhangi birinin imzayı doğrulayabilmesi gibi bir durum söz konusu değildir.

Gizli anahtarlı kriptografide temel problem, göndericinin ve alıcının, üçüncü bir kişinin eline geçmesini engelleyerek ortak bir anahtar üzerinde anlaşmalarıdır. Bu iki tarafın dinlenme korkusu duymadan iletişim kurmasını sağlayacak bir yöntem gerektirir. Gizli Anahtarlı şifrelemede amaç şifrelemede kullanılan iki kullanıcınında anlaştığı anahtarın istenmeyen kişilerin eline geçmesini engellemektir. Anahtarların üretilmesi, iletilmesi ve saklanması anahtar yönetimi olarak bilinir. Güvenli anahtarlı yapılarda, genelde güvenli anahtar yönetimi sağlamada problem yaşanır.

2.11.4. Şifreleme Teknikleri

Tek Yönlü Şifreleme (MD5 - Message-Digest Algorithm5)

Veri bütünlüğü veya özet fonksiyon olarak da bilinir. Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Bir yere gönderilecek veri 128 bitlik özetler hâlinde şifrelenir. Veri bütünlüğünü sağlamak için kullanılır.

Özetleme Algoritması (SHA-1 - Secure Hash Algorithm)

Özetleme algoritmasıdır. Tek yönlü (açık anahtarlı) şifreleme tekniğidir. Veri bütünlüğünü sağlamak için kullanılır. Verileri 160 bit uzunluğunda özetler. SanalDoku (Web) alanında geniş kullanımı vardır.

SHA-2 adı altında hazırlanmış 224,256,384,512 bit uzunluğunda özetler üreten çeşitleri vardır.

NOT: MD5, SHA-1, SHA-2 (SHA-256,-384,-512) gibi algoritmalar "Özetleme(Hash)" Algoritmaları olarak sınıflandırılır.

Simetrik Şifreleme Algoritması (DES-Data Encryption Standard)

Simetrik şifreleme tekniğidir. 56 bit uzunluğunda anahtar kullanır. Blok şifreleme algoritmasını kullanır. (Bitler önce bloklanır sonra şifrelenir.) Hem şifrelemek için hem de şifre çözmek için aynı anahtar veri kullanılır.

Örnek olarak tek kilidi olan bir sandık düşünülebilir.

Birbirinin kopyası iki anahtarı olsun. Anahtarlardan biri kaynakta diğeri ise hedeftedir. Kaynakta anahtarla kilitlenen sandık, hedefe gittiğinde yine aynı anahtarla açılacaktır.

Üçlü Simetrik Şifreleme Algoritması (3DES-Trible DES)

DES'teki açıkları kapatabilmek için DES'te kullanılan algoritmanın üç kez uygulanmasıyla anahtar uzunluğunu artıran yöntemdir.Anahtar uzunluğu 112 bite çıkarılmıştır. (Anahtar uzunluğu ne kadar artarsa güvenlik de o kadar artar.)

Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard)

Günümüzde en yaygın olarak kullanılan şifreleme yöntemlerinden birisidir. Bu da blok şifreleme algoritmasını kullanılır. Veriler 4×4'lük diziler (matris) hâlinde bloklandıktan sonra uzunluğu en az 128 bit olan anahtarlar kullanılarak şifreleme gerçekleştirilir.

Simetrik Anahtar Şifreleme Tekniği (RC-4 - Ron's Code)

Simetrik şifreleme tekniğidir. Ama Simetrik Şifreleme Algoritması (DES) ve Gelişmiş Şifreleme Standardından (AES) farklı olarak dizi şifreleme algoritmasını kullanır. (Veriler bit bit şifrelenir. Aynı karakterin karşılığı her seferinde farklı olur.) Kabloya Eşdeğer Gizlilik (WEP) ve Güvenli Giriş Katmanı (SSL) gibi güvenlikli bağlantı standartlarında yaygın olarak kullanılmaktadır.

3. ORGANİZASYONLAR İÇİN GENEL GÜVENLİK MİMARİSİ

Bu kısımda taşınabilir cihazları ve bilişim güvenliği hakkında teorik bilgiler sunulacaktır. İş yaşamında verimlilik ve yeterlilik gelişimi sağlayacak, taşınabilir cihazlar ve organizasyonlardaki bilgi güvenliğinin önemi vurgulanmaktadır. Organizasyonel bilişim güvenliğinin gerekliliğini, çalışanların verimliliğini arttırmak ve iş yükünü azaltmak amacıyla, yönetimin kullanılmasını gerekli gördüğü güvenlik araçlarına değinilecektir.

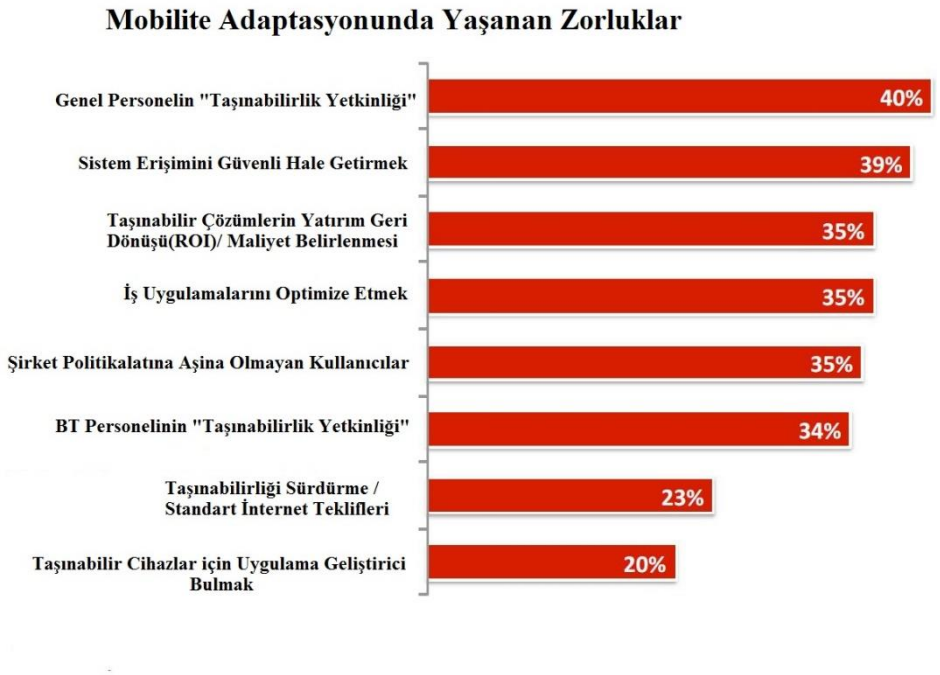
Bazı tehditler ve riskler çalışma aracı olarak kullanılan taşınabilir cihazlarınızla ilişkili güvenlik açıkları üzerine değinilecektir.

3.1. Organizasyonel Bilişim Güvenliği

Akıllı cihazların BT altyapısında tamamlayıcı bir unsur olarak kullanılmasının uygun olduğunu ortaya koyan birçok araştırma yapılmıştır. Kullanımına bağlı olarak, güvenlik riskini arttırmayarak hangi cihazlar iş ortamında kullanılabilir, birçok araştırmacı tarafından araştırılmaktadır (Basole, 2008; Beurer-Zuellig & Meckel, 2008; Allam, 2009; Ahmed et al., 2009; Botha et al., 2009; Büscher & Urry 2009; Ernst & Young, 2011; Fitzgerald, 2009; Cisco, 2013 ve PricewaterhouseCoopers 2013).

Araştırmacıların, akıllı cihazların iş ortamında sosyo- teknik teorilere göre kullanımını analiz etme çalışmalarına karşın (Kisling, 2006; Chen & Nath, 2008) Mobilite teorisi altında sosyo-teknik teorilerle ilgili olarak çok fazla ilerleme mevcut değildir. Son yıllarda mobil çalışma konseptine ilişkin araştırmalara ilgi oldukça artmıştır. Ancak, mobil çalışanlar için kurumsal destek ile ilgili önemli konuları içeren bir kapsamlı bir çerçeve oluşturulurken ele alınması gereken temel sorunlar mevcuttur.

Etkili bir mobil çalışma ortamı yaratarak mobil çalışanlar için, sadece organizasyonların içinde ve dışındaki teknik sorunları değil aynı zamanda bir numaralı engel olan güvenlik gibi sosyal ve kültürel olguları da dikkate alınmalıdır. Bu tür taşınabilir veri çözümlerinin maliyeti ve karmaşıklığı diğer sorunlardan daha önemlidir (Ernest-Jones, 2006).



Şekil.11. Mobilite Adaptasyonundaki Zorluklar

Kaynak: Gagnon D.(Nisan 2013) "*Report: Enterprise mobility boom brings new challenges, jobs for IT pros in 2013"* içinden (Mayıs 2014) tarihinde http://blog.pluralsight.com/enterprise-mobility-trends 'den alındı

Bilişim teknolojisi denilince, organizasyonlar tüm dünyadaki iş anlaşmaları, toplantılar, randevu düzenleme, müşteri hesap takibi, şirket envanter takibi gibi işlemleri tek bir lokasyon üzerinden yapabilmektedirler (Whitman & Mattord, 2004). Teknoloji aracılığı ile küresel market ve ticari operasyonlar mümkündür.

Organizasyonlar bilişim teknolojilerinin yardımı ile farklı lokasyonlardaki, müşterilerinin talepleri karşılamak için çalışmaktadırlar.

Bir organizasyonun piyasada kalabilmesi ve rekabetçi yapıya sahip olması sadece organizasyona bağlı değil, teknolojiyi kullanımına da bağlıdır. Bu durum, müşteriler, son kullanıcılar yada çalışanlar arasında; organizasyon içerisinde ve dışarısında güvenli bilgi transferi gerçekleştirebilmek anlamına gelmektedir.

Transfer edilen bilginin bilgisayar'dan bilgisayar'a aktarımında yada taşınabilir cihazlar aracılığıyla transferinde de güvenliği sağlanmalıdır. Çalışan ve işverenlerin önerdiği, taşınabilir cihazlar üzerindeki fonksiyonların bir çoğunun kullanımı organizasyonlar için bilgi güvenliği riski taşımaktadır (Furnell et al., 2006; Takesue, 2007; Botha et al., 2009; Allam, 2011).

Organizasyonların var olması bilgilerinin sürekli ve düzenli olarak korunabilmesi ile doğru orantılıdır.

