Mobil Yaşamda Siber Güvenlik Yaklaşımı

K. G. Gökce, E. Şahinaslan, S. Dincel

Özet— Bilişim teknolojilerinin ve özellikle internetin hayatımızdaki önemi her geçen gün artmaktadır. Sosyal ağların kullanımının yaygınlaşması, hemen hemen her şeyin internet üzerinden yapılması ve bilgiye kolay erişimin artık lüks değil bir ihtiyaç olması mobil cihazların kullanımını da hızla artırmıştır. Bilgiye tek bir tıkla erişilmesi ve mobil teknolojilerle birçok işlemin daha hızlı ve kolay gerçekleşmesi hem kullanıcıların beklentilerini değiştirmiş hem de kurumların hizmet anlayışının teknolojik olarak farklılaşmasına neden olmuştur. Klasik ve geleneksel yöntemlerin yerini artık globalleşen dünyada mobil cihazlar ve mobil uygulamalar almaya başlamıştır. Mobil cihazların internet erişimi için kullanımının hızla artmasına paralel olarak bu cihazları hedef alan siber saldırı ve tehditlerde artmaktadır.
Bu çalışmada giderek artan mobil yaşam sonucu ortaya çıkan siber güvenlik sorunları ve alınabilecek önlemler belirlenecektir.

Anahtar Kelimeler - mobil cihaz, mobil güvenlik, siber güvenlik, siber tehdit ve saldırı

Abstract— The importance of information technologies and especcially the internet is increasing in our lives each and every day. The usage of mobile devices is increasing rapidly with the spread of social networks usage , almost everything done over the internet and the need of easy access to the information that is no longer be a luxury. One click access to information and many process done faster and easier with mobile technologies are the reason for change both user expectations and techological differentiation in instution's services offered. Classic and traditional method are replaced with mobil devices and mobile applications in globalizing world. The cyber attacks and threats for mobile devices targeted have been increasing with rapidly increasing usage of them for internet connection.
In this study, the cyber security issues resulting from increasing mobile life and actions need to be taken are determined.

Key Words- cyber threat and attack, cyber security, mobile device, mobile security

I. GİRİŞ

Dijital ağların giderek yaygınlaşması ve birbiri ile bağlantılı hale gelmesiyle birlikte globalleşen dünyamızda teknoloji her alanda hızla yerini almaya devam etmektedir. Sanayiden sağlığa, kamu ve özel sektörde birçok kurum ve kuruluş hizmet ve ürünlerini internet üzerinden sunmaktadır. Sosyal ağların, bulut bilişimin, mobil cihazların kullanımının hızla artması, hayatımızda vazgeçilmez hale gelmesi bilgilere hızlı ve kolay erişimi sağlamaktadır. Günümüzde bu hızlı ve kolay iletişimi sağlama noktasında hem kullanıcılar hem de kurumlar tarafından en yaygın kullanılan teknoloji mobil cihazlardır.

İstatistiklere bakıldığında, dünya nüfusunun yaklaşık %35'i internet kullanıcısı iken %26'sının ise sosyal ağlarda hesabı bulunmaktadır. Mobil cihaz kullanıcılarının sayısı ise oldukça yüksek olup %93'lük bir orana sahiptir. Mobil cihazların kullanım yaşı düşerken bir yandan da kişi başına düşen mobil cihaz sayısı artmaktadır. Türkiye'deki kullanım oranına bakıldığında ise nüfusun %84'ünün mobil cihaz kullanıcısı olduğu görülmektedir [2].

Bu gelişmelere bakarak bilişim hizmetlerinin hızla mobil cihazlara kaydığını söyleyebiliriz. Internete erişim için daha birkaç yıl öncesine kadar ağırlıklı olarak kullanılmakta olan kişisel bilgisayarlara (dizüstü, masaüstü bilgisayar) olan eğilim giderek azalmaktadır. Tablo 1'deki verilere bakıldığında 3 yıl içinde mobil telefon sayısının, bilgisayar ve tablet sayısından oldukça fazla olduğu görülmektedir. 2015 yılında ise bilgisayar sayısında düşüş yaşanırken tablet ve mobil telefon sayısında artış olmaktadır. Bu da ilerleyen zaman içinde mobilleşmenin artacağını, geleneksel dizüstü ve masaüstü bilgisayar kullanımının ise azalacağını açıkça göstermektedir.

TABLO I
SEGMENTLERE GÖRE DÜNYA ÇAPINDAKİ CİHAZ SEVKİYATI
(MİLYON TÜRÜNDE) [1]

Cihaz Tipi	2013	2014	2015
Geleneksel Bilgisayarlar (Dizüstü, Masaüstü)	296.1	276.7	263.0
Tablet	195.4	270.7	349.1
Mobil Telefonlar	1,807.0	1,895.1	1,952.9
Diğer Ultramobil Cihazlar (Hybrid ve Clamshell)	21.1	37.2	62.0
Toplam	2,319.6	2,479.8	2,627.0

Mobil cihazlar hem sektörel olarak finastan sağlığa birçok alanda yaygın olarak kullanılmakta hem de uygulama olarak artırılmış gerçeklikten video konferans özelliğine kadar geniş çapta hizmet sunmaktadır. Bu özelliklerin yanında mobilitenin günlük yaşamımızda yaygın olarak kullanımı göz önüne alındığında kurum ve şirketlerin iç ve dış uygulamalarını, müşteriye sunduğu hizmetleri mobil platforma taşımaları kaçınılmaz olmuştur. Mobil cihaz ve uygulamalar vasıtası ile kişisel ve kurumsal verilere kolaylıkla erişilebiliyor olunması da bu cihazları çok çeşitli siber güvenlik tehditlerinin hedefi

haline getirmiştir. Mobil cihazlar bir yandan hayatı kolaylaştırırken diğer yandan da güvenlikle ilgili birçok kaygıyı da doğal olarak ortaya çıkmaktadır [3].

İnternete erişim için mobil cihazların kullanımının artmasıyla birlikte mobil cihazlara ve cihazların kullanıcılarına yönelik siber saldırılarda artmaktadır. Kötü amaçlı mobil yazılım sayısında giderek yükselen bir artış olduğu bilinmektedir. Cihazlara yerleşen bu kötümcül yazılımlar, bilgi çalmak veya farklı siber saldırı yöntemleri ile kişi ve kurumlara büyük çapta zarar vermek, itibar kaybına uğratmak amacı ile kullanılmaktadır.

