Güvenilir Uygulama Mağazaları: Güvenlik ve Bütünlüğün Korunması

Şubat 2024

Derleyen:
Heather West | Kıdemli Müdür
+1 202.344.4597
HEWest@Venable.com

Tim McGiff | Proje Yöneticisi
+1 202.344.4365
TCMcGiff@Venable.com

CENTER FOR
CYBERSECURITY
POLICY AND LAW

İçindekiler

Yönetici Özeti

Avrupa Birliği (AB), dijital pazarlar için yeni politikalar ve düzenlemeler getirirken, ekonomik faktörleri dikkatlice göz önünde bulundurmalı ve aynı zamanda erişim, gizlilik ve güvenlik gibi konuları dengelemelidir. Ancak, Dijital Pazarlar Yasası'nın (DMA) mobil uygulama mağazası hükümleri, mobil telefon ekosistemini güvenilir ve dayanıklı kılan temel güvenlik kontrollerini zayıflatabilir. Siber Güvenlik Politikası ve Hukuk Merkezi, kullanıcıları aşırı yükleme seçenekleriyle karşı karşıya bırakmanın ve kötü niyetli aktörlerin onları kötüye kullanma olasılığını artırmanın endişesini taşımaktadır. Ancak, bu durum kullanıcıların korunamayacağı anlamına gelmez. Önlem almak için şirketlerin ve kullanıcıların harekete geçmeleri gerekecektir. Bu makale, AB vatandaşlarının, cihazlarının ve verilerinin karşı karşıya olduğu potansiyel riskleri ve bu riskleri azaltma yaklaşımlarını ele almaktadır. Ayrıca, düzenleyicilerin ve politika yapıcıların, mobil ekosistemdeki kullanıcı güvenini sağlamak ve kullanıcılar ile işletmeler arasındaki potansiyel güvenlik etkilerini hafifletmek için önerilerini sunmaktadır. Ayrıca, bu raporun diğer ülkelerin kendi dijital pazarlarında rekabeti teşvik ederken vatandaşlarının güvenliğini ve gizliliğini korumalarına yardımcı olabilecek bir kılavuz olmasını umuyoruz.

Siber Güvenlik ve HukukMerkezi Hakkında

Siber Güvenlik Politika ve HukukMerkezi, hükümete, özel sekötüreve sivil topluma güvenlikle ilgili tehditlerin daha iyi yönetilmesi için uygulama ve politikalar sağlayarak dünya çapında siber güvenliğin geliştirilmesini amaç edinen bağımsız bir kuruluştur. 2017 yılında Venable LLP'nin Siber Güvenlik Hizmetleri grubu dahilinde 501(c)(6) kategorili kâr amacı gütmeyen bir kurum olarak kurulan Merkez, politika koalisyonlar kurmak ve somut sonuçlar getiren girişimler başlatmak üzere küresel, ulusal ve yerel düzeylerdeki güçleri politika alanındaki uzmanlığı ile bir araya getirmektedir. Fikir birliğine yönelik ve risk yönetimi temelli bir yaklaşım uygulayan Merkez, dijital altyapı ve bilişim sistemlerinin ön cephelerinde yer alan kişilerin perspektifleri ve uygulamalarından alınan pragmatik çözümler ve politika önerilerini destekleyerek siber güvenlikle ilgili karmaşıklıklara açıklık getirmeyi ve bu konudaki kafa karışıklıklarını gidermeyi amaçlamaktadır.

Giriş

Giderek daha da fazla bağlantılı bir hale gelen dünyamızda, hizmetler, bilgi ve kaynaklardan oluşan zengin bir ekosistem ile etkileşim kurmak için cep telefonlarımızdan yararlanmaktayız. Cep telefonlarımızın avantajları yaygın olarak bilinmektedir.[1] Cep telefonları, dünyaya açılan pencerelerimizdir. Sağlığımızı kontrol etmekte, arkadaşlarımızla paylaşım yapmamızı, ürünler satın almamızı ve hizmetleri yönetmemizi sağlamaktadırlar. Dolayısıyla, mobil uygulamalarımızda her gün dört ile beş saat veya üzerinde, önemli miktarda zaman harcamaktayız.[2] Bu nedenle, cihazlarımız ve uygulamalarımızın güvenli ve güvenilir olmaya devam etmesi çok önemlidir.

