İSTANBUL KÜLTÜR ÜNİVERSİTESİ

BİLGİ SİSTEMLERİ ve TEKNOLOJİLERİ DAİRE BAŞKANLIĞI

MOBİL CİHAZ VE TAŞINABİLİR ORTAM KULLANIM PROSEDÜRÜ (MCTOKP)

HAZIRLAYANLAR	KONTROL EDEN	ONAYLAYAN
Ufuk Dikme		
Bilgi Güvenliği Yönetim Müdürü	Bilgi Sistemleri ve Teknolojileri Daire Başkanı	Genel Sekreterlik Temsilcisi

Doküman Kod	IKU-BSTDB-MCTOKP-002	Revizyon Tarihi	
Yayın Tarihi	24.03.2021	Revizyon No	MCTOKP-002-1.0

İÇİNDEKİLER

1. AMAÇ

Veri taşıma diskleri, kişisel müzik çalarlar ve tabletler gibi taşınabilir cihazlar, kullanıcıların mobil olarak işle ilgili veya kişisel verilerine kolay erişim sağlamalarına imkân vermektedir. Bununla birlikte taşınabilir cihazların kullanımı arttıkça, söz konusu cihazların neden olduğu güvenlik riskleri de artmaktadır. Bu cihazları taşınabilir kılan ve çeşitli ağlara ve bilgisayarlara anında bağlanmasını sağlayan özellikleri aynı zamanda fiziksel kontrol ve ağ güvenliği eksikliğine de neden olmaktadır. Taşınabilir cihazların kullanılması, verinin kaybına, istem dışı açığa çıkmasına ve ağ tabanlı saldırılara maruz kalma riskini artırabilmektedir. Bu Prosedür, T.C. İstanbul Kültür Üniversitesi Bilgi Sistemleri ve Teknolojileri Daire Başkanlığı bünyesindeki taşınabilir depolama ortamlarındaki bilgiye yetkisiz erişim ve bilginin hasar görmesi gibi riskleri azaltmak amacıyla yapılması gerekenleri tanımlamak amacıyla hazırlanmıştır.

2. KAPSAM

Bu dokümanda veri aktarımı için bir bilgisayara kablolu bağlantı gerektiren basit medya aygıtları (örneğin, veri taşıma diskleri, medya kartları, CD'ler, DVD'ler ve Wi-Fi özelliği olmayan müzik çalarlar) ile kablolu bağlantı veya hücresel olmayan kablosuz bağlantı ile veri aktarımı yapabilen akıllı medya cihazlarına (örneğin, tabletler, oyun cihazları, Wi-Fi özellikleri olan müzik çalarlar ve elektronik okuma cihazları) ilişkin riskler ele alınmaktadır. Diğer bir taşınabilir cihaz türü olan mobil telefonların güvenliğine ilişin ayrıntılara bu dokümanda yer ver verilmemiştir.

3. TANIMLAR VE KISALTMALAR

KISALTMALAR	TANIMLAR
ANTISPAM	Anti-sapam: software, hardware veya süreci kullanarak sisteme girişi engelleme anlamına gelmektedir.
ANTIVIRUS	Kötü amaçlı yazılımdan koruma olarak da bilinen virüsten koruma yazılımı veya kötü amaçlı yazılımları önlemek, tespit etmek ve kaldırmak için kullanılan bir bilgisayar programıdır.
AUTOPLAY	Windows 98'de tanıtılan bir özellik olan AutoPlay, yeni keşfedilen çıkarılabilir medya ve aygıtları inceler ve resimler, müzik veya video dosyaları gibi içeriğe dayalı olarak içeriği oynatmak veya görüntülemek için uygun bir uygulama başlatır.
AUTORUN	Otomatik Çalıştır ve tamamlayıcı özelliği Otomatik Kullan özelliği, bir sürücü takıldığında sistemin hangi işlemleri yapacağını belirleyen Microsoft Windows işletim sisteminin bileşenleridir.
BLUETOOTH	Bluetooth, kablo bağlantısını ortadan kaldıran kısa mesafe radyo frekansı teknolojisinin adıdır.