3.2. Bilgi Kaynaklarının Güvenliği

Bilgi kaynakları ister soyut ister somut olsun, organizasyonların sahip olduğu bilgiler en önemli bilgileridir. Musaji (2006), bilgi kaynaklarının sadece iç sistem içerisindeki şirket aktivitelerini destekleyici; bilgi, metin, resim yada ses kayıtları ile kısıtlı olmadığını belirtmektedir.

Bilgi kaynakları organizasyonlar için önemli olsa da organizasyon'a değeri her zaman sayısal değildir ve organizasyon bilançosunda görünmüyor olabilir (Moody ve Walsh, 1999, Allam, 2009). Bilgi, ihmal edilmesi nedeniyle güvenliği en çok atlanılan kaynaktır. Organizasyonun rekabet gücünün arttırılması için anahtar oyuncu olan bilgi değeri vurgulanmadan olmaz. Bilgi güvenliği stratejilerinin etkili bir şekilde yapılandırılması bugünün organizasyonları için yıldırıcı bir task olmaktadır (Ernst &

Young, 2011; Fratto, 2009; TechAmerica, 2012; PricewaterhouseCoopers, 2012; Allam, 2009).

Bu durum aslında transit, beklemedeki ve kullanımda olan verileri ve verilerin depolanması ve hareketini kolaylaştıracak diğer ekipmanları öncelikli olarak etkilemektedir (Allam, 2009; Whitman & Mattord, 2011). Ek olarak, optimum güvenlik kurallarının sürekli değiştiği gerçeği kabul edilebilir.

Hem siber suçlular hem de organizasyonlar teknolojik becerilerini teknolojiyle birlikte arttırmaktadır, dolayısıyla bu durum riskleri en üst seviyeye taşımaktadır ve karşınızdakinin ne derece bilgi sahibi olduğunu yada sizin ne kadar geride/ilerde olduğunuzu anlamanın bir yolu kalmamıştır (PricewaterhouseCoopers, 2012; Fratto, 2009).

Şekil.12. K.C.G. (2013)

Kaynak: SEEBURGER.COM.(Ekim 2013) "*BYOD Is Not Going Away—in fact, it's going to explode"* içinden (Mayıs 2014) tarihinde http://blog.seeburger.com/index.php/byod-is-not-going-away-in-fact-its-going-to-explode/#.U6QGo_l_tOs 'den alındı

Organizasyonlar teknik çözümler için çoğunlukla devasa ücretler ve uzun zaman harcamaktadırlar ve nedense bilgi güvenliğindeki insan faktorünü tamamen ya da kısmen ihmal etmektedirler (Kruger and Kearny, 2008; Dhillon&Backhouse, 2000). Hangi teknik çözüm uygulanırsa uygulansın, bu uygulama insanlar tarafından yapılacağı çoğunlukla organizasyonlar tarafından unutulmaktadır ve bu nedenle insan yaklaşımı gibi unsurlar da her zaman hesaplanarak değerlendirme yapılmalıdır.
Etkili bir teknik sistem kurabilmek için, sosyal sistem de etkili olmalıdır (Kisling, 2006, s. 76).

Teknolojik uygulamaların çalışıp çalışmadığını çalışanlar belirleyecektir. Ne kadar iyi bir teknik kontrol mekanizmanız olursa olsun, eğer çalışanlar bu güvenlik kuralları ile çalışmayı reddederse veya güvenliği ihlal etmek çalışmalarını kolaylaştırırsa, bilgi güvenliği kuralları başarısız olacaktır.

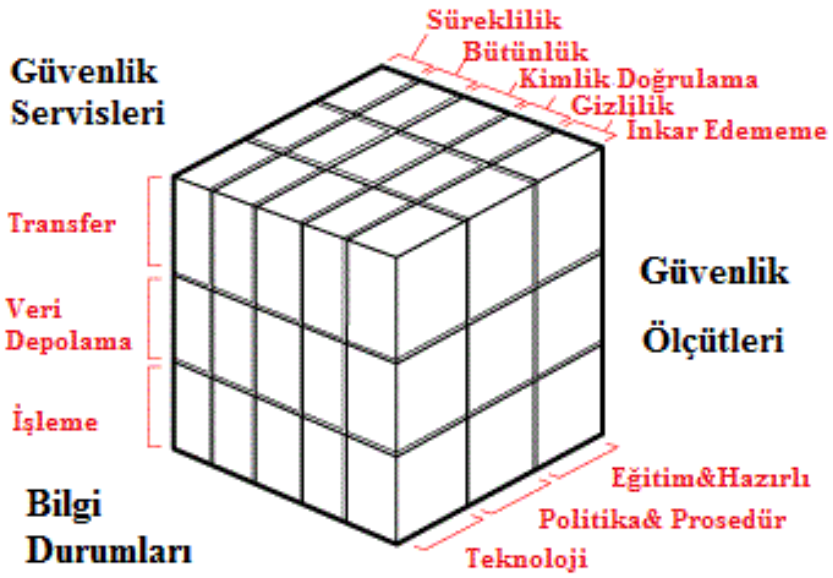
Bilgi güvenliği konularına insanlar ve insan aktivitelerini içeren konuları dahil etmek, güvenlik sorunlarına karşı direnci azaltmak için herhangi bir teknolojinin yapılandırılması kadar önemlidir (Kruger and Kearny, 2008). Hangi bilgisayar sistemlerine erişildiğini ve erişim kayıtlarını tutabilmek ve güvenliği sağlayabilmek adına bilgi güvenliği için teknik kontroller önemlidir (Dhillon & Backhouse, 2000). Bilgi güvenliği uygulamalarına insanlar dahil edilecekse, bilgi güvenliği sadece teknik bir problem değil, organizasyonel ve sosyal teorinin doğru bir karışımı ve yönetim bilimleri ile minimize edilebilecek bir sosyal ve organizasyonel bir problem olacaktır (Dhillon & Backhouse, 2000).

Bilgilerin korunması sadece yönetim ve teknik departmandaki birkaç çalışanın sorumluluğunda değildir. En üstten başlayarak tüm çalışanların ortak sorumluluğundadır. Çalışanların doğru davranışları ile bilgi kaynakları, prosedürler, standartlar ve politikalar da dahil tüm kaynakların güvenliği, doğru eğitim ve pratik ile aynı anda güvenlik sağlanırken, bilginin değeri de ortaya çıkarılabilir. Bu bilgileri güvenceye alınabilmesi, gizliliğinin ve sürekliliğinin sağlanabilmesi, bütünlüğünün korunabilmesi için bilgi güvenliği birinci derecede öneme sahiptir.

3.3. Bilgi Güvenliğinin Önemi ve Bilgi Emniyeti

Güvenlik, tehlikelerden koruyarak özgürlük güvencesi vererek, emniyetli olma durumu veya kaliteden emin olacak tüm aktiviteleri kapsamaktadır.
Dünyadaki en büyük finansal işlemlerini gerçekleştiren firmalardan Inovant'ın Bilgi Güvenliği Vekil Başkanı James Anderson'a göre bugünün kuruluşlarında;
"Çok bilgili, emniyet duygusu, bilginin riskleri ve kontrolü dengede ise mevcuttur."

Bu sebepten dolayı bilgi güvenliği, teknolojik uygulamalar, eğitim, politika ve prosedürlerin vasıtasıyla, kritik unsurlar ve tüm bilgi depolaması ve transferi için kullanılan sistemlerin ve donanımların bilgilerinin korunmasıyla ilgilenmektedir (Whitman & Mattord, 2004; Maconachy, 2001).



Şekil.13. Yüksek Seviye İletişim Modeli

Kaynak: Loeb L.(Ağustos 2001) *"Secure Electronic Transaction"* içinden (Mayıs 2014) tarihinde http://www.ibm.com/developerworks/security/library/s-confnotes2/ 'den alındı.

Şekil 13'de de gösterildiği gibi, kapsamlı McCumber modeli üç boyutlu bilgi güvencesi modelidir. X-apsisi, verinin işlenmesi yada iletilmesi sırasında, depolama birimindeki veriyi göstermektedir. Y-apsisi, Organizasyonlar tarafından sağlanan;

gizlilik, bütünlük, süreklilik, kimlik denetimi ve inkar edememe gibi güvenlik servislerini temsil etmektedir. Z-apsisi ise, eğitim ve hazırlık, teknoloji, prosedür ve politikalar gibi yukarıda belirtilmiş, sayılabilen ölçütler kategorisini göstermektedir.
Bu modele göre veri depolama, işleme ve transfer olarak 3 aşamada olabilir. Modele göre, bilgi emniyetinin tamamen arşivlenmesi için gizlilik, bütünlük, süreklilik, kimlik denetimi ve inkar edememe (non- repudiation) de tamamen arşivlenmelidir.
Bilgi emniyetinde faydayı maksimize edebilmek için, eğitim ve hazırlık, teknoloji, prosedür ve politikaları kullanır.

Bilgi güvenliği, Organizasyonda toplanan ve kullanılan bilgilerin korunması, kullanılan teknolojik varlıklarının güvence altına alınması, organizasyonların yükümlülüklerini yerine getirilebilmesi için ve son olarak da BT sistemi içerisinde kullanılan uygulamalarla güvenli operasyon yapılabilmesi için önemlidir (Whitman & Mattord, 2011). Bilgi güvenliği, aynı zamanda bir kuruluşun verilerinin mülkiyet hırsızlığına ve kötüye kullanımına yönelik korunmasını sağlanmasında önemlidir. Organizasyonun bilgilerinin çalınması veya kaybolması halinde alınabilecek büyük para cezası organizasyonu iflasa sürükleyebilir. Ayrıca bu durum, organizasyonun bütünlüğünü ve itibarını zedeleyerek, müşterilerinin onlarla iş birliği yapmaktan çekinmesine sebep olarak, organizasyonun çöküşünü hızlandırabilir(Allam, 2009).
Bilgi güvenliği, teknolojik gelişim ile birlikte hızlı ve karışık bir şekilde gelişmeye müsait bilgi teknolojisindeki cihazlardaki tehlikelere ve saldırılara karşı gereklidir(Standards South Africa, 2005). Bu saldırılar içeriden yada dışarıdan gelebileceği gibi, içeriden gelen saldırıların yönlendirmesiyle(TechAmerica, 2012) kazara yada kasten de gerçekleşebilir (Kritzinger and Smith,2008; Whitman & Mattord, 2011).