Araştırmalara göre, Amerika Birleşik Devletleri'nde 18 ila 34 yaş arası tüketicilerin %81'i sahip oldukları cihazların güvenli olduğunu düşünmektedir.[3] İşletim sistemi geliştiricileri ve uygulama mağazalarının bu ekosistemlerin güvenli olması için harcadıkları çabalar sayesinde insanların böyle düşünmesi şaşırtıcı değil.

Mobil Gelecek: Mobil Güvenlik ve Gizlilik Alanında Sürekli Gelişimin Yolları adlı 2021 tarihli araştırmamızda,[4] endüstri, akademi ve sivil toplumdan yirmi üç siber güvenlik uzmanı ile mobil güvenliği tartıştık ve "mobil cihazlara yönelik yeni tehditler oluşmaya devam etse de geçerli korumaların, siber güvenliğin diğer alanlarına kıyasla daha iyi performans gösterdiği"[5] sonucuna vardık. Bu odak grubu çalışmamızdaki ortak görüş, mobil ortamın işletim sistemi (OS) ve uygulama mağazası düzeyinde entegre güvenlik ve gizlilik korumalarından avantaj sağladığı ve dolayısıyla kendilerini korumaları için kullanıcıların üzerine düşen yükü azalttığı şeklinde olmuştur.

Henüz üç yıl önce gerçekleştirilen bu araştırma, tanınmış işletim sistemi geliştiricileri ve bunların güvenilir, resmi uygulama mağazalarının geçerli mobil yapıları ve güvenlik özellikleri bağlamında yapılmıştır. Son on yıllık dönem içerisinde mobil ekosistem giderek daha güvenli hale gelmiştir. Ancak, Avrupa Birliği'nin rekabet odaklı DMA[6] yasasının uygulamaların yüklenmesine yönelik hükümleri güvenlik bakımından bu ilerlemeyi sürdürmek yerine bu ekosistemin gerilemesine neden olabilir. Güvenlik bakımından elde edilen bu ilerlemeyi sürdürdüğümüzden emin olmak için beraber çaba sarf etmemiz gereklidir.

DMA'nın hükümleri, işletim sistemlerinin başka kaynaklardan uygulama yüklenmesine izin verme zorunluluğu getiriyor. Bu, kullanıcılar için baskı yaratabilirken, mobil cihaz yönetimi uygulayan kurumsal yöneticiler için bir engel teşkil edebilir ve kötü niyetli kişilere yeni fırsatlar sunabilir. Bu risklerin azaltılması için, önemli pazar payına sahip mobil işletim sistemlerinin

---

[1] https://www.pewresearch.org/internet/2019/03/07/majorities-say-mobile-phones-are-good-for-society-even-amid-concerns-about-their-impact-on-children/

[2] Techcrunch aracılığıyla Data.ai, mobil kullanıcıların uygulamalarda günde 4-5 saat arası zaman harcadığını bildirdi - bağlantı

[3] https://staysafeonline.org/wp-content/uploads/2022/07/Cybersecurity-Awareness-Month-2020-Results-Report.pdf

[4] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[5] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[6] Dijital Pazarlar Yasası'nın metnine aşağıdaki bağlantıdan ulaşabilirsiniz: https://eur-lex.europa.eu/eli/reg/2022/1925

desteklenmesi gerekecek ve DMA'nın hedeflerini gerçekleştirmek için daha açık bir ekosistemi dengeli bir şekilde yönetmek için makul yaklaşımlar benimsenmelidir. Bu araştırmada, DMA dahilindeki uygulama mağazası hükümleri ve bu hükümlerin mobil ekosisteme yönelik artırdığı tehditleri kısaca özetleyip birinci taraf uygulama mağazası ve mobil OS sahiplerinin geçmişte bu tehditler ile nasıl mücadele ettiği hakkında kısa bir inceleme sunulacaktır. Bu araştırmada, hazırlıksız nihai kullanıcıların mobil ekosistem ve cihazlarının güvenliğinden bir anda kendilerinin sorumlu olmaması için AB'ye üye devletlerin DMA'nın uygulanmasında desteklemesi gereken yaklaşım çeşitlerini açıklanacaktır.