CD/DVD	CD (Compact Disc, Taşınabilir Disk) / Digital Versatile Disc (Çok Amaçlı Sayısal Disk)
JAILBREAK	Jailbreak, Apple'ın mobil cihazlarındaki iOS, iPadOS ve TvOS işletim sisteminde bulunan kısıtlamaların kaldırılması amacıyla yapılan erişim işlemidir.
KISMET	Kismet, 802.11 kablosuz LAN'lar için bir ağ detektörü, paket dinleyicisi ve saldırı tespit sistemidir.
ONBOARD	On Board (Dahili/Tümleşik), bir donanımın asıl konumunun neresi olduğunu belirmek için kullanılan bir terimdir.
PIN	Kişisel kimlik numarası bir güvenlik parolasıdır.
USB	Universal Serial Bus: Evrensel Seri Veri yolu. USB dış donanımların bilgisayar ile bağlantı kurabilmesini sağlayan seri yapılı bir bağlantı biçimidir.
WIRESHARK	Wireshark özgür ve açık kaynaklı bir paket çözümleyicisidir. Ağ sorunlarını giderme, çözümleme, yazılım ve iletişim protokolü geliştirme ve eğitim amaçlı olarak kullanılır.
Wİ-Fİ	Wireless Fidelity: Kişisel bilgisayar, video oyunu konsolları, dijital ses oynatıcıları ve akıllı telefonlar gibi cihazların kablosuz olarak birbirlerine bağlanmasını sağlayan teknoloji.

4. MEVCUT RİSKLER

4.1. Basit depolama cihazlarının kullanımı ilk bakışta son derece zararsız gibi görülebilmektedir. Bununla birlikte söz konusu cihazların bireysel veya kurumsal kullanıcılar için birçok güvenlik problemine neden olma potansiyeli bulunmaktadır. Günümüzde zararlı yazılımların yüzde 25'inin USB cihazlar üzerinden yayıldığı bilinmektedir. Bilgisayarınızın USB bağlantı noktasına taktığınız bu cihazlar (veri taşıma diski ya da müzik çalar gibi) bilmeden kopyaladığınız ya da bilgisayarınızın Autorun veya Autoplay özelliği ile otomatik olarak başlatılan zararlı yazılımları içerebilmektedir.

4.2. Buna ilave olarak saldırganların belirli bir tuşa basıldığında veya koşul gerçekleştiğinde kötü niyetli kod başlatmak için klavye ve fare aygıtlarına takılı küçük devre kartları kullanması ile birlikte, saldırılar daha karmaşık ve algılanması zor hale gelmiştir. Zararlı yazılımlar taşınabilir cihazlar aracılığıyla bir bilgisayardan diğerine aktarılmakta, bu bilgisayarların bağlı oldukları ağlar aracılığıyla da hızla yayılabilmektedir.

4.3. Taşınabilir veri depolama aygıtları aracılığıyla bilgisayar veya ağ üzerinde kurulu güvenlik duvarlarının içine zararlı yazılım yüklenebilmektedir. Dolayısıyla bu tip cihazlardan bulaşan zararlı yazılımların büyük hasarlar oluşturana kadar tespiti mümkün olmayabilmektedir. Gizlemesi kolay ve kullanımının izlenmesi zor olduğu için depolama aygıtları, bir kuruluş içinde bulunan kötü niyetli kişilere kolaylıkla ve dikkat çekmeden veri çalma veya sabotaj yapma fırsatı verebilmektedir.

