T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ

ÜÇÜNCÜ NESİL MOBİL İLETİŞİM SİSTEMLERİNDEKİ GÜVENLİK TEHDİT VE ZAFİYETLERİ

Yüksek Lisans Tezi

Mahmut İlker NAİMOĞLU

İstanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİ TEKNOLOJİLERİ YÜKSEK LİSANS PROGRAMI

ÜÇÜNCÜ NESİL MOBİL İLETİŞİM SİSTEMLERİNDEKİ GÜVENLİK TEHDİT VE ZAFİYETLERİ

Yüksek Lisans Tezi

Mahmut İlker NAİMOĞLU

Danışman: Yrd. Doç. Dr. Yalçın ÇEKİÇ

İstanbul, 2011

T.C.
BAHÇEŞEHİR ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü
Bilgi Teknolojileri Yüksek Lisans Programı

Tezin Başlığı : Üçüncü Nesil Mobil İletişim Sistemlerindeki Güvenlik Tehdit ve Zafiyetleri

Öğrencinin Adı Soyadı : Mahmut İlker Naimoğlu

Tez Savunma Tarihi : 21 Ocak 2011

Bu yüksek lisans tezi Fen Bilimleri Enstitüsü tarafından onaylanmıstır.

Yrd. Doç. Dr. F. Tunç BOZBURA
Enstitü Müdür Vekili

Bu tez tarafımızca okunmuş, nitelik ve içerik açısından bir Yüksek Lisans tezi olarak yeterli görülmüş ve kabul edilmiştir.

Tez Sınav Jürisi Üyeleri

Yrd. Doç. Dr. Yalçın Çekiç (Tez Danışmanı) :

Doç. Dr. Adem Karahoca :

Yrd. Doç Dr. Mehmet Alper Tunga :

ÖZET

ÜÇÜNCÜ NESİL MOBİL İLETİŞİM SİSTEMLERİNDEKİ
GÜVENLİK TEHDİT VE ZAFİYETLERİ

Naimoğlu, M. İlker

Bilgi Teknolojileri Yüksek Lisans Programı
Tez Danışmanı: Yrd. Doç. Dr. Yalçın Çekiç

Ocak, 2011, 104 Sayfa

Özellikle son dönemlerde veri iletişimine giderek daha kolay olanak sağlayan mobil iletişim teknolojilerindeki gelişmeler sayesinde, bilgiye daha kolay erişebilme isteği içinde olan insanoğlu, bu teknolojleri daha fazla hayatının önemli bir parçası haline getirmiştir. Bunun sonucu olarak, mobil ortamda bilginin işlenmesi, taşınması ve saklanmasına yönelik yatırımlar yapılmış, bilgiye mekandan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmaya başlamıştır. Bu sayede de bireyler etkin günlük yaşantılarının gereksinimlerini yerine getirebilmek için mobil iletişim teknolojilerinden her geçen gün daha fazla yararlanmaya başlamıştır. Bu teknolojilerin kullanımının yaygınlaşması ile de mobil ortamlar saldırganlar için daha büyük bir hedef olmaya başlamış ve bu ortamlara güven ve bu ortamlardaki güvenlik konuları daha çok sorgulanmaya başlamıştır.

Bu çalışmada, üçüncü nesil iletişim sistemlerinin yapıları incelenerek olası tehditler ve zafiyetler araştırılmış, örnek bir şebeke üzerinde güvenlik prosedürleri uygulanarak şebekenin zayıf noktaları ortaya konmuştur. Ayrıca, üçüncü nesil şebekelerde güvenlikle ilgili standartlara ve Türkiye'deki elektronik haberleşme güvenliğiyle ilgili yapılan düzenlemelere değinilerek atılması gerekecek muhtemel adımlara ilişkin değerlendirmelere yer verilmiştir.

Anahtar Kelimeler: Üçüncü nesil, mobil internet, güvenlik, tehdit, zafiyet

ABSTRACT

SECURITY THREATS AND VULNERABILITIES IN THIRD GENERATION MOBILE COMMUNICATION SYSTEMS

Naimoğlu, M. İlker

Information Technologies Graduate Program
Supervisor: Asst. Prof. Yalçın Çekiç

January, 2011, 104 Pages

Especially in recent years, development of mobile technologies that ease the data communication more than ever, has caused mankind who is in pursuit of accessing information easily, to make these technologies one of the most important parts of his life. As a result, investments for processing, transfering and storing information in the mobile environment have increased and access to required information regardless of the venue has been provided. This has also enabled individuals to start benefiting from the mobile communication technologies increasingly every day in order to fulfill the needs of their daily lives. Widespread use of these technologies have caused mobile environments to become a bigger target for the attackers and hence trust to these environments have become more important leading security issues to be questioned more.

In this study, third generation mobile communication systems' architecture have been examined and potential threats and vulnerabilities have been defined. Existing controls on a sample UMTS network have been tested through a security procedure to define its weaknesses. Additionally, standards for security on third generation networks and regulations especially in Turkey for electronic communication security have been identified with possible steps to be taken.

Key Words: Third generation, mobile internet, security, threat, vulnerability

İÇİNDEKİLER

TABLOLAR

ŞEKİLLER

GRAFİKLER

KISALTMALAR

Abone bilgileri kalıcı veritabanı (Home Location Register)	: HLR
Abone kimlik modülü (Subscriber Identity Module)	: SIM
Ağ geçidi GPRS destek düğümü (Gateway GPRS Support Node)	: GGSN
Avrupa Posta ve Telekomünikasyon Yönetimi Birliği	: CEPT
Avrupa Telekomünikasyon Standartları Enstitüsü	: ETSI
Baz istasyonu (Base Transceiver Station)	: BTS
Baz istasyonu alt sistemi (Base Station Sub-System)	: BSS
Baz istasyonu kontrol merkezi (Base Station Controller)	: BSC
Bilgi İşlem Teknolojileri için Kontrol Hedefleri	: Cobit
Bilgi Teknolojileri ve İletişim Kurumu	: BTK
Bilgi Sistemleri Denetim ve Kontrol Birliği	: ISACA
Bilgisayar Güvenlik Enstitüsü (Computer Security Institute)	: CSI
Birinci Nesil (First Generation)	: 1G
BT Yönetişim Enstitüsü (IT Governance Institute)	: ITGI
Bütünsel erişimli haberleşme sistemi (Total Access Control System)	: TACS
Doğrulama merkezi (Authentication Center)	: AuC
Evrensel mobil haberleşme sistemi	: UMTS
GPRS servis düğümü (Serving GPRS Support Node)	: SGSN
GSM Evrimi için Geliştirilmiş Hız	: EDGE
Hizmet Engelleme Saldırısı (Denial Of Service)	: DoS
Hizmet Sunumu ve Destek (Deliver and Support)	: DS
İkinci Nesil (Second Generation)	: 2G
İleri Hata Düzeltim (Forward Error Correction)	: FEC
İleri Mobil Telefon Sistemi (Advanced Mobile Phone System)	: AMPS
İnternet protokolü (Internet Protocol)	: IP
İzleme ve Değerlendirme (Monitor and Evaluate)	: ME
Kamu telefon şebekesi (Public Switched Telephony Network)	: PSTN
Kısa mesaj servisi (Short Message Service)	: SMS
Kişisel Sayısal Hücresel Sistem	: PDC
Kod bölmeli çoklu erişim (Code Division Multiple Access)	: CDMA

Küresel mobil haberleşme sistemi	: GSM
Mobil anahtarlama merkezi (Mobile Switching Center)	: MSC
Mobil anahtarlama merkezi ağ geçidi	: GMSC
Mobil cihaz kimlik tanımı veritabanı (Equipment Identity Register)	: EIR
Mobil istasyon (Mobile Station)	: MS
Nordic Mobil Telefonlar (Nordic Mobile Phones)	: NMT
Paket anahtarlamalı radyo hizmeti (General Packet Radio Service)	: GPRS
Paket kontrol birimi (Packet Control Unit)	: PCU
Planlama ve Organizasyon (Plan and Organize)	: PO
Radyo alt sistemi (Radio Subsystem)	: RSS
Radyo erişim şebekesi (Radio Access Network)	: RAN
Radyo Network Kontol (Radio Network Controller)	: RNC
Servis kalitesi (Quality of Service)	: QoS
Şebeke yönetim merkezi (Network Management Center)	: NMC
Tümleşik hizmetler sayısal ağı (Integrated Services Digital Network)	: ISDN
Ulusal standartlar ve teknoloji enstitüsü	: NIST
Uluslararası mobil abone numarası	: IMSI
Uluslararası mobil cihaz bilgisi (International Mobile Equipment Id)	: IMEI
Uluslararası standartlar organizasyonu	: ISO
Uluslararası telekomünikasyon birliği	: ITU
Uygulama ve Tedarik (Acquire and Implement)	: AI
Uzun Vadeli Evrim (Long Term Evolution)	: LTE
Üçüncü Nesil (Third Generation)	: 3G
Üçüncü Nesil Ortaklık Projesi (Third Generation Partnership Project)	: 3GPP
Yüksek hızlı devre anahtarlamalı veri (High Speed Circuit Switchd Data)	: HSCSD
Zaman bölmeli çoklu erişim (Time Division Multiple Access)	: TDMA
Ziyaretçi abone bilgileri veritabanı (Visitor Location Register)	: VLR

1. GİRİŞ

Özellikle son dönemde veri iletişimine giderek daha kolay olanak sağlayan mobil iletişim teknolojilerindeki gelişmeler sayesinde, bilgiye daha kolay erişebilme isteği içinde olan insanoğlu, bu teknolojleri daha fazla hayatının önemli bir parçası haline getirmiştir. Giderek küçülen boyutları ve makul fiyatları sayesinde cep telefonu, akıllı telefon, notebook, netbook ya da tablet bilgisayar olarak da adlandırılan bilgisayarlar gibi mobil iletişime olanak sağlayan teknoloji ürünleri insan hayatının giderek daha önemli bir parçası haline gelmiş, insanlar erişebilirliğe o kadar alışmışlardır ki, iletişim teknolojilerinin olmadığı, erişebilirliklerinin kısıtlandığı durumları tercihlerinin dışına itmişlerdir.

Bunun sonucu olarak, mobil ortamda bilginin işlenmesi, taşınması ve saklanmasına yönelik yatırımlar yapılmış, bilgiye mekandan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmaya başlamıştır. Bu sayede de bireyler etkin günlük yaşantılarının gereksinimlerini yerine getirebilmek için mobil iletişim teknolojilerinden her geçen gün daha fazla yararlanmaya başlamıştır. Insanlar haber almak, ürün satın almak, yazılı veya sözlü iletişimde bulunmak, banka işlemleri yapmak için klasik yöntemlerden vazgeçerek bu ihtiyaçlarını internet veya cep telefonu gibi mobil iletişim teknolojilerini kullanarak karşılama eğilimine girmişlerdir. Internet hizmetinin cep telefonları, notebook, netbook gibi cihazlar üzerinden kullanılmaya başlanması ile birlikte bu yöne eğilim daha da artmıştır. Günlük yaşantımızda yapmış olduğumuz birçok iş ve işlem kolaylıkla ve hızlıca yapılabilir hale gelmiştir. Örneğin bankacılık işlemleri bankaya gitmeden, vergi ve ceza ödemeleri vergi dairesine gitmek zorunda kalmadan, fatura ödemesi, pasaport başvurusu, otel rezervasyonu, uçak bileti, ögrenci kaydı, doktor randevusu gibi işlemler zamandan ve mekandan bağımsız olarak mobil ortamlarda halledilebilir olmuştur. Kısacası, sağladıkları kolaylıklar nedeni ile mobil iletişim teknolojileri ve bununla bağlantılı olarak mobil internet hayatımızın vazgeçilmez bir parçası olmuştur.

Bu teknolojilerin kullanımının yaygınlaşması ile de bu ortamlara güven ve bu ortamlardaki güvenlik daha çok sorgulanmaya başlamıştır. Zira, kullanımı gittikçe artan

mobil internet ortamı, sağladığı kolaylıkların yanında bazı güvenlik risklerini de beraberinde getirmektedir. Özellikle, işlemlerini mobil olarak gerçekleştiren kuruluşlar ve finans işlemlerini yapan bireyler için mobil internet bağlantısının güvenliği son derece önemlidir. Mobil internet üzerinden kurumsal ağlara erişim, gerekli güvenlik önlemleri alınmadığında başkalarının kurum ağına erişebilmesi veya kurum ağı ile yapılan haberleşmenin dinlenmesine neden olabilmektedir. Gizliliğin büyük bir rekabet avantajı getirdiği günümüzde erişim için hangi teknoloji kullanılırsa kullanılsın gerekli önlemlerin alınması kaçınılmazdır.

2. MOBİL İLETİŞİM

İletişim alanında Graham Bell'in telefonu icat etmesi ile başlayan gelişmeler günümüzde sınır tanımaz bir boyuta ulaşmıştır. Bu nedenle hızlı bir gelişim süreci içerisinde olan mobil iletişim sistemlerinin gelişiminin incelenmesi yararlı olacaktır. Mobil iletişim teknolojisinde hücresel sistemlerdeki gelişmeler, ortaya çıkan önemli yeniliklere göre çeşitli nesillere ayrılmıştır. Bu nesiller şu ana kadar dört adet olup, gösterim olarak 1G - Birinci Nesil, 2G - İkinci Nesil ve 3G - Üçüncü Nesil şeklinde ifade edilmektedirler. 4G - Dördüncü Nesil mobil iletişim sistemlerinin tüm dünyada uygulamaya konması için hazırlıklar ise hızla devam etmektedir.

Aşağıdaki bölümlerde bu nesiller ve kısaca gelişimleri anlatılmıştır.

2.1 BİRİNCİ NESİL MOBİL RADYO HABERLEŞME SİSTEMLERİ

Dünyada ilk mobil telefon uygulaması 1946'da Amerika Birleşik Devletleri'nde St. Louis Missouuri eyaletinde gerçekleştirilmiştir. İlk mobil telefon sistemleri ise 1950'li yılların başında Avrupa'da kurulmuştur. İletişimde hareketliliği sağlayan, çağrı cihazları ve araç telefonları ile hayatımıza giren mobil iletişim araçlarının kullanımı ise 1980'li yılların başında özellikle İskandinav ülkelerinde ve çeşitli Avrupa ülkelerinde hızla yayılmış; Amerika, İngiltere ve İskandinav ülkelerinde, ulusal mobil iletişim ihtiyacını karşılayabilmek üzere komiteler oluşturularak NMT (Nordic Mobile Phones), AMPS (Advanced Mobile Phone System) ve TACS (Total Access Communication System) adlı analog sistemler geliştirilmiştir (Ürper 2009).

Analog yapıdaki bu sistemlerin bazı karakteristik özellikleri manuel bir işletimin olması, sınırlı servis alanının sunulabilmesi ve düşük kapasiteli tek hücreli sistemler olmalarıydı (Telsim Teknik Eğitim Merkezi 2001).

Analog teknolojilerin bazı sınırlamaları ise şunlardı:

- Sınırlı frekans aralıkları
- Bir analog kanalda profesyonel dijital data iletiminin olmaması
- Arama yönlendirme, SMS ve Broadcast message gibi ilave servislerin olmaması
- ISDN arayüzünün olmaması
- Multimedia arayüzünün olmaması
- Uluslararası dolaşımın olmaması

Özellikle toplumlar arası etkileşimin iyice arttığı 1990'lı yıllarda abonelerin verilen hizmeti ülke sınırları dışında da kullanamamaları bu sistemleri yetersiz kılmıştır. Ülkelerin, ulusal sistem sağlayıcıları arasında anlaşmaları olmaması ve uluslararası standartların eksikliği bu sorunun çözümüne engel olmuştur (Ürper 2009).

Bunun yanı sıra birinci nesil mobil iletişim sistemlerine ait telefonların birbirlerinin yerine kullanılamaması ve farklı teknolojilere sahip olması da büyük bir sorun oluşturmuştur (Ürper a.g.e.).

Birinci nesil sistemler, sabit haberleşme sistemlerinden mobil haberleşme sistemlerine geçişte büyük bir adım olsa da karşılaşılan sorunlar ve müşteri beklentileri bu sistemlerin geliştirilmesi gerekliliğini ortaya koymuştur. Özellikle kapitalizmle birlikte rekabetin de artmasıyla iletişime ve bilgi erişimine olan gereksinim eskisinden daha çok kendini göstermiştir. Bu nedenle, birinci nesil sistemlerin eksiklikleri giderilerek, mobil iletişim sektöründe yeni bir devrin başlangıcı olan ikinci nesil mobil iletişim sistemleri oluşturulmuştur (Ürper a.g.e.).

2.2 İKİNCİ NESİL MOBİL RADYO HABERLEŞME SİSTEMLERİ

İkinci nesil mobil iletişim sistemleri mevcut analog sistemlerin dijitalizasyonu ile geliştirilmiş sistemlerdir. Kısaca "2G" olarak bilinen bu sistemler arasında GSM (Global System for Mobile Communications), CDMA (Code Division Multiple Access), D-AMPS (Digital- Advanced Mobile Phone Services), PDC (Personal Digital

Cellular) gibi bir çok mobil iletişim standardı oluşturulmuştur (Ürper 2009). GSM ikinci nesil mobil iletişim standartları arasında en popüleri ve lider konumundadır. GSM bugün 4.3 milyar abone sayısına ulaşmış durumdadır (The World in 2010: ICT Facts and Figures 2010).

GSM standardı, ilk dijital mobil iletişim standardı olarak tasarlanmıştır. GSM, 1982 yılında Avrupa Posta ve Telekomünikasyon Yönetimi Birliği (CEPT) tarafından kurulan "Group Special Mobile" adlı özel çalışma grubunun oluşturmuş olduğu standartları kapsamaktadır. Bu grubun çalışmaları, ilerleyen zamanlarda, mevcut standartları bir araya getirerek Avrupa genelinde ortak kullanılabilecek sayısal bir haberleşme sistemi oluşturmayı amaçlayan Avrupa Telekomünikasyon Standartlar Komitesi (ETSI) bünyesine aktarılmıştır. ETSI, GSM ile ilgili tüm çalışmaları düzenleyerek küresel iletişim sistemini bir bütün haline getirmiştir. Mobil iletişim endüstrisine yeni bir soluk kazandıran GSM, 1989 yılında ETSI tarafından 900 MHz bandında tüm Avrupa'yı kapsayan mobil iletişim şebekesi olarak meydana getirilmiştir. İlk kullanıma sunulduğunda birinci nesil iletişim sistemlerinde olduğu gibi yalnızca ses iletimine olanak sağlayan GSM teknolojisi daha sonra veri iletimi ve kısa mesaj servisi (SMS) hizmeti de vermeye başlamıştır.

GSM sistemlerinin bazı özellikleri aşağıda sıralanmaktadır:

- Tamamen dijital çalışma
- Daha iyi servis kalitesi
- Yüksek abone yoğunluğunu destekleyebilme
- ISDN (Integrated Services Digital Network)'e adaptasyon, ISDN servislerine karşı düşen servisleri sağlamak için maksimum esneklik.
- Ses bilgisinin kodlanması ve şifrelenmesi sayesinde radyo iletiminin güvenliği ve güvenilirliği
- Radyo sinyallerinin girişimine yüksek bağışıklık
- Dijital işaretin özel konfigürasyonlara esneklik sağlaması
- Dijital iletimin esnek hücre konfigürasyonlarına izin vermesi

- Bir mobil telefon sisteminin mevcut olduğu tüm ülkelerde kullanılabilme, yani global roaming (dolaşım)
- Frekans aralıklarının etkin kullanımı
- Mobil cihazın bulunduğu yeri belirlemek için hangi hücrede olduğunu tam olarak bilmeye gerek olmaması.

2.2.1 GSM Sektörünün Gelişimi

GSM iyi bir konuşma kalitesi, düşük terminal ve hizmet maliyeti, kendisinden önceki sistemlere göre daha yüksek bant verimliliği, ISDN (tümleşik hizmetler sayısal ağı) ile uyumluluk ve uluslararası dolaşım imkanı sağlaması nedeniyle devreye girdikten kısa bir süre sonra büyük ilgi görmüş ve bunun sonucunda da tüm dünyaya hızla yayılmıştır (Dinçkan 2006).

GSM ile ilgili ilk gelişme, var olan devre anahtarlamalı veri hızının 9.6 kbit/sn'den 14.4 kbit/sn'ye çıkartılması olmuştur. Bu aşamadan sonra 1998 yılında, veri iletim hızını arttırmak amacıyla devre anahtarlamalı veri kapasitesine sahip mevcut ikinci nesil GSM şebekelerinin gelişmiş bir uygulaması olan HSCSD (High Speed Circuit Switched Data - Yüksek Hızlı Devre Anahtarlamalı Veri İletimi) yapısı oluşturulmuştur. HSCSD kullanımı ile 57.6 kbps hızına kadar veri iletimi gerçekleştirmek mümkün kılınmıştır (Candan 2002) (Dinçkan 2006 içinde).

Ancak; İnternetin giderek yaygınlaşması ve gün geçtikçe daha fazla kullanım alanına sahip olması ile GSM'in veri haberleşmesi ihtiyaçlarını karşılamakta yetersiz kaldığı görülmüştür. Bu nedenle HSCSD'den sonra GPRS (General Packet Radio Service – Paket Anahtarlamalı Radyo Hizmeti) teknolojisi geliştirilmiştir (Dinçkan 2006). GPRS sistemi ile teorik olarak 171.2 kbit/sn hızı desteklenmektedir. GPRS, mevcut GSM altyapısına paket haberleşmesi için yeni cihazlar ekleyerek bu hizmeti vermektedir. Bu sebeple GPRS ile GSM aynı frekans bantlarını, aynı çerçeve yapısını ve aynı modülasyon tekniklerini kullanmakta, ciddi bir yatırım ihtiyacı doğurmamaktadır. GPRS, bir çok şebekenin kullanıcılarının veri uygulamalarına erişim sağlayabilmek için kullanmak durumunda olduğu verimli bir teknolojidir. GPRS, mobil iletişim teknolojisinde kullanılan devre anahtarlamalı (circuit-switched) yani kullanıcıya tahsis

edilen bir tek hat üzerinden sürekli bağlantı yerine paket anahtarlamalı (packet switched), aynı hattı birden çok kullanıcının paylaştığı bir teknolojidir. GPRS teknolojisi, kullanıcıya yüksek erişim hızının yanı sıra, bağlantı süresine göre değil gerçekleştirilen veri alışverişi miktarı özerinden tarifelendirilen ucuz iletişim olanağı sağlamakta ve böylelikle "sürekli bağlantıda, sürekli gerçek zamanda" (always connected/always online) anlayışını sunmaktadır. GPRS teknolojisi ile ikinci nesil mobil iletişim teknolojileri üçüncü nesile bir geçiş sayıldığı için "2.5G" mobil iletişim teknolojisi olarak da adlandırılmaktadır.

GPRS teknolojisinden sonra ve üçüncü nesilden önce EDGE (Enhanced Data rates for GSM Evoluation – GSM Evrimi için Geliştirilmiş Veri Hızları) teknolojisi gelmektedir ve geliştirilmiş modülasyon teknikleri kullanılarak 384 kbit/sn'lik maksimum teorik hız desteklenmektedir (Ak 2010). EDGE, GSM operatörlerine, 3G şebekeleri üzerinde sunulan servislere yakın hızlarda hizmet sunma olanağı vermektedir. Aynı zamanda EDGE, daha sonra 3G kullanımında gerekli olacak modülasyon değişikliklerinin şimdiden yapılarak, GSM'den 3G'ye geçiş dönemi sürecinde de yardımcı olmaktadır. EDGE sistemi şebeke operatörleri tarafından, kurulumu basit olarak gerçekleştirilebilecek şekilde tasarlanmıştır. Kurulum için EDGE verici birimi her hücreye eklenmekte, baz istasyonu kontrol merkezlerinde ve baz istasyonlarında yazılım yenilemeleri yapılmaktadır (Dinçkan 2006). Yeni EDGE vericileri, standart GSM trafiğini taşıyabilecekleri gibi gerekli durumlarda vericiler otomatik olarak EDGE modunda çalışabilmektedir. EDGE teknolojisi ile üçüncü nesile biraz daha yaklaşıldığı için EDGE, "2.75G" olarak da adlandırılmaktadır.

2.3 ÜÇÜNCÜ NESİL MOBİL RADYO HABERLEŞME SİSTEMLERİ

İkinci nesil sistemler yüksek kalitede ses iletimi sağlamalarına karşın, veri iletiminde küçük boyutlardaki verileri düşük hızla iletebilmekteydi. İnternet ortamında veri iletiminin oldukça hızlı sağlanması ile birlikte kullanıcılar mobil iletişim sistemlerinde de ses iletiminin yanı sıra veri iletiminin de hız kazanmasını talep etmişlerdir. Veri iletiminde talep edilen hizmeti sağlayabilmek için ikinci nesil mobil iletişim

sistemlerinde yapılan GPRS ve EDGE gibi düzenlemeler de yetersiz kalmaya başlamıştır.

Üçüncü nesile geçişin en önemli etkeni müşteri istekleri olmuştur. Çoklu ortam hizmetlerinin (ses, veri, görüntü) tek uçtan sunulması, hizmetlerin evrensel boyutta bir gezginlik alanında sunulması, sunulan hizmet kalitesinin iyi olması (örneğin mobil sistemlerin sunduğu servis kalitesinin sabit sistemlerinkine eşit olması), hizmetlerin güvenli, yüksek ve değişken hızda yani oldukçe geniş bantta sunulabilmesi gibi hizmetler başlıca müşteri talepleri arasında yer almıştır. Bir sonraki aşamada müşteri kendisi için tanımlı hizmet profili istemiş ve nereye giderse gitsin şebeke yapısından ve terminalden bağımsız olarak bu hizmetlere erişebilmeyi talep etmiştir.