Sadece bilginin değil aynı zamanda dijital ortamların, elektrik, elektronik ve bilşim sistemlerinin gizlilik, bütünlük ve erişebilirlik bileşenlerinin korunması amacıyla oluşturan siber güvenlik yaklaşımının mobil cihazlar için neler sunduğu ilerleyen bölümlerde ayrıntılı olarak incelenecektir.

II. SİBER GÜVENLİK

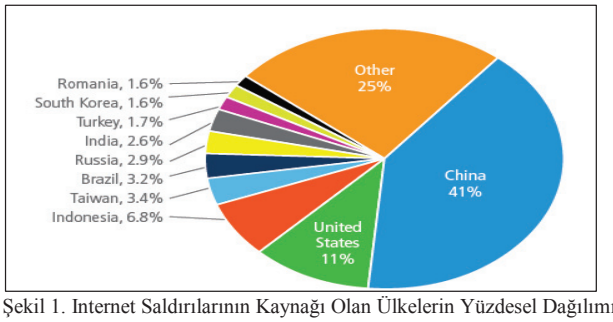
Siber güvenlik tanım olarak şu şekilde ifade edilmektedir; siber ortamda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür [5].

Kurum, kuruluş ve kullanıcıların varlıklarının korunması konusunda bilgi güvenliğindeki 3 temel unsur olan gizlilik, bütünlük, erişebilirlik bileşenlerine dikkat edilmelidir. Gizlilik, varlığı sadece iş ihtiyacı için ilgili olan kişilerin görmesi, kullanması anlamına gelmektedir. Yapılacak herhangi bir siber saldırıda bilginin yetkisiz kişilerin eline geçmesi varlığın gizliliğinin de ihlali anlamına gelmektedir. Bilginin bütünlüğünün korunmasındaki amaç ise herhangi bir bilişim sistemleri vasıtasıyla saklanan verinin yetkisiz kişiler tarafından değiştirilmesini veya bozulmasını önlemektir. Varlığın bilgi güvenliği bileşenlerinden biri olan erişebilirlik ile de kast edilen bilgiye ihtiyaç duyulduğunda erişebilinmesidir [5]. Meydana gelebilecek olan siber saldırılar sonucu bilgiye, veriye olan erişim engellenebilmekte kişi, kurum ve kuruluşları zor duruma düşebilmektedir.

Siber saldırı çeşitleri çok fazla sayıda olmakla beraber sürekli yeni saldırı türlerinin meydana gelmesi de kaçınılmazdır. Siber saldırı türleri genel hatları ile 5 başlık altında toplanabilir[7]:

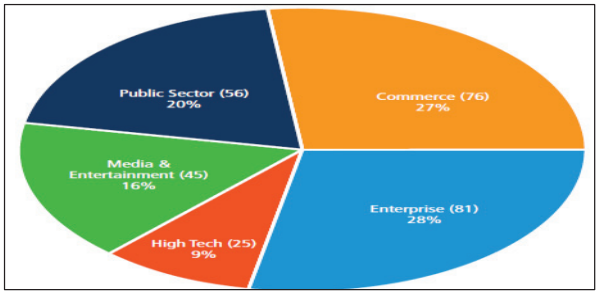
1. Servis Dışı Bırakma Saldırıları (DDOS, DOS)
2. Zararlı Yazılımlar
   i) Bilgisayar Virüsleri
   ii) Solucan
   iii) Truva atı
   iv) Tuş kaydedici
   v) Reklam yazılımları
   vi) Casus Yazılımlar
3. Oltalama
4. İstenmeyen E-Posta
5. Trafiğin Dinlenmesi

Siber güvenlik konusunda yeterli olmasada gün geçtikçe daha fazla çalışma yapılmaktadır. Kurumlar siber saldırıların hedefi olmamak ve bu saldırıları önceden tespit edebilmek için önemli yatırımlar yapmaktadırlar. Yine de dünya üzerinde önemli birçok özel kurum ve devlet kurumu çok ciddi siber saldırılara maruz kalabilmektedir. Aşağıdaki grafikte kaynak IP adresine göre kendisinden en fazla saldırı gerçekleşen ülkeler gösterilmiştir. Araştırmaya göre siber saldırıların %41'i Çin kaynaklı olup, Türkiye %1,7 ile 9.sırada yer almaktadır. Siber saldırılara ev sahipliği yapması açısından Türkiye'nin durumu maalesef pek parlak görünmemektedir [6].



Şekil 1. Internet Saldırılarının Kaynağı Olan Ülkelerin Yüzdesel Dağılımı [6]

Yine aynı araştırmaya göre, DDoS saldırıların sektörel olarak dağılımına bakıldığında ticaretten, medya&eğlence sektörüne birçok alanda yaygın olarak siber saldırıların yapıldığı görülebilmektedir. Grafiğe göre en fazla saldırı yatırım sektörüne düzenlenirken en az saldırlar ileri teknoloji ile ilgili çalışma yapan sektörlere düzenlenmektedir [6].

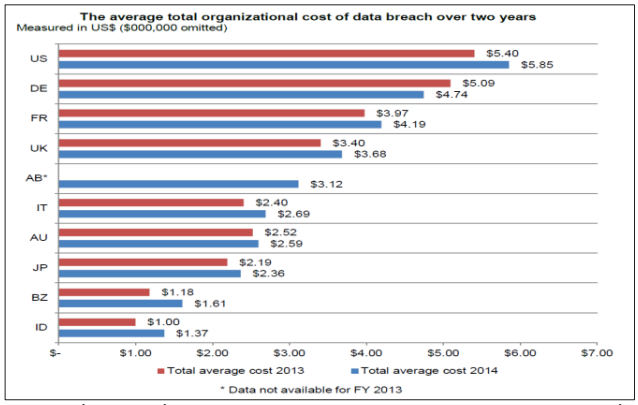


Şekil 2. 2014 Yılındaki DDOS Saldırılarının Sektörlere Göre Dağılımı [6]

Kurumlarda siber güvenliği sağlamanın ilk şartı olarak en üstten en alta kadar tüm çalışanların bilgi güvenliği farkındalığının yüksek seviyede olması ve siber güvenliğinin sağlanabilmesi için zaman, kaynak, bütçe konusunda üst yönetimin gerekli desteği sağlaması gerekir. Özellikle günümüzde tüm sektörlerde teknolojinin, internet altyapısının yoğun olarak kullanılması herbir sektör ve kurumu siber saldırılar konusunda açık hedef haline getirmektedir.