4.4. Yukarıda belirtilen hususlara ilave olarak, zararlı yazılım içeren oyun ya da uygulama indirilen akıllı cihazlar, bağlantı kurulan bilgisayar veya ağlara söz konusu yazılımın bulaşmasına da neden olabilmektedir. Büyük bir nüfus tarafından kullanılmaları ve olgunlaşmamış güvenlik araçları nedeniyle akıllı cihazlar zararlı yazılım saldırılarına karşı nispeten zayıf durumdadır. Ayrıca, kullanıcılar tarafından hassas verilerin bu tip cihazlarda tutulması sıklıkla geri dönülmez veri ifşası ya da veri kaybı olaylarının yaşanmasına neden olmaktadır. Örneğin birçok kullanıcı kişisel banka hesap numaralarını veya özel müşteri bilgilerini güvenilmeyen uygulamalar içeren veya korumasız ağlara bağlanan akıllı cihazlar üzerinde tutmaktadır.

4.5. Buna ek olarak, akıllı cihazları çok cazip kılan Bluetooth ve Wi-Fi gibi özellikler aynı zamanda önemli ölçüde risk oluşturmaktadır. Örneğin Bluetooth özelliği açıldığında cihaz kablosuz kulaklıkla bağlantı sağlamakta aynı zamanda da bağlantıdan yararlanmak isteyen kötü niyetli saldırganların için keşfedilebilir hale gelmektedir. Ayrıca ev ve kamuya açık alanlarda yer alan Wi-Fi ağları saldırganlar tarafında sıklıkla hedef alınmaktadır. Saldırganlar genellikle bu ağlarda Kismet ve Wireshark gibi araçları kullanarak şifrelenmemiş verileri elde etmektedir.

4.6. Depolama aygıtları ve akıllı cihazların genellikle küçük boyutlu ve kolay taşınabilir olmaları, cihazların kolaylıkla kaybolmalarına veya unutulmalarına neden olabilmektedir. Hassas veri bulunduran taşınabilir cihazların kaybolması bireysel ve kurumsal kullanıcılar için ciddi bir problem olabilmektedir.

4.7. Akıllı telefonlarda en büyük güvenlik riski içeren uygulamalar bu kategoride bulunmaktadır. Bu sınıftaki uygulamaların nihai amacı kullanıcıya ait tüm bilgilerin bir merkezde toplanması ve bunu talep eden kullanıcıya online olarak gönderilmesidir. Bu sınıftaki uygulamaların en önemli özelliği telefonda yüklü olup olmadıklarının tespit edilememesidir. Aynı zamanda uygulamanın kaldırılması da mümkün olmamaktadır.

4.8. Bu sınıftaki uygulamaların kendilerine ait internet sayfalarında genellikle; çocuklarınızın güvenliği için takip edin, telefonunuzun çalınması durumunda verilerinizi ve telefonunuzu takip edin, çalışanlarınızın iş telefonlarını takip edin, gibi tanıtımlarla casus yazılımların reklamı yapılmaktadır. Casus yazılımlar ile yapılabilecekler aşağıdaki gibi listelenebilir.

4.8.1. *Ortam Dinlemesi:* Telefonun mikrofonu kullanılarak, kullanıcının haberi olmadan ortamda bulunan sesler kaydedilebilir ve bunlar belirlen hedefe yüklenebilir. Yapılabilecek ayarlamalar ile kaydedilecek ses süresi dahil belirlenebilmektedir.

4.8.2. *Gizli Kamera:* Telefonun kamerası kullanılarak bulunan ortamın fotoğrafı gizlice çekilebilir. Çekilen bu fotoğraflar belirlenen hedefe yüklenebilir ve buradan kullanıcı fotoğrafları temin edebilmektedir.

4.8.3. *Kısa Mesaj Bilgileri:* Telefona gelen ve telefondan gönderilen tüm kısa mesajlar kaydedilir ve program sahibi bunları takip edebilir.

4.8.4. *Konum Bilgileri:* Telefonun bulunduğu konum anlık ve sürekli olarak kayıt altına alınabilir. Böylece telefon sahibinin coğrafi olarak takibi de gerçekleştirilebilir.

4.8.5. *Arama Bilgileri:* Telefona gelen ve telefondan yapılan tüm aramaların kayıtları tutulabilir. Görüşmeye ait telefon bilgisi, zaman ve süre bilgisi tüm detaylar bu kayıtlar ile tutulabilmektedir.