İnsan hataları çoğunlukla güvenlik ihlaline yol açar. Ocak 2005 ile Haziran 2008 tarihleri arasında Liginlal, Sim & Khansa (2009)'nın raporlamalarına göre, "insan hatası" içeriden kaynaklanan saldırıların büyük bir yüzdesini oluşturmaktadır.

Allam (2009), sadece çalışanlardan oluşan geleneksel yöntemlerle ve bireysel güven ile işlerini yürütmek durumunda olan, çalışanların işverenin ve işyerinin lehine

çalıştığı varsayılan küçük organizasyonlarda, insan hatasının tehditlerin büyük çoğunluğuna neden olduğunu öne sürmektedir.

Bazı işverenlerin sadece ve yoğunlukla dışarıdan gelecek bilgi güvenliği saldırılarına yoğunlaştıklarını, çünkü kendi çalışanlarının şirketlerinin lehinde ve en iyi tutumlar içerisinde çalışacağını düşünmekte olduklarını belirtmektedir. Bu durum organizasyonları, insan kaynaklı hatalar ve çalışan suistimalleri sebebiyle, içeriden gelebilecek tehditlere karşı şanşlarıyla baş başa bırakmaktadır (Daniel, 2008). Ayrıca, iyi davranışların iyi sonuçlar doğuracağı konusunda yaygın bir görüş mevcut olduğuna dikkat çekerek, organizasyonların iyi tutumlu politikalarının, fazla güven duygusu ve zamana dayalı olarak kırılacağını gözardı ederek, kendi bilgi güvenlik aktivitelerinin etkili olduğunu düşünmekte oldularını belirtmiştir (Cisco,2013).

Nereden ve hangi nesne aracılığıyla tehdit veya atak geleceğini kimse bilemeyeceği için, iç ve dış tehditlerin, ikisininde birlikte çalışan politikalar, prosedürler, yazılımlar ve cihazlar aracılığıyla güvenli ve adapte olmuş bir sistem oluşturmak amacıyla adreslenerek güvenlik maksimum seviyede sağlanmaya çalışılmalıdır. 1786'daThomas Reid'in "İnsanoğlu'nun entellektüel gücü makalesi"nde belirtmiş olduğu gibi;

"Muhakeme zincirindeki tüm zincirler, son kararın delili zincirdeki en zayıf halkadan daha büyük olamayacaktır, çünkü zincirdeki diğer halkaları güçlendirecektir".

Bu durum bilgi güvenliği sahasında da geçerlidir; bir zincir sadece en zayıf halkası kadar güçlüdür. Eğer organizasyonlar iç tehditleri gözardı ederek, dış güvenlikleri ne kadar kuvvetli olursa olsun sadece dış tehditlere odaklanırlar ise; iç tehditlerin tüm sisteme odaklanması sonucu tüm sistem zayıftır. Bu durum akıllı telefonlar gibi taşınabilir cihazların güvenliklerinin, bir organizasyonun güvenliğinin sağlanması ve organizasyonel güvenlik açısından ne derece hayati önem taşıdığını ortaya koymaktadır.

3.4. Bilgi Güvenliğinin Temel Özellikleri

Bilgi güvenliği üç temel başlık altında toplanabilir. Bunlar; bilgi ve bilgi kaynaklarının gizliliği, sürekliliği ve bütünlüğünün sağlanmasıdır (Whitman & Mattord, 2004). Şekil.14'te CIA üçlemesi olarak da örneklenen bu üç bileşen en uygun seviyede bilgi güvenliğinin elde edilmesinde yardımcı olmaktadır.

Şekil.14. CIA Üçlemesi

Kaynak: Education Online (2013) "*ICT Security"* içinden (Mayıs 2014) tarihinde http://www.educationline.nl/pagina/security/deel1/les2.html 'den alındı.

Bilgisayarlardaki geleneksel bilgisayar ağlarının aksine, taşınabilir cihazlarda kullanıcılara, dahili ve harici ağlar aracılığıyla bilgi kaynaklarına erişim vermektedir. Ne yazık ki akıllı cihazların güvenliği henüz emekleme döneminde olduğu için dikkatle kullanılmalıdır, aksi takdirde bu durum güvenlik ile ilgili bir çok probleme yol açabilir (Allam, 2009; Couture, 2010).

Gizlilik, öncelikle sadece yetkili ve yetkisi doğrulanmış kişilerin bilgilerine erişimi kısıtlamaktadır (Whitman & Mattord, 2011). Yetkili kişiler, bu sistemlerin içinde yer alan bilgilere erişme izni olan, kuruluşların bilgi sistemlerine erişim için izin vermiş olduğu kimliği doğrulanmış kişilerdir.

Cihazların güvenliği taşınabilirlik ve her yerde olan ağlara bağlanabilme özelliğinden dolayı gizlilik, son zamanlarda sorun haline gelmeye başlamıştır. Organizasyonel kaynaklara erişim sağlayan cihazlarla, hem güvenli hem de güvensiz ağlara bağlanılabilmektedir. Allam' a göre (2009), akıllı cihaz kullanıcısının kimliğini

onaylayan ve bağımsız bir servis sağlayıcıdan ağa bağlanabilen kullanıcılar derinlemesine bir güvenlik yaklaşımı gerektirdiğini göstermektedir. Bilgi kaynaklarının düzgün bir biçimde güvenliğinin sağlanabilmesi için, gizlilik ölçütleri tüm depolama cihazlarına uygulanmalı, yetkisiz ve kimliği doğrulanmamış kişilerin bu bilgilere erişimi engellenmelidir.
Eğer bu uygulanmazsa, bilgi ve bilgi kayaklarının bütünlüğü risk altına girecektir.

Fratto (2009, s. 18) bunlara ek olarak gizli bilgilerin kaybının, özellikle "Gizli Bilgi" terimi başlığı altında ve geniş bir alanı kapsayan entelektüel fikir içeriyorsa, kuruluşları yıkıma sürükleyebileceğini belirtmektedir.
Diğer bir taraftan bilginin temellerinden Bütünlük; eksiksiz ve bozulmamış bilgi sağlamak suretiyle, bilginin kesin, orjinal ve güvenilir olduğunu araştırmaktadır (Whitman & Mattord, 2011). Bilgilerin modifiyesi Bilgi Teknolojisi sayesinde kolaylaşmıştır. Bilginin istenmeyen modifikasyonu, bilgi bütünlüğünü kaybettirerek bilgi güvenirliğini yok etmektedir. Bu nedenle, istenmeyen bilgi modifikasyonun engellenmesi, bilgi bütünlüğünün büyük ölçüde korunmasına yardımcı olmaktadır.

Rekabetçi avantaj sağlanabilmesi için, bilgi desteklenen iş içeriğine en uygun formatta saklanmalıdır. Gizlilik aracılığıyla bütünlüğü sağlamak kolay değildir ama bütünlük, gizliliğin yardımıyla elde edilebilir. Akıllı cihazlar çoğunlukla güvenilmeyen ağ kanalları aracılığıyla iletişim sağlarlar. Organizasyonların bu kanallar üzerinde, gönderilen ve alınan verilerin bütünlüğünü sağlamak için, kontrolleri mevcut değildir (Allam, 2009). Bilginin sürekliliği, gerekli olduğunda bilgiye ulaşabilme durumudur (Whitman& Mattord, 2004). Süreklilik eğer layıkıyla adreslenebilirse, işverenlere rekabetçi avantaj sağlayabilir. Akıllı cihazların iş ortamında kullanımı esnasında, örgütler güvenilmez ağlardan olabildiğince çok faydalanmaları gerekmektedir. Yeteri kadar güvenliği olan organizasyonun bilgi stratejileri azaltılarak, güvenilmez ağ erişimi gibi iletişim kanallarına bağlantıların azaltılması ya da yasaklanması üretkenliğin ve akıllı cihazların kullanımının azalmasına neden olacaktır (Allam, 2009). Uygun seviyede gizlilik, bütünlük ve süreklilik bilgi güvenliği geliştirilirken üretkenliği maksimize etmeye yönlendirecektir.

3.5. Bilgi Güvenliği Kültürünün Oluşturulması

Bilgi Güvenliği kültürü insanların bilgi almak ve bunların güvenliği için hangi şekilde davranılması gerektiğinin belirlenmesiyle ortaya çıkar (Ghonaimy, El-Hadidi & Aslan, 2002). Ayrıca teknik güvenlik ölçütlerini destekleyerek, sosyo-kültürel ölçütleri kapsamaktadır. Bu sayede bilgi güvenliği tüm çalışanlar için günlük aktiviteler arasına katılarak doğal bir hal alacaktır (Schlienger & Teufel, 2003).
Bilgi güvenliği yapılandırılırken, kuruluşların organizasyonel kültürü göz önünde bulundurulmalıdır (Connolly, 2000). Chia, Maynard ve Ruighaver'e (2003) göre, bilgi güvenlik sistemi; yönetici tarafından belirleneni yöneticinin inanışları ve aksiyonları doğrultusunda tanımlanan bir sistemdir.

İş, bilgi kaynaklarının varoluşuna bağıdır. Teknik bilgi güvenliği çözümü ne kadar başarılı olsa da, bunlar bilgi kaynaklarını güvence altına almak için yeterli değildir. Dhillon'a (2001) göre, bilgi güvenliğinin kontrolünün etkisi, implementasyonu gerçekleştiren ve kullanan kişilerin yetkinliklerine ve güvenilirliklerine bağlıdır. Bu nedenle, bilgi güvenliğinin etkinliğinin sağlanabilmesi için, çalışan farkındalığı en önemli faktörlerden biri olarak kabul edilmektedir (Olzak, 2006).

Organizasyonlar, çalışanları işe başladığı andan itibaren çalışma süresi sonuna kadar, doğrudan ve dolaylı olarak güvenlik bilinçlendirme çalışmalarına dahil etmelidirler (Whitman & Mattord, 2011; Allam, 2009).
Organizasyonun dış tehditlerden korumak için teknik çözümlerin kullanılarak güvenliğinin sağlanması, iyi yapılandırılmamış güvenlik duvarlarının ve ağ geçitlerinin uygulanması ve tüm bilgi güvenliği yaklaşımı, sistemin nasıl kullanılacağı bilinmiyorsa, organizasyonu iç ve dış tehditlere karşı savunmasız kılacaktır. Bu eninde sonunda çalışanların güvenlik kelimesini çalışmada gözardı ederek rastgele yollarla güvenlik uygulamaları gerçekleştirmelerine ve bu kültürün yerleşmesine neden olacaktır.