Siber saldırıları diğer saldırılardan ayıran en önemli fark, siber silahların ucuz maliyetlerle tahmin edilemeyecek boyutlarda zararlara yol açmasıdır. Hacker olarak adlandırılan siber savaşçılar bir bilgisayar ve bir e-posta ile hedefteki sistemi rahatlıkla ele geçirebilmektedir. Siber saldırıları tespit etmek ve sistemi eski haline dönüştürmenin maliyeti ise oldukça yüksektir.

Şekil 3' de belirtildiği üzere 2014 yılında yapılan bir araştırmaya göre 10 farklı ülkede yer alan şirketler için siber saldırı sonucu oluşan veri kayıplarının ortalama toplam organizasyonel maliyeti aşağıda gösterilmiştir. 5.85 milyon dolar ile Amerika birinci sırayı alırken, 4.74 milyon dolarlık bir maliyetle Almanya takip etmektedir. En az ortalama olarak toplam maliyete sahip olan şirketler ise sırasıyla Brazilya ve Hindsitan ülkelerine aittir. Maliyetlerin yüksek olması siber güvenlik konusunda alınması gereken önlemelerin artırılması gerektiğini açıkça göstermektedir.



Şekil 3. İki Yıl İçindeki Ortalama Toplam Organizasyonel Veri İhlal Maliyetleri [8]

III. MOBİL GÜVENLİK TEHDİTLERİ

Mobilleşme bilgi teknolojilerinin gelişmesiyle birlikte giderek yaygınlaşmış, kurumsal hizmet ve süreçleri kolaylaştırması ile de her alanda hızla yayılmaya başlamıştır.

Mobil çözümlerden daha iyi bir şekilde yararlanabilmek için son zamanlarda birçok inovasyon ortaya çıkmıştır. Donanım alanında Apple'ın ipad cihazları, işletim sistemlerinde Google'ın Android yazılımı, sosyal iletişim alanında Skype gibi yazılımlar ve 4G, LTE gibi ağ teknolojleri bu inovatif teknolojik gelişimlere örnek olarak verilebilir. [9]

Kişi ve kurumlar sürekli gelişen ve değişen mobil teknolojilere hızla adapte olup mobil cihazların kullanımı yaygınlaşırken mobil cihazlardaki güvenlik riskleri kişi ve kurumların en büyük endişeleri arasında yerini almaktadır.

Mobil cihazlardaki bluetooth, kızılötesi, wi-fi gibi kolay erişebilirliği sağlayan birçok özellik, saldırganlar için mobil cihazları masaüstü ve dizüstü bilgisayarlara göre daha cazip hale getirmiştir. Mobil cihazlara ait aşağıdaki özelliklerde herhangi bir açıklık olması durumunda mobil cihazlar siber saldırıya maruz kalabilir: [10]

- SMS
- Wi-fi
- Bluetooth
- Kızılötesi (Infra-red)
- USB
- Ağ tarayıcı
- Email sunucusu
- Third party applications
- İşletim sistemi açıklıkları
- Fiziksel erişim

Mobil cihazlar küçük boyutlarına rağmen birçok özelliği içinde barındırdığından bazı fiziksel ya da teknolojik açıklıklara sahiptirler.

A. Fiziksel Mobil Açıklıklar

Mobil cihazların boyut olarak ufak olması ve kolay taşınabilmesi, cihazların kolaylıkla çalışnmasına ya da kaybolmasına sebebiyet vermektedir [4,8]. Böyle bir durumun meydana gelmesi cihaz içindeki kritik verileri tehlikeye atmaktadır. Özellikle böyle bir durumda oluşabilecek zararı en az seviyeye indirebilmek için iş amaçlı kullanılan kurumsal telefonların uzaktan yönetilebiliniyor olması, otorizasyon ve şifreleme kurallarına dikkat edilmesi önemlidir.

Telefonların kimlik numarası niteliğinde olan IMEI numarası biliniyor ise herhangi bir sebeple çalınan ya da kaybolan telefon kolaylıkla açılabilinmektedir. IMEI numaralarının güvenli bir şekilde güçlü erişim kontrol mekanizmaları ile saklanması ise mobil operatörlerin sorumluğundadır [11].

Ayrıca dışırıdayken örneğin bir yerde sıra beklerken arkamızda bekleyen kişi telefona girdiğimiz şifreyi ya da telefondan baktığımız gizli içerikteki bilgileri rahatlıkla görebilir [4]. Böyle bir zaafiyeti engellemenin tek yolu, kullanıcıların farkındalık seviyesini artırmak, onları bilgilerin korunması noktasında bilinçlendirmektir.

B. Teknolojik Mobil Açıklıklar

Telefonun teknolojik özellikleri (SMS, Bluetooth, GPS gibi) kullanılarak yapılabilecek saldırılara örnek olarak bahsedersek, hacker telefonun

SMS, E-mail: Saldırgan, sms veya e-mail özelliğini kullanarak mesajları kendine yönlendirebilir, kritik bir bilgiyi öğrenmek için mesajları, e-mail hesabını inceleyebilir [4,10]

İşletim sistemi zaafiyetleri: Mobil cihazların işletim sistemindeki açıklıklar konuşmaların saldırgan tarafından dinlenmesine, kaydedilmesine neden olabilmektedir [4, 10].

Lokasyon bilgisi: Günümüzde birçok akıllı cihaz GPS özelliği sayesinde lokasyon bilgisini ulaşılabilir hale getirmektedir [8]. Hacker denilen kişiler bu bilgiyi kullanarak cihazın lokasyon bilgisini rahatlıkla öğrenebilmekte, başka kaynaklardan elde ettiği bilgi ile ilişkilendirebilmektedir [4].