4.8.6. *Internet Bağlantı Bilgileri:* Kullanıcının telefondan girdiği tüm internet adresleri ve bu internet adreslerinde kullandığı kullanıcı adı, şifre gibi tüm bilgiler takip edilebilmektedir.

4.8.7. *Dosya Bilgileri:* Telefonun dahili hafızasında bulunan fotoğraf ve video gibi tüm dosyalar belirlenen hedefe yüklenerek buradan takip gerçekleştirilebilmektedir.

4.8.8. *Sosyal Medya Bilgileri:* Kullanıcının telefonunda kullandığı Facebook, Twitter, Whatsapp gibi sosyal paylaşım uygulamalarında paylaştığı tüm bilgiler, gönderdiği ve gelen tüm mesajlar takip edilebilmektedir.

4.8.9. *E-Posta Bilgileri:* Telefonun e-posta uygulaması ile gönderilen ve gelen tüm e-posta bilgileri takip edilebilmektedir.

4.8.10. *Uygulama Bilgileri:* Telefona yüklenen tüm uygulamalara ait uygulamanın yüklenme tarihi, versiyonu gibi tüm bilgiler takip edilebilmektedir.

4.8.11. *Rehber Bilgileri:* Telefon rehberine kayıt edilen tüm kişilere ait bilgiler, telefonda bulunan şekliyle kayıt edilip takip edilebilmektedir.

4.8.12. *Takvim Bilgileri:* Telefona takviminde bulunan tüm olaylar ve önemli tarihler, kayıt edilen bilgiler takip edilebilmektedir.

4.8.13. *Uygulama Engelleme:* Telefona yüklenen bazı uygulamaların ya da telefonda yüklü bulunan bazı uygulamaların çalışması engellenebilmektedir.

4.8.14. *Uzaktan Program Kaldırma:* Casus yazılım ihtiyacının ortadan kalkması durumunda bu uygulama uzaktan telefondan kaldırılabilmektedir.

4.8.15. *Kısa Mesaj ile Kontrol:* Telefonu kilitleme, kilidi açma, anlık GPS konumunu öğrenme gibi anlık bilgi talebi durumunda, bunlar kısa mesaj ile telefonun kontrolü sağlanarak gerçekleştirilebilmektedir.

4.8.16. *Uyarı Sistemi:* Telefonda veya kullanıcının bazı hareketlerinde anında bilgilendirilmek istendiği durumlarda uyarı sistemi kullanılabilmekte ve belirlenen şartların oluşması durumunda uyarı program sahibine gönderilebilmektedir.

4.9. Telefonlarda kullanılacak casus yazılımlar ile gerçekleştirilebilecek işlemler, neredeyse kullanıcıya ait tüm bilgilerin takibini sağlamaktadır. Kullanıcının farkında olmadan gerçekleştirdiği faaliyetler, programlar sayesinde anlık olarak takip edilip kayıt altına alınabilmektedir.

4.10. Piyasada casus yazılımların genelde özelliklerine ve kabiliyetlerine göre fiyatları bulunmaktadır. Bununla beraber, daha az kabiliyetli olmalarına rağmen ücretsiz uygulamaların temin edilmesi de mümkün olmaktadır.

5. RİSKLERİ AZALTMAYA YÖNELİK UYGULAMALAR

5.1. Veri Depolama Cihazları İçin Yapılması Gerekenler

Veri depolama ve taşıma cihazları, CD ve Wi-Fi özelliği olmayan müzik çalarlar gibi depolama ortamı kullanırken aşağıdakiler uygulanmalıdır:

5.1.1. Bilgisayarınıza çevresel porttan bağlanan (USB gibi) her cihazı tarayan bir anti-virüs yazılımı yükleyin.

5.1.2. Bulunan ve geçmişi hakkında bilgi sahibi olmadığınız bir veri depolama cihazını asla bir bilgisayara bağlamayın. Bu cihazları depolama aygıtını bulduğunuz yere en yakın güvenliğe veya Bilgi Sistemleri ve Teknolojileri personeline verin.

