Taşınabilir Cihaz Kullanımına İlişkin Riskler

Ulusal Siber Olaylara Müdahale Merkezi (USOM -TRCERT)
Bilgi Teknolojileri ve İletişim Kurumu
Telekomünikasyon İletişim Başkanlığı
Tel: (0312) 586 53 05
Web: www.usom.gov.tr
E-posta: iletisim@usom.gov.tr

Kasım 2014
UR.RHB.006

İÇİNDEKİLER

1. GİRİŞ

Veri taşıma diskleri, kişisel müzik çalarlar ve tabletler gibi taşınabilir cihazlar, kullanıcıların mobil olarak işle ilgili veya kişisel verilerine kolay erişim sağlamalarına imkan 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 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.

2. MEVCUT RİSKLER

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.

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.

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.

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.

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.

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.

3. RİSKLERİ AZALTMAYA YÖNELİK UYGULAMALAR

İster bir kuruluşta çalışıyor olun ister bir ev kullanıcısı olun, taşınabilir cihazların kullanımı ile ilgili riskleri azaltmak için yapılabilecek çeşitli uygulamalar bulunmaktadır. Bireysel ve kurumsal kullanıcılar için önerilen uygulamalar aşağıda açıklanmaktadır.

3.1 VERİ DEPOLAMA CİHAZLARI İÇİN ÖNERİLEN UYGULAMALAR

Veri depolama ve taşıma cihazları, CD ve Wi-Fi özelliği olmayan müzik çalarlar gibi depolama ortamı kullanırken aşağıdaki uygulamaların yapılması tavsiye edilmektedir.

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

• 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 işlem personeline verin.

• 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.

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

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

• 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.

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

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

3.2 AKILLI CİHAZLAR İÇİN ÖNERİLEN UYGULAMALAR

Tablet, Wi-Fi özelliği olan müzik çalarlar ve elektronik okuyucu gibi akıllı cihazları kullanırken aşağıdaki uygulamaların yapılması tavsiye edilmektedir.

• 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.

• 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.

• Zararlı yazılımlara karşı yazılımlar kullanın cihazınızı periyodik olarak tarayın.

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

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

• 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.

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

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

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.

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

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

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

3.3 KURUMSAL KULLANIMA YÖNELİK GENEL UYGULAMALAR

Kurumsal düzeyde her türlü taşınabilir cihazın kullanımında aşağıdaki uygulamaların yapılması tavsiye edilmektedir.

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

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

• Çalışanların kayıp cihazlarını derhal bildirmeleri konusunda bilinçlendirilmesini sağlayın.

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

• Güçlü şifre ve PIN kullanımı konusunda çalışanların bilinçlendirilmesini sağlayın.

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

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

• Kuruluşun web sunucularını SSL güvenlik özelliklerini kullanacak şekilde yapılandırın.

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

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

4. SONUÇ

Taşınabilir aygıtların kullanılması birçok kolaylık sağlarken, çeşitli güvenlik risklerini de beraberinde getirmektedir. Güvenlik risklerinin tamamıyla ortadan kaldırılması mümkün olmasa da tavsiye edilen uygulamaların söz konusu risklerin azaltılması açsısından faydalı olacağı değerlendirilmektedir.

5. KAYNAKLAR

[1] Ruggiero, P. & Foote, J. 2011. *Cyber Threats to Mobile Phones.* Carnegie Mellon University.

http://www.us-cert.gov/sites/default/files/publications/cyber_threats-to_mobile_phones.pdf

[2] Walters, P. 2012. *The Risks of Using Portable Devices.* Carnegie Mellon University.

http://www.us-cert.gov/sites/default/files/publications/RisksOfPortableDevices.pdf

[3] US-CERT. 2014. *Protecting Portable Devices: Data Security.* Alerts and Tips.

http://www.us-cert.gov/ncas/tips/ST04-020

[4] US-CERT. 2014. *Protecting Portable Devices: Physical Security.* Alerts and Tips.

http://www.us-cert.gov/ncas/tips/ST04-017