Birinci nesil sistemler analog olduğu için hem kapasiteleri hem de güvenlik ve performansları düşük kalmıştır. Ikinci nesil sistemler sayısal tabanlı olmalarına ve birinci neslin zayıflıklarını büyük oranda gidermelerine karşın müşterilerin taleplerini gidermede yetersiz kalmıştır. Bunun üzerine, ITU (International Telecommunication Union – Uluslararası Telekomünikasyon Birliği) kişisel iletişimi zaman ya da yer kısıtlaması yapmadan sağlamayı amaçlayan ve ikinci nesil sistemlerinin aksine ses ve görüntü iletimini yüksek kalitede gerçekleştirebilen yeni sistem ve standartlar üzerinde çalışmaya başlamıştır. Küresel tanıtımı IMT2000 (International Mobile Telecommunication – Uluslararası Mobil İletişim) olarak yapılan yeni bir sistem, 1998 yılında üçüncü nesil mobil haberleşme standartlarının genel adı olarak kabul edilmiş, aynı yıl Avrupa haberleşme standartları enstitüsü (ETSI) Avrupa'da üçüncü nesil sistemler için kullanılacak standartları evrensel mobil haberleşme sistemi (UMTS) adı altında ITU'ye evrensel standart önerisi olarak sunmuştur.1998 yılı Aralık ayında Avrupa'dan ETSI, Japonya'dan ARIB ve TIC, ABD'den ANSI ve Kore'den TTA gibi dünyanın önde gelen standart enstitülerinin altı tanesi üçüncü nesil mobil haberleşme siteminin mevcut GSM alt yapısı ile uyumlu olmasını sağlayacak teknik özellik ve standartları belirlemek amacı ile bir araya gelerek; üçüncü nesil ortaklık projesi 3GPP'i (3G Partnership Project) oluşturmuşlardır. Daha sonraki gelişmeler ile IMT-2000 bir dünya standardı haline gelmiştir. ITU, IMT-2000 spesifikasyonlarından sorumludur. IMT-2000, tüm dünyada üçüncü nesil mobil iletişimin tüm standartları için bir kılavuz

referans olarak planlanmıştır. Pek çok bölgesel standardizasyon IMT-2000 çatısı altında çalışmaktadır.

Tüm bu gelişmelerle, üçüncü nesil, dünyada bu alanda kullanılan tüm standartlara uyumluluğu temsil etmiş, üçüncü nesil sistemler, abonelerine o anki konumlarından bağımsız olarak servis sağlama ve bu servisin içerisinde mümkün olan spesifik yapıları sunma imkanı sunmuştur. Bu sayede de tüm operatörlerden bağımsız olarak; herhangibir lokasyonda ulusal ve herhangibir coğrafik sınırda düzgün bir mobilite sağlanmıştır. Yüksek data hızı ve geliştirilmiş mobil şebeke fonksiyonları bu neslin karakteristiğini yansıtmaktadır.

2.3.1 UMTS (Universal Mobile Telecommunication System – Evrensel Mobil Haberleşme Sistemi)

UMTS, yüksek hızlı veri iletimine ve gerçek küresel gezinmeye olanak tanıyan IMT-2000'nin standartlarına uygun olarak Avrupa'da kabul edilen üçüncü nesil bir haberleşme sistemidir. UMTS, temel radyo erişim tekniği olarak WCDMA (Wideband Code-Division Multiple Access – Genişbant Kod Bölmeli Çoklu Erişim) kullanmaktadır. UMTS ile tüm dünyada, herhangi bir zamanda, lokasyondan bağımsız olarak 1. ve 2. Nesil sistem operatörlerinin sunduğu hizmetlerle, multimedya erişimi mümkündür. 8 kbit/s den 2 Mbit/s kadar data hızları UMTS ile desteklenmektedir. UMTS şebekeleri mevcut bir GSM şebekesinin alt yapısı üzerine kurulabilmekte, yani 2. Nesil ve 3. Nesil sistemler bir arada çalışabilmektedir (Castro 2001).

UMTS talebe göre hizmet sunmaktadır. Yüksek kalitede eğlence hizmetleri, büyük dosyaları indirme ve internette dolaşma bu kavram içinde sunulan hizmet türleri arasındadır. Çoklu ortam hizmetlerinin sunumuna ilave olarak, kullanıcıların gereksinim duyduğu mevcut iletişim hizmetleri UMTS sistemi içinde verilmektedir.

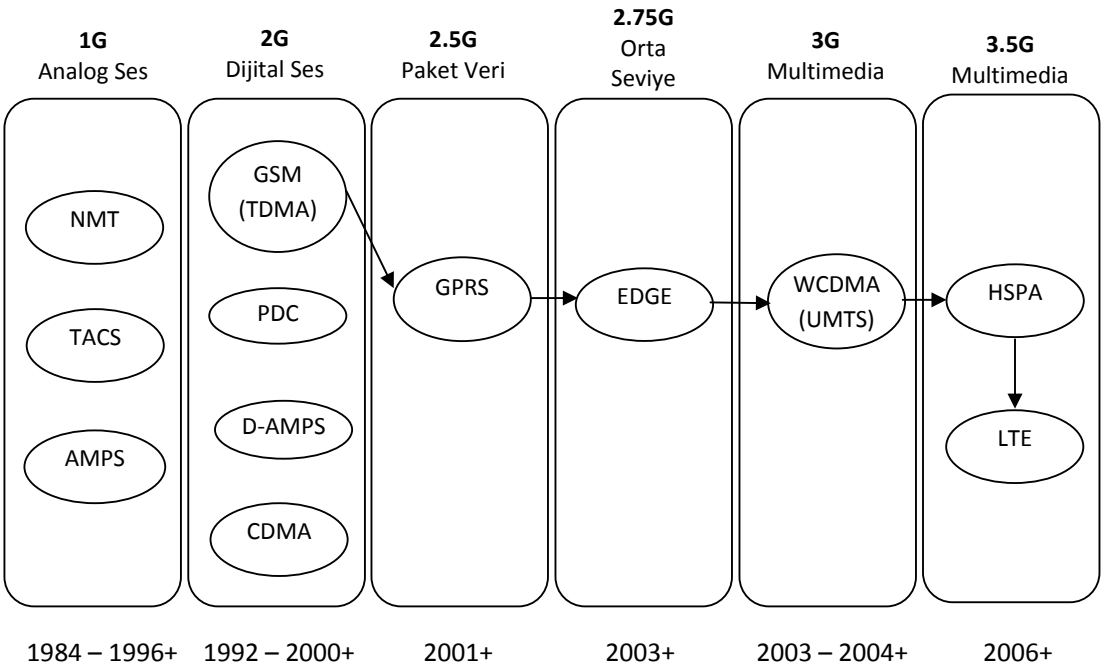
UMTS ile birlikte mobil sistemler bir çok alanda kullanılmaya başlamıştır. 2. nesil ile de sunulan telefon, kısa mesaj hizmeti (SMS), multimedia mesajlaşma hizmeti (MMS), Sesli Mesaj gibi servislerin yanı sıra UMTS sayesinde mobil sistemlere bir çok yenilik eklenmiştir.

2.3.2 HSPA (High Speed Packet Access – Yüksek Hızlı Paket Erişimi) ve HSPA+ (Evolved High Speed Access – Evrimleştirilmiş Yüksek Hızlı Paket Erişimi)

Yüksek hızlı paket erişimi HSPA (High Speed Paket Access – Yüksek Hızlı Paket Erişimi) UMTS'in radyo arayüzü ile ilgili 5inci ve 6ıncı sürüm teknik spesifikasyonlar setinde yayınlanan gelişmeler için kullanılan bir terim olup WCDMA standardı için paket veri servisidir. Pik veri oranları downlink için 42 Mbit/s ulaşabilmekte olup operatörlerin hizmetlerini arttırmıştır. HSPA "3.5G" olarak da adlandırılmaktadır. HSPA+ ise UMTS radyo arayüzü ile ilgili yedinci sürüm teknik spesifikasyon setinde yayınlanan gelişmeleri ifade edip 56 Mbit/s downlink hızlarına ulaşabilmektedir.

HSPA ve HSPA+ ile oldukça tatmin edici bir kablosuz genişbant hizmeti sunulabilmesine rağmen, 3GPP, LTE (Long Term Evolution) olarak adlandırılan ve en az 100 Mbit/s hızların hedeflendiği yeni bir teknoloji üzerinde çalışmaktadır. LTE, hücresel mobil haberleşme teknolojilerinin uçtan uca genişband ip şebekesine doğru evrimleşmesi olup III. nesil ortaklık projesi'nin (3rd Generation Partnership Project (3GPP) 8. versiyon Teknik Özellikler Setinde yeni bir kablosuz arabirimini ifade etmek üzere tanıtılmıştır. LTE, kullanıcılara gerek bant genişliği gerekse tepki süresi açısından sabit hatlardaki genişbanta benzeyen bir kişisel medya deneyimi sağlayabilmektedir. Downlink pik veri oranı 20 MHZ bant genişliğinde 100 Mbps'dır. Uplink pik veri oranı 20 MHZ bant genişliğinde 50 Mbps'dır. LTE, WCDMA radyo teknolojisinden farklı olarak OFDMA (Orthogonal Frequency Division Multiple Access Ortagonal Frekans Bölmeli Çoklu Erişim) tekniğini kullanmaktadır (Holma and Toskala 2006).

Aşağıdaki şekilde birinci nesil mobil iletişim sistemlerinden günümüze kadarki gelişimin özet bir gösterimi yer almaktadır.



Şekil 2.1: Mobil iletişim sistemlerinin gelişimi

2.3.3 Üçüncü Nesil Mobil Radyo Haberleşme Sistemlerinin Kullanım Alanları

Üçüncü nesil teknolojileri sayesinde aşağıda özetlenen kullanım alanları mobil sistemlerle entegre olmuştur (Dinçkan 2006).

Kişisel kullanım için uygulamalar:

- Telefondan TV izleme
- Online olarak video gösterimi
- Güvenlik kamerasıyla ev, işyeri vs. izleme
- Müzik indirme ve dinleme
- VideoCam uygulamaları (Gideceğiniz şehirdeki hava, trafik durumunu izleme vs.)
- İşitme engeliler için telefonu kullanma
- Taşınabilir bilgisayardan mobil olarak internete bağlanma
- İnteraktif alışveriş
- Gazetelere ya da yazılı medya ürünlerine internet üzerinden erişim
- Geliştirilmiş tarama ve filtreleme yeteneği

Kişiler Arası İletişim Hizmetleri:

- Görüntülü konuşma
- Mobil video konferans
- Sesli cevap ve tanıma
- Kişisel konum belirleme
- İnternet üzerinden sesli görüşme

Eğitim Uygulamaları:

- Sanal okul
- Internet üzerinden bilimsel laboratuarlara, kütüphanelere, web sitelerine erişim
- Internet üzerinden dil eğitimi
- Diğer çeşitli eğitimler

Eğlence:

- İsteğe bağlı müzik, yüksek kalitede müzik indirimi ve depolama
- İsteğe bağlı online oyunlar
- Sabit ve mobil ağlar arasında çevrimiçi oyun deneyimi
- İsteğe bağlı video klipler (Video on Demand), televizyon yayın hizmetleri (Mobil TV)
- Fotoğraf ve video mesajları
- Sosyal ağ sitelerine içerik yükleme

Toplum Hizmetleri:

- Acil servis hizmetleri
- Hastane veya tıp hizmetlerine uzaktan erişim

İş Uygulamaları:

- Mobil ofis
- Sanal çalışma grupları
- Gelişmiş araç navigasyonu/şehir rehberleri
- Video tabanlı mobil reklamcılık

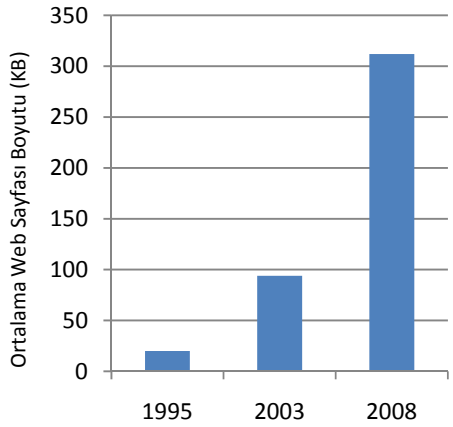
- P2P dosya transferi, iş uygulamaları, uygulama paylaşımı
- M2M iletişimi, mobil intranet/extranet
- Video yardım masası
- Mobil sunum

Ticari ve Finansal Hizmetler:

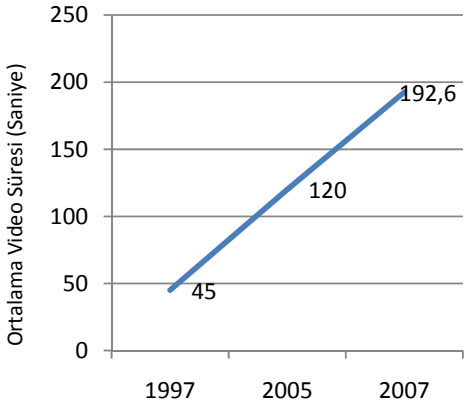
- Mobil bankacılık
- Internet üzerinden fatura ödeme
- Güvenlik kamerası hizmeti
- Dijital katalog alışverişi
- Ortak B2B uygulamaları
- Mobil ödeme
- Görüntülü çağrı merkezi
- İşitme engelliler için çağrı merkezi.
- Video broşür

2.4 MOBİL INTERNET TRENDLERİ

Internet hızlarının ve kullanımının artışıyla birlikte web tasarımcıları daha detaylı ve özenli, daha çok grafik içeren tasarımlara yönelmiş, web sayfalarında video kullanımları her geçen gün biraz daha artmıştır. Analysys Mason adlı araştırma şirketinin raporuna göre ortalama bir web sayfasının boyutu Ocak 2003'te 94KB iken Ocak 2008'de üç katına çıkarak 312KB'a ulaşmıştır (Grafik 2.1). 1997 yılında Internet ortamında yer alan bir videonun süresi 45 saniye iken, 2007'de bu süre 193 saniyeye ulaşmıştır (Grafik 2.2). Mobil içerik sanayisi de "mobil web"den (basit WAP sayfaları) her türlü ortamdan erişilebilecek standart web sayfalarına yönelmiştir. Web sayfalarının boyutları ve karmaşıklığının artışı mobil network trafiğinin de artmasına neden olmaktadır. (Health and Brydon 2008)

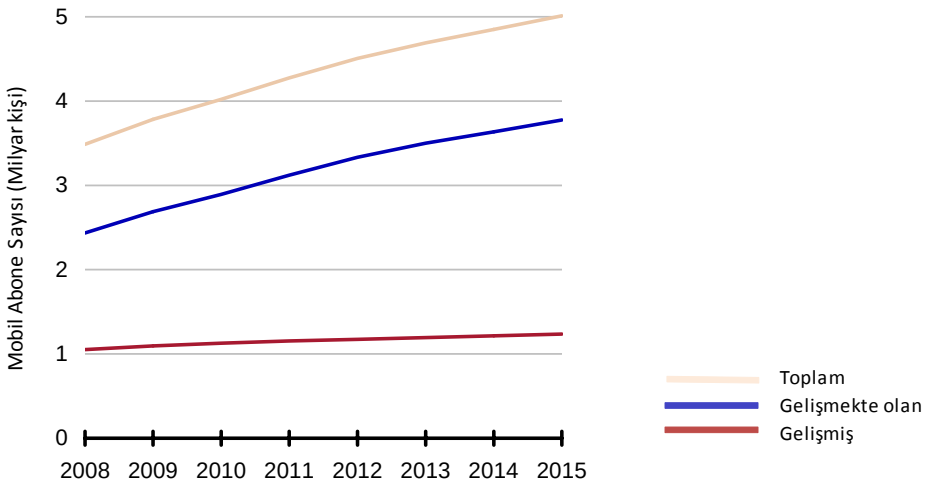


Grafik 2.1: Internet sayfalarının ortalama boyutları (1995- 2008)
Kaynak: Analysis Mason Report, 2008



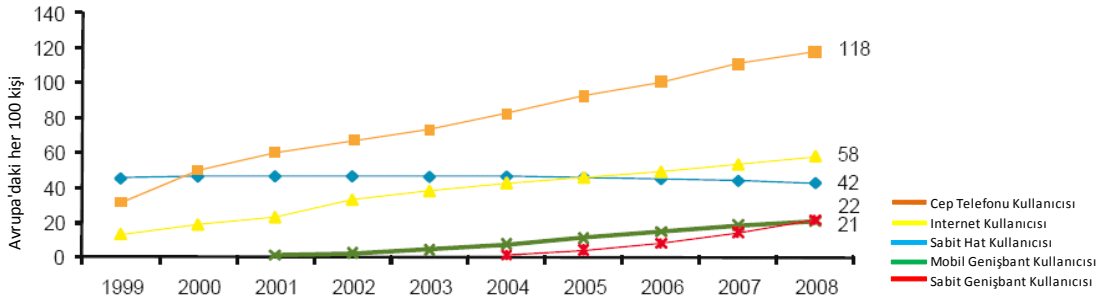
Grafik 2.2: Internette yer alan videoların ortalama süreleri (1997-2007)
Kaynak: Analysis Mason Report, 2008

Mobil abone sayısının da artışı toplam mobil network trafiğini arttırmaktadır. Analysis Mason şirketinin aynı araştırmasına göre gelişmiş ülkelerdeki mobil abone sayısının 2008'deki 1.05 milyar abone sayısından, 2015'te 1.24 milyar aboneye ulaşması beklenmektedir. Gelişmiş ülkelerdeki bu artışın abonelerin mobil modemler gibi ikinci cihazları da kullanmaya başlamaları nedeniyle olacağı düşünülmektedir. Gelişmekte olan ülkelerdeki 2008'de 2.43 milyar olan abone sayısının 2015'te 3.77 milyara ulaşması öngörülmektedir. (Grafik 2.3)

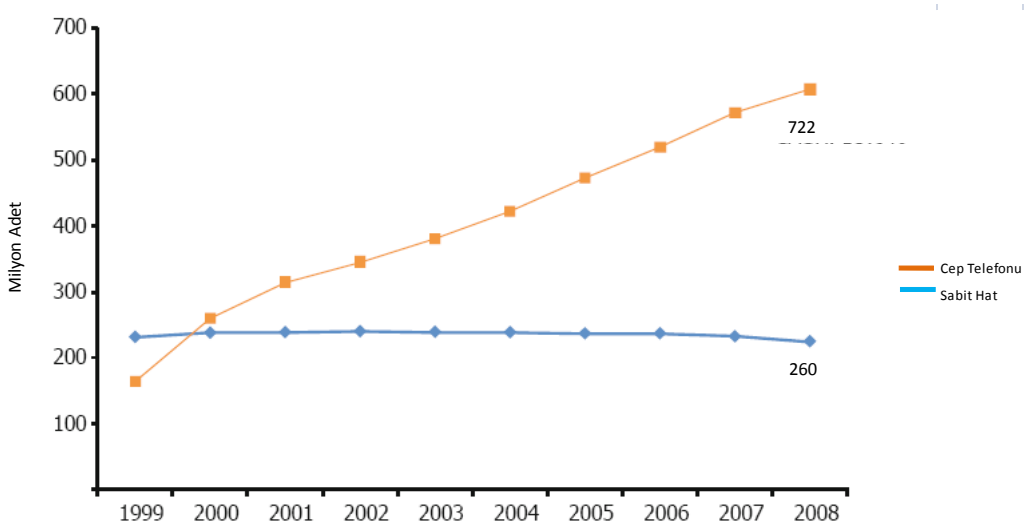


Grafik 2.3: Gelişmiş, gelişmekte olan ülkeler ve dünyadaki mobil abone sayıları

Uluslararası Telekomünikasyon Birliği'nin 2009'da yayınladığı "Avrupa Bilgi Toplumu İstatistiksel Profiller 2009" başlıklı raporuna göre de Avrupa'da cep telefonu ve mobil geniş bant abone sayıları 1999-2008 yılları arasında sırasıyla %11 ve %21 artarak %118 ve %22 penetrasyona ulaşmış durumdadır (Grafik 2.4). Aynı raporda, 2008 yılında Avrupa'da 722 milyon cep telefonu abonesi bulunurken sabit hat abonelerinin 260 milyon dolayında olduğu belirtilmektedir (Grafik 2.5) (The Information Society Statistical Profiles 2009)

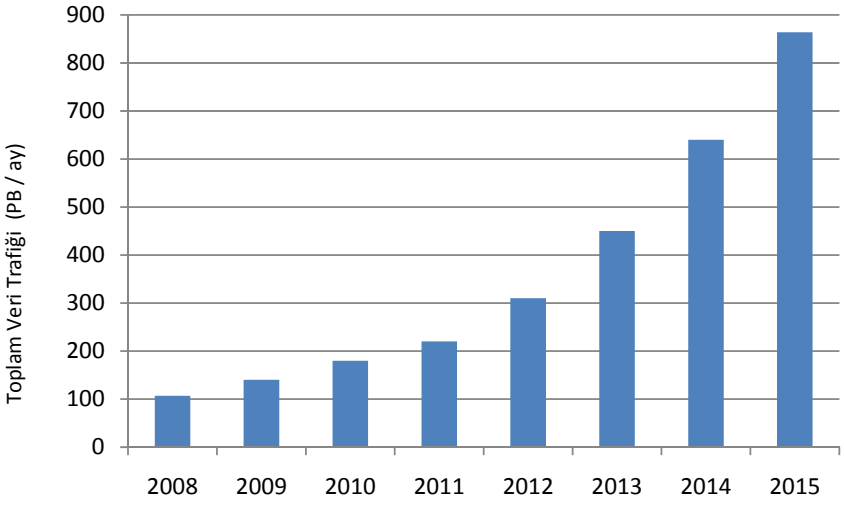


Grafik 2.4: Avrupa'daki mobil penetrasyon

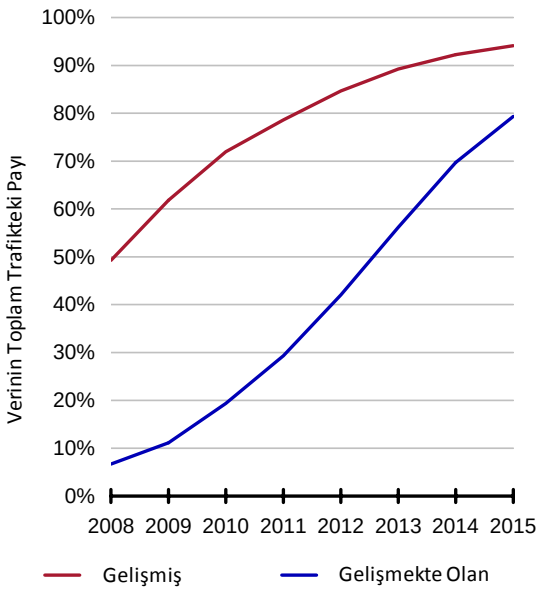


Grafik 2.5: Avrupa'daki cep telefonu ve sabit hat sayıları

Toplam network trafiğinin (ses ve data) ise 2015'te 2008'in yaklaşık sekiz katı büyüklüğe ulaşması beklenmektedir. 2008 yılında aylık 107 Petabyte civarında olan network trafiğinin 2015'te aylık 864 Petabyte seviyelerine çıkması beklenmektedir. (Grafik 2.6). 2015'te gelişmiş ülkelerde toplam trafiğin %94'ünün, gelişmekte olan ülkelerde ise %79'unun veri trafiğinden oluşacağı düşünülmektedir (Grafik 2.7) (The Information Society Statistical Profiles 2009).

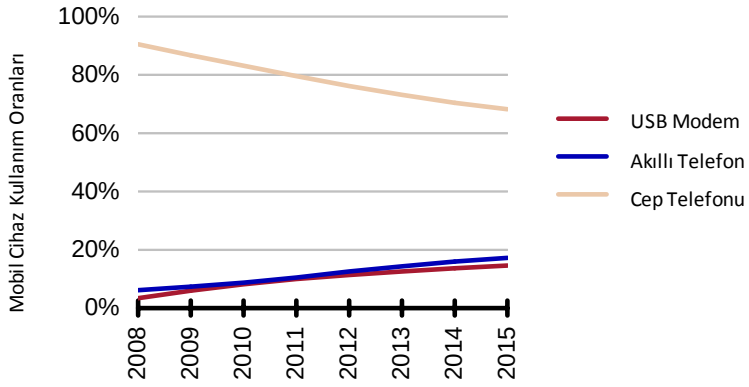


Grafik 2.6: Toplam network trafiği (2008-2015)



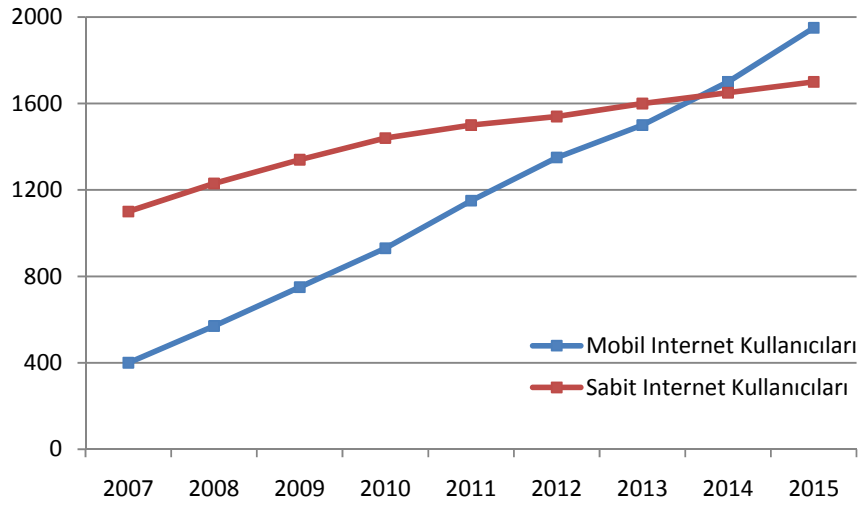
Grafik 2.7: Data trafiğinin toplam trafik içindeki payı

Mobil trafiğin özellikle USB modem ve akıllı telefonların da etkisiyle artması beklenmektedir. Gelişmiş ülkelerdeki basit cep telefonlarının kullanımının %90'lardan 2015'te %68 lere düşmesi beklenmektedir. Gelişmiş ülkelerde 2015'te USB modemlerin %15 ve akıllı telefonların %17 civarında bir kullanıcısının olması beklenmektedir. Gelişmekte olan ülkelerde ise USB modem ve akıllı telefonların %5'erlik kullanıcı oranlarına ulaşacağı düşünülmektedir (Grafik 2.8) (The Information Society Statistical Profiles 2009).