5.1.3. Tüm taşınabilir medya aygıtları için Autorun ve Autoplay özelliklerini devre dışı bırakın. Bu özellikler USB portuna takılan veya bir sürücüye yerleştirilen taşınabilir medyayı otomatik olarak açar.

5.1.4. Kişisel ve iş verilerinizi ayrı tutun. Kişisel müzik çalarınızı iş bilgisayarınıza takmayın, ya da işte kullandığınız veri depolama cihazınızı ev bilgisayarınıza takmayın.

5.1.5. Taşınabilir cihazlarda yer alan hassas verileri şifreleyin. Ayrıca güvenli bir yerde bir yedek kopya bulunduğundan emin olun.

5.1.6. Bilgisayarınıza (ve ağdaki tüm bilgisayarlara), güvenlik duvarı, anti-virüs ve anti-spyware yazılımlarını yükleyin. Otomatik güncellemeleri etkinleştirin veya bilgisayarınızdaki tüm yazılımların güncel güvenlik yamalarının yapılmasını sağlayın.

5.1.7. Hassas verilerin bir USB sürücüden aktarılması durumunda, güvenli bir silme programı kullanarak USB sürücüden verilerin sildiğinden emin olun.

5.1.8. Gerekli durumlarda otomatik olarak kendisini ve takıldığı bilgisayarı tarayan onboard anti-virüs yeteneğine sahip taşıma sürücüleri kullanın.

5.2. Akıllı Cihazlar İçin Yapılması Gerekenler

Tablet, Wi-Fi özelliği olan müzik çalarlar ve elektronik okuyucu gibi akıllı cihazları kullanırken aşağıdakiler uygulanmalıdır:

5.2.1. Cihazda tahmin edilmesi kolay olmayan nitelikte, güçlü şifre veya PIN kullanın ve periyodik olarak değiştirin. Uygulama ve oyun yüklemeden önce, söz konusu oyun veya uygulamanın cihazınızda ne tür erişim yetkilerinin olacağını öğrenin. Birçok uygulama yükleme aşamasından önce erişim yetkisi bilgilerini kullanıcıya göstermektedir. Bu tip bilgileri paylaşmayan uygulama veya oyunları yüklemeyin.

5.2.2. Uygulama, oyun ve müzik için sadece güvenilir kaynaklardan indirme yapınız. Örneğin, yalnızca tanınmış oyunları saygın ve doğrulanmış satıcılardan veya cihazın üretici veya sağlayıcı tarafından desteklenen ticari mağazasından indirin.

5.2.3. Zararlı yazılımlara karşı yazılımlar kullanın cihazınızı periyodik olarak tarayın.

5.2.4. Mümkün olduğu durumlarda, gelen ve giden trafiği filtrelemek ve zararlı yazılımları bloklamak için cihaz üzerinde yerel bir güvenlik duvarı kurun.

5.2.5. Kullanmadığınız zaman cihazı otomatik olarak kilitleyecek bir zaman aşımı periyodu ayarlayın.

5.2.6. Cihazı "kırdırmayın". "Kırdırmak" veya "jailbreak yapmak" terimi genellikle özel işletim sistemi bileşenleri veya diğer üçüncü parti yazılım kurularak, üretici tarafından cihaz üzerinde uygulanan sınırlamaları kaldırmak için kullanılmaktadır. Bu tip işlemler cihazda bulunan, zararlı yazılımlara karşı önlemleri kaldırdığından güvenlik açıklıklarına neden olmaktadır.

5.2.7. Kullanmadığınız zaman, Bluetooth, Wi-Fi ve diğer hizmetleri devre dışı bırakın.

5.2.8. Wi-Fi kullanırken, ev ve kurumsal ağınızı şifrelediğinizden emin olun.

5.2.9. Yarı-güvenilir bir ortamda (örneğin, kablosuz erişim noktasına güvendiğinizde fakat ağdaki diğer kullanıcılara güvenmediğinizde) VPN kullanın veya başka bir şekilde trafiğinizin şifreli olduğundan emin olun.