DMA metninde kullanıcıların korunması için hem teknik hem de sözleşme düzeyinde potansiyel yollara atıfta bulunulmaktadır. Ayrıca, kanun koyucular ve yönetmelik belirleyicilerin, uygulama revizyonları, kötü yazılımlara karşı artırılmış koruma, şeffaflık gereklilikleri ve izin ayarları ile mobil cihazların işletim sistemlerine entegre güvenlik modelleri aracılığıyla kullanıcıları koruyan sistem geliştiricilerin görevini desteklemelidir. Canlı ve yenilikçi bir mobil ekosistem oluşturmak üzere beraber çalışmamız önemlidir. Politika yapıcıların DMA'nın uygulamaya yönelik hükümlerinde ve önemli pazar gücüne sahip dijital platformlarınnuyuma yönelik çalışmalarında güvenliğin önemini vurgulamasını önermekteyiz.

DMA(Dijital Pazarlar Yasası) Uygulama Mağazası Hükümleri

Mart 2024 itibarıyla DMA kapsamında, "geçit bekçisi(önemli pazar gücüne sahip dijital platformlar) " tanımı kapsamına giren, "kilit platform hizmetleri" sunan şirketler, uygulama mağazaları ve üçüncü taraf uygulama mağazası ve uygulamalar ile mobil OS etkileşimleri ile ilgili olarak DMA hükümlerine tabi olacaktır. Geçit bekçileri, Avrupa Komisyonu tarafından tanımlandığı şekliyle, Avrupa piyasasında önemli bir etkisi olan ve işletmeler (örn. uygulama geliştiricileri) ile nihai kullanıcılar (örn. uygulamaları yükleyen cep telefonu kullanıcıları) arasındaki ilişkiye aracılık eden bir hizmet sunan şirketlerdir.[7] DMA'nın amacı, Avrupa temelli daha küçük şirketlerin piyasada daha "köklü" konuma sahip ülkeler ile rekabet edebilmesini kolaylaştırmaktır.

DMA hükümleri, mobil işletim sistemlerinin, uygulama mağazaları dışındaki kaynaklardan veya diğer yöntemlerle uygulama yükleme imkanı sağlamasını ve işletim sistemlerinin, birinci ve üçüncü taraf uygulamalara aynı sistem erişimi ve araçları sağlamasını gerektirmektedir..Bu hükümlerin merkezinde aşağıdakiler yer almaktadır:

- *Bölüm 6.4:Avrupa Komisyonu tarafından Geçit Bekçisi olarak tanımlanmış dijital platformlar,Geçit bekçilerii, kendi işletim sistemini kullanan veya bununla beraber çalışan üçüncü taraf yazılım uygulamaları veya yazılım uygulama mağazalarının kurulumu ve etkin bir şekilde kullanımına izin verecek ve bunu teknik olarak mümkün kılacak, bu yazılım uygulamaları veya yazılım uygulama mağazalarına işbu denetçinin ilgili kilit platform hizmetleri dışında yollarla erişilmesine izin verecektir.*

- *Bölüm 6.7: Geçit bekçisi dijital platformlar, hizmet sağlayıcıları ile donanım sağlayıcılarının, işletim sistemi veya sanal asistan [...] aracılığıyla erişilen veya kontrol edilen aynı donanım veya yazılım özellikleri ile beraber etkin çalışması ve beraber çalışma amaçlı erişimine ücretsiz olarak izin verecektir. Ayrıca, denetçi, [...] aynı işletim sistemi, donanım veya*

[7] Bu çalışmanın yayınlandığı tarih itibarıyla, Apple'ın iOS işletim sistemi ile Google'ın Android işletim sistemi, kilit platform hizmetleri olarak değerlendirilmektedir. Microsoft'un Windows masaüstü bilgisayar işletim sistemi de kilit bir platform hizmeti olsa da bu araştırmanın kapsamı dışındadır. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

Bu DMA hükümleri, diğer Avrupa Birliği yasaları ile bir araya geldiğinde önemli pazar gücüne sahip uygulama mağazalarının mobil cihazlarda üçüncü taraf uygulamaları ve uygulama mağazalarını daha kolay kurmasına izin vermesini, mobil kullanıcılarca üçüncü taraf uygulama mağazalarına daha kolay erişime izin vermesini ve mevcut durumda denetçilerin mobil işletim sistemlerinin sahip olduğu aynı erişim, beraber çalışma ve işlevselliği üçüncü taraf geliştirici ve uygulamalara sunmasını gerektirecektir.