Organizasyonların organizasyonel güvenliklerini elde etmek için kullandığı politikalar, prosedürler ve standartlar, organizasyonel kültür olarak değerlendirilmelidir ve mevcut güvenlik prosedüründe yapılan değişiklik ve geliştirmeler işverenler tarafından çalışanlara benimsetilmelidir.

3.5.1. Bilgi Güvenliği Farkındalık Kültürü

"*Organizasyonun çalışma ortamında nasıl davranılabileceği, hangi zaman ve hangi işlerle, hangi insanlar ve hangi yolla bilgi kaynaklarıyla etkileşime geçebileceği belirlenmiştir*" Martins ve Eloff (2001; s. 1).

Çalışanların tutum çerçevesi, yöneticilerin ve nüfuzlu kişilerin birlikte rehberliğiyle, işlem ve prosedürler organizasyonel seviyede tanımlanmıştır (Martins & Eloff, 2001). Bu durum zamanla organizasyonun kültürü haline gelecektir. Birşeylerin nasıl yapılacağını bilmeyen insanlar nadiren bu şeyleri doğru yaparlar (PricewaterhouseCoopers, 2012, s. 23). Yeterli eğitim alınmadan güvenlik programları etkili olamaz (Whitman & Mattord, 2011;PricewaterhouseCoopers, 2012). Bilinçlendirme ve eğitim aracılığıyla bilgi güvenliği kültürü oluşturmak için donanımlı bireylere ihtiyaç vardır.

Güvenlik sistemlerinin kalbinde kullanıcılar yer almaktadır. Özellikle bilgisayar güvenliğinde, birçok teknolojik denetim, kullanıcı tarafından devre dışı bırakılabilmektedir. Örneğin, bir bilgisayar sistemine bağlanıldığında, kullanıcıdan kendisine ait, başkası tarafından bilinmeyen gizli şifreyi girmesi beklenmektedir. Böylece sistem, o kullanıcının adıyla bir başkasının sisteme girmesine izin vermemekte, kimlik doğrulaması gerçekleştirilmektedir. Eğer kullanıcı, şifresini başka birine söylerse, gerçekte erişim yetkisi olmayan başka bir kullanıcı sisteme bağlanabilecektir. Sistemin bu kullanıcıyı saldırgan olarak algılaması mümkün olmayacaktır.

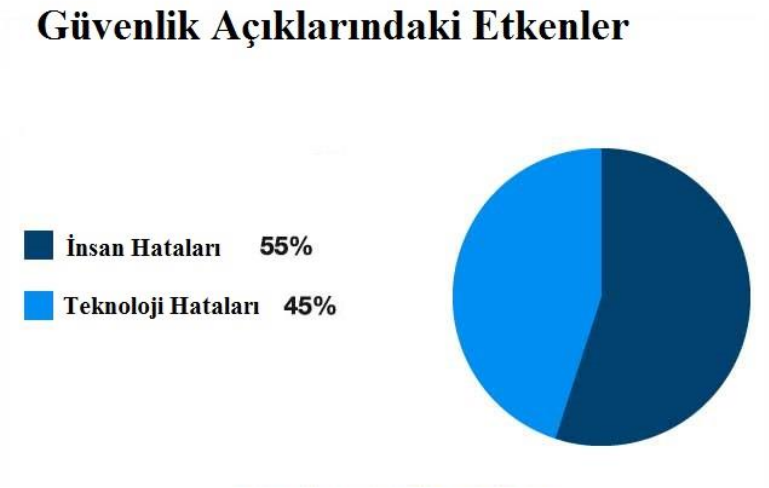
Bir kurumun sistemine saldırmak isteyen ve sisteme girme yetkisi olmayan kişiler sistem için ciddi bir tehdit oluşturmaktadırlar. Ancak, kurumun sistemine girme yetkisi olan, kurumun kendi çalışanları daha ciddi bir tehdit unsuru olmaktadırlar. Çünkü bu çalışanlar, sistemin çalışma prensiplerini bilen, sistemin belirli noktalarına erişim izni/hakkı olan, sistemin güvenlik kontrol noktalarını bilen kişilerdir. Bu kullanıcılar, bu kritik bilgileri kullanarak, sistemin birçok güvenlik kontrol noktasını atlatarak sisteme zarar verebilmektedirler.

Yeterince eğitim almamış bilinçsiz personel, sistem güvenliğini tehdit eden önemli bir diğer unsurdur. Örneğin, yedekleme sisteminde, bilgilerin yedeğini teyp ünitelerine alırken, yedeğin doğrulamasını yapmayan sistem kullanıcısı, herhangi bir saldırganın sistemdeki kritik dosyaları silmesi sonucu, yedek ünitelerinden ilgili dosyaların geri alınmasını sağlayamayabileceği için sistem zarar görmüş olacaktır.

Güvenlik mekanizmalarının sonuçlarını doğru değerlendiremeyen sistem yöneticileri, sisteme bir saldırının yapıldığını fark edemeyebilirler. Bunun yanı sıra, güvenlik ayarlarında hata yapmaları durumunda, sistemin güvenliğini zayıflatmış olacaklardır. Ayrıca, kullanıcılar da güvenlik mekanizmalarını doğru bir şekilde kullanmadıklarında, yine güvenliği zayıflatmış olacaklardır. Tahmin edilebilen basit kullanıcı şifreleri buna örnek olarak gösterilebilmektedir.

Çoğunlukla organizasyonları yıkabilecek güvenlik ihlalleri, güvenilen iç çalışanlar tarafından yapılmaktadır (Dhillon, 2001). Ruighaver (2007), çalışanların sistem güvenliği pratiği edinmek için doğal olarak motivasyon elde ettiklerine dair bir kanıt olmadığını belirtmektedir.

Sistem operatörlerinin, şifresini unutan kullanıcıların şifrelerini değiştirme isteklerini telefon çağrıları ile yapmaları başka bir güvenlik açığına sebep olacaktır. Böyle bir yöntem izlendiğinde, saldırganın tek yapması gereken, sistem operatörünü arayarak, sistemdeki bir kullanıcının adını vermesidir. Bu durumda operatör, ilgili kullanıcının şifresini telefonda saldırgana vermiş olacak, böylece saldırgan da normal sistem kullanıcısı olarak sisteme bağlanabilecek ve saldırısını gerçekleştirebilecektir.



Şekil.15. Güvenlik Açıklarındaki Etkenler

Kaynak: Vizard M. (2013) "*Channel Could Help Spur Security Adoption in 2014"* içinden(Mayıs2014)tarihinde,http://www.channelinsider.com/security/slideshows/channel-could-help-spur-security-adoption-in-2014.html'den alındı.

Sağlıklı bir organizasyonel kültürde, deneyimli yönetim tarafından herhangi bir verimlilik seviyesini gerektiren teşvikler desteklenecektir (Allam, 2009). Eğer çalışanlar akıllı cihazların kullanımının yaratacağı riskleri ve riskleri minimize ederek bu cihazları nasıl kullanılacağını bilirlerse, verimlilik seviyesi açıkça artış gösterecektir.

3.6. Bilgi İşgücü

Organizasyonun sahip olduğu tüm bilgiler her zaman açık değildir. Bazı bilgiler gizlidir ve çalışanların zihinlerindedir. Allam (2009; 50) 'ın dediğine göre;

"*İnsanlar organizasyonlar içerisinde bulunan bilgilerin en uç kaynağı ve bu bilgilerin hedefidir."*

Bilginin maksimum fayda kazanımı sağlayabilmesi için, insan olmadan tek başına kullanılmasıyla, hemen hemen hiç birşey tek başına çalışamaz. Bu nedenle organizasyonlar modern işgücünün bilgi ile tamamlanması gerektiğini kabul etmelidirler. Bilgi güvenliği organizasyonların bilgilerinin gizliliğin, bütünlüğün ve sürekliliğin uygulatılabilmesi ile çalışanları iş ortamında ekstra stres ve prosedüre maruz bırakmadan, günlük vazifelerini gerçekleştirmeleri esnasında sağlanmalıdır. Bilginin korunması ve erişim yetkilerinin uygulanması arasında bir denge olmalıdır (Post & Kagan, 2007). Bilgiye erişim kısıtlaması, dikkatle değerlendirilerek yapılmalıdır (Whitman & Mattord, 2011). Sistemleri ulaşılamaz hale getiren sıkılaştırılmış güvenlik, çalışanların cesaretlerini kırarak, zamanla daha az verimliliğe sebebiyet verecektir. Dolayısıyla herhangi bilgi güvenlik çözümünün başarısı için bu dengenin sağlanması hayati önem taşımaktadır.

Mahoney (2009), yeni teknolojilerle uyum artarken, iş süreçlerini daha etkin, esnek ve mobil yapmak için bir yol olarak teknolojiyi gören işçilerin çoğalması ile yeni teknolojilere adaptasyonun hızla arttığını belirtmektedir. Günümüzün dünyasında bu durum, akıllı cihazların hayatlarımızdaki günlük aktivitelere dahil olmasıyla örneklenebilir. Mobil çalışanlar genellikle teknolojik cihazlara bağımlıdır ve sürekli, güvenli yada güvensiz servis sağlayan ağlara bağlanmak mecburiyetindedir. Bu esneklik bilgilere, organizasyonları tarafından yönetilmeyen farklı ağlar aracılığıyla bağlanan çalışanları ve organizasyonları büyük bir risk altına sokmaktadır. Bu durum eğer organizasyonların kaynakları iyi yönetilmiyorsa, dış ağlardan bağlanan çalışanlar aracılığıyla, bilgisayar karsonalrına virüs ve zararlı yazılımlarını sisteme bulaştırmalarına olanak verecektir.

3.7. Bilgi Güvenliğini Etkileyen Organizasyonel Davranışlar

Eğer çalışanlar güvenlik için gereksinimlerinin mantığını anlayabilirler ise büyük ihtimalle bunları kabul edeceklerdir. Diğer bir yandan, bilgi güvenliğinin gereksinimlerini anlamazlarsa durumu kabul etmeyebilirler. Eğer oluşturulan politikalar çalışanları çalışmaktan alıkoymakta ve işleri kullanışsız hale getiriyorsa, çalışanlar bu politikaları görmezden gelerek bilgi güvenliğini hiçe sayabilir ve organizasyonun bilgi güvenliğini tehlikelere atabilirler. Bu nedenden dolayı Hughes ve Stanton (2006) organizasyonların ihtiyaçlarını empati yapılarak belirlenmesi, çalışanların aklen ve kalben formule edilen güvenlik prosedürlerini benimseyerek, adapte olmasının gerekliliğini açıklamıştır.