C. Mobil Uygulama Açıklıkları

Farklı amaçlar için kullanılan birçok uygulama kolaylıkla erişebilmek amacıyla mobil cihaz üzerine kullanıcılar tarafından indrilmektedir. Bu uygulamaların çoğu çok fazla sayıda güvenlik riski ve mobil ajan içermektedir [4,11]. Bazı işletim sistemleri uygulamaları mağazalarında uygulamaları yayınlamadan önce güvenlik açıklıklarını kontrol ederken bazılarında ise böyle bir kontrol bulunmamaktadır. Bu durumda kullanıcıların uygulamaları mobil cihazından indirirken daha dikkatli olması gerekmektedir.

D. Güvenli Olmayan Ağların Kullanılması

Mobil cihazlar üzerinden internet erişimi için güvenilir olmayan ağların kullanılması birçok saldırıya davetiye çıkarmaktadır. Mobil cihazlar ile kablosuz erişimi sağlayan cihaz arasındaki verilerin dinlemenebilmesi saldırganlar için oldukça kolay olmaktadır [4,11].

VPN gibi güçlü şifreleme teknolojileri kullanılarak güvenilmeyen ağların sebep olabileceği riskler azaltılarak, verinin gizlilik, bütünlük, erişebilirlik bileşenlerinin korunması sağlanabilir [4].

E. Sosyal Medyanın Kullanılması

Sosyal medya erişim ve kullanım açısından pek çok güvenlik riski içermektedir. Özellikle mobil cihazlar üzerinden sosyal medya uygulamalarına erişildiğinde genel olarak cihazların güvenlik ayarlarının kullanıcıların kişisel verilerini paylaşmaya yönelik olarak ayarlandığı bilinmektedir [12]. Sosyal medya üzerinde gezinirken ya da herhangi bir paylaşımda bulunulurken Wi-fi ve GPS aracılığı ile konum bilgileri kolaylıkla başkaları ile paylaşılabilmektedir. Ayrıca sosyal ağ uygulamaları mobil cihazın üzerinde sürekli olarak açık bulunduğundan bazı zararlı uygulamalar sosyal ağlardaki verilerinizi kolaylıkla ele geçirebilmektedir [13].

Mobil cihazlarda sosyal medya güvenliğinin sağlanabilmesi için yapılması gereken en önemli 2 madde şu şekilde sıralanabilir [10]:

- Wi-Fi, GPS, Bluetooth, hücresel veri gibi fonksiyonlar sadece ihtiyaç anında aktif hale getirilip sonrasında pasif edilmeli. Böylece mobil cihazımızı sürekli bir hedef haline getirmekten kurtarabiliriz.
- Mobil cihaz üzerine indirilen sosyal ağ uygulamaları konum bilgisi ya da fotoğraflarımıza sürekli erişmek istediğinde izin verilmemeli, yine ihtiyaç olduğunda aktif hale getirilmelidir.

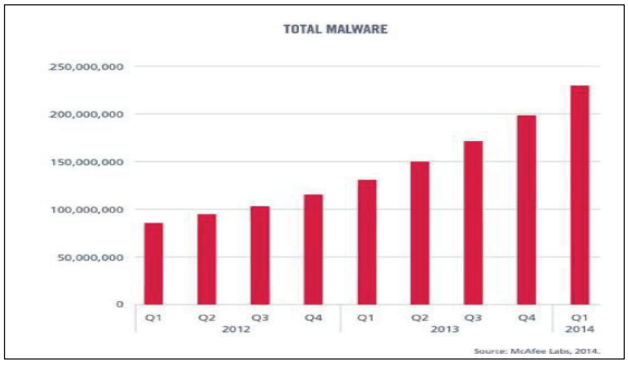
F. Zararlı Yazılımlar

İnternetten indirilen dosyalar, mesajlaşma servisleri, bluetooth gibi iletişim kaynakları mobil cihazlara zaralı yazılım ya da virüs bulaşma riskini artırmaktadır [11].

McAffe Labs tarafından yapılan araştırmaya göre Şekil 4'teki grafiğe bakıldığında 2012'den 2014'e kadarki süreçte zararlı mobil yazılımların sayısı giderek artmıştır. Bu artıştaki en önemli etmenler arasında mobil cihaz kullanım sayısının artması ve internete erişim için kablosuz erişimin kullanılmasının yaygınlaşması sayılabilir [14].

Zararlı yazılımların cihazlara bulaşması durumunda yapılabilecek potansiyel saldırılar aşağıdaki şekilde sıralanabilir [15]:

- Yerine geçme: Zararlı yazılım sayesinde cihaz üzerinde adeta uzak masa üstü erişimi sağlanarak mobil cihaz üzerinden bilgiler alınabilir.
- Veri akışını kesme: Cihaza doğru olan her türlü veri akışı kesilebilir.
- Bilgi hırsızlığı: Cihaza yerleşen zararlı yazılım tüm bilgileri toplayarak cihazdan dışarı gönderebilir.
- Arka kapı (Backdoor): Zararlı yazılım cihazda korunmasız bir arka kapı oluşturarak diğer ataklara açık hale getirir.
- Servisi kötüye kullanma: Cihaza yerleşmiş yazılım, servisi çok amaçlı kullanarak, kullanıcının fazla ücret ödemesine yol açar.
- Erişilebilirlik: Cihaz üzerindeki zararlı yazılım diğer cihazlarla etkileşimi sağlayarak farklı verilere erişim sağlayabilir.
- Şebekeye giriş: Cihaz üzerindeki zararlı yazılım farklı bir kimlik doğrulamaya gerek kalmaksızın şebekeye erişebilir.
- Solucan (Wormable): Cihaz üzerindeki zararlı yazılım, son derece rahat çoğalan solucanlar olabilir ve diğer cihazlara doğru hızla yayılır.



Şekil 4. 2012 Yılından 2014 Yılının İlk Çeyreğine Kadar Mobil Zararlı Yazılımların Toplam Sayısı [14]

G. Kurumlar için Yeni Endişe: Kendi Cihazını Getir (BYOD (Bring Your Own Device))

Mobil cihazların kullanımının artmasıyla birlikte iş hayatında da yeni ihtiyaçlar ortaya çıkmaktadır. Eskiden mobil cihazlar kurumlarda sadece e-maillere erişme, acil çağrılara cevap verme gibi temel iş ihtiyaçları için kullanılmaktaydı. Fakat günümüzde mobil cihazların kullanımının artması ve kolay taşınabilmesi ile birlikte bu cihazların kişisel bilgisayarların sunduğu nerdeyse tüm hizmetleri sağlaması akıllı telefonların ve tabletlerin kurumsal amaçlı kullanım isteğini artırmaktadır. Çalışanların kurum tarafından verilen yeni bir cihazı kullanmak yerine kendi akıllı cihazını aynı zamanda iş için kullanmak istemesi "Kendi Cihazını Getir (BYOD)" konseptini gündeme getirmiştir [16]. "Kendi Cihazını Getir" yeni bir teknoloji değildir, sadece bir kurum politikası olarak ifade edilebilir. Bazı şirketler bunu yasaklama yoluna giderken, bazıları ise veri güvenliği politikası izleyerek çalışanların kendi cihazlarıyla kurumsal ağa bağlanmasına izin veriyor.