Bu hükümlere ek olarak ve mobil ekosistemin "açılması" ile ortaya çıkan güvenlik ve gizlilik riskini vurgulayan ancak pek bahsedilmeyen bir güvenlik uyarısı bulunmaktadır. DMA'nın gererkçesinin anlatıldığı dökümanın 50. maddesi, üçüncü taraf uygulama ve uygulama mağazalarına sağlanan ek erişimin kullanıcı ve cihaz güvenliğini tehlikeye atmaması gerektiğini belirtmektedir. Ancak, DMA, işletim sistemlerinin, uygulamalara erişimi sınıflandırma ve engelleme bakımından getirilen sınırlamalar göz önünde bulundurulduğunda mobil cihazları ve kullanıcıları nasıl korumasını beklediğini açıklamamaktadır. DMA'nın yukarıdaki hükümleri, dikkatli bir şekilde değerlendirilmeden uygulandıklarında mevcut mobil tehdit ekosistemini kötüleştirebilir.

Mobil Tehdit Ekosistemi

Mobil cihazlara yönelik kötü amaçlı yazılımlarla mücadele, mobil işletim sistemi geliştiricileri ve dünya çapında kurumlar için önceliklidir. Mobil cihazlar, başarılı ve koruyucu güvenlik yapılarına rağmen, yaygınlıkları, gün boyu bize eşlik etmeleri, hayatımızın ayrılmaz bir parçası olmaları ve dijital etkileşimlerimizin birçoğunun merkezinde yer almaları nedeniyle cazip bir hedeftir.

İşletim sistemleri kapalı ekosistemler yerine daha açık platformlar haline geldikçe mobil tehditler de artmıştır ve mobil işletim sistemi geliştiricileri ile tanınmış uygulama mağazası operatörleri, bu zamandan beri işletim sistemi tasarım tercihleri, uygulama ve veri eleme sistemleri, uygulama moderasyonu, uygulama işlevsellik ve kalite kontrolleri ve giderek daha detaylı izin modelleri aracılığıyla tehditleri engellemek için çalışmalar yürütmektedir. CrowdStrike'ın 2019 Mobil Tehdit Ortamı Raporu, mobil platformların suçlular tarafından giderek daha fazla hedeflendiğini göstermektedir.

Birincil Mobil Tehditler

Kötü amaçlı ve fırsatçıoyuncular, popüler platformları kullanmanın her tür yolunu aradığından dolayı mobil ekosistemleriihedefleyen çeşitli tehditler bulunmaktadır. Önemli pazar gücüne sahip dijital platformlarve politika koyucular DMA'yı uygulamaya geçirirken bu tehditleri en aza indirmenin yollarını göz önünde bulundurmalıdır.

Depolanan hassas veriler ve mobil cihazın kilit işlevselliği ile doğrudan etkileşime geçebilme potansiyelleri nedeniyle, kötü amaçlı uygulamalar, uzun zamandır mobil cihazlara yönelik en önemli tehdidi olmuştur. Nokia[8] ve Kaspersky araştırmalarına göre,[9] kötü amaçlı yazılımların çoğu, mobil cihazlara truva atı uygulamalar ile girmektedir. Bu uygulamalar, fener uygulamasından pahalı yazılımların ücretsiz sürümlerine kadar insanların yüklemek isteyeceği şeylerin görünümünü almaktadır,

[8] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[9] https://securelist.com/mobile-malware-evolution-2020/101029/

fakat truva atı uygulamalar, hassas bilgileri veya kimlik bilgilerini toplama gibi istenmeyen davranışları gizlemektedir.[10] Bunun mümkün olmasının nedeni, konum verileri veya telefonda kayıtlı kişilere erişim talep eden bir fener uygulaması gibi yüzeydeki işlevleri için gerek duymayacağı izinleri istemeleridir.[11] Kullanıcı zararsız bir uygulama veya oyun gibi görünen bu programı genellikle ücretsiz olarak yüklemekte, ancak cihazını ve verilerini kötü amaçlı oyuncuların erişimine açmaktadır. Check Point, özellikle ücretsiz bir deneme veya ek bir işlevsellik sunan uygulamalar olmak üzere bu uygulamalarda bir artış bildirmiştir.[12] Bu uygulamaların birçoğu alışıldık marka ve ürün adlarını kullandığından ve sonrasında verileri, kimlik bilgilerini çaldığından veya cihazı bir botnet'e eklediğinden alıştığımız adlara güvenmenin risk doğurduğunu belirtmektedirler.[13]