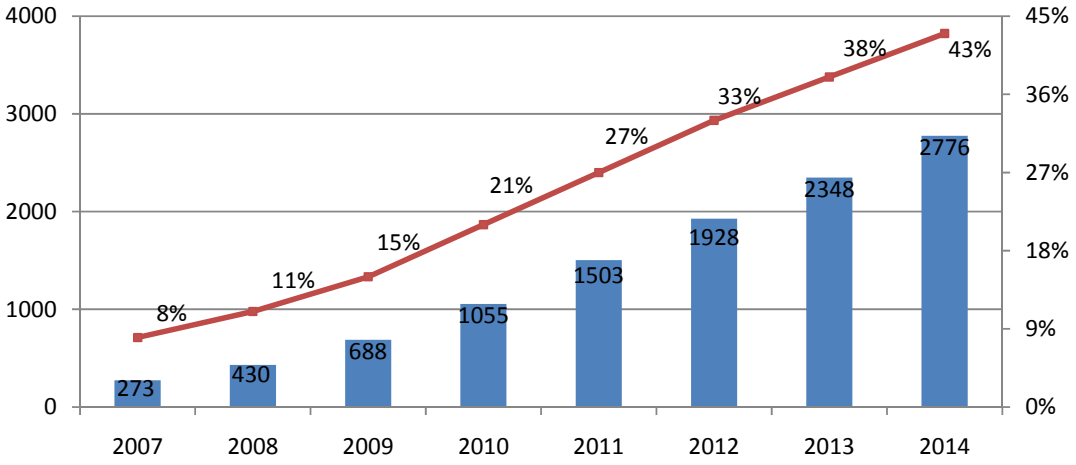
Grafik 2.8: Mobil cihaz kullanım oranları

ABD'li yatırım şirketi Morgan Stanley'in Nisan 2010'da yayınladığı rapora göre, 2013'te mobil internet kullanıcılarının, sabit internet kullanıcılarını geçmesi beklenmektedir (Grafik 2.9) (Meeker, Devitt and Wu 2010).



Grafik 2.9: Mobil ve sabit internet kullanıcıları (milyon kişi)

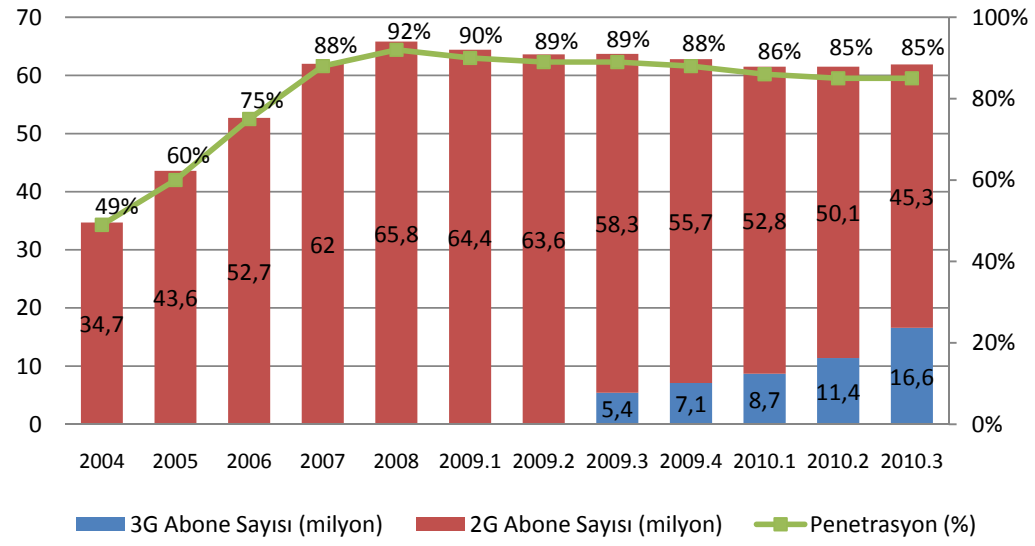
Yine, Morgan Stanley raporuna göre, tüm dünyadaki üçüncü nesil abone sayısı 2007'deki % 8'lik orandan 2014'te % 43'lük bir abone sayısına ulaşacaktır (Grafik 2.10) (Meeker, Devitt and Wu 2010).



Grafik 2.10: Üçüncü nesil (3G) abone sayıları ve penetrasyonu

Informa Telecoms and Media adlı araştırma firmasının Haziran 2010'da yayınladığı Mobil Internet Trafiği : İstatistikler ve Küresel Kullanım Trendleri başlıklı raporuna göre de 2009 yılında tüm dünyada 666 milyon kişi aktif olarak mobil Internet'i kullanmış, bu rakamın 2010 yılı sonu itibariyle de 878 milyon kişiye ulaşacağı öngörülmüştür. Bir başka deyişle yaklaşık 3.9 milyar mobil abone sayının dörtte birinin 2010 yılı sonu itibariyle aktif olarak mobil Internet deneyimine sahip olması beklenmektedir (Hobbs 2010).

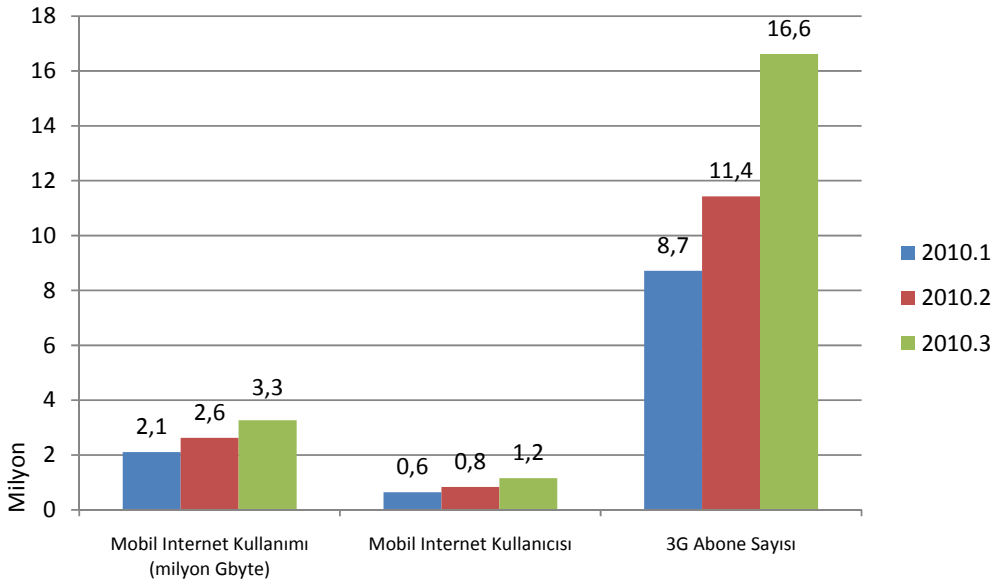
Türkiye'de ise, Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Stratejiler Dairesi Başkanlığı'nın Kasım 2010'da yayınladığı Türkiye Elektronik Haberleşme Sektörü 2010 Yılı 3. Çeyrek Üç Aylık Pazar Verileri Raporu'na göre Eylül 2010 itibariyle %85 penetrasyon oranına karşılık gelen toplam 61,9 milyon mobil abone bulunmaktadır. Bununla birlikte; Temmuz 2009'da 3G hizmet sunumunun başlamasıyla Eylül 2010 itibariyle 3G abone sayısı 16,6 milyonu aşmıştır (Grafik 2.11) (Bilgi Teknolojileri ve İletişim Kurumu 2010).



Grafik 2.11: Türkiye'deki mobil abone pazarı

Aynı rapora göre 2010 birinci çeyrekte 8,7 milyon olan 3G abone sayısı 2010 üçüncü çeyrekte 16,6 milyona ulaşırken, 3G hizmetiyle birlikte mobil internet hizmeti alan kullanıcı sayısı da aynı dönemler için 640.580'den 1.158.866'ya yükselmiştir (Grafik

2.12). Bu dönemde toplam mobil internet kullanım miktarı ise 3274 TByte olarak gerçekleşmiştir (Bilgi Teknolojileri ve İletişim Kurumu 2010).



Grafik 2.12: Türkiye'de mobil internet kullanımı

2.5 UMTS ŞEBEKE MİMARİSİ

UMTS şebeke mimarisi temel olarak Telsiz Erişim Şebekesi (UTRAN – Universal Terrestrial Radio Access Network), Çekirdek Şebeke (CN – Core Network) ve kullanıcı terminali (UE – User Equipment) olmak üzere üç alt sistemden oluşmaktadır. Telsiz erişim şebekesi ve Çekirdek Şebeke birbirlerine 'Iu' denilen bir arabirimle bağlantı halindedir. 'Iu' arabirimi Devre Anahtarlamalı (Circuit Switched) veya Paket Anahtarlamalı (Packet Switched) olabilir.

Şebeke birimlerinin içerdikleri elemanlar şu şekilde sıralanabilir.

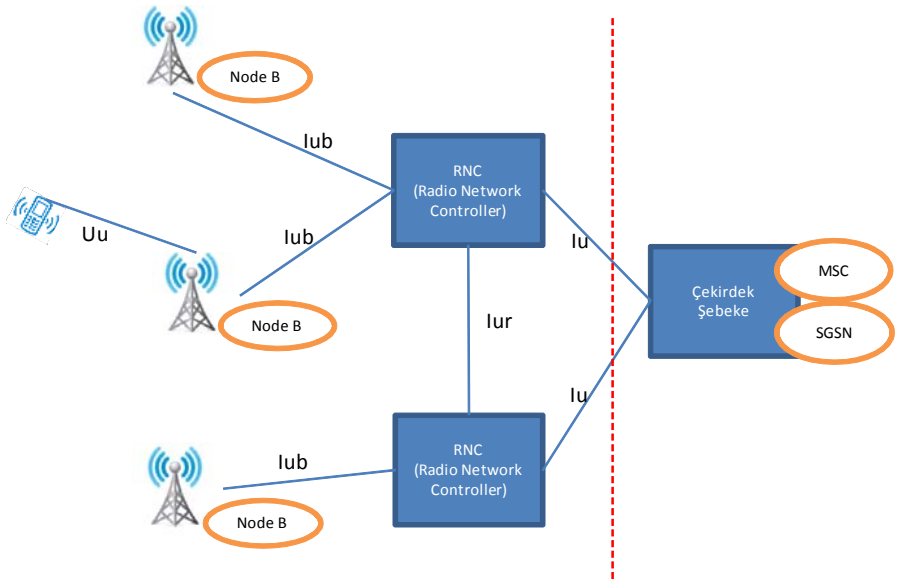
- UTRAN (UMTS Terrestrial Radio Access Network - UMTS Karasal Telsiz Erişim Şebekesi): Node-B ve RNC (Radio Network Controller)'den oluşmaktadır. Node-B GSM'deki baz istasyonlarına (BTS - Base Transceiver Station)'e eş değerdir. RNC ise GSM'deki BSC (Base Station Controller)'e eş değerdir.

- Çekirdek Şebeke (Core Network): GSM'deki NSS (Network Switching Subsystem)'e eş değerdir.

2.5.1 UTRAN

UMTS'de farklı bir telsiz arayüzü kullanıldığı için UTRAN adında yeni bir telsiz erişim şebekesi tanımlanmıştır. UTRAN, bir veya daha fazla RNS'ten oluşmaktadır. Her bir RNS ise bir adet RNC ve bu RNC'ye bağlı Node-B'lerden oluşmaktadır. UTRAN telsiz arayüzünü diğer şebekelerden farklı kılan yönü, 2 adet farklı, fakat birbirini tamamlayan telsiz erişim modu içermesidir. Bunlar, UTRA FDD (Frequency Division Duplex) ve UTRA TDD (Time Division Duplex)'dir (Holma and Toskala 2004).

FDD modu tamamen WCDMA tabanlıdır. TDD modunda ise ilave olarak bir TDMA kısmı mevcuttur. UMTS, 2. nesil sistemlerden farklı olarak "Iu", "IuR", "IuB" ve "Uu" isimli dört yeni arabirim tanımlamaktadır. Iu arayüzü telsiz erişim şebekesi (UTRAN) ile Çekirdek Şebeke (CN) arasındaki bağlantıyı, IuR arayüzü RNC'ler arası bağlantıyı, IuB ise Node-B ile RNC arasındaki bağlantıyı sağlamaktadır. Uu arayüzü de kullanıcı terminaliyle Node-B arasında bağlantı sağlamaktadır. Diğer arayüzlerin aksine IuR arayüzünün GSM'de benzer bir karşılığı yoktur. Iu, Iub ve Iur arayüzleri mantıksal birimler olup ATM transmisyon prensiplerine göre çalışmaktadırlar (Holma and Toskala a.g.e). Şekil 2.2 bu arayüzleri göstermektedir.



Şekil 2.2: UTRAN arayüzleri

2.5.1.1 Node-B

UMTS baz istasyonu olarak da adlandırılmaktadır. Node-B, WCDMA erişim tekniği kullanarak kullanıcı terminaliyle UMTS şebekesi arasında hava arayüzü bağlantısı sağlayan fiziksel ünitedir. 2. Nesil sistemlerle UMTS'nin en büyük farkı bu noktada ortaya çıkmaktadır. Node-B temel olarak İleri Hata Düzeltme (FEC), WCDMA spreading/despreading ve modülasyon (QPSK) işlevlerini yerine getirerek kullanıcıdan gelen ve kullanıcıya giden bilginin dönüşümünü gerçekleştirir. Bir veya birden fazla Node-B, bir Iub arayüzü üzerinden bir RNC'ye bağlanır. Her Node-B bir veya birkaç hücreye hizmet verebilmektedir. GSM'in aksine UMTS'de, FDD modunda iken Node-B'ler arası bir senkronizasyona ihtiyaç yoktur. Bir Node-B hem FDD hem TDD modunu destekleyebilmektedir (Holma and Toskala 2004).

2.5.1.2 RNC (radio network controller – radyo şebeke kontrolörü)

GSM'deki Baz İstasyon Kontrolörü'yle (BSC) eş değer fonksiyonlara sahiptir. Her RNC bir veya bir çok Node-B'yi kontrol eder. RNC'ler, Iu arabirimi yoluyla çekirdek şebekeyle bağlantı halindedirler. Devre anahtarlamalı Iu arabirimi ile ses, Paket anahtarlamalı Iu arabirimi ile de veri iletimi gerçekleştirilir. RNC, kullanıcı terminaliyle sinyalleşmeyi gerektiren 'handover' kararları ile tüm Radyo Şebeke Altsistem'in (RNS) merkezi işlem ve bakımından sorumludur. UTRAN'ın bağımsız olarak radyo kaynak yönetimi yapmasına olanak tanır. Iu, Iub ve Iur arayüzleri arasındaki protokol değişimini idare eder (Holma and Toskala 2004).

2.5.1.3 RNS (radio network subsystem - radyo şebeke altsistemi)

Bir adet RNC ve bu RNC'ye bağlı Node-B'lerden oluşmaktadır. Her RNS kendi hücre setinin kaynaklarını yönetmekle sorumludur. GSM'in aksine RNS, mobilite yönetimi (handover algılama ve kontrol) ve radyo kaynak yönetimi (bağlantı kurulması, kapatılması ve paketlerin transferi) ile tamamıyla sorumludur.

2.5.1.4 UE (user equipment - kullanıcı terminali)

GSM'deki mobil istasyon (MS) ile aynı prensiplere dayanmakta olup Mobil Ekipman (ME) ve UMTS Abone Kimlik Modülü (USIM) olmak üzere iki parçadan oluşur. Mobil

ekipman istasyonla radyo dalga alışverişini yaparken USIM adlı smart kart ise kullanıcı abonelik ve kişisel bilgilerini tutmaktadır.

Şekil 2.3: Kullanıcı terminali

2.5.2 Çekirdek Şebeke

UMTS çekirdek şebekesi, devre ve paket anahtarlamalı trafiğin entegre bir şekilde kullanıldığı, evrimleşmiş GSM çekirdek şebekesine dayanmaktadır. Çekirdek şebekede bir Devre Anahtarlı (CS) etki alanı bir de Paket Anahtarlı (PS) etki alanı vardır. Bu iki alan örtüşmektedir ve bazı ortak elemanlar içermektedirler. Çekirdek şebeke elemanları temel olarak, HLR (Home Location Register – Abone Kayıt Kütüğü), MSC/VLR (Mobile Switching Center – Mobil Anahtarlama Merkezi / Visitor Location Register – Ziyaretçi Kayıt Kütüğü), Gateway MSC (Mobil Anahtarlama Merkezi Ağ Geçidi), SGSN (Serving GPRS Support Node – GPRS Destek Düğümü Sunucusu) ve GGSN (Gateway GPRS Support Node – GPRS Geçit Destek Düğümü)'dir. Çekirdek şebeke genel olarak, şebeke içi ve şebekeler arası ses ve veri iletimi için gerekli anahtarlama ve yönlendirme işlemlerini yürütmektedir. Çekirdek şebekedeki asıl değişiklik paket anahtarlamaya geçiş ve IP protokolünü tam olarak desteklemesidir. Zaman-kritik yani gerçek zamanlı olması gereken işlemler olan ses ve görüntü servisleri MSC GMSC ve VLR üzerinden devre anahtarlama tekniği kullanılarak yürütülürken, mesajlaşma ve bilgilendirme gibi zaman kritik olmayan veri iletim hizmetleri ise SGSN ve GGSN üzerinden paket anahtarlama ile gerçekleştirilmektedir. HLR, EIR, AuC gibi şebeke elemanları ise her iki etki alanına da hizmet vermektedir.

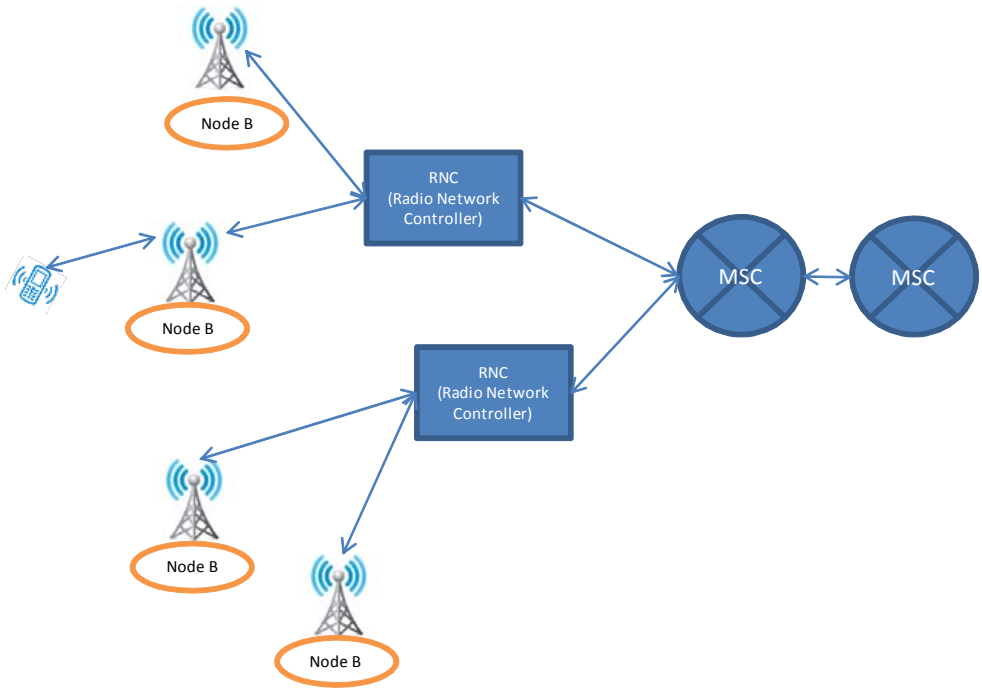
2.5.2.1 MSC (mobile switching center – mobil anahtarlama merkezi) ve MSS (mobile switching center server – mobil anahtarlama merkezi sunucusu)

MSC sabit şebekenin santrali ile aynı görevi yapmaktadır. Sabit şebekeden farklı olarak, birbirlerine kablo ile bağlı olan kullanıcılar yerine coğrafi olarak özgür dolaşan mobil

kullanıcıların görüşmelerine imkan sağlamaktadır. MSC, mobil istasyonlardan gelen ve mobil istasyonlara doğru olan tüm devre anahtarlamalı hizmetleri yürütmektedir (Dinçkan 2006).

MSC'nin görevleri aşağıda belirtilmiştir;

• Diğer anahtarlama merkezlerine gerektiğinde bağlantı kurmak
• Diğer şebekelere bağlantı kurmak (sabit şebeke ve mobil şebeke)
• Devre anahtarlamalı hizmetler için serbest hareketlilik yönetimi (MM) sağlamak
• Servis hizmetlerinin yüklenmesini yapmak
• Kullanıcıların VLR'a kaydedilmesi
• Dahili veya harici aktarmalarda Node-B'ler arası geçişi sağlamak.
• Mobil şebekeyle sabit şebekenin arasında olabilecek yankıları gidermek
• Verilerin modem üstünden PSTN şebekelerine uyumunu sağlamak
• Bağlantı ve sinyallerin idare edilmesini sağlamak
• Sistem verileri, sistem kayıtları, ücretlendirme verilerinin kayıt edilmesini sağlamak

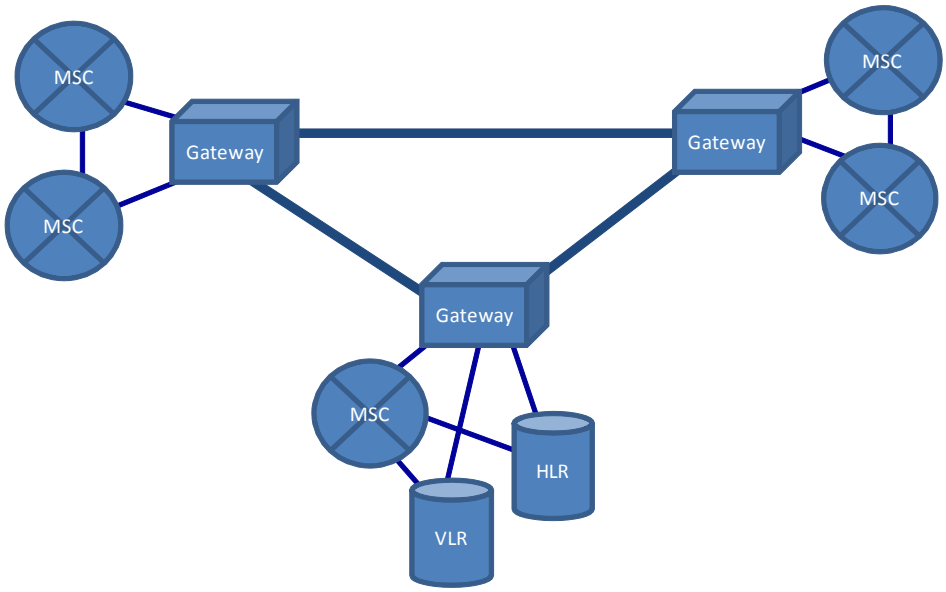


Şekil 2.4: Mobil Anahtarlama Merkezi

MSS, üçüncü nesil şebekeler için özelleştirilmiş mobil şebeke santralidir. Üçüncü nesil şebekeler; Control ve User plane olarak birbirinden ayrılmıştır. MSS control ve user plane'in birbirinden ayrılmasını sağlar. Böylece network elemanlarının daha optimize şekilde network içinde yerleşmesine olanak sağlanır (Holma and Toskala 2006).

2.5.2.2 GMSC (gateway msc - mobil anahtarlama merkezi ağ geçidi)

Gateway MSC (GMSC) UMTS şebekesinin harici devre anahtarlamalı şebekelere (PSTN gibi) bağlantısının yapıldığı noktada anahtar görevini yerine getirmektedir. Tüm gelen devre anahtarlamalı bağlantılar GMSC üzerinden diğer devre anahtarlı şebekelere aktarılır. GMSC'ler MSC'lere servis veren daha üst seviye santrallerdir. Farklı yerlerdeki MSC'ler ve HLR gibi platformlar birbirlerine GMSC'ler üzerinden bağlıdır. GMSC olmazsa bütün network elemanları birbirleri ile bağlanmalıdır. Bu nedenler network büyüdükçe bağlantı sayısı ve sinyalleşme yönetimi karmaşık hale geldiği için GMSC'ler tercih edilmektedir (Dinçkan 2006).