Bu uygulamanın avantajları olduğu gibi pek çok güvenlik riski de bulunmaktadır. En büyük risk, her türlü saldırıya açık olan

mobil cihazlar kurumsal ağın içine dahil edildiğinde kurumsal verilerin güvenliğinin sağlanmasının çok kolay olmamasıdır.

Erişim politikalarının tüm rol ve sorumluluklar için açıkça belirlenmesi, kurumsal veri güvenliğinin korunması konusunda çalışanların farkındalığının artırılması, antivirüs, VPN gibi teknik olarak alınması gereken önelemlerin alınması, "Kendi cihazını getir" uygulamasının başarılı bir şekilde hayata geçmesi için kurumların alması gereken güvenlik önlemleri arasında sıralanabilir. Ayrıca kurumlar mobil cihazları uzaktan kontrol edebilmek ve çalınma, kaybolma durumlarında cihaza uzaktan müdahale ederek verilere erişilmesini önleyebilmek için Mobile Device Management (MDM) teknolojisinden de yararlanabilirler. Aynı zamanda MDM sayesinde mobil cihazlara sadece güvenirliliğinden emin olunan uygulamaların yüklenmesine izin verilmektedir. Böylece kurumlar hem kendi yerel ağlarını ve verilerini hem de çalışanlarının ve müşterilerinin verilerini korumuş olurlar.

H. Mobil İletişim Operatörlerinden Kaynaklanan Kısıtlar

Mobil operatörler hücresel mobil telefon haberleşmesi için gerekli sistemi sağlarlar. Abonelere ait son derece kritik verilerin iletimi, saklanması mobil operatörlerin sorumluluğunda olduğu için operatörler birçok ulusal ve uluslararası kuruluş tarafından iletişim güvenliğinin sağlanması konusunda düzenleme ve denetimlere tabi tutulmaktadırlar.
Mobil operatörlerden kaynaklanabilecek muhtemel tehditler aşağıdaki şekilde sıralanabilir [17]:

- Şebeke kaynaklarının ve verinin tahrip edilmesi
- Suistimal, sisteme izinsiz giriş ve müdahale
- Hırsızlık, veri veya diğer kaynakların çalınması veya kaybı
- Yetkisiz erişim
- Şebekelere erişimin engellenmesi, kesinti

Yukarıda bahsedilen zaafiyetlerin önüne geçmek için operatörler, kişisel verilerin işlenmesine, saklanmasına ve iletimine ilişkin güvenlik gerekliliklerini belirlemeli ve sundukları hizmetin güvenirliliğini sağlanmaya yönelik tedbirleri almalıdır [20].

IV. MOBİL GÜVENLİK İÇİN YAPILMASI GEREKENLER

Kullanıcıların alması gereken önlemleri ve kurumların mobil güvenlik konusunda izlemesi gereken politikalar ayrı başlıklar altında incelenecektir.

A. Kullanıcıların Dikkat Etmesi Gereken Kurallar

Kişisel mobil cihazların siber tehditlere karşı korunabilmesi için yapılması gerekenler aşağıdaki gibi sıralanabilir [17]:

- Mobil cihaza erişebilmek ve kullanmak için şifre oluşturulmalı, cihaz belirli bir süre kullanılmadığı durumlarda otomatik olarak kilitlenecek şekilde limit süresi ayarlanmalı. Bu şekilde yetkisiz kişilerin mobil cihazdaki kişisel verilere erişimi engellenebilir.
- Cihazı herhangi bir saldırı ve bozulmadan koruyabilmek için işletim sisteminin ve yüklenen uygulamalara ait yazılımlar güncel tutulmalı.
- Şüpheli e-mail ya da sms yoluyla gelen linklere tıklanmamalı. Bu linkler zararlı yazılımların cihaza yüklenmesine sebep olabilir.
- Web sitelerinde telefon numarası istenildiğinde ilgili kurum tarafından istenildiğine ve güvenilir olarak saklanacağına emin olunmadığı sürece telefon numarası yazılmamalı. Saldırganlar kullandıkları zararlı yazılımlar sayesinde telefon numaralarını web sitelerinden toplayarak bu numaralara karşı saldırı düzenleyebilmektedir.
- Truva atı ya da zararlı kod içeren uygulamalardan korunabilmek için mobil cihaz üzerine güvenilirliğine emin olunan uygulamalar yüklenmelidir.
- Mobil cihazlar için özel geliştirilmiş antivirüsler kullanılarak zararlı yazılımlara karşı mobil cihazlardaki verilerin korunması sağlanabilir.
- Wi-fi, bluetooth, kızılötesi gibi fonksiyonlar sadece ihtiyaç anında aktif hale getirilmeli. Böylelikle bu özellikler kullanılarak yapılan saldırılardan korunma sağlanabilir.
- Güvenilmeyen kablosuz ağlarla internete bağlanılmamalı.
- Cihazda bluetooth teknolojisinin kullanılması halinde açık ve keşfedilir özelliği devre dışı bırakılmamalı. Bu özellik kullanılarak yapılabilecek saldırlar bu şekilde engellenebilir.
- Sosyal ağ uygulamaları kullanılırken dikkatli olunmalı, bilinmeyen uygulamaların konum bilgisine ve fotoğraflara erişimine izin verilmemeli.
- Cihazınızda jailbreak (yazılım kırma) veya root (sistem tüm yetkilerini kullanacak hale getirme) özellikleri aktif hale getirildiğinde normalde izin verilmeyen zararlı yazılım içeren uygulamalarda dahil olmak üzere istenilen programları yükleme, silme gibi birçok hakka sahip olmaktasınız. Özellikle yetkin olmayan, bilgi güvenliği konusunda farkındalığı düşük kullanıcılar tarafından bu özelliklerin aktif hale getirilmesi kötü niyetli yazılımlara karşı korumayı ortadan kaldırmaktadır.
- Cihazınızın çalınma ve kaybolmalara karşı Find My Phone ya da benzer ayarlamalar yapılmalı. Böylelikle cihazın harita üzerinde konumu ve çalınma/kaybolma durumu kolaylıkla öğrenilebilir.
- Çalınma, yağmalanma, kaybolma veya her ne suretle olursa olsun, mobil cihazların sahibinin rızası dışında elden çıkması durumlarında tüketiciler telefonla Bilgi Teknolojileri ve İletişim Kurumunun Bilgi ve İhbar Merkezine ihbarda bulunarak cihazlarının elektronik haberleşme şebekesinden hizmet almasını engellenmesini sağlayabilir [19].