Çalışanları, zihin ve kalpleri kazanılarak oluşturulan polikaları uygulamaya davet etmek ve eğitimlerini gerçekleştirmek daha kolay olacaktır. Neyin ne için konulduğunu ve arkasındaki sebeplerin önemini anlamak için, çalışan ve kullanıcıların anlayışı gerekli olduğunu öne sürmektedirler. Furnell ve Thomson (2009) tarafından ortaya atılan görüşe göre, insanlar sıklıkla bilgi güvenliği fikir ve çabalarını engelleyen bir varlık olarak algılanmaktadır.

Hughes ve Stanton (2006), çalışanların kazanılan zihin ve kalpleri ile bilgi güvenliği politikalarının uygulanmasında, çalışanların dikkati çekilmek isteniyorsa sabit bir yaklaşım izlenmesi gerektiğini açıklamaktadır. Çünkü bilgi teknolojileri geliştikçe ve tehditler karmaşık hale geldikçe, bu durum organizasyonları politikalarında değişiklik yapmaya zorlayacaktır.

İşverenler bu politikaları çalışanların adapte olacağı şekilde düzenlemeyi alışkanlık haline getirmezlerse, çalışanları işlerini yapabilmek için daha basit yollar arayışlarına yönlendirebilirler. Bu durum organizasyonu bazı risklerle uğraşmakla bırakmayarak, bilgi güvenliği hedeflerinin elde edilememesine neden olacaktır.

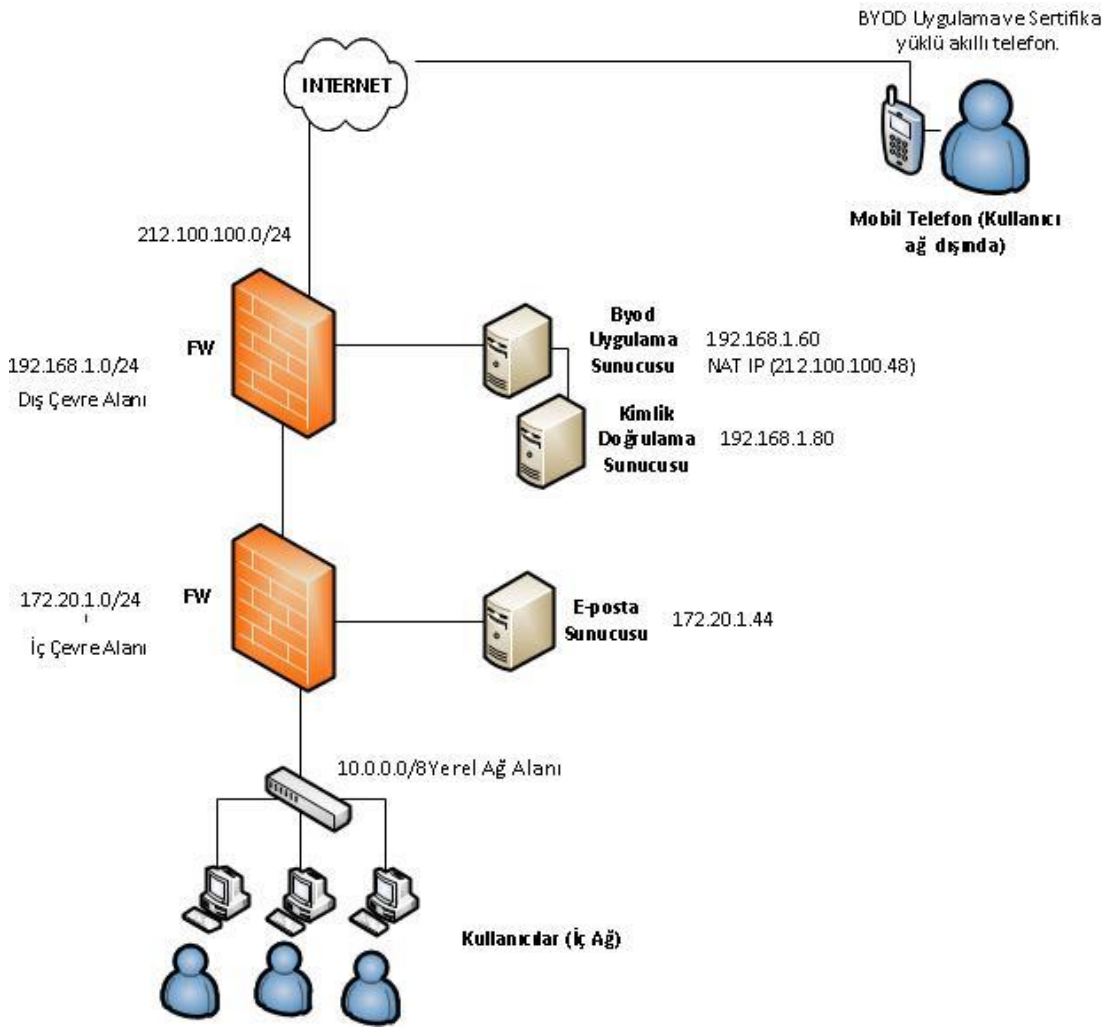
Ayrıca, kuruluşlar yerinde önlemler ve politikalar oluşturarak organizasyonel bilgilerini korumalıdırlar. Sadece kurumsal bilgi güvenliğini destekleyecek politikalar değil, çalışanları eğitimli kılacak ve onların bu politikalarla belirlenen amaç ve elde edilecek avantajlar hakkında bilgi sahibi ve farkında olmasını sağlayacak politikalar düzenlenmelidir. Bu sayede çalışanlar, bilgi güvenliği politikalarına karşı dirençlerini azaltarak bu politikaları kabul ederek, güvenli çalışma alışkanlığını edineceklerdir.

4. VERİLERİN K.C.G VE GELİŞMİŞ ŞİFRELEME STANDARDI (AES) İLE ŞİFRELENMESİ

Önceki bölümler de detayları ile verdiğimiz bilgiler doğrultusunda, K.C.G. teknolojisinin kullanıldığı ağlarda güvenlik çalışmalarının genel olarak cihaz ve sunucu arasındaki bağlantılarda olduğu görülmektedir. Fakat verinin şifrelenmesi, şifrenin ve güvenlik zafiyet detaylarının aktarılması, mevcut'da kullanılan şifreleme ve güvenlik metodlarının detaylıca incelenip, kullanıcı ortamlarına entegre edildikten sonra heterojen ortamlarda bu ilkelerin gözlemlenmesi olası güvenlik zafiyetlerinin tamamını ortadan kaldıracaktır.

Sunucu ile mobil cihazlar arasında kurulacak sanal özel ağ (VPN) tüneller ya da benzer şifreli bağlantılar güvenlik duvarı gibi gelişmiş ağ cihazları ile sağlanmaktadır. Bu cihazlar güvenlik politikalarını detaylıca oluşturup yerel veya internet ağından gelebilecek tehditleri anlamlı bir şekilde ağınızdan bertaraf edecektir. Şirket ortamlarında güvenlik duvarı (Firewall) cihazlarının detaylarına göre ciddi yatırımlar yapılmaktadır. Burada kaçırılan en büyük nokta ağ cihazlarında oluşacak güvenlik zafiyetleri bu cihazların dışında ya kullanıcı hatası ile yada bu tip cihazların kullandığı hatların tıkanık/doygun olması ile cihazın devre dışı kalmasından kaynaklanmaktadır. Bu noktada yaşanabilecek herhangi bir sosyal mühendisliğin/bilgi hırsızlığı'nın önüne verilerin uygulama ile şifrelenmesini sağlayarak geçebiliriz.

Burada kullanımını önereceğim yöntem, Gelişmiş Şifreleme Standardı (AES-Advanced Encryption Standard) dır. Bu şifreleme yöntemi hem yaygın hem de 128bit şifreleme potansiyeli olan bir yöntemdir. Aşağıdaki diyagram kendi tasarımımdır. İki ayrı bölümü ve çift katmanlı kontrol sistemi bulunan bir firma sistem örneğinde K.C.G'yi aktif etmek istediğimde ihtiyaç duyacağım donanımları göstermektedir. K.C.G için uygulama sunucusu, uygulamaya erişim sağlayacak kişinin doğrulanması için dizin (directory) sunucusu ve K.C.G'ye konu olan elektronik posta sunucusu ile dışarıda kendi akıllı telefonundan e-postalara ulaşmak isteyen kullanıcı mobil cihazı içerisinde ki K.C.G.sistemini temsil etmektedir.



Şekil. 16. K.C.G. Sistem Örneği

Yukarıda ki sistem örneğine göre örneklersek;

Kullanıcı şirket dışından e-postalarına ulaşmak istediğinde cihazında kurulu olan K.C.G. istemcisi sayesinde, kullanmak istediği uygulamayı çalıştırır. Uygulama içerisine bir sertifika ile birlikte iç ağ içerisinde bulunan uygulama sunucusunun adresi yerleştirilir. Kullanıcı uygulamayı çalıştırdığında trafik akıllı telefondan uygulama sunucusunun bulunduğu iç ağa doğru başlar. Kullanıcı isteği güvenlik duvarından geçerek uygulama sunucusuna ulaşır. Öncelikle uygulama sunucusu sertifika doğrulaması yapar. Sertifika doğrulanmasının ardından istek kullanıcının programa girdiği kullanıcı adı ve şifreyi doğrulamak üzere aktif dizin (AD) sunucusuna gider. Aktif dizin sunucusu, doğrulanan kullanıcı bilgilerini tekrar uygulama sunucusuna gönderilmesini sağlar ve paket içerisinde ki kullanıcının isteği yorumlanır. Uygulama sunucusu kullanıcının elektronik postalarına erişmek istediğini anlar ve isteği farklı bir IP bölümünde (segment) bulunan elektronik posta sunucusuna iletir. Elektronik Posta sunucusu isteğe cevap verir. Paketi alan uygulama sunucusu cevabı internette bulunan mobil cihaza göndermeden önce belirlediğimiz Gelişmiş Şifreleme Standardı (AES) yöntemi ile veriyi şifreler. Şifreli veri kullanıcıya gönderilmek üzere yola çıkar. Bu sefer trafik tam tersi yönünde hareket etmeye başlamıştır. Kullanıcıya gelen paket cihaz içerisinde ki uygulama tarafından karşılanır. Daha öncesinde kullanıcının akıllı telefonuna gönderilen politika (policy) sayesinde diske yazma yetkisi kaldırılarak işlem ram üzerinde çalışmaya başlar. Gelen sertifika dönüşü ile şifrelenen veri açılarak kullanıcı elektronik postalarını okumaya başlar.