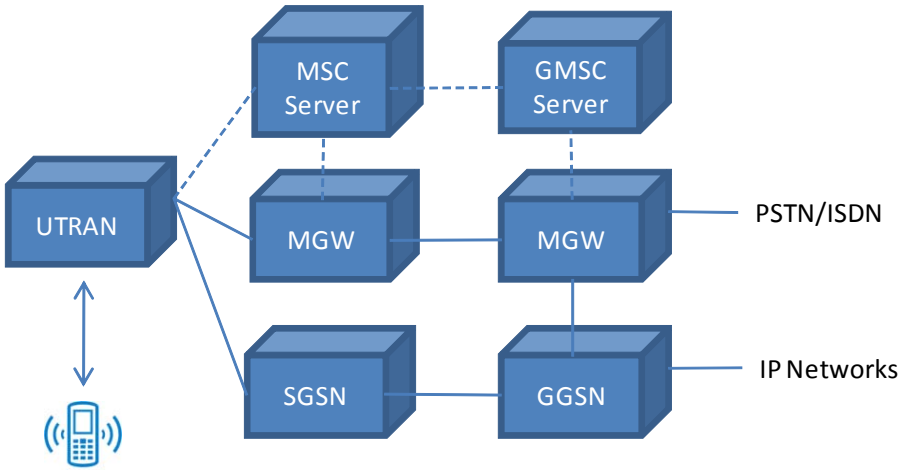


Şekil 2.5: Gateway MSC bağlantısı

2.5.2.3 MGW (media gateway – medya geçidi)

MGW, UMTS şebekelerinde trafik yönetimini sağlayan platformdur. Media Gateway, devre anahtarlamalı aramaları, ATM (Asynchronous Transfer Mode) ve IP (Internet

Protocol) gibi protokollere dönüştürerek çoklu medya iletişimine olanak sağlar. MGW, lokal anahtarlama özelliği sayesinde lokal şebeke trafiği üzerindeki iletim maliyetlerini de aşağıya çekmektedir (Dinçkan 2006).



Şekil 2.6: MGW bağlantısı

2.5.2.4 HLR (home location register – abone kayıt kütüğü)

Abonenin ve kullandığı servislerin bilgilerinin kalıcı olarak tutulduğu veritabanı ve buna ev sahipliği yapan platformdur. Yani mobil abonelerin yönetiminin yapıldığı veritabanıdır. Ayrıca, abonenin o an hangi MSC'den servis aldığı bilgisini güncel olarak tutar. İçinde tuttuğu abone ve yer bilgisi sayesinde çağrıların fiyatlanması ile çağrıların abonenin kayıtlı olduğu MSC veya SGSN tarafına yönlendirilmesi işlemleri gerçekleştirilmektedir. Bir operatöre ait bir şebekede abone sayısına, şebeke yapısına ve ekipmanların kapasitesine göre bir veya birkaç tane HLR bulunabilir (Telsim Teknik Eğitim Merkezi 2001).

2.5.2.5 VLR (visitor location register – ziyaretçi kayıt kütüğü)

Bir mobil abonenin bir MSC alanı içindeki dolaşımı ise VLR yoluyla kontrol edilmektedir. VLR, MSC'nin içerisinde yeralan bir veritabanıdır. VLR mobil kullanıcıların geçici verilerini kayıt etmekle görevlidir. Sürekli dolaşım halinde bulunan mobil abonelerin yönetimi, serbest hareketlilik yönetimi ile sağlanmaktadır. Serbest hareketlilik yönetimi mobil istasyonların şebeke içerisindeki yerlerini ilgili

veritabanlarında doğru olarak tutmak üzere kullanılan bir prosedürdür. Bu geçici veriler bir yandan serbest hareketlilik yönetimi için, diğer yandan da güvenlik fonksiyonları için kullanılmaktadır. MSC ile VLR birbirleriyle yoğun şekilde veri alış verişi yaptığından şebekede bulunan her MSC'de kendine ait bir VLR bulunmaktadır. Böylece MSC ve VLR bütünleşik biçimde hizmet vermektedir.VLR'nin gerektiğinde HLR'da kayıtlı bilgilere ulaşabilmesi için VLR ile HLR arasında bir bağlantı vardır.
MSC'den servis alan abonelerin bilgilerini ve LAC (Location Area Code) bazında konumlarını güncel olarak tutar. Aşağıda VLR üzerinde kayıt edilen önemli veriler sıralanmıştır (Telsim Teknik Eğitim Merkezi 2001).

• Mobil abone geçici kimliği (TMSI)
• Konum alanı belirteci (LAI)
• Doğrulama merkezinden alınan güvenlik verileri (RAND/ SRES ve Kc)
• Desteklenen servislerin verileri
• Cep telefonunun durum bilgisi (aktif, pasif, meşgul)
• Mobil istasyon uluslararası sayısal servis şebekesi (MSISDN) numarası
• Uluslararası mobil abone numarası (IMSI numarası)
• Mobil istasyon dolaşım numarası (MSRN)

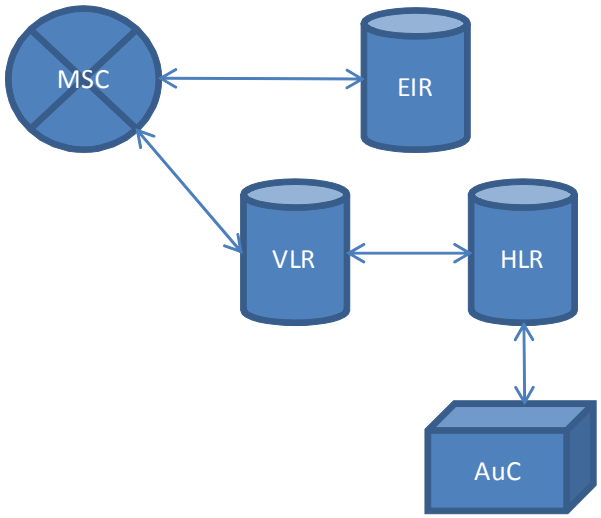
2.5.2.6 AuC (authentication center – doğrulama merkezi)

Doğrulama Merkezi'nin görevi kullanıcıya ait belirli bilgilerin doğrulanmasıdır. Bunlar, parola, parola onaylanması, şifreleme vs. gibi bilgilerdir. Abonenin şebekeye girişinde doğrulanması için doğrulama merkezi (AuC), HLR ile irtibatlandırılmıştır. AuC'nin işlevi, güvenlik nedeni ile kullanılan doğrulama parametrelerini ve şifreleme anahtarlarını HLR'ye ulaştırmaktır (Telsim Teknik Eğitim Merkezi 2001).

2.5.2.7 EIR (equipment identity register – mobil ekipman tanımlama kütüğü)

Mobil Ekipman Tanımlama Kütüğü, kullanıcı bilgilerinin dışında olan cihaz bilgileri, üretici bilgileri, IMEI (International Mobile Station Equipment Identity) gibi bilgileri tutar. Çalıntı ve şüpheli cihazlar bu veritabanı üzerinden takip edilerek bulunur. IMEI, her cep telefonunu uluslararası bazda tanımlayan bir numaradır ve her IMEI numarası

bir tek cihazı tanımlar. IMEI, üretici tarafından cihaza atanır ve GSM operatörü tarafından EIR veritabanına kaydedilir (Telsim Teknik Eğitim Merkezi 2001).



Şekil 2.7: HLR, VLR, EIR ve AUC yapısı

2.5.2.8 SGSN (serving gprs support node – gprs destek düğümü sunucusu)

MSC/VLR'a benzer bir fonksiyona sahip olup farkı, paket anahtarlamalı servisler için kullanılmasıdır. SGSN bünyesinde SLR isimli bir veritabanı bulunmakta ve abone ile ilgili bilgiler bu veritabanında tutulmaktadır.

SGSN'in fonksiyonları aşağıdaki gibidir (Dinçkan 2006):

• Belirli bir alan içerisindeki bütün mobil istasyonlara hizmet verir.
• Konum yönetimi yapar. Mobil istasyonun yer bilgisini tutar.
• Doğrulama kontrolü yapar. Mobil istasyonun GPRS/EDGE/UMTS/HSPA hizmetine erişme hakkı olup olmadığını kontrol eder.
• Mobil istasyon ile GPRS/EDGE/UMTS/HSPA şebekesi arasında mantıksal bağlantı kurulmasını sağlar.
• Sisteme bağlanma, kopma, yönlendirme alanı güncellemesi gibi serbest hareketlilik yönetimi fonksiyonlarını yerine getirir.

• Oturumun açılması/sonlandırılması, PDP (Paket veri protokolü) oturum etkinleştirmesi ve iptali gibi oturum yönetimi fonksiyonlarını yerine getirir.
• Paket kontrol ünitesinden gelen veriyi GGSN'e gönderme gibi paket işleme fonksiyonlarını yerine getirir.
• SGSN'ler arası yönlendirme alanı güncellemelerini kontrol eder
• Ücretlendirme verisi toplama görevini yerine getirir
• Performans ve hata yönetimi gerçekleştirir. Transmisyon anında ortaya çıkan problemlerin tespitini yapar.

2.5.2.9 GGSN (gateway gprs support node – gprs geçit destek düğümü)

GGSN'ler GMSC gibi UMTS şebekesinin harici paket anahtarlı şebekelere (Internet gibi) çıkışını sağlamaktadır. GGSN bir yönlendirici gibi davranmakta ve trafik kontrolü yapmaktadır. GGSN aynı zamanda mobil istasyonun izlenmesini sağlamaktadır. Internet tarafında sadece GGSN görülmekte ve mobil istasyonun hareketliliği iletişimin sürekliliğini etkilememektedir.

GGSN, GSM şebekesinde bulunan ve başka devre anahtarlamalı sistemlere bağlantıyı sağlayan GMSC'ye karşılık gelmekte ve paket anahtarlamalı dış şebekelere bağlantıyı sağlamaktadır.

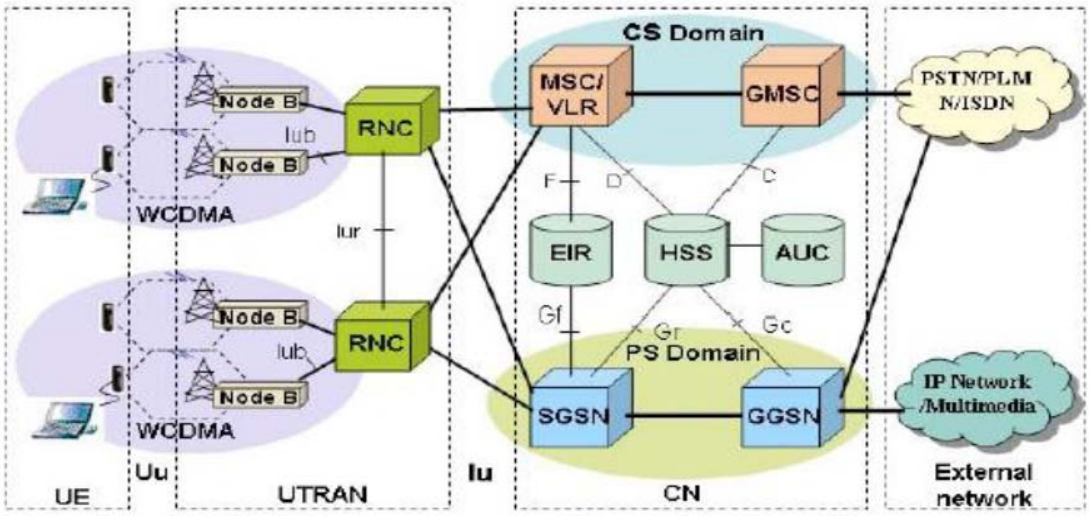
GGSN Fonksiyonları aşağıdaki gibidir (Dinçkan 2006):

• SGSN'den gelen veriyi dış veri şebekelerine gönderme fonksiyonunu gerçekleştirir.
• PDP oturum etkinleştirmesi ve iptali, belirli bir SGSN'ye bağlantı kurulması veya bırakılması gibi oturum yönetimi fonksiyonlarını yerine getirir.
• Şebekeye giren yeni mobil istasyonlar için DNS ve IP adresi atamalarını yapar.
• Ücretlendirme verisi toplama görevini yerine getirir.
• Şebekenin kendi bulunduğu bölüm için trafik ölçümü yapar.
• Veri transferi sırasında oluşan problemleri tespit eder. Hata yönetimi gerçekleştirir.

2.5.2.10 PCU (packet control unit – paket kontrol ünitesi)

PCU, GPRS/EDGE/UMTS datasını SGSN'e gönderen birimdir. PCU'nun kalite, paket büyüklüğü, format kontrolü, kanal erişim kontrolü, trafik ve güç kontrolü, paket veri birimlerinin parçalanması ve yeniden birleştirilmesi gibi işlevleri vardır. SGSN-PCU bağlantısı Frame Relay veya IP ile sağlanır. BSC'den gelen tüm data call'lar için bu bağlantı ortaktır, yani her bir bağlantı için sabit/garanti iletim hızı yoktur. PCU'lar ayrı bir ekipman olabileceği gibi PCU'nun fonksiyonları RNC içinde PCU kartları ile de sağlanabilir (Dinçkan 2006).

Aşağıdaki şekilde örnek bir UMTS topolojisi gösterilmektedir.



Şekil 2.8: Örnek bir UMTS Topolojisi
Kaynak: Holma and Toskala, 2004

3. GÜVENLİK

Birbirinden bağımsız katmanlardan oluşan üçüncü nesil şebekelerin, paket anahtarlamalı mimarinin de doğası gereği geleneksel telekomünikasyon şebekelerine göre güvenlik tehditlerine karşı daha savunmasız olacağı söylenebilir. Hem bireysel ve kurumsal abonelerin kendilerini güvende hissetmesi ve mobil operatörlerin ticari ve maddi kaygıları, hem de düzenleyici otoritelerin kullanıcı mahremiyeti ve haklarını koruma çabası gibi nedenlerden dolayı üçüncü nesil şebekelerde güvenlik konusu daha çok önem kazanmıştır. Ayrıca mobil ortamlarda verilen hizmetlerin sayısının da her geçen gün artması ve bu ortamların kullanımının da giderek yaygınlaşması, saldırganlar için bu hizmetlerin verildigi sistemleri birer cazibe merkezi haline getirmektedir. Güvenligi tehdit eden unsurlar sadece mobil ortamda yapılan saldırılarla da sınırlı degildir. İnsan hataları, yangın, sel, deprem, terör saldırıları, sabotaj gibi istenmeyen olaylar veya dogal felaketler sonucunda da sistemler tamamen ya da kısmen zarar görebilmektedir.

Çalışmanın bu bölümünde bir önceki bölümde açıklanmış olan şebeke mimari yapısı üzerindeki olası tehditler ve saldırı türleri araştırılmış, üçüncü nesil şebekelerin zayıf yönleri ortaya konularak güvenliğin sağlanmasına yönelik çözüm önerileri getirilmiştir. Ayrıca, üçüncü nesil şebekelerde uygulanabilecek güvenlikle ilgili standartlara ve Türkiye'de elektronik haberleşme şebekelerinde güvenlikle ilgili yapılan düzenlemelere değinilerek atılması gerekecek muhtemel adımlara ilişkin değerlendirmelere de yer verilmiştir.

3.1 GÜVENLİK KAVRAMI VE PRENSİPLERİ

Güvenlik genel olarak bilginin bir varlık olarak her türlü tehditten korunması olarak tanımlanabilir. Bilgi ve iletişim teknolojileri de dikkate alınarak güvenlik, bilgi ve bilginin işlenmesi, aktarılması, kullanılması ve depolanmasına aracılık eden her türlü teknolojik ortamın, istenmeyen, yetkisiz kişilerce erişilmesi, değiştirilmesi, bozulması, yok edilmesi gibi her türlü tehditi önleme olarak tanımlanabilir.

Güvenlik kavramının bir çok boyutu olmasına karşın, temel olarak üç prensipten söz edilebilir: Bunlar, gizlilik, bütünlük ve sürekliliktir.

3.1.1 Gizlilik

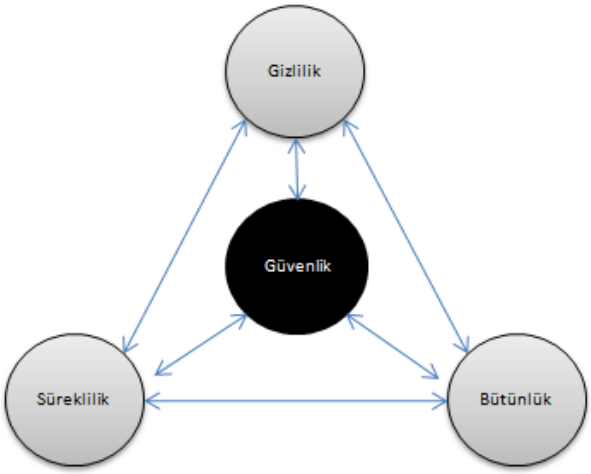
Gizlilik, bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik, hem kalıcı ortamlarda (disk, teyp, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler. Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir (Yıldız 2007).

3.1.2 Bütünlük

Bütünlük, kısaca veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır (Yıldız a.g.e.).

3.1.3 Süreklilik

Süreklilik prensibi, bir sistemi kendisinden beklenen işleri gerçekleştirirken, o sistemde hedeflenen performans hedefini düşürücü tehditlere karşı korumayı ifade eder. Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dahilinde, ilgili kaynağa zamanında ve güvenilir bir şekilde ulaşabilirler. Sistem sürekliliği, yalnızca kötü amaçlı bir "hacker"ın, sistem başarımını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Yazılım hataları, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir (Pro-G Bilişim Güvenliği 2003).



Şekil 3.1: Temel güvenlik prensipleri

Aşağıda, yukarıdaki üç temel prensibe ek olarak ikinci planda değerlendirilebilecek izlenebilirlik, kimlik sınaması, güvenilirlik ve inkâr edememe prensiplerinden bahsedilmiştir.

3.1.4 İzlenebilirlik

Bu hizmetin hedefi sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak göndermek gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin örüntülerine rastlanabilir ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktiviteler tespit edilebilir (Pro-G Bilişim Güvenliği 2003).

3.1.5 Kimlik Sınaması

Kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Örneğin bir sisteme erişirken bir parola girmek kimlik sınaması çerçevesinde değerlendirilebilir. Kimlik sınaması, fiziksel olarak sistemlere erişim için de çok önemli bir hizmet haline gelmiştir (Vural 2007). Akıllı kart ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri fiziksel erişimlerde yaygın olarak kullanılmaktadır.

3.1.6 Güvenilirlik

Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir (Pro-G Bilişim Güvenliği 2003).

3.1.7 İnkâr Edememe

Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır.

Bu prensipler, zaman içinde sistemlere karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir prensip, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir (Yıldız 2007).

3.2 TEHDİTLER

Tehdit, bir sistemin zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli neden, olarak tanımlanabilir. Her tehdidin bir kaynağı ve bu kaynağın yararlandığı sistemdeki bir "güvenlik boşluğu" yani zafiyet vardır (Vural 2007).

Tehditler, tehdit kaynağı açısından bakıldığında iki gruba ayrılarak incelenebilir:

3.2.1 İnsan Kaynaklı Tehditler

Bu tür tehditler de kendi içinde iki alt gruba ayrılabilir:

a. Kötü niyet olmayan davranışlar sonucu oluşanlar: Bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklardır (Vural 2007).

b. Kötü niyetli davranışlar sonucu oluşanlar: Sisteme zarar verme amacıyla, sisteme yönelik olarak yapılacak tüm kötü niyetli davranışlardır. Bu tür tehditlerde, tehdit kaynağı, sistemde bulunan güvenlik boşluklarından yararlanır (Vural 2007).

3.2.2 Doğa Kaynaklı Tehditler

Bu tür tehditler genellikle önceden tespit edilemezler ve gerçekleşmeleri de büyük bir olasılıkla engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak verilebilir (Vural 2007).

Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre;

a. İç tehditler: Kurum içinden kuruma yönelik yapılabilecek saldırılar,

b. Dış Tehditler: Kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanabilir (Pro-G Bilişim Güvenliği 2003).

3.3 ZAFİYETLER

Güvenlik zafiyeti, herhangibir sistem üzerindeki yazılım ve donanımdan kaynaklanan ya da sistemin işletim kuralları ve/veya yönergelerinde yer alan açık noktalar ve zayıf kalmış yönlerdir. Bir güvenlik boşluğu sayesinde bir saldırgan, sistem kaynaklarına yetkisiz olarak erişebilir. Bir güvenlik duvarı üzerinde açık unutulmuş bir erişim noktası, şebeke elemanlarının bulunduğu lokasyona giriş çıkışlarda fiziksel erişim denetimi eksikliği, sunucular üzerinde belli bir politikaya dayandırılmadan belirlenen parolalar güvenlik boşluklarına örnek olarak verilebilirler. Yazılım ya da donanımdan kaynaklanan güvenlik boşlukları, üreticisi ya da başka bir kaynak tarafından geliştirilen bir "yama" yardımıyla kapatılmalı ve eldeki yazılım ve donanımların üreticilerinin yayınladığı yama listeleri sürekli olarak takip edilmeli, çıkan yamalar kontrollü bir şekilde sistemlere uygulanmalıdır.

Tehditler, sistemlerdeki güvenlik zafiyetlerine yönelik olarak tanımlanırlar. Yani bir güvenlik zafiyeti ortadan kaldırılırsa ya da bir "yama" yardımıyla düzeltilirse, söz konusu tehdit ortadan kaldırılmış olur. Bir tehdidin oluşması için bir güvenlik zafiyetine ve bu güvenlik zafiyetinden yararlanabilecek bir tehdit kaynağına ihtiyaç vardır.

3.4 RİSK

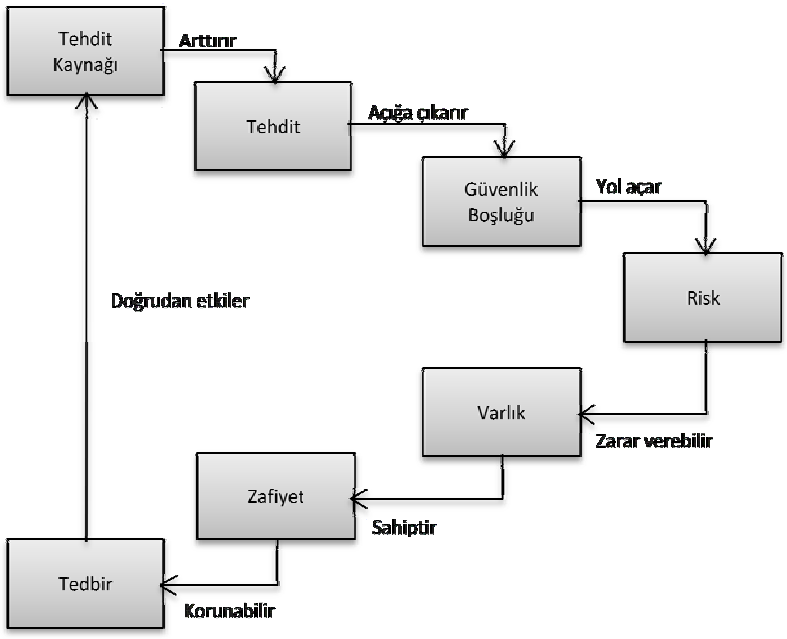
Bir tehdit kaynağının, bir sistemdeki güvenlik zafiyetinden yararlanarak sisteme yetkisiz erişimde bulunması olasılığı, bu tehdidin riski olarak ifade edilir. Tehdit kaynaklarının ya da güvenlik zafiyetlerinin azaltılması, tehdide ait riskleri de aynı oranlarda azaltacaktır (Kamu Bilişim Platformu 2006). Tablo 3.1'de tehdit kaynağı, güvenlik zafiyeti ve risk ilişkisine örnekler verilmiştir.

Tablo 3.1: Tehdit kaynağı, güvenlik zafiyeti ve risk ilişkisine ait örnekler

Tehdit Kaynağı	Etkileyebileceği Güvenlik Boşluğu	Oluşan Risk
Virüs	Antivirüs yazılımının eksikliği	Virüs bulaşması
Hacker	Sunucu bilgisayar üzerinde çalışan güçlü hizmet programları	Gizli bilgilere yetkisiz erişim hakkının elde edilmesi
Kullanıcılar	İşletim sisteminde yanlış ayarlanmış bir parametre	Sistemin çalışamaz duruma gelmesi
Yangın	Yangın söndürme cihazının eksikliği	Bina ve sistemlerin zarar görmesi
Çalışanlar	Erişim denetim mekanizmalarının yetersizliği	Görev-kritik bilgilerin zarar görmesi
İş ortağı olan bir firmanın yetkilisi	Erişim denetim mekanizmalarının yetersizliği	Ticari sırların çalınması
Saldırgan	Kötü yazılmış bilgisayar programları	"tampon taşması" hatasının alınması
Kötü Niyetli Ziyaretçi	Güvenlik görevlisinin olmayışı	Kıymetli cihaz ve bilgilerin fiziksel olarak çalınması
Çalışan	Tutulan kayıtlardaki yetersizlik	Veri işleme programına verilen giriş verileri ve çıkış olarak elde edilen veriler üzerinde değişiklikler yapılması
Saldırgan	Güvenlik duvarının ayarlarının iyi yapılmamış olması	Bir "hizmet durdurma saldırısının" gerçekleşmesi

Potansiyel riskler, tedbirler yardımı ile azaltılabilirler. Bir tedbir, bir güvenlik zafiyetini ortadan kaldırır ya da bir tehdit kaynağının bir güvenlik zafiyetini kullanması riskini azaltır. Tedbirler, yazılım, donanım ya da geliştirilen bir kullanım yönergesi şeklinde oluşturulabilir. Tedbirlere, sağlam bir parola yönetim politikası, bir güvenlik görevlisi, bir işletim sistemi üzerinde akıllı kartlara dayalı bir erişim denetim mekanizması,

güvenlik konusunda kullanıcıların eğitimi gibi örnekler verilebilir. Şekil-3.2'de yukarıda bahsedilen kavramların birbirleri ile etkileşimleri gösterilmektedir.