5.2.10. Bluetooth kullanırken, kimliği doğrulanmamış cihazlara karşı cihazınızı görünmez konuma ayarlayın.

5.2.11. Tabletler üzerinde saklanan verileri şifreleyin. Ayrıca verilerin güvenli bir yerde saklanan yedek bir kopyasını tuttuğunuzdan emin olun.

5.2.12. Varsa, kaybolduğunda cihaz üzerindeki tüm verileri silmek için uzaktan silme özelliğini etkinleştirin.

5.3. Kurumsal Kullanıma Yönelik Yapılması Gerekenler

Kurumsal düzeyde her türlü taşınabilir cihazın kullanımında aşağıdakiler uygulanmalıdır:

5.3.1. Geçerli bir gerekçe veya ihtiyaç bulunan durumlar haricinde, tüm taşınabilir medya aygıtlarının kullanımını sınırlayın.

5.3.2. Tüm taşınabilir medya aygıtları için güvenlik ve kabul edilebilir kullanım politikaları oluşturun ve bu politikalar konusunda çalışanların eğitilmesini sağlayın.

5.3.3. Çalışanların kayıp cihazlarını derhal bildirmeleri konusunda bilinçlendirilmesini sağlayın.

5.3.4. Güvenlik özelliklerini ve açıklarını dikkate alarak kullanılacak cihazları seçip sadece bu cihazları destekleyin.

5.3.5. Güçlü şifre ve PIN kullanımı konusunda çalışanların bilinçlendirilmesini sağlayın.

5.3.6. Kurumsal ağa erişimi sadece güvenli bir VPN bağlantısı üzerinden sağlayın.

5.3.7. Gerekli olması halinde işyerinde izlenemeyen ya da kontrol edilemeyen kişisel, taşınabilir medya aygıtlarının kullanımını yasaklayın.

5.3.8. Kuruluşun web sunucularını SSL güvenlik özelliklerini kullanacak şekilde yapılandırın.

5.3.9. Gerekli durumlarda çalışanların sınırlandırılmış, kurum-kontrolünde cihazlar ile çalışmasını sağlayın.

5.3.10. Gerekli durumlarda hassas şirket bilgilerini taşıyabilecek mobil cihazların envanterini tutun ve bu cihazları düzenli olarak denetleyin.

5.4. Akıllı Telefonlar İçin Yapılması Gerekenler

5.4.1. *Ekran Koruyucu Şifre:* Telefonun kaybolması veya çalınması gibi durumlarında, telefonun izinsiz kullanımını önlemek için telefonun ana ekranına şifre/PIN/ekran koruması koyun.

5.4.2. *Cihazın Temel Güvenlik Ayarları:* Güvenlik ayarları üzerinde değişiklik yapmayın. Telefonun fabrika ayarlarının ve işletim sisteminin ayarlarının değiştirilmesi (jailbreak, rooting) gibi işlemler, akıllı telefonun siber saldırılara karşı daha duyarlı yaparken, işletmeci ve akıllı telefon tarafından sunulan güvenlik özelliklerini zayıflatmaktadır.

5.4.3. *Telefonun Yedeklenmesi ve Veri Güvenliği:* Telefonda saklanan bütün verileri (rehber öğeleri, belgeler, fotoğraflar vb.) yedekleyin. Söz konusu bu veriler kişisel bilgisayarlarda ve harici depolama aygıtlarında saklanabilir.

5.4.4. *Uygulama Erişim Yetkilerinin Kontrolü:* Uygulamaların, akıllı telefonlarınızda bulunan kişisel bilgilerinize erişme yetkisi konusunda dikkatli olun. Aksi halde indireceğiniz uygulama ile kişisel bilgileriniz (örneğin konum veriniz) üzerinde işlem yapılmasına izin vermiş olabilirsiniz. Ayrıca yüklemeden önce her uygulama için gizlilik ayarlarını kontrol ettiğinizden emin olun.