B. Kurumların Yapması Gerekenler

Kurumsal verilere kişisel ya da kurum cihazıyla erişilmesine izin verildiğinde iç ve dış tehditlere karşı alınması gereken önlemler aşağıdaki gibi sıralanabilir:

- Mobil cihaz ve uygulamalara erişim için kurum şifre

politikaları baz alınarak güçlü şifre kullanımı sağlanmalı, kullanıcıların düzenli aralıklarla şifre değiştirmesini sağlamak için gerekli ayarlamalar yapılmalıdır.

- İlgili tüm birimlerin görüşü alınarak mobil cihazlar vasıtası ile erişilen kurumsal veriler ve uygulamalar iş gereksinimleri doğrultusunda belirlenmeli. Böylece yetkisiz kişilerin ihtiyacı olmayan veriye erişmesi engellenebilir.
- Her bir rol ve sorumluluk için erişim yetkileri, kullanıcı hakları açıkça belirlenmeli ve yazılı hale getirilmelidir.
- Mobil cihazların taşınabilirlik özelliği sebebiyle kurum dışında kullanılması durumunda birçok güvenlik zaafiyeti oluşabilmektedir. Kullanıcı kaynaklı zaafiyetleri azaltabilmek için mobil cihaz kullanıcılarının uyması gereken kurallar belirlenmelidir.
- Mobil cihaz vasıtası ile kurumsal verilere erişen çalışanlara gizlilik ve güvenlik sözleşmesi imzalatılarak gizli verilerin yetkisiz bir şekilde kullanılması engellenebilir.
- Kullanıcıların güvenlik konusundaki farkındalığını yükseltmek amacıyla düzenli olarak eğitimler verilmelidir. Bu sayede çalışanların dikkatsizliği ya da bilgi eksikliğinden kaynaklanan veri kaybının önlenmesi sağlanabilir.
- Mobil cihaz ve uygulamalara erişim ile ilgili kurallar belirlenirken sadece BT birimlerinin değil, kurumdaki ilgili tüm birimlerin görüşü alınmalıdır.
- Kötü niyetli yazılımların kurum verilerine ve kurum ağına vereceği zararı önleyebilmek için mobil araçlar üzerine üçüncü parti imzasız, güvenilir olmayan yazılımların yüklenmesine izin verilmemeli.
- Zararlı yazılım ve virüsler mobil cihazlara bulaşarak kurumsal verilerin gizlilik, bütünlük, erişebilirlik bileşenlerini bozabilir. Bu durumu önleyebilmek için uygun antivirüs yazılımları kullanılmalı ve sürekli güncellenmelidir.
- Mobil cihazın yeni çıkan açıklıklara karşı korunabilmesi için işletim sisteminin düzenli olarak güncellendiğinden emin olunmalı.
- Mobil cihaz kurum ağına bağlanırken iletişim güvenliğinin sağlanması adına kurum ağı ile operatör ağı arasında sanal özel ağ oluşturulabilir ya da uygulamaya erişmeden önce mobil cihaz kurum ağına sanal özel ağ ile bağlanabilir [11].
- Mobil cihazlar vasıtasıyla erişilen kurumsal uygulamalarda yapılan işlemlerin denetim izleri alınmalı, kritik işlem ve uygulamalara ait izler düzenli olarak rapolanıp incelenmelidir.
- Cihazların kaybolması, çalınması durumunda ya da verilerin güvenliğinin tehlikeye girdiği durumlarda cihaza kolaylıkla müdahale edebilmek için merkezi bir yönetim konsolu uygulanmalıdır. Böylece lokasyon izleme, veri temizleme, şifre/PİN değiştirme ve güçlü kullanıcı yetkilendirmesi gibi fonksiyonlar uzaktan kontrollü bir şekilde yapılabilir.

V. SONUÇ

Hemen hemen herkesin bir veya daha fazla mobil cihazının olduğu ve bu cihazların insanların hayatında vazgeçilmez bir parça haline dönüştüğü bilinmektedir. Artık çoğumuz en kritik bilgilerimizi kişisel bilgisayarlardan çok, akıllı telefon ve tabletlerde taşımaktayız. Sadece kişisel veriler değil en mahrem kurumsal verilere bile mobil cihazlar vasıtasıyla tek bir tıkla kolaylıkla erişebilmemiz alınması gereken güvenlik önlemleri için daha fazla araştırma yapılması gerektiğini açıkça göstermektedir.

Mobil cihazların kolay taşınabilme, erişilebilme özelliği ve içerdiği bazı teknolojilerin doğru kullanılmadığı takdirde bir takım güvenlik zaafiyetlerine sebebiyet vermesi mobil cihazları saldırganlar için hedef haline getirmiştir. Gittikçe daha fazla zarara sebep olan siber tehditler mobil cihazları bilgisayarlardan bile daha yüksek oranda etkilenmektedir [14].

Bilinen tüm güvenlik açıklıklarına rağmen kişi ve kurumlar mobil cihazların sağladığı avantajlardan dolayı bu cihazları kullanmaktan vazgeçememektedir. Mobil cihazları etkileyen siber saldırıların sayısının artması kullanıcıların güvenlik konusundaki farkındalığını da artırmasına sebep olmuştur. Vazgeçilemeyen ve gittikçe hayatımıza daha fazla dahil olan cihazları güvenli bir şekilde kullanabilmek için tüm güvenlik riskleri, iç ve dış tehditler, kullanıcı dikkatsizlikleri belirlenip her bir risk için ayrı bir aksiyon ve önlem planı oluşturulmalıdır.