Mevcut yapıyı sanal olarak oluşturacağım bir firma ağ yapısı üzerinde göstermek isterim. X firması için oluşturduğum çok basit ağ şeması Şekil.16.'deki gibidir.

Bu firma için iki sivil bölge (DMZ) ve bir yerel alan ağ'ından (LAN) oluşan bir yapı planlamış bulunmaktayım.

Örneğin firmanın dış IP bloğu 212.100.100.0/24 olsun. K.C.G. uygulaması için anons edilen IP adresi 212.100.100.48 olsun. Firmanın her güvenlik duvarı arkasında kullandığı özel IP blokları olsun. Bu firma için K.C.G. teknolojisini kurmak istediğimiz de nasıl bir ağ (network) sistem örneği oluşacağı ile ilgili temsil niteliğinde bir çalışma hazırladım.

192.168.1.0/24 IP (İnternet Protokolü) bloğunun kullanıldığı diş sivil bölge (Ext DMZ) olarak adlandırdığım alanda, dış güvenlik duvarı arkasına K.C.G. uygulamasını yöneteceğimiz uygulama sunucunu konumlandırdım. Bu sunucuya 192.168.1.60 IP (İnternet Protokolü) adresini atadım. (istenilmesi durumunda küme(cluster) çalışacak (birbirini yedekleyen) bir yapı kurulabilir.) Aynı sivil bölge (DMZ) üzerinde IP adresi 192.168.1.80 olan bir aktif dizin (AD) sunucusu konumlandırdım. Firmanın elektronik posta sunucusunu da iç sivil bölge (Int DMZ) olarak adlandırdığım ve 172.20.1.0/24 IP(İnternet Protokolü) bloğunu atadığım iç güvenlik duvarı (Int FW) arkasına konumlandırdım. Dış sivil bölge(Ext DMZ) de uygulama sunucusuna atadığım 192.168.1.60 IP (İnternet Protokolü) adresini dış güvenlik duvarında (Ext FW) 212.100.100.48 IP (İnternet Protokolü) adresine Ağ Adresi Dönüştürme (NAT) aracılığıyla yönlendirdim.

Mobil cihaz ile uygulama sunucusunun paket alışverişini güvenli olarak sağlayabilmesi için içerisinde özel anahtar (private key) bulunan ve uygulama sunucu üzerinde oluşturduğum 2048 bit'lik bir sertifikayı uygulama ile birlikte kullanıcı akıllı telefonuna kurulduğumuzu farz edelim.

Şirket iç ağlarında kullanıcı şirket bilgisayarından elektronik postalarına ulaşabiliyor. Elektronik Posta sunucusu aynı zaman da kullanıcı elektronik posta erişimini aktif dizin (AD) sunucusu üzerinden kimlik doğrulayarak sağlıyor. Bizim bu noktada yapmamız gereken şey K.C.G. uygulamasını yöneteceğimiz uygulama sunucusuna aktif dizin (AD) sunucusunu tanımlamaktır.

Bu noktadan sonra mobil cihazına K.C.G. uygulaması kurulmuş olan kullanıcı mevcut uygulama üzerinde kullanıcı adı ve şifresini girdikten sonra istek doğrudan uygulama içerisinde gömülü olan 212.100.100.48 IP (İnternet Protokolü) adresine güvenli hiper metin aktarım iletişim kuralı (https) protokolü ile gelecektir. İstek dış güvenlik duvarından (Ext FW) geçtikten sonra uygulama sunucusuna ulaşacaktır. Uygulama sunucusu kuyruğunda sertifika bilgisini taşıyan paketin öncelikle sertifika doğrulama işlemini gerçekleştirecektir.
Bu işlemden sonra paket içerisinde bulunan kullanıcının uygulamaya girmek için kullandığı kullanıcı adı ve şifresini aktif dizin (AD) sunucusuna soracaktır. Aktif dizin (AD) sunucusu kimliği doğruladıktan sonra isteği tekrar K.C.G. uygulama sunucusuna gönderecektir.

Bu noktada K.C.G. uygulama sunucusu paket içerisinde ki son isteği yorumlayarak trafiği iç sivil bölge (Int DMZ)'de bulunan elektronik posta sunucusuna gönderecektir. Elektronik posta sunucusundan alınan paket tekrar K.C.G. sunucusuna ulaşacak ve bu noktada benim tezimin de anafikrini oluşturan data şifreleme yöntemi Gelişmiş Şifreleme Standardı (AES) ile paket şifrelenerek kullanıcı akıllı cihazına bir politika paketi ile birlikte ulaşacaktır.

Mobil cihaz uygulama sunucusundan gelen politika aracılığı ile o an da bu uygulama üzerinde ki verileri diske yazmaya izin vermeyip Rastlantısal Erişim Hafızası (RAM) üzerinde çalıştıracak ve şifrelenmiş paketi çözerek içerisinde elektronik posta bilgileri bulunan veriyi kullanıcının anlayacağı şekilde yayınlayacaktır. Paketler bu ağ yapısı içerisinde belirlenen kural ve yöntemler ışığında iletilerek kullanıcını şirket dışından elektronik postalarını okuması sağlanmış olacaktır. Ayrıca elektronik posta sunucusuna konulacak bir kontrol sayesinde kullanıcının hem iç ağ den hem de banka dışından elektronik posta alışverişi yapması engellenebilir. Aktif oturum (session) özelliğinin sunucu üzerinde devreye alınması ile oluşabilecek bir diğer güvenlik açığıda engellenmiş olacaktır.

5. SONUÇ

Şirketler taşınabilirliği arttırmak amacıyla çalışanların şirket ağına her an ve heryerden ulaşabildiği sistemler üzerine yatırım yapmaktadırlar. Çalışanlar ve şirket yöneticileri cihaz sadeliği ve maliyet düşürücü çözümler ile keşfettiği kendi cihazını getir teknolojisi önümüzde ki yıllarda bütün firmalar tarfından kullanılmaya başlanacaktır.

Hali hazırda birkaç kurumsal şirket tarafından kullanılan bu teknolojideki en kaygı verici nokta veri güvenliğinin şirket ağı dışında istenildiği şekilde korunamamasıdır. Tam da bu noktada birçok şirket mecutda kullandıkları iç ağ güvenlik cihazlarını ağ dışında bir noktaya erişmek için kullanmaya çalışmaktadır.Aradaki bağlantının güvenli hale getirilmesi ne kadar önemli olsa da birçok yöntemle sosyal mühendislik ya da farklı saldırı yöntemleriyle bağlantılarda güvenlik açıkları yakalanilmekteidr ve aradaki bağlantı doygunluğa erişebilmektedir. Veri Güvenliği Esaslı "Kendi Cihazını Getir" Sistem Taraması" yöntemi ile ağ dışına gönderilecek veri, uygulama sunucusu üzerinden dışarıya doğru hareket ederken şifrelenmektedir. Burada kulanılan şifreleme yönteminin gelişmiş şifreleme standardı (AES) seçilmesi güvenlik açısından önemlidir.

Bu çalışma ile mobil cihazların şirket iç ağlarında ki verilerin izlenmesi sırasında oluşacak güvenlik açıklarına odaklanmış ve bunun sonucunda da veri güvenliği esaslı kendi cihazını getir sistem tasarımı tezini ortaya koymuştur.

KAYNAKLAR

Ahmed, M. H., Penney, J., Ikki, S., Salami, A., Bath, T. L., Allah, M. A., & Mansour, S.(2009). *Threats to Mobile Phone Users' Privacy*. Memorial University of Newfoundland, St John's, NL, Canada.

Akbari, H., & Land, F. (2005). Theories Used in IS Research: Socio-Technical Theory.RetrievedFebruary18,2013,from;http://www.istheory.yorku.ca/sociotechnicaltheory Allam, S. A. (2009*). A model to measure the maturity of Smartphones security at software consultancies'*, Faculty of Management and Commerce of the University of Fort Hare Allam, S. (2011). An Adaptation of the Awareness Boundary Model towards Smartphones Security. *Information Security South Africa (ISSA)*

Arthur, C. (2011). More Than 50 Android Apps Found Infected With Rootkit Malware. Retrieved March 15, 2013, from http://m.guardian.co.uk/technology/blog/2011/mar/02/android-market-appsmalware?cat=technology&type=article#

Balasubramanian,S., Peterson, R., & Jarvenpaa, S.L. (2002). Exploring the Implications of M-Commerce for Markets and Marketing. *Journal of the Academy of Marketing Science*, 30 (4), 348–361.

Ballano, M. (2011). Android Threats Getting Steamy | Symantec Connect Community.RetrievedMarch17,2013,from,http://www.symantec.com/connect/blogs/android-threatsgetting-steamy#

Banks, L. (2010). Mobile Devices Pose Security Dilemma for CIOs. Retrieved February10,2013,from,http://www.cio.com.au/article/346474/mobile_devices_pose_security_dilemma_cios/

Basole, R.C. (2008). Enterprise Mobility: Researching a New Paradigm. *Information Knowledge Systems Management*, 7, 1–7.

Berelson, B. (1952). Content Analysis in Communication Research. Glencoe, Ill: FreePress. Berg, B.L. (2001). Qualitative Research Methods for the Social Sciences.Boston: Allyn and Bacon.

Beurer-Zuellig, B., & Meckel, M. (2008). Smartphones Enabling Mobile Collaboration. In *Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (p. 49). Presented at the Hawaii International Conference on System Sciences, Proceedings of the 41st Annual. doi:10.1109/HICSS.2008.399

Bostrom, R. P., & Heinen, J. S. (1977). MIS Problems and Failures: A Socio-Technical Perspective PART II: The Application of Socio-Technical Theory. *MIS Quarterly* 1(4), 11–28. 85

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From Desktop to Mobile: Examining the Security Experience. *Computers & Security*, *28*(3-4), 130–137.