Şekil 3.2: Temel güvenlik kavramlarının birbirleri ile olan ilişkileri

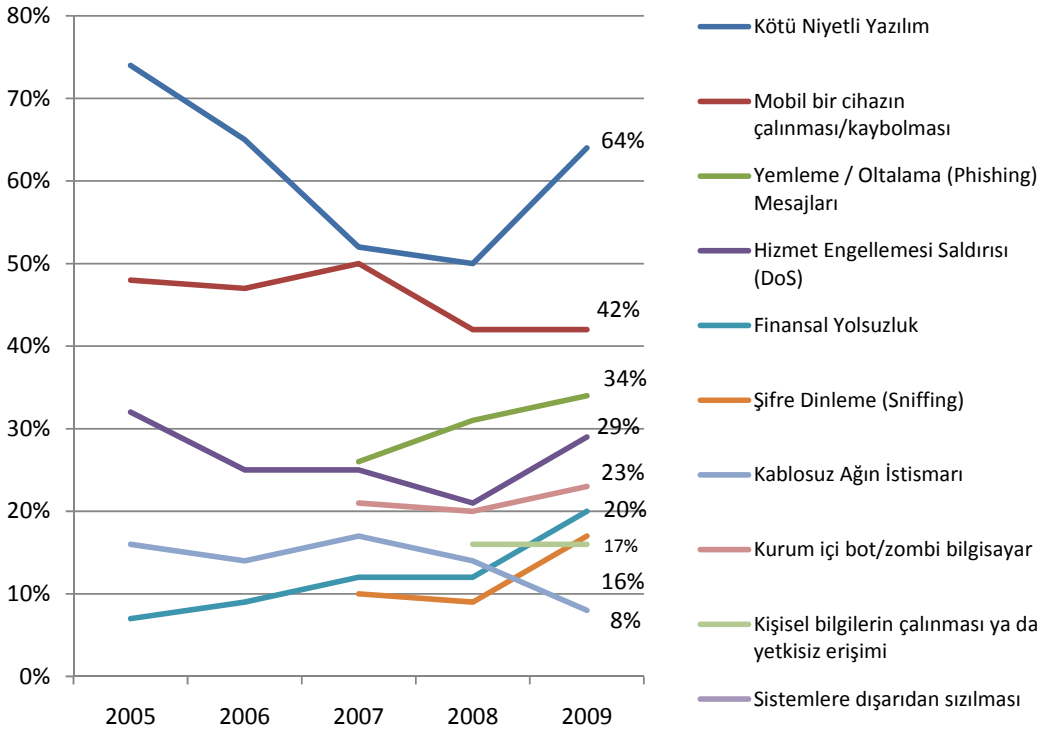
3.5 GÜVENLİK KONUSUNDA YAPILAN ÇALIŞMALAR

Güvenlik konusunda geniş çaplı araştırmalar dünyanın ileri gelen güvenlik kuruluşları tarafından düzenli olarak yapılmakta ve yüksek seviyede güvenlik sağlanması için gerekli olan çözümler araştırılmakta ve öneriler sunulmaktadır. Güvenlik tehditlerinin neler oldugu, yol açtıgı zararların miktarı, kimleri tehdit ettigi ve buna benzer soruların cevaplarının yer aldıgı önemli raporlar dünyanın bu konuda hangi düzeyde olduğunu göstermeyi amaçlamaktadır.

Sağıroğlu ve Mohammed'in (2009) mobil ortam saldırılarına yönelik yaptığı araştırmaya göre operatörlere karşı yapılan saldırıların çok fazla olduğu ve operatörlerin en zayıf noktalardan biri olduğu görülmüştür. Aynı çalışmada mobil ortam güvenliği bilgi güvenliği açısından değerlendirildiğinde ise erişebilirlik, gizlilik bütünlük ve kanıtlama öne çıkan unsurlar olarak dikkat çekmektedir. Bunlardan bir tanesinin ihlali bile güvenliğin ihlaline sebep olmaktadır.

Dünyadaki güvenlik konusunda yapılan en kapsamlı çalışmalardan biri Bilgisayar Güvenlik Enstitüsü (Computer Security Institute – CSI)'nün 14 senedir periyodik olarak yayınladığı Bilgisayar Suçları ve Güvenliği Anketi (Computer Crime and Security Survey) adlı çalışmadır. 2009 yılında yapılan ve 443 katılımcı firma ve kamu kuruluşu ile gerçekleştirilen araştırmaya dair yayınlanan raporla ilgili bazı veriler aşağıdaki gibidir.

Katılımcıların 185 tanesi 2009 yılı içinde bir veya birden fazla çeşit saldırıya maruz kaldıklarını belirtmiştir. Buna göre en büyük tehdit kaynağı %64'lük oranla kötü niyetli yazılımlar olarak belirtilmiştir. Bunu %42'lik oranla kuruma ait mobil bir cihazın çalınması ya da kaybolması takip etmiştir. Yemleme / oltalama mesajları ise diğer önemli bir tehdit olarak sıralanmıştır. Araştırmaya katılanların %29'u ise 2009 yılı içinde bir hizmet engelleme saldırısına maruz kaldıklarını belirtmişlerdir (Grafik 3.1) (Computer Security Institute 2009).



Grafik 3.1: Bilgisayar Suçları ve Güvenliği Anketi'nde Raporlanan SaldırıTipleri
Kaynak: Computer Security Institute, 2009

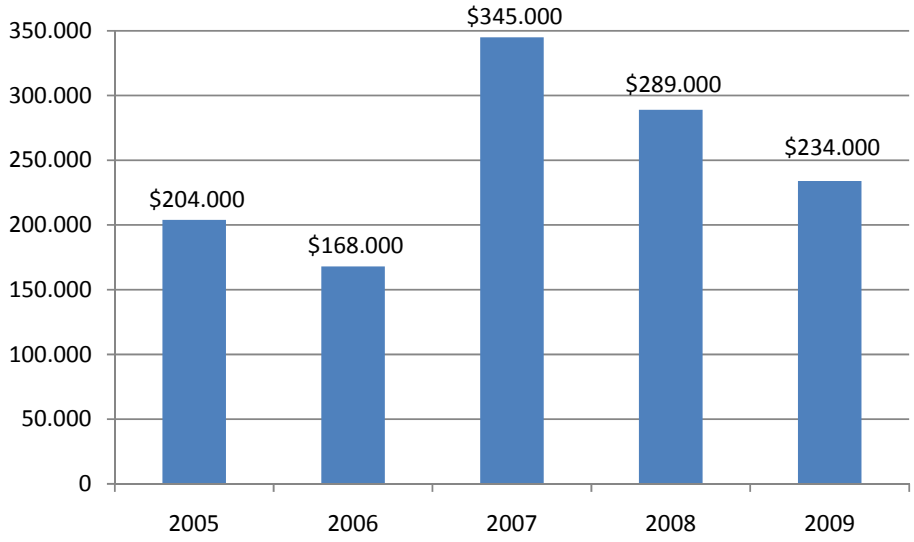
Tablo 3.2'de ise 2005 – 2009 yılları arasında bu çalışmaya katılan ve ilgili yıl içinde bir ya da birden fazla saldırıya maruz kalmış kurumların maruz kaldıkları saldırılara dair detaylar yer almaktadır.

Tablo 3.2: Bilgisayar Suçları ve Güvenliği Anketi'ne göre tehdit kaynakları

Tehdit Kaynağı	**2005**	**2006**	**2007**	**2008**	**2009**
Kötü niyetli yazılım	74%	65%	52%	50%	**64%**
Kurum içi bot/zombi bilgisayar	n/a		21%	20%	**23%**
Yemleme / Oltalama (Phishing) Mesajları	n/a		26%	31%	**34%**
Şifre Dinleme (Sniffing)	n/a		10%	9%	**17%**
Finansal yolsuzluk	7%	9%	12%	12%	**20%**
Hizmetin Engellenmesi Saldırısı (DoS)	32%	25%	25%	21%	**29%**
Çalınan veri ya da saldırı neticesinde yapılan şantaj	n/a				**3%**
Web sitesi tahrifatı	5%	6%	10%	6%	**14%**
Halka açık web sitesinin istismarı	n/a				**6%**
Kablosuz ağın istismarı	16%	14%	17%	14%	**8%**
DNS Sunucusunun istismarı	n/a		6%	8%	**7%**
İstemci web tarayıcısının istismarı	n/a				**11%**
Sosyal ağ profilinin istismarı	n/a				**7%**
Anlık mesajlaşma suistimali	n/a		25%	21%	**8%**
İçerden Internet erişimi ya da e-posta kullanımında suistimal	48%	42%	59%	44%	**30%**
Kurum içi yetkisiz erişim ya da yetki eskalasyonu	n/a				**15%**
Sistemlere dışarıdan sızılması	n/a				**14%**
Laptop ya da mobil bir cihazın çalınması/kaybolması	48%	47%	50%	42%	**42%**
Kişisel bilgilerin çalınması ya da yetkisiz erişimi	n/a			16%	**16%**
Fikri mülkiyetin çalınması ya da yetkisiz erişimi	n/a			9%	**14%**

Kaynak: Computer Security Institute, 2009

Bilgisayar Suçları ve Güvenliği anket çalışmasına göre maruz kaldıkları saldırılar sebebiyle para kaybı yaşadıklarını belirten katılımcıların 2009 yılı içinde katılımcı başına ortalama senelik kayıpları 234.000 USD olmuştur. Bu rakam 2008 yılında 289.000 USD ve 2007 yılında 345.000 USD olarak belirtilmiştir (Grafik 3.2).



Grafik 3.2: Bilgisayar Suçları ve Güvenliği Anketi'nde raporlanan maddi kayıplar
Kaynak: Computer Security Institute, 2009

3.6 ÜÇÜNCÜ NESİL ŞEBEKELERDE GÜVENLİK TEHDİT VE ZAFİYETLERİ

3G teknolojisi ile birlikte kullanmaya başlanabilecek servislerin kullanıcının hatalı kullanımına ve çeşitli suistimallere karşı korunaklı olması gerekmektedir. Hatta önlemlerin, daha servisin geliştirme aşamasında alınması gerekmektedir. Güvenlik kriterlerinin net ve dünya çapında kolay erişilebilir olması gerekmektedir.

Üçüncü nesil şebekelerin güvenlik kriterleri ile ilgili çeşitli araştırmalar yapılmaktadır. Üçüncü nesil şebekeler hakkında çalısmalar yapan en önemli çalışma ekibi 3GPP – Third Generation Partnership Project (Üçüncü Nesil Ortaklık Projesi)'dir.

3GPP'nin yayımlamış olduğu 3G TS 21.133 versiyon 3.1.0 numaralı teknik spesifikasyon dokümanında üçüncü nesil şebeklerdeki güvenlik tehditleri aşağıdaki gibi sınıflandırılmaktadır:

3.6.1 Hassas Veriye Yetkisiz Erişim (Gizliliğin İhlali)

- Gizlice Dinleme Yolu ile Bilgi Edinme (Eavesdropping): Saldırgan farkedilmeden veriyi elde eder.

-Maskeleme (Masquerading): Saldırgan yetkili bir kullanıyı kendisinin meşru sistem olduğu konusunda aldatarak gizli bilgiyi kullanıcıdan alır, ya da saldırgan meşru sistemi kendisinin yetkili kullanıcı olduğu konusunda aldatarak gizli bilgiyi elde eder.

- Trafik Analizi: Saldırgan önemli bir işlemin gerçekleşip gerçekleşmediği öğrenmek ya da bir kullanıcının lokasyonunu belirlemek için ağ üzerinde iletilen verinin zamanını, boyutunu, kaynağını ya da hedef noktasını gözlemler.

- Ağ Taraması (Browsing): Saldırgan hassas bilgiye erişim için veri depolarını tarar.

- Sızma (Leakage): Saldırgan yetkisi dahilindeki erişimlerle mevcut süreçlerden yararlanarak hassas bilgiyi elde eder

- Müdahale (Inference): Saldırgan sisteme bir sorgu ya da sinyal göndererek sistemin tepkisini gözlemler. Örneğin, saldırgan aktif bir oturum girişiminde bulunur ve sistemin yanıtını inceler.

3.6.2 Hassas Veriye Yetkisiz Müdahele (Bütünlüğün İhlali)

-Manipülasyon (Manipulation): Veri kasıtlı olarak saldırgan tarafından değiştirilebilir, içine ekleme yapılabilir, tekrarlanabilir ya da silinebilir.

3.6.3 Ağ Hizmetlerini İhlal ya da Suistimal Etme (Hizme Dışı Bırakma ve Erişilebilirliğin İhlali)

- Araya Girme (Intervention): Saldırgan yetkili bir kullanıcının bir hizmete erişimini sisteme müdahale ederek engelleyebilir.

- Kaynakları Tüketme (Resource Exhaustion): Saldırgan hizmete aşırı yüklenerek yetkili bir kullanıcının bir hizmete erişimini engelleyebilir.

- Ayrıcalıkların Suistimali (Misuse of privileges): Saldırgan kendisine sunulan ayrıcalıkları suistimal ederek gizli bilgi ya da hizmete erişebilir.

- Hizmetlerin Kötüye Kullanımı (Abuse of services): Saldırgan bazı özel hizmet ya da tesisleri suistimal ederek şebekede kesintiye sebep olabilir.

- İnkar (Repudiation): Bir kullanıcı ya da servis gerçekleşmiş vakaları ispatlayacak yeterli kanıt olmadığı için reddedebilir.

3.6.4 Hizmetlere Yetkisiz Erişim

- Saldırgan yetkili bir kullanıcı ya da şebeke elemanı/servisiymiş gibi davranarak yetkisiz erişim sağlayabilir.
- Kullanıcı ya da şebeke elemanları/servisleri kendi erişim haklarını suistimal ederek yetkisiz erişim sağlayabilirler.

Ülkemizde de, Bilgi Teknolojileri ve İletişim Kurumu (BTK) 20.07.2008 tarihinde Elektronik Haberleşme Güvenliği Yönetmeliği'ni yayımlayarak elektronik haberleşme güvenliği usul ve esaslarını belirlemiştir. İlgili yönetmeliğin ikinci bölümünün altıncı maddesinde elektronik haberleşmeye ilişkin başlıca tehditler;

a) Yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi,

b) Yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması,

c) Donanım-yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi,

ç) Deprem, sel, su baskını, yangın gibi doğal afetler ile grev ve lokavt hali,

d) Kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi,

e) Elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi,

f) Doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi,

g) Elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesi olarak tanımlanmıştır.

3.6.5 Üçüncü Nesil Şebekelerin Başlıca Tehdit Kaynakları

Yukarıda da bahsi geçen tehditlerin belli başlı tehdit kaynakları ise kötü niyetli kullanıcılar, aboneler, altyüklenici firmalar, internet hizmet sağlayıcıları ve iç kullanıcılar (şirket çalışanları) olarak tanımlanabilir (Dinçkan 2006).

3.6.5.1 Kötü niyetli internet kullanıcıları

Kendi kabiliyetlerini gösterme veya şebekeye zarar vermek için çalışan kişilerdir. Üçüncü nesil şebekenin doğrudan internet bağlantısı olması nedeni ile internet için var olan tehditler mobil şebeke için de tehdit unsurudur.

3.6.5.2 Aboneler

Aboneler şebekenin bir parçasıdır. Aboneler kendilerine tanınan haklardan yaralanarak şebekeye veya diğer abonelere zarar verebilirler. Abonelerden gelebilecek muhtemel saldırılardan korunmak için, operatörler abonelerin sadece belirli servis ve cihazlara erişimine izin vermelidir.

3.6.5.3 Altyüklenici firmalar

Şebeke içerisinde kullanılan yazılımların güncellenmesi, cihazların bakımı gibi bazı işler altyüklenici firmalara yaptırılabilir. Dikkatsiz yazılım güncellemeleri ve izin alınmadan yapılan cihaz bakımları şebekeye kasıtlı ya da bilmeden zarar verebilir.

3.6.5.4 Internet hizmet sağlayıcıları

Operatörler, abonelerine internet bağlantısı sağlayabilmek için internet hizmet sağlayıcılarından yararlanırlar. Internet hizmet sağlayıcılarının iç ağları, doğrudan mobil şebekeye bağlıdır. Bu nedenle operatörler, saldırı riskini mümkün olan en az seviyeye çekmek üzere güvenlik duvarı, erişim kontrol listeleri gibi gerekli önlemleri almalıdır.

3.6.5.5 İç kullanıcılar (Operatör çalışanları)

Sistemlerin çalışamaz duruma gelme nedeni yüksek oranda iç kullanıcılardan kaynaklanmaktadır. Çalışanlara güvenilmeli fakat cihaz ve uygulamalara hak verilirken dikkatli olunmalıdır. Çalışanlar bilinçi ya da bilinçsiz bir şekilde şebekeye zarar verebilirler.

3.7 ELEKTRONİK HABERLEŞME GÜVENLİĞİ KONTROL ALANLARI

Elektronik haberleşme güvenliği konusunda genel kabul görmüş belli başlı standartlar bulunmaktadır. Bunlardan bir tanesi Uluslararası Standardizasyon Kurumu (ISO) tarafından yayımlanmış olan ISO/IEC 27001:2005 standardını baz alan ISO/IEC 27011 güvenlik standardıdır. ISO/IEC 27011 telekomünikasyon sektörüne özel olarak hazırlanmış bir güvenlik standardıdır. Bu uluslarası standart, telekomünikasyon sektöründe yer alan kurumların, bilgi güvenliğinin en temel gereksinimleri olan "gizlilik", "bütünlük" ve "erişilebilirlik" ilkelerini sağlayarak, ortak asgari düzeyde bir bilgi güvenliğine sahip olmalarına yardımcı olmak amacıyla oluşturulmuştur. ISO/IEC 27011 standardı, ISO/IEC 27002'yi temel alarak genel güvenlik kontrolleri ve telekomünikasyon sektörüne özel güvenlik kontrolleri ile bu kontrollerin seçilmesine ve uygulanmasına yol gösteren uygulama kılavuzlarını kapsamaktadır. ISO 27011 standardı ile telekomünikasyon kurumları için kabul edilmiş uluslarası hedeflere uygun bir bilgi güvenliği yönetim sisteminin oluşturulması, telekomünikasyon araçlarının ve servislerinin gizliliği, bütünlüğü ve erişilebilirliği garanti altına alınarak, bilgi güvenliğinin sağlanması, güvenli süreç ve kontroller ile telekomünikasyon hizmetlerindeki mevcut risklerin minimize edilmesi hedeflenmektedir.

Telekomünikasyon sektörüne özel bu güvenlik standardı, ISO/IEC 27002 standardında tanımlanmış olan 11 ana kontrol alanından oluşmaktadır:

- **Güvenlik Politikası**
    - Bilgi güvenliği politikası
- **Bilgi Güvenliği Organizasyonu**
    - İç organizasyon
    - Dış taraflar
- **Varlık Yönetimi**
    - Varlıkların sorumluluğu
    - Bilgi sınıflandırması
- **İnsan Kaynakları Güvenliği**
    - İstihdam öncesi İnsan Kaynağı Güvenliği
    - Çalışma esnasında İnsan Kaynağı Güvenliği

    - İstihdamın sonlandırılması veya değiştirilmesi

- **Fiziksel ve Çevresel Güvenlik**
    - Güvenli alanlar
    - Teçhizat güvenliği
- **Haberleşme ve İşletim Yönetimi**
    - Operasyonel prosedürler ve sorumluluklar
    - Üçüncü taraf hizmet sağlama yönetimi
    - Sistem planlama ve kabul
    - Kötü niyetli ve mobil koda karşı koruma
    - Yedekleme
    - Ağ güvenliği yönetimi
    - Ortam işleme
    - Bilgi değişimi
    - Elektronik ticaret hizmetleri
    - İzleme
- **Erişim Kontrolü**
    - Erişim kontrolü için iş gereksinimi
    - Kullanıcı erişim yönetimi
    - Kullanıcı sorumlulukları
    - Ağ erişim kontrolü
    - İşletim sistemi erişim kontrolü
    - Uygulama ve bilgi erişim kontrolü
    - Mobil bilgi işleme ve uzaktan çalışma
- **Bilgi Sistemleri Edinim, Geliştirme ve Bakımı**
    - Bilgi sistemlerinin güvenlik gereksinimleri
    - Uygulamalarda doğru işleme
    - Kriptografik kontroller
    - Sistem dosyalarının güvenliği
    - Geliştirme ve destekleme proseslerinde güvenlik
    - Teknik açıklık yönetimi
- **Bilgi Güvenliği İhlal Olayı Yönetimi**
    - Bilgi güvenliği olayları ve zayıflıklarının rapor edilmesi

- Bilgi güvenliği ihlal olayları ve iyileştirmelerin yönetilmesi

- **İş Sürekliliği Yönetimi**
  - İş sürekliliği yönetiminin bilgi güvenliği hususları

- **Uyum**
  - Yasal gereksinimlerle uyum
  - Güvenlik politikaları ve standardlarla uyum ve teknik uyum
  - Bilgi sistemleri denetim hususları

Ayrıca, ISO/IEC 27011 standardı kapsamında ek olarak sunulan "Telekomünikasyon Sektörü İçin Genişletilmiş Kontroller" ve "Ek Uygulama Kılavuzu" kısımlarında, telekomünikasyon altyapı ve servislerinde güvenliği sağlamaya yönelik yeni kontroller ve uygulama kılavuzları tanımlanmaktadır.

Telekomünikasyon Sektörü için Genişletilmiş Kontroller ek olarak aşağıdaki kontrol alanlarını da içermektedir.

- **Fiziksel ve Çevresel Güvenlik**
  - Güvenlik Alanı
  - İletişim merkezinin güvenliğinin sağlanması
  - Telekomünikasyon ekipman odasının güvenliğinin sağlanması
  - Fiziksel olarak izole edilmiş çalışma alanlarının güvenliğinin sağlanması
  - Diğer kurumların kontrolü altında güvenlik
  - Taşıyıcının lokasyonunda bulunan ekipman güvenliği
  - Kullanıcı lokasyonunda bulunan ekipman güvenliği
  - Bağlantılı telekomünikasyon hizmetleri

- **İletişim ve İşletme Yönetimi**
  - Şebeke Güvenliğinin Yönetilmesi
  - Sunulan Telekomünikasyon Hizmetlerinin Güvenlik Yönetimi
  - Spam Maillere Karşı Tepki
  - DoS/DDoS Saldırılarına Karşı Tepki

- **Erişim Denetimi**
  - Ağ Erişim Denetimi
  - Kullanıcı tarafından taşıyıcı tespiti ve kimlik denetimi

- **Uyum**
    - Yasal Gereklere Uyumluluk
    - İletişim Gizliliği
    - Temel İletişim
    - Acil Tedbirlerin Uyumluluğu

Ek Uygulama Kılavuzu'nda ise aşağıdaki kontrol alanları yer almaktadır.

- **Siber Saldırılara karşı ağ güvenlik önlemleri**
    - Ağ Araçlarının Korunması
    - Kimlik Sahteciliğine karşı önlemler
    - Telekomünikasyon Servis Kullanıcılarının Dikkatini Çekmek
- **Şebeke Tıkanmasına Yönelik Ağ Güvenlik Önlemleri**
    - Şebeke Tıkanmasını tespit ve önlemeye yönelik mekanizmalar
    - Şebeke Tıkanmasına sebep olabilecek bilginin önceden toplanması
    - Geçici hız yükseltme tedbirleri
    - Temel iletişimlerin tespiti ve önceliklendirilmesi
    - Arıza tetikleyebilecek bilginin toplanması

Bunların yanı sıra, ISACA (Information Systems Audit and Control Association – Bilgi Sistemleri Denetim ve Kontrol Birliği) ve ITGI (IT Governance Institute – BT Yönetişim Enstitüsü) tarafından geliştirilmiş olan COBIT (Control Objectives for Information and Related Technology - Bilgi İşlem Teknolojileri için Kontrol Hedefleri) çerçevesi bilgi güvenliği yönetimi için kullanılabilecek kontrol alanlarını da içeren bir kontrol seti sunmaktadır. COBIT çerçevesi toplam 4 alan altında gruplanmış 34 kontrol hedefi ve 318 detaylı kontrol hedefi içermektedir. Bunlar;

Planlama ve Organizasyon Alanı (Plan and Organize - PO):

Planlama ve organizasyon, kurumların bilgi teknolojilerini kullanarak hedeflerine nasıl ulaşabileceklerini açıklamaktadır. Bu kapsamda bilgi teknolojileri hedeflerine ulaşmak için nasıl bir organizasyon, nasıl bir altyapı ya da tesis gerektiği konuları aydınlığa kavuşturulur. Aşağıda COBIT'in 34 kontrol hedefinden planlama ve organizasyon bölümünde yer alan 10 kontrol hedefi yer almaktadır.