5.4.5. *Güvenilir Kaynaklardan Uygulama Yüklenmesi:* Bir uygulamayı indirmeden önce, uygulamanın yasal ve güvenilir olduğundan emin olmak için araştırma yapın. Akıllı telefonlara indirilecek uygulamaları, işletim sisteminin resmi uygulama ortamından edinin.

5.4.6. *Uzaktan Erişim ile Silmeyi Etkinleştirecek Güvenlik Uygulamaları:* Akıllı telefonlarda, uygulama olarak edinilebilecek veya varsayılan olarak yaygın olarak kullanılan önemli bir güvenlik özelliği; telefonun GPS'i kapalı olsa bile, telefonunuzda depolanan tüm verilere uzaktan erişebilmeye ve söz konusu verileri silebilmeye imkân sağlamasıdır. Bu durumda telefonunuzu kaybettiğinizde, telefonunuz sessiz olsa bile bazı uygulamalar yüksek sesli bir alarmı aktif edebilir. Bu uygulamalar aynı zamanda telefonunuzu kaybettiğinizde daha kolay bulabilmenize yardımcı olabilir.

5.4.7. *Açık Wi-Fi Bağlantıları:* Şifresiz herkese açık kablosuz ağ trafiği bu hizmeti bedava veren kişi tarafından dinleniyor olabilir. Halka açık ağ kullanımını kısıtlamalı ve onun yerine güvenebileceğiniz bir operatöre ait güvenli Wi-Fi veya kablosuz mobil bağlantı kullanın.

5.4.8. *Yazılım Güncellemelerinin Yapılması:* Otomatik güncellemeleri etkinleştirerek, telefonunuzun işletim sistemini güncel tutmalısınız veya servis sağlayıcınızdan, işletim sistemi sağlayıcınızdan, cihaz üreticisinden ve uygulama sağlayıcınızdan gelen güncellemeleri kabul etmelisiniz. İşletim sisteminizi güncel tutarak, siber tehditlere maruz kalma riskinizi azaltabilirsiniz.

5.4.9. *Telefon Verilerinin Silinmesi:* Telefonunuzu satmak istemeniz durumunda, akıllı telefonunuzda kişisel verileriniz olabileceğini unutmayın. Gizliliğinizi korumak için, verileri tamamen silin veya telefonunuzu fabrika ayarlarına sıfırlayın. Aynı zamanda sıfırlama işleminin; telefonunuzda yer alan uygulamalar, mesajlar, arama geçmişi, müzik, fotoğraf gibi içeriklerin silinmesini de kapsadığını unutmayınız.

5.4.10. *Çalınan Telefonun Bildirilmesi:* Telefonunuzun çalınması veya kaybolması durumunda, hattınızı kapatmak için işletmenize başvurun. Telefonunuzun ülkemizde kullanımını engellemek için durumu Bilgi Teknolojileri ve İletişim Kurumu'na (BTK)(www.btk.gov.tr) bildirebilirsiniz.

5.4.11. *Uygulama Marketinde Kredi Kartı Kullanımı:* Sadece ücretsiz uygulamaları kullanıyorsanız telefonunuzun uygulama marketinde kullanıcı oluştururken bunu sizden talep etse de kredi kartı bilgilerinizi girmeyiniz. Uygulama satın almayı düşünüyorsanız limiti düşük sanal kart bilgilerinizi kullanmalısınız. Ek olarak kredi kartı ekstrenizi düzenli olarak takip edin.

5.4.12. *Telefondaki Verilerin Şifrelenmesi:* Eğer telefonunuzun veri şifreleme özelliği varsa bu özelliği kullandığınızdan emin olun. Böyle bir özellik yoksa, veri şifreleyen uygulama kullanın. Telefonun çalınması ya da kaybolması durumunda veriler ele geçirilse bile ilgili şahıs tarafından kullanılamayacak ve anlaşılamayacaktır.

6. REVİZYON BİLGİSİ

Revizyon Numarası	Yürürlük Tarihi	Revizyon Tanımı	Hazırlayanlar