Bu kötü amaçlı uygulamalar sıklıkla gerçek amaçlarını başarılı bir şekilde gizlemektedir. Kullanıcıların istemediği, sinir bozucu veya zararlı davranışlar içeren truva atı uygulamalar çok yaygındır (hackleme araçlarından erişim yazılımlarına, casus yazılımlardan reklam yazılımlarına, otomatik arama ve şaka programlarına kadar).[14] Hesapları ele geçirmek ve cihazları botnet'lere eklemek üzere uygulamalar yapan hizmet sağlayıcı olarak hareket eden kötü amaçlı yazılımlar bile vardır.[15]

Bu uygulamaların bazıları yine son derece hedeflidir. Örneğin, Hindistan genelinde ve Asya, Afrika ve Latin Amerika'daki diğer ülkelerde birkaç anlık kredi uygulaması üzerinden dolandırıcılık dönmektedir. Yüklendikten sonra, bu uygulama kredi sağlasa da telefondan bilgi de toplamkta (hem kullanıcı hakkında bilgiler hem de telefonda bulunan çıplak fotoğraflar dahil diğer veriler) ve bu bilgiler sonrasında kullanıcılara taciz etmek, onları sindirmek ve tehdit etmek üzere kullanılmaktadır.[16]

Birincil mobil tehdit tanımlandıktan sonra "peki bu kötü amaçlı yazılımlar nasıl yükleniyor" sorusunu sormak doğal bir tepkidir. Google Play Store ve Apple App Store gibi birinci taraf uygulama mağazaları, kötü uygulamaları uzak tutmak bakımından kusursuz olmasa da mağazalarının güvenli kalmasını sağlamak üzere harcadıkları çabalar sayesinde mağazalarında bulunan çoğu uygulama güvenlik ve mahremiyet açısından zararsızdır. Kötü amaçlı yazılımlara yönelik en riskli vektörler, üçüncü taraf uygulama mağazaları ile başka yollarla yapılan indirmelerden kaynaklanmaktadır. Her bir yöntemin getirdiği risk miktarını doğru bir şekilde belirtmek son derece zor olsa da bazı araştırmalar kullanıcılar için önemli riskler olduğunu öne sürmektedir.

Üçüncü Taraf Uygulama Mağazaları

Bazı araştırmalar, ana üçüncü taraf uygulama mağazalarının Google Play Store gibi birinci taraf uygulama mağazalarına kıyasla güvenli *olabileceğini* belirtmiş olsa da, kanıtlar, üçüncü taraf mağazaların mobil kullanıcılar için güvenlik ve gizlilik riskini artırdığını göstermektedir. Ancak, bunun nedeni işletim sistemi ile bağlantılı olmamaları değildir. Daha çok, genel olarak uygulamalarını denetlemek konusunda aynı özeni göstermemeleri veya gösterememelerinden kaynaklanmaktadır. Bu da, ana mobil işletim sistemlerinin geçmişten bu yana standart olarak üçüncü taraf uygulama mağazalarına izin vermemelerinin

---

[10] https://www.mcafee.com/blogs/mobile-security/mobile-spyware/, https://www.appdome.com/dev-sec-blog/mobile-payment-security/

[11] https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

[12] Check Point, 2023 Cyber Security Report, 2023

[13] https://www.verizon.com/business/resources/T9bc/reports/mobile-security-index-report.pdf

[14] https://docs.broadcom.com/doc/istr-23-03-2018-en

[15] https://www.androidpolice.com/android-botnet-trojan-steal-banking-data/

[16] https://www.bbc.co.uk/news/world-asia-india-66964510

nedenlerinden biridir.[17] Ayrıca, tamamen kötü amaçlı uygulamaların yüklenmesini hedef alan uygulama mağazalarına örnekler de bulunmaktadır.[18] 2021 yılında gerçekleştirilen bir odak grup çalışmasında, CrowdStrike, kötü amaçlı yazılımların büyük bölümünün, sağladıkları uygulamalara yönelik kapsamlı kontroller gerçekleştirmeyen üçüncü taraf kaynaklardan dağıtıldığına dikkat çekmiştir.[19]