PO1 – Stratejik BT Planının Tanımlanması
PO2 – Bilgi Mimarisinin Tanımlaması
PO3 – Teknolojik Yönün Belirlenmesi
PO4 – BT Süreç, Organizasyon ve İlişkilerinin Tanımlanması
PO5 – BT Yatırımlarının Yönetimi
PO6 – Yönetim Amaç ve Hedeflerinin Aktarılması
PO7 – İnsan Kaynakları Yönetimi
PO8 – Kalite Yönetimi
PO9 – Risk Yönetimi
PO10 – Proje Yönetimi

Tedarik ve Uygulama Alanı (Acquire and Implement – AI):

Tedarik ve Uygulama, kurumların bilgi teknolojisi ihtiyaçlarını nasıl belirlemeleri gerektiğini ve iş süreçlerini bilgi teknolojileri ortamına nasıl aktaracaklarını anlatır. Bu alan, aynı zamanda bilgi teknolojileri sistemlerinin bakımının doğru yapılmasını ve ömrünü uzatacak önlemleri de içerir. COBIT'in tedarik ve uygulama adımları şunlardır:

AI1 – Otomasyon Çözümlerinin Belirlenmesi
AI2 – Uygulama Yazılımlarının Geliştirilmesi ve Bakımı
AI3 – Teknoloji Altyapısının Oluşturulması ve Bakımı
AI4 – Operasyon ve Kullanımın Sağlanması
AI5 – BT Kaynaklarının Tedarik Edilmesi
AI6 – Değişiklik Yönetimi
AI7 – Sistem Çözümlerin ve Değişikliklerinin Uygulanması ve Akredite Edilmesi

Hizmet Sunumu ve Destek Alanı (Deliver and Support – DS):

Hizmet sunumu ve destek alanı bilgi teknolojilerinin kendine has özelliklerini barındırır. Bilgi teknolojisi sistemlerinde uygulamaların çalıştırılmasını, bu sistemlerin etkin ve verimli çalıştırılmalarını garanti altına almaya çalışır. Bu alan şu adımlardan oluşur:

DS1 – Hizmet Seviyelerinin Tanımlanması ve Yönetimi
DS2 – Tedarikçi Hizmetlerinin Yönetimi

DS3 – Performans ve Kapasite Yönetimi
DS4 – Hizmet Sürekliliğinin Sağlanması
DS5 – Sistem Güvenliğinin Sağlanması
DS6 – Maliyetlerin Belirlenmesi ve Dağıtımı
DS7 – Kullanıcıların Eğitimi
DS8 – Hizmet Sunumu Yönetimi ve Olay Yönetimi
DS9 – Konfigürasyon Yönetimi
DS10 – Problem Yönetimi
DS11 – Veri Yönetimi
DS12 – Fiziksel Ortamların Yönetimi
DS13 – Operasyon Yönetimi

İzleme ve Değerlendirme Alanı (Monitor and Evaluate – ME):

İzleme ve değerlenirme alanı belirlenmiş olan stratejik bilgi teknolojileri hedeflerine ulaşmak için mevcut altyapının hala yeterli olup olmadığını gözlemler. Gözlem aynı zamanda bağımsız olarak verimliliği ölçen bir alandır. Gözlem alanını oluşturan dört adım şu şekilde sıralanmaktadır:

ME1 – BT Performansının Değerlendirilmesi ve İzlenmesi
ME2 – İç Kontrolün Değerlendirilmesi ve İzlenmesi
ME3 – Düzenlemelere Uygunluk
ME4 – BT Kurumsal Yönetişiminin Sağlanması

Cobit çerçevesi içinde bilgi güvenliği yönetimi konusunda faydalanılabilecek kontrol hedefleri aşağıdaki tabloda gösterilmektedir.

Tablo 3.3: Üst Seviye Cobit – ISO 27001 ilişkilendirmesi

	1	2	3	4	5	6	7	8	9	10	11	12	13
Planlama ve Organizasyon	**-**	**o**	**-**	+	**-**	+	**o**	**-**	**-**	**-**			
Tedarik ve Uygulama	**o**	**o**	+	**-**	**-**	**o**	**o**						
Hizmet Sunumu ve Destek	**-**	**o**	**o**	**o**	+	**-**	**o**	**-**	**-**	**o**	+	+	**o**
İzleme ve Değerlendirme	**-**	**o**	**o**	**o**									

(+) ikiden daha fazla detaylı kontrol hedefi ilişkili
(o) en fazla iki detaylı kontrol hedefi ilişkili
(-) ilişkisiz

Kaynak: ITGI Mapping of ISO/IEC 17799:2005 with Cobit 4th Edition

Ülkemizde de, BTK tarafından elektronik haberleşme güvenliğine ilişkin usul ve esasları belirlemek amacıyla düzenlenmiş olan Elektronik Haberleşme Güvenliği Yönetmeliği kapsamında işletmecilerin fiziksel alan güvenliği, veri güvenliği, donanım-yazılım güvenliği ve güvenilirliği ile personel güvenilirliğinin sağlanması için tehditlerden ve/veya zafiyetlerden kaynaklanan risklerin bertaraf edilmesine veya azaltılmasına ilişkin olarak alacakları tedbirlere yer verilmektedir.

- **Fiziksel alan güvenliği**

Elektronik Haberleşme Güvenliği Yönetmeliği kapsamında fiziksel güvenlik konusunda aşağıdaki kontroller tanımlanmıştır.

a) Giriş ve erişim yetkisi ile bu yetkinin kapsamı işletmeci tarafından önceden tanımlanarak, giriş ve erişim sadece yetkili kişilerle sınırlandırılır.

b) Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak, tarih, saat ve kimlik gibi bilgiler kaydedilerek, her ziyaretçinin sadece izin verilen yerlere girişi ve çıkışı sağlanır.

c) Tüm personel ve personel harici kişiler, kimlik bilgilerini, yetki ve erişim seviyelerini açık bir şekilde görünür kılacak giriş veya kimlik kartı taşır.

ç) Güvenlik hassasiyetli alanlara giriş ve erişim yetkisi, düzenli olarak gözden geçirilerek güncellenir ve gerekli değilse iptal edilir.

Bina dışı güvenlik hassasiyetli alanlarda aşağıdaki hükümler uygulanır:

a) Sahada yer alan, elektronik haberleşme altyapısını içeren bina, kule, dolap ve kutu gibi güvenlik riski oluşturabilecek alt yapı bileşenlerine erişim kontrol altında tutulur ve yetkisiz kişilerin kolaylıkla erişim sağlayamayacağı şekilde tesis edilir.

b) Elektronik haberleşme maksatlı kullanılan kule ve saha dolapları, yetkisiz kişilerin müdahale etmesini engellemek amacıyla uyarıcı levhalar ile donatılır.

Güvenlik hassasiyetli alanlarda ilave olarak aşağıdaki tedbirler alınır:

a) Kötü niyetli faaliyetleri engellemek amacıyla planlanmamış çalışmalardan kaçınılır.

b) Ses ve/veya video kayıt cihazlarının güvenlik hassasiyetli alanlara, izinsiz olarak girişini engellemek amacıyla gerekli önlemler alınır.

c) Güvenlik hassasiyetli alanların, tehditlere karşı korunması amacıyla fiziki güvenlik tedbirleri planlanır ve gerekli önlemler alınır.

- **Personel güvenilirliği**

Elektronik haberleşme altyapısında istihdam edilen teknik personel, konusunda yeterli mesleki deneyime sahip ya da eğitim almış olmalıdır. Bu personelin görev tanım ve sorumlulukları açıkça belirlenmelidir.

Elektronik haberleşme altyapısında istihdam edilecek personel hakkında adli sicil kaydı belgesi istenir.

Personelin haberleşme gizliliğine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için her türlü önlem alınarak, işlerin ve hizmetlerin düzenli yürütülmesi sağlanır.

- **Veri güvenliği**

Veri güvenliği aşağıdaki hükümler uyarınca sağlanır:

a) Veri erişim yetkisi ve bu yetkinin kapsamı, veri türüne göre önceden belirlenir ve kayıt altına alınır.

b) Yetki sınırları dahilinde erişim sağlanması için kullanılacak teknolojilerin seçimi, işletmecinin tasarrufundadır.

- **Donanım-yazılım güvenliği ve güvenilirliği**

Elektronik haberleşme altyapılarında kullanılan donanım-yazılım güvenliği ve güvenilirliği aşağıdaki hükümler uyarınca sağlanır:

a) Donanım-yazılımın ulusal düzenleme ile ulusal ve/veya uluslararası standartlara uygun olması sağlanır.

b) Aynı fiziksel alanda ve/veya farklı fiziksel alanlarda bulunan donanım-yazılım bileşenleri arasındaki iç haberleşmeyi sağlayan kablolu ve/veya kablosuz ağ yönetimi sadece yetkili kişiler tarafından erişilecek şekilde şifrelenir.

c) Donanım-yazılım bileşenleri, herhangi bir güvenlik tehdidinin gerçekleşmesini önlemek üzere kontrol ve izleme altında tutulur.

ç) Donanım-yazılım bileşenlerinin, yasal olmayan elektronik haberleşme dinleme ve/veya izleme tehdidi oluşturacak unsurları içerip içermediğini belirlemek üzere satın alma, kullanım, bakım ve onarım sırasında kontrolleri yapılır. Donanım-yazılım bileşenlerinde bu tür bir unsurun varlığının saptanması durumunda ilgili bileşenin kullanımına son verilir. Bu durum kayıt altına alınarak raporlanır ve oluşan tehdidi bertaraf edecek önlemler ivedilikle alınır.

d) İşletmeci, elektronik haberleşmenin gizliliği, bütünlüğü ve devamlılığının sağlanması için kritik donanım-yazılım bileşenlerinin tespitini yapar. Tespit edilen kritik donanım-yazılım bileşenlerinin yedekli çalışması esastır.

4. VERİ VE YÖNTEM

Üçüncü nesil mobil iletişim sistemlerindeki güvenlik tehdit ve zafiyetlerinin belirlenmesini amacıyla gerçekleştirilen bu çalışmanın araştırma yöntemine ilişkin bilgiler aşağıda sunulmaktadır.

4.1 ÖRNEK UMTS ŞEBEKESİNDEKİ GÜVENLİK ZAFİYETLERİNİN BELİRLENMESİ

Çalışmanın bu bölümünde örnek bir UMTS şebekesinde güvenlik testleri gerçekleştirilerek varolan güvenlik zafiyetleri ortaya konmuştur. Tehdit kaynakları tez çalışması kapsamında incelenmiş tüm standartlar, yönetmelikler ve yönetim çerçeveleri doğrultusunda en kritik görülen aşağıdaki dört ana başlık altında incelenmiştir:

- Fiziksel Alan Güvenliği
- Personel Güvenilirliği
- Veri Güvenliği
- Donanım ve Yazılım Güvenliği

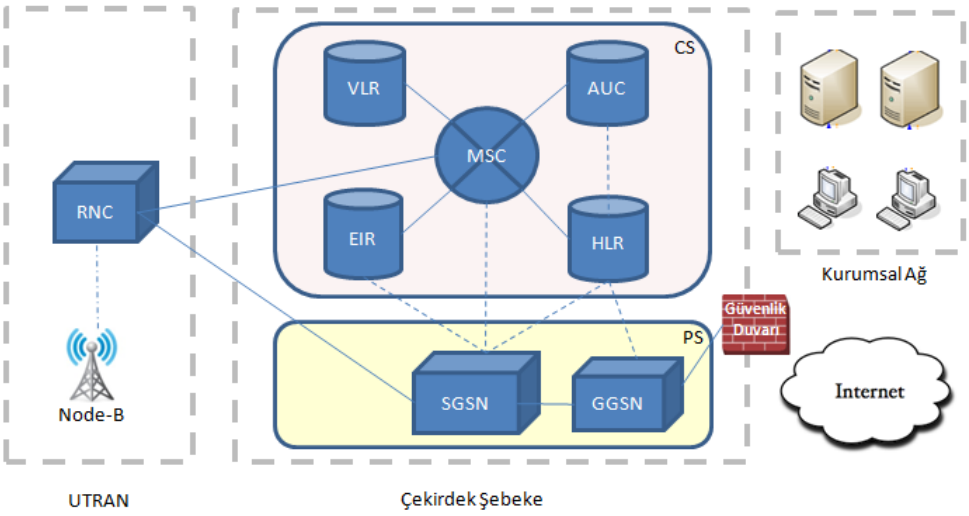
Güvenlik testleri oluşturulurken, bilgi teknolojileri alanında uluslararası kabul görmüş bir yönetim ve kontrol çerçevesi olan Cobit (Control Objectives for Information and Related Technology – Bilgi İşlem Teknolojileri için Kontrol Hedefleri) ve onun denetim uygulamalarını içeren BT Güvence Kılavuzu (IT Assurance Guide), Mapping of ISO/IEC 17799:2005 with Cobit 4.0, Cobit Security Baseline, ISO/IEC 27011 standardı ve kapsamında ek olarak sunulan "Telekomünikasyon Sektörü İçin Genişletilmiş Kontroller" ve "Ek Uygulama Kılavuzu" ve BTK Elektronik Haberleşme Güvenliği Yönetmeliği'nden faydalanılmıştır. Hedeflenen güvenlik kontrolleri, oluşturulan güvenlik testlerine göre incelenmiş ve test sonuçları raporlanarak tespit edilen bir güvenlik zafiyeti var ise belirtilmiştir.

Çalışma kapsamında varlıklar, ön tanımlı kategoriler altında sınıflandırılmış, testler seçilen bilgi varlık grupları üzerinde gerçekleştirilmiştir. Aşağıda güvenlik testlerinin gerçekleştirildiği varlık grupları yer almaktadır.

Tablo 4.1: Örnek şebeke için seçilen varlık grupları

#	Varlık Grubu	Platform	Node Sayısı	İşletim Sistemi	Veritabanı	Varlığın Lokasyonu
1	MSC	Nokia DX-200-i series	1	M13	Ürüne özel veritabanı	İstanbul Anadolu Yakası Santrali
2	HLR	Nokia DX-200-i series	1	M13	Ürüne özel veritabanı	
3	MSC/VLR	Nokia DX-200-i series	1	M14	Ürüne özel veritabanı	
4	HLR/AuC	Nokia DX-200-i series	1	M13	Ürüne özel veritabanı	
5	EIR	Nokia DX-200-i series	1	M13	Ürüne özel veritabanı	
6	SGSN	Nokia DX-200 serisi	1	M14	Ürüne özel veritabanı	
7	GGSN	Nokia DX-200 serisi	1	M14	Ürüne özel veritabanı	
8	Node-B	Huawei	1	n/a	n/a	
9	RNC	Huawei	1	n/a	n/a	
10	Firewall	Checkpoint R60 NGX	1	n/a	n/a	

Güvenlik testleri için seçilen örnek şebekenin mimarisi aşağıdaki şekilde gösterilmektedir.



Şekil 4.1: Örnek şebeke mimarisi

5. BULGULAR

5.1 FİZİKSEL ALAN GÜVENLİK TESTLERİ

Hedeflenen Güvenlik Kontrolleri: Giriş ve erişim yetkisi ile bu yetkinin kapsamı işletmeci tarafından önceden tanımlanarak, giriş ve erişim sadece yetkili kişilerle sınırlandırılır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.1'de açıklanmaktadır.

Tablo 5.1: Fiziksel Alan Güvenlik Test Sonuçları - 1

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Fiziksel erişim tanımlanması ile ilgili formlar mevcut mudur?	Operatörün şebeke elemanlarının da bulunduğu kritik lokasyonlarının taşıması gereken minimum güvenlik gerekliliklerin açıklandığı "Çevresel Kontrol Prosedürü" bulunmaktadır. Santral odalarına erişim yetkileri ilgili prosedürde tanımlanmış, yetkiler erişim formları ile prosedürde belirtilen kişilere verilmiştir.
Güvenlik hassasiyetli lokasyonlara erişim sınırlandırılması belli güvenlik katmanları ile yapılmakta mıdır?	Güvenlik testi için seçilen santral binasına girişler manyetik kartlarla yapılmaktadır. İlgili odalara geçiş seviyeleri prosedürde tanımlanan personele verilmiştir. Bunun dışında sistem ve santral odalarına girmesi gereken ancak manyetik kartı olmayan personel veya bakım/destek amacıyla hizmet alınan bir kuruluş çalışanı, güvenlik görevlilerinin gözetiminde ve "Santral Odası Giriş Kayıt Defteri"ne kaydı alınarak sistem odası sorumlusu nezaretinde santral odalarına girebilmektedirler.

Tablo 5.1: Fiziksel Alan Güvenlik Test Sonuçları - 1 (devam)

	Ayrıca, giriş ve çıkışları kayıt altına almak adına santral odasının kapısını görüntüleyen kamera sistemi mevcuttur.

Hedeflenen Güvenlik Kontrolleri: Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak, tarih, saat ve kimlik gibi bilgiler kaydedilerek, her ziyaretçinin sadece izin verilen yerlere girişi ve çıkışı sağlanır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.2'de açıklanmaktadır.

Tablo 5.2: Fiziksel Alan Güvenlik Test Sonuçları - 2

Gerçekleştirilen Güvenlik Testleri	**Test Sonuçları**
Güvenlik hassasiyetli lokasyonlara girişler kaydedilmekte (log) ve bunlar gözden geçirilmekte midir?	Manyetik kart girişlerine ait iz kayıtları (log) saklanmakta, ayrıca, "Santral Odası Giriş Kayıt Defteri"ne ziyaretçi girişleri kaydedilmektedir. Ayrıca bu kayıtlar düzenli olarak Fiziksel Güvenlik Müdürlüğü tarafından kontrol edilmektedir.
Sınırlandırılmış bölgelere giriş yetkilendirilmekte, dokümante edilmekte, iz kayıtları (logları) 3. taraf ve dış hizmet sağlayıcı girişlerini de kapsamakta mıdır?	Santral odasına girmesi gereken ancak manyetik kartı olmayan personel veya bakım/destek amacıyla hizmet alınan bir kuruluş çalışanı, güvenlik görevlilerinin gözetiminde ve "Santral Odası Giriş Kayıt Defteri"ne kaydı alınarak Sistem odası sorumlusu nezaretinde santral odalarına girebilmektedirler. Kayıt defterinde, ziyaretçinin giriş ve çıkış tarih ve saati, 3. taraf ya da dış hizmet sağlayıcı ise hangi firmadan ve ne amaçla girdiği bilgileri kayıt altına alınmaktadır.

Hedeflenen Güvenlik Kontrolleri: Tüm personel ve personel harici kişiler, kimlik bilgilerini, yetki ve erişim seviyelerini açık bir şekilde görünür kılacak giriş veya kimlik kartı taşır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.3'te açıklanmaktadır.

Tablo 5.3: Fiziksel Alan Güvenlik Test Sonuçları - 3

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Tüm personelin kimliklerini sürekli olarak görünebilir halde bulundurmalarını sağlayan ve gerekli onay alınmadan kimlik çıkarmalarını engelleyen bir politika bulunmakta mıdır?	"Fiziksel Güvenlik Politikası"nın fiziksel giriş kontrolleri başlığı altında tüm çalışanların ve ziyaretçilerin, kimlik ve yetkilerini belirten kartlarını, görünür şekilde üzerlerinde bulundurmaları gerektiği belirtilmektedir. Kimlik kartları Fiziksel Güvenlik Müdürlüğü prosedürlerinde tanımlandığı şekilde personel, taşeron ve ziyaretçi kartları olarak verilmekte her kartın erişim yetkisi ihtiyaçları kadar tanımlanmaktadır. Şirket içinde bu kartların görünür şekilde taşınma zorunluluğu bulunmaktadır.

Hedeflenen Güvenlik Kontrolleri: Güvenlik hassasiyetli alanlara giriş ve erişim yetkisi, düzenli olarak gözden geçirilerek güncellenir ve gerekli değilse iptal edilir. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.4'de açıklanmaktadır.

Tablo 5.4: Fiziksel Alan Güvenlik Test Sonuçları - 4

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Fiziksel erişim yetkileri düzenli olarak gözden geçirilmekte midir?	Sistem ve santral odalarına erişim yetkileri "Çevresel Kontrol Prosedürü"nde tanımlanmış olup,

Tablo 5.4: Fiziksel Alan Güvenlik Test Sonuçları – 4 (devam)

	yetkiler prosedürde belirtilen kişilere verilmiştir. İlgili prosedür kapsamında erişim yetkilerinin her üç ayda bir gözden geçirilmesi gerekliliği belirtilmektedir. Ancak erişim yetkileri incelendiğinde şirketten ayrılan personele ait yetkilerin aktif olduğu gözlemlenmiştir. Bu nedenle erişim yetkilerinin periyodik olarak gözden geçirilmediği tespit edilmiştir.

Hedeflenen Güvenlik Kontrolleri: Sahada yer alan, elektronik haberleşme altyapısını içeren alt yapı bileşenlerine erişim kontrol altında tutulur ve yetkisiz kişilerin kolaylıkla erişim sağlayamayacağı şekilde tesis edilir. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.5'de açıklanmaktadır.

Tablo 5.5: Fiziksel Alan Güvenlik Test Sonuçları - 5

Gerçekleştirilen Güvenlik Testleri	**Test Sonuçları**
Sahada yer alan güvenlik hassasiyetli lokasyonlara erişim sınırlandırılması belli güvenlik katmanları ile yapılmakta mıdır?	Güvenlik testi için seçilen baz istasyonu binasına ait girişler tek bir giriş kapısından ve manyetik kartlar ile yapılabilmektedir. Giriş çıkışlara ait kayıtlar uzaktan izleme sistemi ile sürekli olarak kaydedilmektedir.
Sahada yer alan güvenlik hassasiyetli lokasyonlara girişler kaydedilmekte (log) ve bunlar gözden geçirilmekte midir?	Güvenlik testi için seçilen baz istasyonu binasına ait girişler yetkilendirilmiş personele ve bakım çözüm ortaklarına ait manyetik giriş kartı ile yapılabilmektedir. Giriş çıkışlara ait kayıtlar uzaktan izleme sistemi ile sürekli olarak kaydedilmektedir.

Hedeflenen Güvenlik Kontrolleri: Güvenlik hassasiyetli alanların, tehditlere karşı korunması amacıyla fiziki güvenlik tedbirleri planlanır ve gerekli önlemler alınır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.6'da açıklanmaktadır.

Tablo 5.6: Fiziksel Alan Güvenlik Test Sonuçları - 6

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Kritik varlıkların çevresel faktörlerden korunması için izleme araçları kurulmuş mudur? (ısı ve nem algılayıcıları, otomatik havalandırma vb.)	Santral odasının cam duvarları zorlamaya karşı alarm mekanizması ve cam filmi ile korunmakta, odada Fm200 yangın söndürme tertibatı bulunmaktadır. Fm200 yangın söndürme tertibatı tavandan ve tabandan müdahale edecek şekilde yerleştirilmiştir. Ayrıca klima ve nem detektörleri kurulmuş, santral odasından geçen su boruları ve kalorifer tesisatları iptal edilmiştir. Santral odalarında periyodik bakımlar Destek Hizmetler Müdürlüğü tarafından yapılmakta, yangın söndürücüler tüm sistem odalarında mevcut bulundurulmaktadır. Mevcut kamera sistemi sistem odasındaki hareketleri ve ses düzeyindeki değişiklikleri algılamaktadır. Oda kamera ile 24 saat gözlenmekte ve alarm mekanizması bulunmaktadır.
Çevresel tehditleri (nem, yangın, sıcaklık vb.) tespit edecek izleme mekanizmaları bulunmakta mıdır?	Santral odası Netbotz adlı aktif bir izleme sistemi ile kameralar vasıtasıyla izlenmekte, izleme odasında 24 saat vardiyalı çalışan personel bulunmakta, yangın, nem ve sıcaklık detektörlerine ait alarm mekanizmaları mevcut bulunmaktadır. Alarm mekanizmaları hem kısa mesaj hem de e-posta ile ilgili personeli bilgilendirecek şekilde kurulmuştur.

5.2 PERSONEL GÜVENİLİRLİĞİ TESTLERİ

Hedeflenen Güvenlik Kontrolleri: Elektronik haberleşme altyapısında istihdam edilen teknik personel, konusunda yeterli mesleki deneyime sahip ya da eğitim almış olmalıdır. Bu personelin görev tanım ve sorumlulukları açıkça belirlenmelidir. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.7'de açıklanmaktadır.

Tablo 5.7: Personel Güvenilirliği Test Sonuçları - 1

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Teknik personelin eğitim gereksinimlerinin analiz edilmesi ve planlanmasına yönelik bir prosedür var mıdır?	Teknoloji Direktörleri ve Teknoloji Eğitim Müdürlüğü tarafından teknik personelin eğitim ihtiyaçları Teknoloji Eğitim Müdürlüğü'nün koordinatörlüğünde sağlanmaktadır. Bu ihtiyaçların belirlenmesinde yöneticilerinin personeli takibi ve personelin görev alanının gereklilikleri ön planda tutulmaktadır. Ancak teknik personelin eğitim gereksinimlerinin analizini yönlendiren yazılı bir prosedür bulunamamıştır. Teknoloji Eğitim Müdürlüğü teknik birimler ile ilgili eğitim ihtiyaçlarını değerlendirmek üzere dönemsel toplantılar yapmaktadırlar.
Teknik yetkinlik (beceri setleri) gereksinimleri görev tanımları bazında açıklanmış mıdır?	Yetkinlik bazlı resmi ve onaylanmış görev tanımları bulunmaktadır. Ancak görev tanımlarının düzenli gözden geçirilmesine yönelik olarak bir prosedür bulunmamaktadır. Ayrıca, incelenen bütün görev tanımlarının güncel olmadığı gözlemlenmiştir.
Teknik beceri setlerini gözden geçirme ve güncelleme prosedürü var mıdır?	Teknik personelinin sahip olması gereken yetkinlikler görev tanımları içerisinde açıklanmaktadır. Ancak görev tanımları düzenli olarak gözden geçirilmemekte ve güncellenmemektedir.