Boyce, C., & Neale, P. (2006).Conducting In-Depth Interviews: A Guide for Designing and Conducting In-Depth Interviews for Evaluation Input. *Pathfinder International Tool Series*

Bradley, J. (1993). Methodological issues and practices in qualitative research. *LibraryQuarterly*, 63(4), 431-449.

Büscher, M., & Urry J. (2009). Mobile Methods and the Empirical. *European Journal of Social Theory* 12(1), 99–116.

Chen, L., & Nath, R. (2003). A Framework for Mobile Business Applications. *I nternational Journal of Mobile Communications*, 2(4), 368–381.

Chen, L., & Nath, R. (2006). An Empirical Examination of the Impact of Wireless Local Area Networks on Organisational Users. *Journal of Electronic Commerce in Organisations,* 4 (2), 62–81.

Chen, L., & Corritore, C. (2008). A Theoretical Model of Nomadic Culture: Assumptions,Values, Artefacts and the Impact on Employee Job Satisfaction. *Communications of the AIS*, 22, 235–260.

Chen, L., & Nath, R. (2008). A Socio-Technical Perspective of Mobile Work. *Information Knowledge Systems Management,* 7, 41–60.

Chen, L., & Nath, R. (2011). Impediments to mobile work: an empirical study. *International Journal Of Mobile Communications*, *9*(5), 522-540.

Chia, P., Maynard, S., and Ruighaver, A. (2003): Understanding Organisational Security Culture, In Hunter, M. G. and Dhanda, K. K. (Eds.) Information Systems: The Challenges of Theory and Practice, Information Institute, Las Vegas, USA, pp.: 335 – 365.

Cisco (2013). Cisco Annual Security Report. Retrieved February 10, 2013, from http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

Clarke, N., and Furnell, S. (2007). Advanced User Authentication for Mobile Devices.*Computers and Security*, 26 (2), 109-119.

Conlin, M. (2006). Smashing the Clock. *Businessweek*, 60–68.

Connolly, P. J. (2000). Security Starts from Within. *Info World*, 22(28)

Corbin, J., & Strauss, A. (1990). Grounded Theory Research: Procedures, Canons, and Evaluative Criteria. *Qualitative Sociology*, 13(1), 3-21.

Couture, E. (2010).*MobileSecurity: Current Threats and Emerging Protective Measures*.

SANS Institute InfoSec Reading Room. Retrieved November 7, 2012, from http://www.sans.org/reading_room/whitepapers/incident/wireless-mobile-security_33548

Cresswell, T. (2006). *On the Move: Mobility in the Modern West*. London: Routledge.Cyber Future Will Bring Mixed Blessings.(1996).*USA Today Magazine*, *124*(2613), 4.

Ruggiero, P., & Foote, J. (2011). *Cyber Threats to Mobile Phones*. Carnegie Mellon University. US-CERT. Retrieved November 05, 2012, from http://www.us-cert.gov/reading_room/cyber_threats_to_mobile_phones.pdf

Daniel, D. (2008). Human Error Tops the List of Security Threats. Retrieved Dec.17,2012,fromhttp://www.cio.com/article/179802/Human_Error_Tops_the_List_of_Security_Threats

DeSanctis, G., & Poole, M.S. (1994). Capturing the Complexity in Advanced Technology Use: Adaptive Structuration Theory. *Organization Science*, 5 (2), 121-147.

De Wever, B., Schellens, T., Valcke, M., & Van Keer, H. (2006). Content Analysis Schemes to Analyze Transcripts of Online Asynchronous Discussion Groups: A Review. *Computer &Education*, 46, 6-28.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. Association for Computing Machinery. Communications of the ACM, 43(7), 125-128.

Dhillon, G. (2001). Violation of Safeguards by Trusted Personnel and Understanding Related Information Security Concerns. *Computers and Security*, 20(2), 165-172.

Drew, M. (2006). Bringing Enterprise Mobility to Industry. *Manufacturers' Monthly*, December, pg. 28.

Dunn, J. E. (2011). Mobile malware exaggerated by "charlatan" vendors, says Google engineer - PC Advisor. Retrieved February 15, 2013, from http://www.pcadvisor.co.uk/news/network-Wi-Fi/3320818/mobile-malware-exaggerated-bycharlatan-vendors-says-google-engineer/

Dunning, J. P. (2010). Taming the Blue Beast: A Survey of Bluetooth Based Threats. *IEEE Security & Privacy, 8*(2), 20-27.

Eason, K. (2001). Changing Perspectives on the Organizational Consequences of Information Technology. *Behavior & Information Technology, 20*(5), 323-328.

Elgan, M. (2007). It's Time We Stopped Talking About Smartphones. Retrieved December31,2012,from,http://www.techworld.com/mobility/features/index.cfm?featureid=320487

Enisa (2010). Smartphones: Information Security Risks, Opportunities and Recommendations for Users. Retrieved April 25, 2013, from https://www.enisa.europa.eu/activities/identity-andtrust/risks-and-data-breaches/smartphones-information-security-risks-opportunities-andrecommendations-for-users

Ernest-Jones, T. (2006). Pinning Down a Security Policy for Mobile Data. *Network Security*,6, 8–12.

Ernst & Young (2011). Into the Cloud, Out of the Fog - Ernst & Young's 2011 Global Information Security Survey. Retrieved February 21, 2013, from http://www.ey.com/Publication/vwLUAssets/Into_the_cloud_out_of_the_fog-2011_GISS/$FILE/Into_the_cloud_out_of_the_fog-2011%20GISS.pdf

Fitzgerald, J. (2009). Managing Mobile Devices. *Computer Fraud & Security*, 2009(4), 18-19.

Fratto, M. (2009). 2009 Strategic Security Survey. Retrieved February 21, 2013 from http://i.cmpnet.com/custom/strategicsecurity/assets/InformationWeek_Analytics_2009_Strategic_Security_Survey.pdf

Furnell, S., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers and Security*, *25*(1), 27–35.

Furnell, S., and Thomson, K.-L. (2009). Recognising the Varying User Acceptance of IT Security. *Computer Fraud and Security* (2), 5-10.

Gartner (2009). Gartner Glossary. Retrieved December 31, 2012, from http://www.gartner.com/6_help/glossary/GlossaryS.jsp

Carabott E., (2009). Taking Security Seriously. Retrieved February 21, 2013 from http://www.gfi.com/blog/taking-security-seriously/

Ghonaimy, M. A., El-Hadidi, M. T., & Aslan, H. K. (2002). Security in the Information Society:Visions and Perspectives. *Kluwer Academic Publishers*

Hannam, K., Sheller, M., & Urry, J. (2006). Editorial: Mobilities, Immobilities and Moorings. *Mobilities, 1*(1), 1–22.

Heikkila, F. M. (2007). Encryption: Security Considerations for Portable Media Devices.*Security & Privacy, IEEE*, *5*(4), 22–27.

Help Net Security (2013). Researchers Discover more BadNews on Google Play. Retrieved April 29, 2013, from http://www.net-security.org/malware_news.php?id=2475#

Hildenbrand, J. (2012). Android 4.2 brings new security features to scan sideloaded apps | Android Central. Retrieved February 15, 2013, from http://www.androidcentral.com/android-42-brings-new-security-features-scan-sideloaded-apps

Hoang, A.T., Nickerson, R.C., Beckman, P. and Eng, J. (2008). Telecommuting and Corporate Culture: Implications for the Mobile Enterprise. *Information Knowledge Systems Management*, 7 (1–2), 77–97.

Holsti, O.R. (1969). Content Analysis for the Social Sciences and Humanities. Reading, MA:Addison-Wesley.

Hsieh, H. F., & Shannon, S.E. (2005). Three Approaches to Qualitative Content Analysis.*Qualitative Health Research*, 15(9), 1277-1288.

Hughes, M., and Stanton, R. (2006). Winning Security Policy Acceptance. *Computer Fraud and Security*, 2006 (5), 17-19.

Jacobs, G. (2004). Diagnosing the Distance: Managing Communication with Dispersed Technical Workforces. *Corporate Communications*, 9(2), 118–127.

Johnson, J. (2009). Memory Cards for Your PDA: Expand Your PDA's Storage Potential.Retrieved December 31, 2012, from http://palmtops.about.com/od/accessoriesperipherials/ss/flashcards.htm

Juniper Networks (2011). Mobile Device Security, Emerging Threats And Essential Strategies - Key Capabilities For Safeguarding Mobile Devices And Corporate Assets. White paper, Juniper Networks, Inc.

Jürjens, J., Schrek, J., & Bartmann, P. (2008). Model-based Security Analysis for Mobile Communications. *ACM International Conference on Software Engineering*, 683-692

Kisling, E. L. (2006). An implementation of information technological change: A sociotechnical systems methodology perspective at the black chemical company. Indiana University. ProQuest Dissertations and Theses, 347-347

Kim, B. & Han, I. (2009). What Drives the Adoption of Mobile Data Services? An Approach from a Value Perspective. *Journal of Information Technology*, 24 (1), 35–45.

Kleinrock, L. (2001). Breaking Loose. *Communications of the ACM*, 44(9), 41–45.
Kothari, C, (2009). Research Methodology: Methods and Techniques. *New Age International Krippendorff, K. (1980). Content Analysis: An Introduction to Its Methodology. Newbury Park, CA: Sage.*

Kritzinger, E., and Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers and Security* , 27 (5-6), 224- 231.

Kruger, H. A., and Kearny, W. D. (2008). Consensus Ranking – An ICT Security Awareness Case Study. *Computers and Security*, 27 (7-8), 254-159.

Kvale, S. (1996). Interviews: An Introduction to Qualitative Research Interviewing. Thousand Oaks, CA: Sage Publications, Inc.

Landman, M. (2010). Managing Smartphones Security Risks. *Information Security Curriculum Development Conference*,145-155

Levine, J. H. (2007). Introduction to Data Analysis: The Rules of Evidence. RetrievedFebruary09,2012,from http://www.dartmouth.edu/~jlevine/stuff/intro%20copy/introfrset.html

Liginlal, D., Sim, I., and Khansa, L. (2009). How Significant Is Human Error as a Cause of Privacy Breaches? An Empirical Study and a Framework for Error Management. *Computers and Security*, 28 (3-4), 215-228.