Kullanıcı ve kurumların alması gereken güvenlik önlemlerinin yanı sıra mobil iletişim operatörlerine de mobil güvenliğin sağlanması konusunda çok büyük görevler düşmektedir. Veri, kurumsal ağdan çıktıktan sonra kontrol operatörlerin sorumluluğunda olduğundan erişim ve iletişim altyapı hizmetleri ve uygulamalara ait tüm risk ve tehditler operatörler tarafından belirlenmeli, gerekli kontroller sağlanmalıdır. Haberleşme güvenliğinin sağlanması, verinin gizlilik, bütünlük, erişebilirlik bileşenlerinin tam olarak korunduğunun garanti edilmesi, erişim kontrolü ve kimlik denetimi gibi tedbirlerin alınması oluşabilecek güvenlik açıklıklarının önüne geçilmesi için hayati önem arz etmektedir. Abone ve kullanıcılara ait iletişim bilgileri, trafik verileri, konum bilgisi gibi gizli verilerin saklanması, korunması, imhası ile ilgili kurallar AB Mevzuatı Veri Koruma Direktifi'nde de açıkça belirtilmiştir. Veri Koruma Direktifi'ne göre operatörler tarafından saklanan verilerinn kaybolması, değiştirilmesi, depolanması, işlenmesi, ifşa edilmesi, belirtilen verilere erişilmesine karşı uygun teknik ve idari tedbirler alınması gerektiği belirtilmiştir. Yine mobil operatörlerin düzenli denetimi ve teftişi ile ilgili çalışmalar ülkemizde Bilgi Teknolojileri Kurumu kontrolünde gerçekleşmektedir [21].

Mobilleşmenin her alanda yaygınlaşmasıyla birlikte pazarlama stratejisi olarak mobil iletişimin kullanılması işletmeciler için kaçınılmaz olmuştur. SMS gibi haberleşme vasıtaları

sayesinde bir anda çok sayıda müşteriye ulaşabilme imkanı çok cazip görülmekle birlikte müşterileri rahatsız etmemek ve istemedikleri sürece onlara mesaj yollamamak gerekmektedir. Bunların yanı sıra milyonlarca kişinin iletişim bilgilerini elinde bulunduran mobil operatörlerin bu bilgileri müşterinin bilgisi ve izni olmadan kullanması, üçüncü kişilere ifşa etmesi ve bu yollarla haksız kazanç elde etmesi ise hukuka ve dürüstlük kurallarına aykırıdır [21].

Son zamanlarda ülkemizde ve dünya genelinde yaygın olarak görülen telefon dinlemelerinin ifşasında veri gizliliğini sağlamakla yükümlü olan operatörlerin ve diğer kurumların görevlerini yerine getirmediği ve gizli olarak korumaları gereken bilgilerin dışarı sızmasına sebebiyet verdikleri ortaya çıkmıştır. Yasal olmayan yollarla usulsuz bir şekilde yapılan telefon dinlemeleri ile ilgili operatörlerin herhangi bir zaafiyetinin olup olmadığının tespiti ile ilgili soruşturmaların açılmasındaki sorumluluk ülkemizde Bilgi Teknolojileri Kurumu'na aittir. Kurallara uymayan ve zaafiyete sebebiyet veren mobil operatörlerin cezalandırılması ile ilgili örnekler ise geçmiş zamanlarda meydana gelmiştir [21].

Bazı özel yasal takip durumlarında ilgili yargı kararları ve yetkilendirmeler ile telefon dinleme hakkına sahip olan istihbarat birimlerinin yetkileri de belli kurallar çerçevesinde belirlenmiş olup, yetki sorumsuzluğu gibi bir durum söz konusu değildir. Ülkemizde Milli İstihbarat Birimi görev ve sorumlulularının dışında hareket eden kişilerle ilgili olarak konuyu açıkça şu şekilde ifade etmiştir: "Teknik takip sırasında elde ettiği bilgileri şahsi amaçlarla kullanmaya kalkan veya teşkilatın dışına çıkaran personel teşkilat yasası gereği devlet sırrını ifşa etmekten yargılanır ve yapılabilecek suistimallere karşı kurulan kontrol sistemi sayesinde bilgi sızdıran mutlaka yakalanır." [22]. Yine Alman Federal Anayasa Mahkemesi, istihbarat birimlerinin teknik araçlar yoluyla yaptıkları yetkisiz erişimleri ve dinlemeleri yasaklamıştır [21]. Ulusal ve uluslararası birçok yasa ile kişilere ait verilerin korunması düzenlenmiş olsa bile hem yetkisini farklı amaçlar için kullanan personeller ve kurumlar hem de saldırganlar tarafından giderek artan teknolojik imkanlar kullanılarak kullanıcıların dinlemesinin ve bunun servis edilmesinin önüne geçmek maalesef çok kolay görünmüyor. Özellikle son zamanlarda Wikileaks belgelerinin ortaya çıkması ve birçok NATO ülkesinin birbirini dinlediği gerçeği siber güvenlikle ilgili uluslarası geçerliliği olan, daha ciddi ve yaptırımı yüksek önlemler alınması gerektiğinin bir zorunluluk olduğunu açıkça göstermiştir.

Mobil yaşamda siber güvenliğin sağlanabilmesi için ilgili tüm tarafların hem hizmet alan hem hizmet veren kurumlarla birlikte denetleyici, düzenleyici kurumların koordineli olarak çalışması önemlidir. Mobil güvenlikle ilgili yetki ve sınırların net olarak çizilmesi, zaafiyet durumlarındaki ceza ve yaptırımların artırılması da oluşması muhtemel siber saldırılar için caydırıcı olabilir.

Bu çalışmada kişilerin mobil cihazlar üzerinde yer alan hem kendilerine ait özel bilgileri hem de kurumlara ait bilgileri koruması konusunda yapması gerekenlerden bahsedildi. Ayrıca mobil cihazlar vasıtası ile kurumsal verilere erişilmesine izin veren kurumların alması gereken önlemler ve yapılması gereken kontroller açıkça belirtilmiştir.