Hedeflenen Güvenlik Kontrolleri: Elektronik haberleşme altyapısında istihdam edilecek personel hakkında adli sicil kaydı belgesi istenir. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.8'de açıklanmaktadır.

Tablo 5.8: Personel Güvenilirliği Test Sonuçları - 2

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Şirkette personel, sözleşmeli personel, orta ve uzun süreli çalışacak olan danışmanlar için adli sicil kaydı kontrolünü de içeren bir inceleme prosedürü mevcut mudur?	Şirkete alınan tüm personelden yasal gereklilik nedeniyle sabıka kaydı talep edilmektedir. Ayrıca yeni alınan personel için referans kontrolü yapılmaktadır. Ancak, sözleşmeli personel ya da danışmanları kapsayan bir istihbarat prosedürü oluşturulmamıştır.

Hedeflenen Güvenlik Kontrolleri: Personelin haberleşme gizliliğine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için her türlü önlem alınarak, işlerin ve hizmetlerin düzenli yürütülmesi sağlanır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.9'da açıklanmaktadır.

Tablo 5.9: Personel Güvenilirliği Test Sonuçları - 3

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Şirkette yürürlükte olan bir Davranış Kuralcası var mıdır?	Çalışanların uyması gereken çalışma ilkelerini ve davranış kurallarını açıklayan "Çalışma İlkeleri ve Davranış Kuralcası" işe başlamadan önce iş akitleri ile birlikte çalışanlara iletilmekte ve bir Sorumluluk Belgesi aracılığıyla imzalı onayları alınmaktadır.
İş Sözleşmesinde, personelin hem iç hem de dış düzenlemelerden doğan haberleşme gizliliği, milli güvenlik ve	"Çalışma İlkeleri ve Davranış Kuralcası" İletişim Gizliliği başlığı altında çalışanların sahip oldukları bilgileri gizli tutmaları gerektiği ifade edilmektedir.

Tablo 5.9: Personel Güvenilirliği Test Sonuçları – 3 (devam)

kamu düzenine dair sorumlulukları açıkça ifade edilmekte midir?	İlgili başlık altında haberleşme gizliliğini korumak için hangi maddelere uymaları gerektiği anlatılmaktadır.
İç ve dış düzenlemelere uymamaları durumunda personelin karşılaşabileceği yaptırımlar açıkça ve yazılı olarak belirtilmiş midir?	"Çalışma İlkeleri ve Davranış Kuralcası" dokümanında çalışanların kişisel bilgilerini saklamakla ilgili yükümlülükleri yer almakta ve güvenlik gerekliliklerine uyulmadığı takdirde alınacak aksiyonlar ve yaptırımlar belirtilmektedir.
Bütün tedarikçiler ve dış hizmet sağlayıcılar ile gizlilik anlaşmaları imzalanmakta mıdır?	Şirket bünyesinde tedarikçi ve dış hizmet sağlayan firmalarla şirketin bilgi varlıklarının korunmasına yönelik olarak hazırlanmış gizlilik anlaşmaları bulunmaktadır. Yapılan sözleşmelere bu gizlilik anlaşmaları eklenmekte ve bunlar imzalanmadan önce hukuk görüşü alınmaktadır.

5.3 VERİ GÜVENLİĞİ TESTLERİ

Hedeflenen Güvenlik Kontrolleri: Veri erişim yetkisi ve bu yetkinin kapsamı, veri türüne göre önceden belirlenir ve kayıt altına alınır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.10'da açıklanmaktadır.

Tablo 5.10: Veri Güvenliği Test Sonuçları - 1

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Hassas verilerin belirlenmesine ilişkin bir süreç bulunmakta mıdır? Bu süreç içerisinde - verilerin gizliliğine ilişkin iş ihtiyaçları - uygulanabilir yasalar ve düzenlemelere uyum - iş süreç sahipleri ile mutabık kalınmış veri sınıflandırılması tanımlanmakta mıdır?	Şirkette kullanıcıların veriye erişimleri, erişim kontrolleri ile sağlanmakta ve bu şekilde hassas verilere erişimler kontrol edilmektedir. Veri sınıflandırması gizlilik esasına göre yapılıp dört kategoride gizlilik seviyeleri belirlenmiştir. Bu kategoriler "Sınıflanmamış", "Sınırlı", "Gizli" ve "Ticari Sır" olarak dokümante edilmiştir. Bu süreç Bilgi Güvenliği Politikası Bilgi Varlıkları Sınıflandırma Standardı kapsamında ele alınmaktadır. Bu standartla bilgi varlıklarının sınıflandırma derecelerine göre tasnif edilmesi, sınıflandırma kriterleri, sınıflandırma işaretleri ve sınıflandırılan bilgi varlıklarının önceden tanımlanmış güvenlik önlemlerine uygun olarak işlenmesi amaçlanmaktadır.
Hassas verilerin yetkisiz erişimlerden korunmasına ilişkin bir politika bulunmakta mıdır?	Hassas verilerin yetkisiz erişimlerden korunmasına ilişkin kurallar Bilgi Güvenliği Politikası, Bilgi Varlıkları Sınıflandırma Standardı ve Erişim Prosedürü kapsamında ele alınmaktadır.

Tablo 5.10: Veri Güvenliği Test Sonuçları – 1 (devam)

Veri çıktılarına erişime ilişkin fiziksel ve mantıksal güvenlik gereksinimleri belirlenmiş midir? Veri çıktılarının gizliliği açıkça tanımlanmış mıdır ve bu gizlilik unsuru erişime ilişkin fiziksel ve mantıksal gereksinimler belirlenirken göz önünde bulundurulmakta mıdır?	Bilgi Güvenliği Politikası Bilgi Varlıkları Sınıflandırma Standardı kapsamında farklı sınıflandırma seviyeleri için gereken genel güvenlik önlemlerini tanımlamaktadır. Her seviye için fiziksel erişim, kopyalama ve dağıtım, daha düşük seviyede yeniden sınıflandırma, elektronik depolama, elektronik transfer, fiziksel transfer, değişiklik kontrol ve denetimi, fiziksel imha ve elektronik bilginin imhası alanlarında güvenlik önlemleri detaylandırılmıştır.
Son kullanıcıların verilere erişimi, hassas verinin yönetimi ve yedeklenmesine ilişkin kurallar ve prosedürler tanımlanmış mıdır?	Şirkette, Bilgi Güvenliği yönetimi kapsamında oluşturulan Mantıksal Erişim Yönetimi Politikası oluşturulmuş, bu politika da Kullanıcı Hesapları Yönetimi Politikası, Şifre Politikası, 3. Tarafların Erişim Yönetimi Politikası, Ağ Güvenliği ve Erişimi Politikası ve Uzaktan Erişim Politikası ile desteklenmiştir.
Kullanıcı hesaplarının yaratılması /değiştirilmesi / silinmesi konularını yöneten bir kullanıcı yönetimi/kimlik yönetimi politikası mevcut mudur? Şifre ve parola yönetimi bu kapsamda tanımlanmış mıdır?	Şirkette kullanıcı hesapları Kullanıcı Hesapları Yönetimi politikası uyarınca yönetilmektedir. Yeni hesaplar ilgili prosedürde tanımlanmış formlar vasıtasıyla ve gerekli onayların alınması şartıyla yaratılmaktadır. Kritik sistemlerde yer alan tüm kullanıcı hesapları periyodik olarak gözden geçirilmektedir. Örnek olarak seçilen platformlara ilişkin kullanıcı hesabı gözden geçirme formlarının mevcut olduğu görülmüştür. Şifre ve parola yönetimi kritik sistemler için oluşturulmuş olan Referans Güvenlik Dokümanları (Minimum Security Baseline – MSB) içinde belirlenmektedir.

Tablo 5.10: Veri Güvenliği Test Sonuçları – 1 (devam)

	Örnek olarak seçilen şebeke elemanına ait MSB dokümanında şifre uzunluğu, karmaşıklığı, maksimum denemenin aşılması halinde hesabın geçersiz kılınması, önceki şifrelerin hatırlanması ve belli periyotlarda şifrelerin değiştirilme zorunluluğu gibi kontrollerin olduğu gözlemlenmiştir.
Hassas verinin yönetilmesi ve işlenmesi sürecinde güvenlik farkındalığı oluştuma programları oluşturulmuş mudur?	Şirkette hassas verilerin nasıl sınıflandırılması ve sınıflarına göre bilgi varlıklarının nasıl yönetilmesi gerektiği konusunda değişik bilinçlendirme çalışmaları yapılmaktadır. Bilgi Güvenliği Bilinçlendirme Eğitimleri periyodik olarak düzenlenmekte, çalışanlar bu konuda yetiştirilmektedir.

5.4 DONANIM – YAZILIM GÜVENLİĞİ TESTLERİ

Hedeflenen Güvenlik Kontrolleri: Donanım-yazılımın ulusal düzenleme ile ulusal ve/veya uluslararası standartlara uygun olması sağlanır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.11'de açıklanmaktadır.

Tablo 5.11: Donanım - Yazılım Güvenliği Test Sonuçları - 1

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Şirketin ulusal ve uluslararası düzenleme ve kontratlarına bağlı gereksinimlerini belirleyen bir süreç var mıdır?	Şirket, tâbi olduğu düzenleyici otorite olan Bilgi Teknolojileri ve İletişim Kurumu'nun ve diğer düzenleyici mercilerin yasal zorunluluklarına uygun hareket etmekten sorumludur. Mevzuat gereği yapılması gereken işler Regülasyon Bölümü'nün yönetiminde planlanmakta ve uygulanmaktadır.
Şirketin uyması gereken yasal ve düzenleyici gereksinimlerini karşılayıp karşılamadığını değerlendirdiği bir prosedürü bulunmakta mıdır?	Şirketin uyması gereken yasal yükümlülükleri Regülasyon Bölümü tarafından takip edilmektedir.
Şirket bünyesinde yazılım ve donanım satın alımı ve destek sözleşme şartlarını belirleyen bir standartlar bütünü mevcut mudur? Bu standartlar ulusal ve uluslararası standartlara uygun olarak oluşturulmuş mudur?	Şirkette yazılım ve donanım satın alma ve destek sözleşme standartlarını (fikri mülkiyet hakları ve lisansları, bakım, garanti, güncelleme şartları, güvenlik, erişim hakları, kaynak kod paylaşımı vb.) kapsayan bir süreç bulunmaktadır. Bu süreç Satın Alma Müdürlüğü'nden başlamakta ve şirketin çalışmayı tercih ettiği belli tedarikçilerin belli kriterler doğrultusunda değerlendirilerek seçilmesiyle devam etmektedir. Tedarik Yönetimi Bölümü ise tedarikçilerin şirketin standartlarına uygun çalışılıp çalışmadığını takip etmektedir.

Hedeflenen Güvenlik Kontrolleri: Aynı fiziksel alanda ve/veya farklı fiziksel alanlarda bulunan donanım-yazılım bileşenleri arasındaki iç haberleşmeyi sağlayan kablolu ve/veya kablosuz ağ yönetimi sadece yetkili kişiler tarafından erişilecek şekilde şifrelenir. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.12'de açıklanmaktadır.

Tablo 5.12: Donanım - Yazılım Güvenliği Test Sonuçları - 2

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Güncel ağ güvenliği politikası (sağlanan hizmetler, izin verilen trafik bağlantı türleri) oluşturulmuş mudur?	Şirkette ağ güvenliğine yönelik bir ağ güvenlik yönetim politikası ve bu politikayı destekleyen prosedürler bulunmaktadır. Politika ve prosedürler kapsamında şebeke içerisindeki trafiğin akışı, bileşenlerden sorumlu personelin görevleri ve sorumlulukları, güvenlik duvarı, ağ geçit cihazı gibi güvenlik bileşenlerinin konfigürasyon bilgileri, omurganın IP adres dağılımı, abonelere verilen IP adreslerinin dağılımı, sistemin işletimine dair kayıtların izlenme yöntemi, yeni bileşen ekleme ve çıkarmanın hangi kurallara göre yapılacağı, konfigürasyon ve çalışma esasları dokümanının güncellenmesine dair hususlar açıklanmaktadır.
Uzaktan erişim hakları düzenli olarak gözden geçirilmekte midir?	Şirkete uzaktan erişim hakları talep edilen süre boyunca verilmektedir. Bu süre dolmadan önce de güvenlik yöneticisine ve uzaktan erişime sahip olan kişiye bilgilendirme e-postası iletilmektedir. Kullanıcı uzaktan erişim talebini uzatmak isterse geçerli sebepleri ile ilgili yöneticilerden onay alarak talebini yenileyebilmektedir. Aksi taktirde güvenlik yöneticisi tarafından uzaktan erişim hakkı geri alınmaktadır.

Tablo 5.12: Donanım - Yazılım Güvenliği Test Sonuçları - 2 (devam)

Ağ erişilebilirliği ve güvenliği için kritik olan network cihazları fiziksel olarak korunuyor mudur?	Kritik şebeke elemanlarının da yer aldığı santral odasının cam duvarları zorlamaya karşı alarm mekanizması ve cam filmi ile korunmakta, odada Fm200 yangın söndürme tertibatı bulunmaktadır. Fm200 yangın söndürme tertibatı tavandan ve tabandan müdahale edecek şekilde yerleştirilmiştir. Ayrıca klima ve nem detektörleri kurulmuş, santral odasından geçen su boruları ve kalorifer tesisatları iptal edilmiştir. Mevcut kamera sistemi sistem odasındaki hareketleri ve ses düzeyindeki değişiklikleri algılamaktadır. Oda kamera ile 24 saat gözlenmekte ve alarm mekanizması bulunmaktadır.
Aboneler arası trafiği, aboneler tarafından başlatılmamış (Internet üzerinden veya diğer operatörlerin şebekelerinden gelen) trafiği filtreleyen bileşenler şebekede mevcut mudur?	Şebekede aboneler arası, Internet üzerinden gelen veya diğer operatörlerin şebekelerinden gelen trafiği filtreleyen ve bu iletişimi düzenleyen ve şifreleyen güvenlik duvarı ve ağ geçit cihazları bulunmaktadır. İnternet bağlantısını sağlayan GGSN cihazı üzerinde güvenlik duvarı hizmetlerini vermek üzere Checkpoint firmasının ürünleri kullanılmaktadır.
Örnek olarak seçilen şebeke elemanları arasındaki haberleşme şifrelenerek mi sağlanmaktadır?	Seçilen şebeke elemanlarından SGSN ve GGSN arasında bulunan Gn arayüzünde yapılan incelemeler sonucunda ise şifreleme yapılmadığı tespit edilmiştir.

Hedeflenen Güvenlik Kontrolleri: Donanım-yazılım bileşenleri, herhangi bir güvenlik tehdidinin gerçekleşmesini önlemek üzere kontrol ve izleme altında tutulur. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.13'te açıklanmaktadır.

Tablo 5.13: Donanım - Yazılım Güvenliği Test Sonuçları - 3

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Tüm ayrıcalıklı kullanıcı ve sistem yöneticisi hesaplarının denetim izlerinin (log) yaratılması ve gözden geçirilmesini sağlayan bir politika mevcut mudur?	Şirkette kritik sistemleri kapsamına alan bir güvenlik olayı loglama ve izleme prosedürü bulunmaktadır. Bu sistemlere ait denetim izleri Arcsight ESM (Enterprise Security Management) yazılımı ile merkezi olarak toplanmakta ve Bilgi Güvenliği Uzmanı'nca periyodik olarak gözden geçirilmektedir. Olay ve güvenlik izleri, çalıştırılabilir kaynak kodlara erişimler ve bu kodlarda yapılan değişiklikler, üretim ortamlarına yapılan yazılım geliştirme personeli ve üçüncü parti geliştiricilerin erişimleri ve kritik sistemler üzerindeki işlem kayıtları, uygulama, veritabanları ve işletim sistemi seviyesinde Arcsight ESM ürünü ile toplanmakta prosedür uyarınca aylık olarak gözden geçirilmektedir.
Kritik iz kayıt (log) dosyalarına erişim / değişiklik yapma / silme hakları kısıtlı ve kontrollü müdür?	Kritik iz kayıtları sistemlerden anlık olarak merkezi bir sunucuya toplanmakta ve bu kayıtlara erişim / değişiklik yapma ve kayıtları silme hakkı sadece yetkilendirilmiş Bilgi Güvenliği Uzmanları'nda bulunmaktadır.
İz kayıtlarının (logların) gözden geçirilme sürecine destek veren otomasyon sistemi ve uyarı araçları kurulmuş mudur?	Kritik iz kayıtlarının gözden geçirilmesine destek vermek üzere Arcsight ESM (Enterprise Security Management) yazılımından yararlanılmaktadır.

Tablo 5.13: Donanım - Yazılım Güvenliği Test Sonuçları – 3 (devam)

	Güvenlik olayı loglama ve izleme prosedürü kapsamında tanımlanan kritik işlemler, yetkili kullanıcı erişimleri, kritik dizinler, veritabanı tabloları gibi log kaynakları bu yazılım vasıtasıyla takip edilmektedir.
İz kayıtları (loglar) yedeklenip dijital ortamda veya basılı olarak güvenli bir şekilde saklanmakta mıdır?	İz kayıtlarının yedeklenme işletmeri Yedekleme Prosedürü uyarınca belirlenen kurallara göre gerçekleştirilmektedir. Buna göre, bir buçuk sene öncesine kadar olan iz kayıtları sıkıştırılarak arşivlenmekte, daha eski kayıtlar ise yedek kartuşlarına alınıp Data Center'a iletilmektedir.
Şirkette lisanssız yazılım kurulumunu ve lisanslı yazılımların yetkisiz ve yasal olmayan şekilde kullanımını engelleyen resmi bir politika bulunmakta mıdır?	Sunucu ve kullanıcı bilgisayarlarında hangi yazılımların bulunduğu bir envanterde tutulmakta belli aralıklarda bu envanter güncellenmektedir. Systems Management Server (SMS) yazılımı aracılığıyla kullanıcı bilgisayarlarında ve kritik sunucularda yüklü yazılımlar takip edilmektedir. Şirkette ayrıca lisansız yazılım kullanımımı engelleyen politikalar bulunmaktadır. Bu amaçla lokal yönetici hakları son kullanıcılardan alınmıştır.
Tüm kritik sunucu ve kullanıcı bilgisayarlarına anti-virüs programı , kötü niyetli yazılım bulma araçları ve güvenlik duvarı yüklenmiş midir?	Şirkette Symantec firmasına ait virüs koruma çözümleri kullanılmaktadır. Windows tabanlı tüm sunucu ve kullanıcı bilgisayarlarında bu firmanın anti-virus yazılımları yüklüdür ve merkezi virüs sunucusu vasıtasıyla kontrol edilmektedir. Windows tabanlı sistemlerde virüs yamalarının sunucu tarafından güncellenmesi her gün otomatik

Tablo 5.13: Donanım - Yazılım Güvenliği Test Sonuçları – 3 (devam)

	olarak yapılmaktadır. Tüm istemci makineleri her gün belirlenmiş zaman diliminde otomatik olarak merkez sunucuya bağlanarak gerekli güncellemeleri yapmaktadır. Anti virüs sistemleri makineler açıldığında devreye girmekte ve kullanıcılar bu yazılımı devre dışı bırakamamaktadır. Prosedürlerde belirlenmiş zaman dilimlerinde tüm istemci ve sunucularda otomatik virüs taraması gerçekleştirilmektedir. Ağ trafiğinin gözetlenmesi amacıyla IPS (Intrusion Prevention System) sistemi bulunmaktadır. Ayrıca GGSN'in doğrudan Internet ortamına erişimi olması nedeniyle GGSN'in Gi arayüzü üzerinden akan trafiği yönetmek için güvenlik duvarı ile virüs solucan, truva atı ya da hizmet engelleme saldırısı gibi tehditlere karşı filtreleme işlemi yapılmaktadır.

Hedeflenen Güvenlik Kontrolleri: Donanım-yazılım bileşenlerinin, yasal olmayan elektronik haberleşme dinleme ve/veya izleme tehdidi oluşturacak unsurları içerip içermediğini belirlemek üzere satın alma, kullanım, bakım ve onarım sırasında kontrolleri yapılır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.14'te açıklanmaktadır.

Tablo 5.14: Donanım - Yazılım Güvenliği Test Sonuçları - 4

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
Satın alınan donanım, yazılım ve hizmetler için tedarikçi yönetim prosedürü var mıdır?	Şirkette teknoloji tedarikçilerinin yönetimi Tedarik Yönetimi Bölümü tarafından sağlanmaktadır. Satın alınan donanım, yazılım ve hizmetler için tüm

Tablo 5.14: Donanım - Yazılım Güvenliği Test Sonuçları – 4 (devam)

	tedarikçilerle gizlilik sözleşmesi yapılmaktadır. Tedarikçi seçimi sürecinde tüm tedarikçiler şirketin bilgi güvenliği standartları konusunda bilgilendirilmekte ve bu standartlara uyumları konusunda taahhütleri alınmaktadır.
Şebeke elemanlarına dış hizmet sağlayıcı personelinin erişimlerini yöneten bir prosedür var mıdır?	Şirkete uzaktan erişim yöntemi bulunmaktadır. Uzaktan erişim için tek kullanımlık şifre ile SSL-VPN bağlantı yöntemi kullanılmaktadır. SSL-VPN bağlantısı ile bağlanan kullanıcılar hard token (tek kullanımlık şifre üretme cihazı) ile şirket ağına bağlanabilmektedirler. Tüm uzaktan erişimler için hard token atanmasının basılı formlar aracılığıyla olmasından dolayı, erişimler yönetim onayı ile sağlanmaktadır. Üçüncü parti firmaların şirket ağına erişimleri ise ilgili firmadan sorumlu olan personel tarafından tek kullanımlık şifre üretme cihazıyla üretilen şifrenin telefonla ya da yazılı olarak iletilmesi vasıtasıyla gerçekleştirilmektedir.
Önemli sistem güncellemeleri kritik sunuculara ve kullanıcı bilgisayarlarına uygulanmakta mıdır?	Windows tabanlı kritik sunucular ve kullanıcı bilgisayarlarının yama yönetimi Office IT Sistemleri Yönetim Yetkilileri tarafından yönetilmektedir. Yama ve güncellemelerin otomatik dağıtımı, merkezi SMS sunucusu vasıtasıyla yapılmaktadır. Veritabanı ve uygulama seviyesinde ve diğer Unix tabanlı sistemler için güncellemeler Yama Yönetimi Prosedürlerinde belirlenen periyotlarda "Yama ve Kritik Güncelleme Gözden Geçirme Formları" vasıtasıyla ilgili sistem yöneticileri tarafından gerçekleştirilmektedir.

Tablo 5.14: Donanım - Yazılım Güvenliği Test Sonuçları – 4 (devam)

	Ancak örnek olarak seçilen sistemin veritabanı ve işletim sistemi seviyesindeki güncelleme versiyonlarının üretici firma web sitesinde yayınlanan en son güncelleme ile örtüşmediği tespit edilmiştir. Aynı şekilde tüm şebeke elemanlarının üretici firmalarının yayınladığı kritik yama ve güncellemeler network mühendislerince periyodik olarak takip edilmekte ve gerekli güncellemelerin yapılması sağlanmaktadır. Örnek olarak seçilen şebeke elemanının üretici tarafından yayınlanan en son güncelleme seviyesinde olduğu gözlemlenmiştir.
Yamalar ve güvenlik güncellemeleri kurulmadan önce test edilmekte midir? Test edilen yamalar yüklenmeden önce yönetim tarafından onaylanmakta mıdır? Seçilen şebeke elemanlarının yama seviyesi güncel midir?	Şebeke elemanlarına ilişkin güncellemeler bir güncelleme planı dahilinde Operasyon Destek Sistemleri Müdürlüğü personelince yapılmaktadır. Bu plan içerisinde bölüm tarafından hazırlanmış yama inceleme betikleri (script) de çalıştırılarak güncellemenin canlı şebekeye herhangi bir olumsuz etkisinin olup olmayacağı da test edilmektedir. Test işlemi tamamlandıktan sonra sonuçların Operasyon Destek Sistemleri Yöneticisi tarafından da onaylanmasını takiben gerekli güncellemeler yapılmaktadır. Unix tabanlı diğer sistemlerin yama geçişleri öncesinde üst yönetim onayının arandığı görülmüş, ancak Windows tabanlı sistemler için herhangi bir yönetim onayına rastlanamamıştır.

Tablo 5.14: Donanım – Yazılım Güvenliği Test Sonuçları – 4 (devam)

	Örnek olarak seçilen şebeke elemanı için oluşturulan en son "Yama ve Kritik Güncelleme Gözden Geçirme Formu"nda güncelleme planı doğrultusunda ve gerekli onaylar alınarak geçilen son güncellemenin üretici firma tarafından yayınlanan en son kritik güncellemeyle aynı olduğu görülmüştür.
Tüm kritik cihazlar için yapılan bakım ve onarım aktivitelerinin iz kayıtları (log) tutulup saklanıyor mudur? Bakım faaliyetleri güvenlik tehditlerini de göz önüne alarak gerçekleştirilmekte midir?	Kritik şebeke elemanları için yapılan bakım aktiviteleri üretici firmalar ile yapılan bakım onarım sözleşmeleri uyarınca gerçekleştirilmektedir. Ayrıca tüm şebeke elemanlarının arıza takibi, pasif bakımları gibi aktiviteler ülke genelinde yayılan ve "Bakım Çözüm Ortakları" olarak nitelendirilen şirketin yetkinlik kriterlerini karşılayabilmiş taşeron firmalar tarafından gerçekleştirilmektedir. Bu firmalar IBM Tivoli ürünlerinden olan Netcool alarm yönetim sistemi üzerinden kendilerine otomatik olarak iletilen alarmları sürekli takip etmekte ve herhangi bir arıza durumunda duruma anında müdahale etmektedirler.