Lincoln, Y.S., & Guba, E.G. (1985). Naturalistic Inquiry . Beverly Hills, CA: Sage Publications.

Lopez-Nicolas, C., Molina-Castillo, F.J., & Bouwman, H. (2008). An Assessment of Advanced Mobile Services Acceptance: Contributions from TAM and Diffusion Theory Models. *Information & Management*, 45 (6), 359–364.

Lyons, G., & Urry, J. (2005). Travel time use in the information age. *Transportation Research Part A: Policy and Practice*, *39*(2-3), 257-276.

Maconachy, V. W., Schou, C. D., Ragsdale, D., & Welch, D. (2001). A Model for Information Assurance: An Integrated Approach. *IEEE Workshop on Information Assurance and Security*, 306–310.

Mahoney, C. (2009). Talk Generation Y's Language. *HR Magazine* , 25

Manz, C. C. & Stewart, G. L. (1997). Attaining flexible stability by integrating total quality management and socio-technical systems theory. *Organizational Science, 8*(1), 59-70.

Martins, A., and Eloff, J. (2001). Information Security Culture. Retrieved December 12,2012, from http://etd.rau.ac.za/theses/available/etd-04292004-10222/restricted/SEC2002FinalVersion.pdf -12th December,2012

Mayring, P. (2000). Qualitative Content Analysis. Forum: Qualitative Social Research, 1(2).Retrieved June 17, 2013, from http://217.160.35.246/fqs-texte/2-00/2-00mayring-e.pdf.

McDonough, C. (2003). Identifying the Risk Involved In Allowing Wireless Portable Devices Into Your Company. *InfoSec Reading Room*. SANS Institute McDowell, M. (2008). Business Mobility: A Changing Ecosystem. *Information Knowledge Systems Management*, 7, 25–37.

McIntosh, J.C., & Baron, J.P. (2005). Mobile Commerce's Impact on Today's Workforce. *International Journal of Mobile Communications*, 3 (2), 99–113.

Michael, H. (2012). Android malware perspective: only 0.5% comes from the Play Store. Retrieved February 15, 2013, from http://www.phonearena.com/news/Android-malwareperspective-only-0.5-comes-from-the-Play-Store_id36696

Moody, D., & Walsh, P. (1999). *Measuring the Value of Information: An Asset Valuation Approach.* University of Melbourne, Department of Information Systems, Melbourne

Musaji, Y. (2006). A Holistic Definition of IT Security—Part 2. *Infromation Controls Journal (ISACA)*

Olzak, T. (2006). Strengthen Security with an Effective Security Awareness Program.RetrievedDecember17,2012,from,http://adventuresinsecurity.com/Papers/Build_a_Security_Awarsseness_Program.pdf

Önal, H.(2006).”Kablosuz Ağlar ve Güvenlik”. www.enderunix.org/docs/kablosuz_aglar_ve_guvenlik.pdf

Patton, M.Q. (2002). Qualitative Research and Evaluation Methods.Thousand Oaks,

Sage. Post, G. V., & Kagan, A. (2007). Evaluating Information Security Tradeoffs: Restricting Access Can Interfere With User Tasks. *Computers and Security*, 26 (3), 229 - 237.

PricewaterhouseCoopers (2012). Changing the Game: Key Findings from the Global State of Information Security Survey 2013. Retrieved February 21, 2013, from http://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/2013- giss-report.pdf

Reardon, M. (2007). Smartphones Sales Skyrocket. Retrieved December 31, 2012, from http://news.cnet.com/8301-10784_3-9816072-7.html

Restine, K. A. (1999). How Beliefs About Teaching and Learning Influence the Technology Training Experience: An Explanatory Case Study. Unpublished doctoral dissertation, Oklahoma State University, Stillwater.

Rouse, W.B., & Baba, M.L. (2006). Enterprise Transformation. *Communications of the ACM*, 49(7), 67–72.

Sacco, A. (2007). Study: Average Value of Business Info on Travellers' Laptops Equals $525K. Retrieved November 06, 2012, from http://www.cio.com/article/147000/Study_Average_Value_of_Business_Info_on_Travelers_Laptops_Equals_525K

Sale, N. (2007). The Way We Will All Work. *Global Telecoms Business*, 93, 66 - 67.
Schlienger, T. & Teufel, S. (2003). Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture", *Database and Expert Systems Applications conference proceedings* ,14, 405-409

Schilling, J. (2006). On the Pragmatics of Qualitative Assessment: Designing the Process for Content Analysis. *European Journal of Psychological Assessment*, 22(1), 28-37.

Schlienger, T., & Teufel, S. (2002). Information Security Culture: The Socio-Cultural Dimension in Information Security. *Management, Proc. Of IFIP TC11 17th International Conference on Information Security (SEC2002), IFIP Conference Proceedings* 214, 191-202

Scott, J.E. (2007). Mobility, Business Process Management, Software Sourcing, and Maturity Model Trends: Propositions for the IS Organisation of the Future. *Information SystemsManagement*, 24, 139–145.

SecurityWeek News. (2011). Multiple Variants of Android Malware "Hong Tou Tou" Surface in China | SecurityWeek.Com. Retrieved March 17, 2013, from http://www.securityweek.com/multiple-variants-android-virus-hong-tou-tou-surface-china#

Seybold, A.M. (2008). The Convergence of Wireless, Mobile, and the Internet and itsRelevance to Enterprises. *Information Knowledge Systems Management*, 7, 11–23.

Smith, H.W. (1975). Strategies of Social Research : The Methodological Imagination. Englewood Cliffs, NJ: Prentice-Hall.

Spender, J. C. (1996). Organizational Knowledge, learning and Memory: ThreeConcepts in Search of a Theory. *Organizational Change Management*, 9(1), 63-78.

Stallings, W. (2003). Network Security Essentials (Applications and Standards). Second Edition. Pearson Education. ISBN 0-13-035128-8

Standards South Africa (2005). SANS 17799:2005. Pretoria: Standards South Africa.

Stemler, Steve (2001). An overview of content analysis. Practical Assessment, Research &Evaluation, 7(17). Retrieved April 24, 2013 from http://PAREonline.net/getvn.asp?v=7&n=17

Streubert, H. J., & Carpenter, D. R. (1999). Qualitative Research in Nursing, Advancing the Humanistic Imperative. 2nd Edition. Philadelphia, PA: Lippincott

Takesue, M. (2007). Emerging Security Information, Systems, and Technologies. *SecureWare*

Taflinger, R. F. (1996). Introduction to Research. Retrieved November 05, 2012, from http://public.wsu.edu/~taflinge/research.html

TechAmerica (2012). Fiscal constraints and future challenges: Driving innovation at the CIO level. *22nd Annual Survey of Federal Chief Information Officers,* Retrieved February 21,2013, from http://www.federalciosurvey.com/ Urry, J. (2007). *Mobilities*. Cambridge: Polity Press.

U.S. General Accounting Office (1996). Content Analysis: A Methodology for Structuring and Analyzing Written Material. GAO/PEMD-10.3.1. Washington, D.C. VARBusiness (2006). Mobile Users Pursue Risky Business. *VARBusiness*, 22 (22), 51.

Verge Staff (2012). How to Buy a Smartphone: A Guide. Retrieved April 28, 2013, from http://www.theverge.com/2011/11/16/2565102/smartphone-buyers-guide#Walker, G. H., Stanton, N. A., Salmon, P. M., & Jenkins, D. P. (2008). A Review of Sociotechnical Systems Theory: A Classic Concept for New Command and Control Paradigms. *Theoretical Issues in Ergonomics Science*, *9*(6), 479–499.

Walters, P. (2012). *The Risks of Using Portable Devices*. Carnegie Mellon University. US CERT. Retrieved November 05, 2012, from http://www.us-cert.gov/reading_room/RisksOfPortableDevices.pdf

Walton, R. E. (1985). From control to commitment in the workplace. *Harvard Business Review, 63*(2), 77-84.

Waterson, P. E., Gray, M. T. O., & Clegg, C. W. (2002). A sociotechnical method for designing work systems. *Human Factors*, 44(3), 376-391.

Weber, R. P. (1990). Basic Content Analysis, 2nd ed. Newbury Park, CA.

Webster, J. & Watson, R., T., (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26 (2), 13–23

Whitman, M. E. & Mattord, H. J. (2004). *Management of Information Security*. Thompson Course Technology

Whitman, M. E., & Mattord,H. J. (2011).*Principles of Information Security* (4th Ed.).

Woo, D. M., & Vicente, K. J. (2003). Sociotechnical systems, risk management, and Public health: comparing the North Battleford and Walkerton outbreaks. *Reliability Engineering and System Safety*, 80, 253-269.

ÖZGEÇMİŞ

9 Haziran 1984 tarihi, Sivas ili Suşehri ilçesi doğumluyum. Liseyi Yalova ilinde, Anadolu Meslek Lisesinde 2002 yılında tamamladıktan sonra aynı yıl A.C.S. Proje Yönetimi şirketinde çalışmaya başladım. 2004-2005 yılları arasında Tübitak yazılım birincisi olan bir arkadaşım ile Global Yazılım Tasarım ve Danışmanlık firmasını kurarak Yalova ve Bursa bölgelerinde faliyet gösterdik. 2005 yılında Sakarya Üniversitesi Bilgisayar Programcılığı Bölümü'ne kaydoldum. 2006 yılında ise Anadolu Üniversitesi İktisat Fakiltesi Kamu Yönetimi (uzaktan) Bölümüne kayıt olarak Lisans ve Önlisans eğitimimlerimi birlikte tamamladım. 2005 yılında Sakarya Üniversitesi eğitimim devam ederken Superonline şirketinde işe girdim. 1 yıllık çalışmanın ardından 2006 yılında HSBC Bankasında kariyer hayatıma devam ettim. Yaklaşık 8 yıldır HSBC Bank bünyesinde çalışmaktayım. Bilgi Teknolojileri ekibinde Network ve Inter Güvenlik Uzmanlığı görevini üstelenmiş durumdayım. Bu süreçde bir çok teknik eğitim, seminer ve konferansa katılma şansım oldu.

İlgi alanlarım internet erişim cihazları üzerinde ki içerik ve web kategorileri filtreleme methodları ve bilgi günveliği ve farkındalığı alanlarıdır. Ayrıca Eğitmenlik Programı, İlk Yardım, Tiyatro gibi alanlarda sertifikalarım var. Yabancı dilim İngilizcedir

Aday: Volkan YILMAZ