KAYNAKÇA

[1] http://www.gartner.com/newsroom/id/2692318
[2] We Are Social, "Global Digital Statistics 2014"
[3] Hekim, H ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. Uluslararası Güvenlik ve Terörizm Dergisi, 4, 135-158
[4] National Institute of Standards and Technology. "Guidelines for Managing the Security of Mobile Devices in the Enterprise (SP 800-124)." http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
[5] http://tk.gov.tr/bilgi_teknolojileri/siber_guvenlik/index.php
[6] Akamai, "Akamai's State of The Internet Q1 2014 Report" http://www.akamai.com/dl/akamai/akamai-soti-q114.pdf?WT.mc_id=soti_Q114
[7] http://www.biakraporu.org/docs/rapor.kisim3.bolum01.pdf
[8] Ponemon Institute, "2014 Cost of Data Breach Study: Global Analysis" http://public.dhe.ibm.com/common/ssi/ecm/en/sel03027usen/SEL03027USEN.PDF
[9] Kietzmann, J., Plangger, K., Eaton, B., Heilgenberg, K., Pitt, L., & Berthon, P. (2013). Mobility at work: A typology of mobile communities of practice and contextual ambidexterity. The Journal of Strategic Information Systems, 22(4), 282-297.
[10] Verizon,"Mobile devices and Organizational Security Risk", http://www.verizonenterprise.com/resources/whitepapers/wp_mobile-devices-and-organizational-security-risk_en_xg.pdf
[11] Birliği, k. B. İ. M. Y. Mobil Uygulamalarda Güvenlik.
[12] Tunca, Sosyal ağlarda güvenlik - 1: Akıllı telefon ve tablet güvenliği,6 Mayıs 2012. [Çevrimiçi]. Available: http://dijitalekoloji.blogspot.com/2012/05/sosyal-aglarda-guvenlik-1-akll-telefon.html . [Ağıstos'ta erişilmiştir].
[13] Yıldırım, N., & Varol, A. (2013). Sosyal Ağlarda Güvenlik: Bitlis Eren ve Fırat Üniversitelerinde Gerçekleştirilen Bir Alan Çalışması (Security On Social Network: A Case Study Done At Bitlis Eren and Fırat Universities). TÜRKİYE BİLİŞİM VAKFI BİLGİSAYAR BİLİMLERİ ve MÜHENDİSLİĞİ DERGİSİ, 7(7).
[14] McAfee. "McAfee Labs Threat Report" http://www.mcafee.com/hk/resources/reports/rp-quarterly-threat-q1-2014.pdf
[15] Wayne Jansen, Karen Scarfone Guideliness on Cell Phone and PDA Security Recommendations of the National Institute of Standards and Technology
[16] Disterer, G., & Kleiner, C. (2013). BYOD—Bring Your Own Device. HMD Praxis der Wirtschaftsinformatik, 50(2), 92-100.
[17] Özcan, S. , Mayıs 2009, Yeni Nesil Şebekelere (NGN) Düzenleyici Yaklaşım ve Türkiye Önerileri, Sadullah Özcan, Uzmanlık Tezi, Bilgi Teknolojileri İletişim Kurumu
[18] Cyber Threats to Mobile Phones, US-CERT United States Computer Emergency Readiness Team, By Paul Ruggiero and Jon Foote, 2011 Carnegie Mellon University, Produced for US-CERT
[19] https://tuketici.btk.gov.tr/
[20] http://www.tk.gov.tr/mevzuat/yonetmelikler/dosyalar/EHSKVIGKHak_Yon_Konsolide_Metin_2013.pdf
[21] Şahin, O. , Haziran 2011, Elektronik Haberleşme Sektöründe Kişisel Verilerin İşlenmesi, Saklanması ve Gizliliğin Korunması, Osman Şahin, Uzmanlık Tezi, Bilgi Teknolojileri İletişim Kurumu
[22] https://www.mit.gov.tr/2937.pdf

Kevser Gülnur GÖKCE – 1989 yılında Ankara'da doğdu. Yeditepe Üniversitesi Endüstri Mühendisliği'nde lisans eğitimini tamamladıktan sonra, Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri'nde yüksek lisansına devam etmektedir. Aynı zamanda Bank Asya'da Bilgi Güvenliği, BT Risk ve Uyum Müdürlüğü'nde uzman olarak çalışmaktadır. Araştırma ve çalışma konuları arasında siber güvenlik, BYOD, PCI DSS bulunmaktadır.

Dr. Ender ŞAHİNASLAN – 1972'de doğdu, evli ve üç cocuk babasıdır. Trakya Üniversitesi Bilgisayar Mühendisliği Lisans, Gebze Yüksek

Teknoloji Enstitüsü Bilgisayar Mühendisliği bölümünde 'Yazılımda Kalite Modellerinin Değerlendirilmesi' adlı çalışmayla Yüksek Lisans, Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde 'Standartlara Dayalı Bilgi Güvenliği Risk Analiz ve Ölçümleme Metodolojisinin Bankacılık Sektörüne Özgü Modellenmesi ve Uygulama Yazılımının Geliştirilmesi' adlı çalışmayla doktora programını tamamladı.

1996 yılında Gazi Üniversitesi'nde başladığı çalışma hayatına Gebze Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Araştırma Görevlisi, Maltepe Üniversitesi Öğretim Görevlisi, Sabancı Üniversitesi Bilgi Teknolojileri Birimi'nde Uygulama Sorumlusu olarak devam etti. 2004 yılında Bank Asya Yazılım Geliştirme Müdürlüğü'nde başladığı göreve, Organizasyon Kalite ve Sistem Geliştirme Müdürlüğünde devam etti halen Bilgi Güvenliği, BT Risk ve Uyum Müdürü olarak çalışmaktadır. ISO 27001 LA, ITIL Fv3 ve CRISC sertifikalarına sahiptir.

Said Dincel – 1985 doğumlu, Beykent Üniversitesi Yönetim Bilişim Sistemleri bölümünden mezun oldu. Bank Asya, Bilgi Güvenliği BT Risk ve Uyum Müdürlüğü'nde Bilgi güvenliği uzmanı olarak çalışmaktadır. Veri tabanı ve merkezi log yönetimi, log analizi, bilgi güvenliği ihlal olayları inceleme ve çözümleme, sızma test proje yönetimi başlıca çalışma alanlarını oluşturmaktadır. Halen İstanbul Şehir Üniversite'sinde, Bilgi Güvenliği Mühendisliği alanında Yüksek Lisans eğitimini sürdürmektedir.