Bu riskin tam olarak ne düzeyde olduğunu belirtmek güç olsa da 2020 yılında gerçekleştirilen bir araştırma, "diğer en popüler alternatif pazarlardaki" Android kullanıcılarının risk düzeyinin ortalama beş kat daha fazla olduğunu ve Google Play Store'u kullananlara kıyasla kötü amaçlı bir yazılım veya uygulama ile karşılaşma olasılıklarının on dokuz katın üzerinde olduğunu saptamıştır.[20] Ayrıca, siber güvenlik şirketi Symantec, 2018 yılında, keşfettikleri mobil kötü amaçlı yazılımların %99.9'unun üçüncü taraf uygulama mağazalarında barındırıldığını bildirmiştir.[21]

Bu durum, güvenlik uzmanları ve yasa düzenleyicilerarasında, çoğu üçüncü taraf uygulama mağazasından uygulama indirmenin güvenilir birinci bir tarafa kıyasla çok daha riskli olduğu şeklindeki ortak görüşe yol açmıştır. Devletkuruluşları ve özel kuruluşlar, resmi ve güvenilir olmayan kaynaklardan uygulama indirilmesini önermemektedir ve ENISA, Europol,[22] ABD'den NSA,[23] ABD'den tüketici korumadan sorumlu FTC, Birleşik Krallık Ulusal Siber Güvenlik Merkezi,[24] Hindistan'dan CERT-In,[25] ABD'den DHS'nin CISA birimi[26], Ticaret Bakanlığı'nın NIST birimi,[27] Yeni Zelanda'dan CERT NZ[28] ve diğerlerinden gelen uyarılara yer vermektedir. Buna rağmen, araştırmalar, uygulamalar ücretsizse veya tanınmış oyun ya da uygulamaların değiştirilmiş sürümlerini içeriyorsa, tüketicilerin üçüncü taraf uygulama mağazalarını kullandığını göstermiştir.[28] Kullanıcılar, dijital ortamda güvenliklerini göz önünde bulundurmayı ihmal etmektedirler.[29] Yalnızca, gerçek olamayacak kadar iyi görünen uygulamaları tercihen para ödemeden elde etmek istemektedirler.

---

[17] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[18] https://www.makeuseof.com/what-are-the-dangers-of-third-party-app-stores/#:~:text=Many%20malicious%20actors%20have%20created,hidden%20trackers%20and%20malicious%20code.

[19] 2021 Center paper

[20] https://arxiv.org/pdf/2010.10088.pdf

[21] https://docs.broadcom.com/doc/istr-23-03-2018-en

[22] Europol: https://www.europol.europa.eu/sites/default/files/documents/infographic_-_apps.pdf

[23] U.S. NSA Mobile Device Best Practices V3: https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

[24] U.K. NCSC: https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf

[25] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013

[26] U.S. CISA: https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf

[28] U.S. NIST: https://www.nccoe.nist.gov/sites/default/files/legacy-files/mtc-nistir-8144-draft.pdf

[28] N.Z. CERT: https://www.cert.govt.nz/individuals/guides/keep-mobile-phone-safe-secure/

[29] https://www.jamf.com/blog/what-are-third-party-app-stores-and-are-they-safe/

Yan Yükleme(Sideloading)Yan yükleme, bir uygulama mağazasından başka bir uygulama mağazası veya platforma uygulama yüklenmesine izin veren bir durumdur. DMA'nın yükümlülüklerinden biri, yan yüklemenin DMA'nın belirlediği geçit bekçisi dijital platformlar ve şirketler için zorunlu olmasıdır. Yan yükleme, yukarıda tanımlanan üçüncü taraf uygulama mağazalarıyla karşılaştırıldığında, herhangi bir geleneksel uygulama mağazası gerektirmez ve bu şekilde yüklenen uygulamalar, arka planda çok az bağlamla, güvenlik incelemesi yapılmaksızın ve güvenlikle orijinalliğe ilişkin yalan veya yanıltıcı iddialarla dağıtılabilir veya tanıtılabilir. Yan yükleme, web siteleri, mesaj ekleri veya belirsiz bağlantılar aracılığıyla gerçekleştirilebileceğinden, bu titizlik işlemini yapacak herhangi bir aracı yoktur. Yan yükleme, bireylerin, uygulamaların kurcalanıp değiştirilmediğini garantileyecek itibarı, deneyimi veya olanağı olmayabilen üçüncü taraflara güvenmesini gerektirse de kullanıcılar genellikle denemek istedikleri yeni bir oyun bulduklarında bunu göz önünde bulundurmamaktadır. Birçok üçüncü taraf site ve mağaza güvenli olabilse de, kullanıcılara uygulamanın güvenlik incelemesinin nasıl yapıldığıyla ve ne tür izinler gerektirdiğiyle ilgili aynı düzeyde şeffaflık sağlanması pek olası değildir. Ayrıca, tanınmış bir uygulama mağazasının altyapısı olmadan, gerçek olmayan iddialar öne sürmek çok daha kolaydır.