Hedeflenen Güvenlik Kontrolleri: İşletmeci, elektronik haberleşmenin gizliliği, bütünlüğü ve devamlılığının sağlanması için kritik donanım-yazılım bileşenlerinin tespitini yapar. Tespit edilen kritik donanım-yazılım bileşenlerinin yedekli çalışması esastır. Hedeflenen güvenlik kontrolüne ilişkin test adımları Tablo 5.15'te açıklanmaktadır.

Tablo 5.15: Donanım – Yazılım Güvenliği Test Sonuçları - 5

Gerçekleştirilen Güvenlik Testleri	Test Sonuçları
İş süreçleri kritikliklerine göre sınıflandırılmış mıdır? Kritik iş süreçleri ve bunları destekleyen teknoloji kaynakları süreklilik planı içerisinde yer almakta mıdır?	Şirket bünyesinde iş sürekliliğine ilişkin süreçlerin belirlenmesi tam olarak tamamlanmamıştır. Kritik iş süreçlerinin belirlenmesine yönelik çalışmalar devam etmekte, şirketi etkileyebilecek riskler ve bunlara ilişkin önleyici ve azaltıcı kontrollerin belirlenmesine ilişkin yapılanma devam etmektedir. İş sürekliliği politikası ortaya konmuş ancak detaylı prosedürler henüz tamamlanmamıştır. Teknoloji süreklilik yönetimi yapılanmasının oluşturulmasına ilişkin çalışmalar da bu çerçevede devam etmektedir. Network grubunun hazırladığı ve herhangi bir felaket anında ekiplerinin uygulaması gereken prosedürleri açıklayan bir teknoloji felaket kurtarma planı bulunmaktadır. Ancak doküman güncelliğini yitirmiş ve mevcut yapıyı desteklememektedir.
Dış lokasyonlara taşınan veri yedekleri için yeterli güvenlik mekanizmaları oluşturulmuş mudur? Taşıma sırasında ve muhafaza bölgesinde gerekli güvenlik kontrolleri sağlanmakta mıdır?	Yedekleme gereklilikleri yedekleme prosedürlerinde tanımlanmamıştır. Prosedürlere uygun şekilde alınan yedekler şirketin Anadolu Yakası Santral binasına haftalık olarak, İzmir Santral binasına ise aylık olarak gönderilmektedir. Bu yedekler binalardaki şifreli kasalarda ve yeterli güvenlik önlemleri sağlanarak saklanmaktadır. Kasalar su ve yangın geçirmezlik özelliğine sahip olmasına rağmen binaların zemin katlarında tutulmaktadır. Transfer edilen yedek kartuşları kilitli çantalarda ve nakil aracı içerisinde taşınmaktadır.

Tablo 5.15: Donanım - Yazılım Güvenliği Test Sonuçları – 5 (devam)

Sürekliliği planı; mutabık kalınmış hizmet seviyeleri ve erişebilirlik hedefleri doğrultusunda oluşturulmuş alternatif çalışma yöntemleri ve kurtarma prosedürlerini, rolleri ve sorumlulukları, iletişim süreçlerini, minimum kabul edilebilir kurtarma konfigürasyonunu içermekte midir?	Şirkette iş sürekliliği planlaması henüz tamamlanmamış olduğundan mutabık kalınmış hizmet seviyeleri ve erişebilirlik hedefleri doğrultusunda oluşturulmuş alternatif çalışma yöntemleri ve kurtarma prosedürleri, rol ve sorumluluklar, iletişim süreçleri ve kurtarma konfigürasyon bilgilerine ait bir çalışma gözlemlenmemiştir. Network grubunun hazırladığı ve herhangi bir felaket anında Network ekiplerinin uygulaması gereken prosedürleri açıklayan bir felaket kurtarma planı ise güncel bilgileri içermemektedir.
Süreklilik planı için oluşturulmuş ve güncellenen bir dağıtım planı bulunmakta mıdır? Dağıtım listesi oluşturulurken, bilmesi gerekli prensibi uygulanmış mıdır?	Şirkette iş sürekliliği ve teknoloji sürekliliği planlaması çalışmaları devam etmekte olup, hali hazırda bulunan Network grubuna ait felaket kurtarma planında bir dağıtım planı gözlemlenmiştir. Ancak doküman güncelliğini yitirdiğinden dağıtım planı da güncel değildir.

5.5 TESPİT EDİLEN GÜVENLİK ZAFİYETLERİ

Örnek UMTS şebekesi üzerinde yapılan güvenlik testleri sonucunda aşağıdaki güvenlik zafiyetleri tespit edilmiştir.

- **Fiziksel Alan Güvenliği**

Seçilen santral odasına erişim yetkileri incelendiğinde şirketten üç aydan daha önce ayrılan personele ait yetkilerin hala aktif olduğu gözlemlenmiştir. Bu nedenle erişim yetkilerinin prosedürde belirtilen üç aylık periyotlarda gözden geçirilmediği tespit edilmiştir. Kritik lokasyonlara giriş yetkilerinin prosedüre uygun olmaması yetkisiz erişim riskini doğurmaktadır.

- **Personel Güvenilirliği**

Teknik personelin eğitim gereksinimlerini belirleyen yazılı bir prosedür bulunamamıştır. Gerekli teknik eğitim ve gelişim imkanının sağlanamaması, personelin bilgi ve beceri düzeyi, yetkinlikleri, iç kontrol ve güvenlik bilinçlerinin şirketin hedeflerine erişebilecek seviyede tutulamaması riskini doğurmaktadır.

Şirkette görev tanımlarının düzenli gözden geçirilmesine yönelik olarak bir prosedür bulunamamıştır. Ayrıca, incelenen görev tanımlarının güncel olmadığı ve organizasyonel yapıyla uyumlu olmadığı gözlemlenmiştir. Görev tanımlarının düzenli olarak gözden geçirilmediği ve güncellenmediği tespit edilmiştir. Rol ve sorumlulukların net olmaması ya da yapılan işin görev tanımlarıyla uyumlu olmaması sorumlulukların düzgün atanamaması riskini doğurmaktadır.

Sözleşmeli personel ya da danışmanları kapsayan bir istihbarat prosedürü oluşturulmamıştır. Özellikle kritik fonksiyonlarda çalışan dış hizmet sağlayıcılarının sabıka kaydı temini, özgeçmiş araştırması gibi bir kontrol prosedüründen geçirilmemesi personelden kaynaklanabilecek güvenlik tehditlerinin oluşması riskini doğurmaktadır.

- **Veri Güvenliği Testleri**

Veri güvenliği alanında herhangi bir güvenlik zafiyeti tespit edilmemiştir.

- **Donanım – Yazılım Güvenliği ve Güvenilirliği**

Seçilen şebeke elemanlarından SGSN ve GGSN arasında bulunan Gn arayüzünde yapılan incelemeler sonucunda ise şifreleme yapılmadığı tespit edilmiştir. SGSN ve GGSN düğümleri arasında şifreleme yapılmaması, şebekeye ulaşabilen bir saldırganın abonelere ait trafiği dinleyebilmesi, değiştirebilmesi ya da kesebilmesi riskini doğurmaktadır.

Örnek olarak seçilen sistemin veritabanı ve işletim sistemi seviyesindeki güncelleme versiyonlarının üretici firma web sitesinde yayınlanan en son güncelleme ile örtüşmediği tespit edilmiştir. Bu durum, sistem ve verilerin kötü niyetli yazılımların saldırılarına karşı korumasız kalması riskine sebep olabilmektedir.

Şirket bünyesinde iş sürekliliğine ilişkin süreçlerin belirlenmesinin tam olarak tamamlanmadığı görülmüştür. Network grubunun hazırladığı ve herhangi bir felaket anında network yönetim ekiplerinin uygulaması gereken prosedürleri açıklayan bir teknoloji felaket kurtarma planı oluşturulmuş olmasına rağmen doküman güncelliğini yitirmiş ve mevcut yapıyı desteklememektedir. Ayrıca dokümana ait dağıtım planının da güncel olmadığı tespit edilmiştir. Bu durum, olağanüstü durum ya da büyük çaplı bir kesinti meydana gelmesi halinde sorunlara cevap verme süresini uzatabilecek ve iş sürekliliğinin sağlanamamasına neden olabilecektir.

6. SONUÇ, TARTIŞMA VE ÖNERİLER

Son dönemlerdeki mobil iletişim teknolojilerindeki gelişmeler, insanların bu teknolojileri giderek daha fazla hayatlarının bir parçası haline getirmelerine neden olmuştur. Önceleri sadece ses ya da kısa mesaj gibi hizmetler sağlayabilen mobil sistemler, üçüncü nesil hizmetlerin de başlaması ile birlikte insanların günlük ihtiyaçlarını rahatlıkla karşılayabilecekleri hızlarda mobil internet imkanını sunabilmiştir. Mobil cihazların da her geçen gün gelişmesi ve kullanım alanlarının çeşitlenerek yaygınlaşmasının sonucu olarak, mobil ortamlarda bilginin işlenmesi, taşınması ve saklanmasına yönelik yatırımlar giderek artmış, bilgiye mekandan bağımsız olarak istenilen ortamlardan erişilmesi giderek daha kolay sağlanmaya başlamıştır. Bu sayede de bireyler etkin günlük yaşantılarının gereksinimlerini yerine getirebilmek için mobil iletişim teknolojilerinden her geçen gün daha fazla yararlanmaya başlamıştır. Bu teknolojilerin kullanımının yaygınlaşması ile de mobil ortamlar saldırganlar için daha büyük bir hedef olmaya başlamış ve bu ortamlara güven ve bu ortamlardaki güvenlik konuları daha çok sorgulanmaya başlamıştır. Bu sebeplerden dolayı mobil ortamlardan sağlanan hizmetler için uçtan uca güvenliğin sağlanması önem kazanmıştır.

Üçüncü nesil şebeklerin genel olarak yetkisiz olarak veya yetki aşımıyla güvenlik hassasiyetli alana girilmesi, yetkisiz olarak veya yetki aşımıyla silme, ekleme, değiştirme, geciktirme, başka bir ortama kaydetme veya ifşa etme yoluyla veri gizliliğinin, bütünlüğünün ve/veya devamlılığının bozulması, donanım ve yazılım bileşenlerinin ulusal düzenleme ile ulusal ve/veya uluslararası standartlar uyarınca belirlenen gereklilikleri yerine getirmesinin kısmen veya tamamen engellenmesi, deprem, sel, su baskını, yangın gibi doğal afetler, kullanıcıyı yanıltarak doğru tarafla elektronik haberleşmede bulunduğu izleniminin verilmesi, elektronik haberleşmenin yasal olmayan bir şekilde izlenmesi ve/veya dinlenmesi, doğru olmayan bir bilgi üretilerek bu bilginin başka bir taraftan alındığının iddia edilmesi veya başka bir tarafa gönderilmesi, elektronik haberleşme altyapısının kısmen veya tamamen hizmet veremez hale getirilmesi veya altyapıya ait kaynakların, hizmet sunumunu aksatacak şekilde tüketilmesi gibi güvenlik tehditleri altında olduğu söylenebilir.

Bu tez çalışması yukarıda bahsi geçen tehditlere karşı operatörlerin alabilecekleri önlemleri ortaya koymayı amaçlamaktadır. Çalışma kapsamında belirli bir tehdidin, operatörün belirli bir zafiyetini suiistimal ederek istenmeyen sonuçlara neden olma olasılığını yani risklerini azaltmak için güvenlik kontrolleri önerilmektedir.

Önerilen güvenlik kontrolleri aşağıdaki gibidir:

- Giriş ve erişim yetkisi ile bu yetkinin kapsamı operatör tarafından önceden tanımlanarak, giriş ve erişim sadece yetkili kişilerle sınırlandırılmalıdır.
- Ziyaretçi giriş ve çıkışlarında gerekli kontroller yapılarak, tarih, saat ve kimlik gibi bilgiler kaydedilerek, her ziyaretçinin sadece izin verilen yerlere girişi ve çıkışı sağlanmalıdır.
- Tüm personel ve personel harici kişiler, kimlik bilgilerini, yetki ve erişim seviyelerini açık bir şekilde görünür kılacak giriş veya kimlik kartı taşımalıdır.
- Güvenlik hassasiyetli alanlara giriş ve erişim yetkisi, düzenli olarak gözden geçirilerek güncellenmeli ve gerekli değilse iptal edilmelidir.
- Sahada yer alan, elektronik haberleşme altyapısını içeren alt yapı bileşenlerine erişim kontrol altında tutulmalı ve yetkisiz kişilerin kolaylıkla erişim sağlayamayacağı şekilde tesis edilmelidir.
- Elektronik haberleşme maksatlı kullanılan kule ve saha dolapları, yetkisiz kişilerin müdahale etmesini engellemek amacıyla uyarıcı levhalar ile donatılmalıdır.
- Elektronik haberleşme altyapısında istihdam edilen teknik personel, konusunda yeterli mesleki deneyime sahip ya da eğitim almış olmalıdır. Bu personelin görev tanım ve sorumlulukları açıkça belirlenmelidir.
- Elektronik haberleşme altyapısında istihdam edilecek personel hakkında adli sicil kaydı belgesi istenmelidir.
- Personelin haberleşme gizliliğine, milli güvenliğe ve kamu düzenine aykırı davranışta bulunmaması için önlemler alınmalıdır.
- Veri erişim yetkisi ve bu yetkinin kapsamı, veri türüne göre önceden belirlenmeli ve kayıt altına alınmalıdır.

- Donanım ve yazılımın ulusal düzenlemeler ile ulusal ve/veya uluslararası standartlara uygun olması sağlanmalıdır.
- Aynı fiziksel alanda ve/veya farklı fiziksel alanlarda bulunan donanım ve yazılım bileşenleri arasındaki iç haberleşmeyi sağlayan kablolu ve/veya kablosuz ağ yönetimi sadece yetkili kişiler tarafından erişilecek şekilde şifrelenmelidir.
- Donanım ve yazılım bileşenleri, herhangi bir güvenlik tehdidinin gerçekleşmesini önlemek üzere kontrol ve izleme altında tutulmalıdır.
- Donanım ve yazılım bileşenlerinin, yasal olmayan elektronik haberleşme dinleme ve/veya izleme tehdidi oluşturacak unsurları içerip içermediğini belirlemek üzere satın alma, kullanım, bakım ve onarım sırasında kontroller yapılmalıdır.
- Elektronik haberleşmenin gizliliği, bütünlüğü ve devamlılığının sağlanması için kritik donanım ve yazılım bileşenlerinin tespiti yapılmalıdır ve tespit edilen kritik donanım ve yazılım bileşenlerinin yedekli çalışması sağlanmalıdır.

Çalışma kapsamında oluşturulan güvenlik prosedürü,örnek bir UMTS şebekesi üzerinde uygulanmış ve hedeflenen güvenlik kontrollerinin varlığı test edilmiştir. Gerçekleştirilen güvenlik testleri sonucunda güvenlik zafiyetleri tespit edilmiştir. Bu zafiyetler fiziksel alan güvenliği, personel güvenilirliği ile donanım ve yazılım güvenliği ve güvenilirliği alanlarında gözlemlenmiştir. Tespit edilen güvenlik zafiyetlerinin ilki fiziksel erişim yetkilerinin güncel olmaması ile ilgilidir. Bu konuda kritik lokasyonlar için fiziksel erişim yetkilerinin azami üçer aylık periyotlarda gözden geçirilerek güncelliğinin sağlanması önerilmektedir. Yapılan güvenlik testleri sonucunda tespit edilen bir diğer zayıflık teknik personelin eğitim gereksinimlerini belirleyen yazılı bir prosedürün olmamasıdır. Gerekli teknik eğitim ve gelişim imkanının sağlanabilmesi, personelin bilgi ve beceri düzeyi, yetkinlikleri, iç kontrol ve güvenlik bilinçlerinin şirketin hedeflerine erişebilecek seviyede tutulabilmesi için eğitim planlamalarının prosedürel bir biçimde yapılması önerilmektedir.

Şirkette görev tanımlarının düzenli gözden geçirilmesine yönelik olarak bir prosedür bulunamamıştır. Ayrıca, incelenen görev tanımlarının güncel olmadığı ve organizasyonel yapıyla uyumlu olmadığı gözlemlenmiştir. Görev tanımlarının düzenli olarak gözden geçirilmediği ve güncellenmediği tespit edilmiştir. Rol ve sorumlulukların net olması ve yapılan işin görev tanımlarıyla uyumlu olması için görev tanımlarının düzenli olarak gözden geçirilmesi önerilmektedir.

Personel güvenilirliği alanında tespit edilen son zayıflık, sözleşmeli personel ya da danışmanları kapsayan bir istihbarat prosedürünün olmamasıdır. Özellikle kritik fonksiyonlarda çalışan dış hizmet sağlayıcılarının sabıka kaydı temini, özgeçmiş araştırması gibi bir kontrol prosedüründen geçirilmemesi personelden kaynaklanabilecek güvenlik tehditlerinin oluşması riskini doğurabileceği için kapsamlı bir istihbarat prosedürüne ihtiyaç duyulduğu düşünülmektedir.

Donanım ve yazılım güvenliği ve güvenilirliği alanında tespit edilen zayıflıklar ise aşağıdaki gibidir. Seçilen şebeke elemanlarından SGSN ve GGSN arasında bulunan Gn arayüzünde yapılan incelemeler sonucunda ise şifreleme yapılmadığı tespit edilmiştir. Şebekeye ulaşabilen bir saldırganın abonelere ait trafiği dinleyememesi, değiştirememesi ya da kesememesi için kritik şebeke elemanları arasında şifreleme yöntemlerinin uygulanması önerilmektedir.

Örnek olarak seçilen sistemin veritabanı ve işletim sistemi seviyesindeki güncelleme versiyonlarının üretici firma web sitesinde yayınlanan en son güncelleme ile örtüşmediği tespit edilmiştir. Sistem ve verilerin kötü niyetli yazılımların saldırılarına karşı korumasız kalmaması için kritik güncellemelerin test ve onay süreçlerinden geçirilerek uygulanması önerilmektedir.

Şirket bünyesinde iş sürekliliğine ilişkin süreçlerin belirlenmesinin tam olarak tamamlanmadığı görülmüştür. Network grubunun hazırladığı ve herhangi bir felaket anında network yönetim ekiplerinin uygulaması gereken prosedürleri açıklayan bir teknoloji felaket kurtarma planı oluşturulmuş olmasına rağmen doküman güncelliğini yitirmiş ve mevcut yapıyı desteklememektedir. Ayrıca dokümana ait dağıtım planının

da güncel olmadığı tespit edilmiştir. Olağanüstü durum ya da büyük çaplı bir kesinti meydana gelmesi halinde sorunlara hızlı müdahale edebilmek ve iş sürekliliğini sağlayabilmek için yapısal bir iş sürekliliği yaklaşımının benimsenmesi önerilmektedir.

KAYNAKÇA

Kitaplar

Castro, Dr. Jonathan P., 2001. *The UMTS Network and Radio Access Technology: Air Interface Techniques for Future Mobile Systems.* John Wiley & Sons Ltd

Holma H. & Toskala A., 2006. *HSDPA/HSUPA For UMTS: High Speed Radio Access For Mobile Communications.* John Wiley & Sons Ltd

Holma H. & Toskala A., 2004. *WCDMA for UMTS: Radio Access for Third Generation Mobile Communications.* John Wiley & Sons Ltd

Peltier T., Peltier J. & Blackley J., 2005. *Information Security Fundementals.* Auerbach Publications

Süreli Yayınlar

Ak Ç., (2010). Üçüncü Nesil Mobil UMTS Ağlarında Noktadan Noktaya Hizmet Kalitesi ve Performans Ölçümü *Yüksek Lisans Tezi*. Yıldız Teknik Üniversitesi FBE.

Bilgi Teknolojileri ve İletişim Kurumu, Ağustos 2010. *Bilgi Güvenliği: Riskler ve Öneriler Raporu.* Ankara

Bilgi Teknolojileri ve İletişim Kurumu Sektörel Araştırma ve Stratejiler Dairesi Başkanlığı, Kasım 2010. *Türkiye Elektronik Haberleşme Sektörü Üç Aylık Pazar Verileri Raporu 2010 Yılı 3. Çeyrek Temmuz – Ağustos - Eylül.* Ankara

Computer Security Institute (CSI), 2009. *2009 – Computer Crime and Security Survey*. New York, ABD

Dinçkan A., (2006). GPRS Sistemlerinde Güvenlik *Yüksek Lisans Tezi*. Yıldız Teknik Üniversitesi FBE.

Health M. & Brydon A., 2008. *Wireless Network Traffic 2008–2015*: *Forecasts and Analysis*. Analysis Mason Report

Hobbs P., 2010. Mobile Internet traffic. *Key statistics and global usage trends*. Informa Telecoms & Media

Kamu Bilişim Platformu. 27 Mart 2006. *Bilişim Teknolojilerinde Risk Yönetimi.* Ankara

Market Information and Statistics Division within the Telecommunication Development Bureau of ITU, 2009. *The Information Society Statistical Profiles 2009*. Geneva, İsviçre

Market Information and Statistics Division within the Telecommunication Development Bureau of ITU, 2010. *The World in 2010: ICT Facts and Figures*. Geneva, İsviçre

Meeker M., Devitt S. & Wu L., 2010. *Internet Trends*. Morgan Stanley Report

Sağıroğlu Ş. ve Mohammed M., 2009. Mobil Ortamlara Yapılan Saldırılar Üzerine Bir İnceleme. *Tübav Bilim Dergisi* **2** (2), s.s. 138-147.

Telsim Telekomünikasyon A.Ş. Teknik Eğitim Merkezi, 2001. *GSM'e Giriş Ders Notları*. 2001

Ürper C., (2009). GSM Sektöründe Numara Taşınabilirliği ve Operatör Değiştirme Davranışları: Üniversite Öğrencilerinin Numara Taşıma Niyeti Üzerine Bir Araştırma *Yüksek Lisans Tezi*. Anadolu Üniversitesi SBE.

Vural Y., (2007). Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri *Yüksek Lisans Tezi*. Gazi Üniversitesi FBE.

Vural Y. ve Sağıroğlu Ş., 2008. Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme. *Gazi Üniv. Müh. Mim. Fak. Dergisi* **23** (2), s.s. 507-522.

Yıldız B., (2007). Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması *Yüksek Lisans Tezi*. Gebze Yüksek Teknoloji Enstitüsü SBE.

Diğer Yayınlar

3rd Generation Partnership Project, 1999. *Technical Specification Group Services and System Aspects; 3G Security; Security Threats and Requirements (3G TS 21.133 version 3.1.0.).* 3GPP

Elektronik Haberleşme Güvenliği Yönetmeliği **Resmî Gazete**, 26942; 20 Temmuz 2008

European Telecommunications Standards Institute, 1996. *Telecommunications Security; Guidelines for security management techniques.* ETSI

ISO/IEC 27001:2005, "Information Technology – Security Techniques – Information Security Management Systems – Requirements".

ISO/IEC 27011:2008(E), "Information technology — Security techniques — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002"

IT Governance Institute (ITGI), 2007. Control Objectives for IT and Related Technology (COBIT) 4.1.

IT Governance Institute (ITGI), 2007. Cobit Security Baseline: An Information Security Survival Kit.

IT Governance Institute (ITGI), 2006. Cobit Mapping: Mapping of ISO/IEC 17799:2005 with Cobit 4th Edition.

IT Governance Institute (ITGI), 2007. *IT Assurance Guide Using Cobit.*

Kotapati K., Liu P., Sun Y. & LaPorta T., 2005. *A Taxonomy of Cyber Attacks on 3G Networks*. The Pennsylvania State University, http://nsrc.cse.psu.edu/tech_report/NAS-TR-0021-2005.pdf

Pro-G Bilişim Güvenliği ve Araştırma Ltd., *Bilişim Güvenliği, 2003*, http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf

TS ISO/IEC 27001, *"Bilgi Teknolojisi – Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler"*.

ÖZGEÇMİŞ

Adı Soyadı : M. İlker Naimoğlu

Sürekli Adresi : Bahariye Cad. Dr. İhsan Ünlüer Sk. 6/5 Kadıköy İstanbul

Doğum Yeri ve Yılı : Samsun 1980

Yabancı Dili : İngilizce

İlk Öğretim : Fevzi Çakmak İlkokulu 1991

Orta Öğretim : Kadıköy Anadolu Lisesi 1999

Lisans : İstanbul Teknik Üniversitesi İşletme Mühendisliği Bölümü 2003

Yüksek Lisans : Bahçeşehir Üniversitesi

Enstitü Adı : Fen Bilimleri Enstitüsü

Program Adı : Bilgi Teknolojileri Yüksek Lisans Programı

Yayımları : İş Sürekliliği Planlamasına Genel Bakış Uluslararası Standartlar ve Türkiye'deki Yasal Düzenlemeler, Vergi Dünyası Aylık Dergi Yıl: 27 Sayı: 324 Ağustos 2008 Maliye Hesap Uzmanları Derneği Yayınevi

Çalışma Hayatı : **Ağustos 2008 - Telekom Şirketi / İSTANBUL**

ITIL Süreç Yönetimi ve Servis Güvencesi Destek Kıdemli Uzmanı

Ağustos 2006 / Ağustos 2008 – Deloitte Türkiye / İSTANBUL

Kıdemli Danışman, Bilgi Sistemleri Denetçisi

Ekim 2005 / Ağustos 2006 – Petrol Ofisi A.Ş. / İSTANBUL

Bilgi Sistemleri Denetçisi

Eylül 2004 / Ekim 2005 – Ernst&Young Türkiye / İSTANBUL

Bilgi Sistemleri Denetçi Yardımcısı