Yan yükleme, kullanıcıların mobil uygulamaları indirmesine yönelik en riskli yöntemdir. Bu risk, başka yollarla yapılan indirmelerin sık sık birçok nihai kullanıcının sahip olmadığı teknik bir uzmanlık düzeyi gerektirdiğinden dengelense de, mobil işletim sistemlerinin varsayılan ayarlarında başka yollarla yapılan indirmelere izin vermemesi halinde bu sıkıntı önlenecektir. Başka yollarla indirme yapan çok bilinçli kullanıcılar bile sonuçta sık sık bilinmeyen ve şüpheli geliştiricilere ve uygulama mağazalarına güvenmektedir ve yalnızca doğrudan köklü şirketlerden indirme yapmadığınız sürece ne kadar teknik bilgi sahibi olursanız olun bu risk önemli ölçüde hafiflememektedir.

Nihai Kullanıcıların Sorumluluk Kusuru

Araştırmalar, kullanıcıların güvenlikle ilgili kararlarının her zaman güvenliğe yönelik tehditler hakkında sahip oldukları bilgilerle bağlantılı olmadığını göstermektedir.[30] Kötü amaçlı uygulamaların yol açabileceği son derece gerçek zararlara rağmen mobil kullanıcılar uygulamaların talep ettiği izinleri eleştirel olarak incelemeye nadiren zaman ayırmakta ve zaman ayırsalar bile genellikle bu izinlerin doğuracağı sonuçları anlamamaktadır.[31] Ayrıca, kullanıcılar karşılarına çıkan güvenlik uyarılarını genel olarak görmezden gelmektedir.[32]

Birçok kullanıcı, mobil cihazlarına yönelik temel güvenlik önlemlerini bile almamaktadır. Örneğin, bir araştırma,kullanıcıların %40'ının pratik değilse işletim sistemleri ve uygulamalarını güncellemediğini ve %28'inin ekran kilidi kullanmadığını göstermiştir.[33] Başka bir araştırma, akıllı telefon kullanıcılarının üçte dördünün uygulama mağazalarından indirdikleri uygulamaların doğal olarak güvenli olduğuna inandıklarını,[34] dolayısıyla bunlardan şüphe duymaları olasılığının düşük olduğunu göstermiştir. Aynı araştırma, uygulama kullanıcılarının farklı uygulama mağazaları tarafından sunulan güvenlik düzeylerinin

[30] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

[31] https://link.springer.com/chapter/10.1007/978-3-031-35822-7_36

[32] https://news.sophos.com/en-us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/

[33] https://www.pewresearch.org/short-reads/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

[34] https://www.sciencedirect.com/science/article/pii/S0167404812001733#fn6

arasında bir fark göremediğini veya görmeye çaba harcamadığını göstermiştir. Kısa zaman önce yapılan ek araştırmalar, kullanıcıların güvenlik risklerine önem verse de kendilerini etkin bir şekilde korumak için gerekli bilgi ve becerilere sahip olmadığını ve sıklıkla kendilerini koruma girişimini bile göstermediklerini onaylamıştır.[35]

Kullanıcıların kendilerini online ortamda korumak bakımından daha aktif bir rol oynayacağını umsak da, en iyi uygulama kriterleri, bu yükü kullanıcılar için giderek olabildiğince azaltmak şeklindedir. Ulusal siber stratejiler ve hükümetlerin en iyi uygulama kriterleri, giderek bu sorumluluğu kullanıcılardan alıp cihazları, verileri ve kişileri koruma görevini bunları dağıtan şirketlere atamaktadır. 2023 yılında, ABD'den ulusal siber güvenlik kurumları (CISA), Çek Cumhuriyeti, İsrail, Singapur, Kore, Norveç, OAS/CICTE CSIRTAmericas Ağı, ve Japonya (JPCERT/CC ile NISC) riski nihai kullanıcılardan almaya yönelik olarak ortak bir rehber çıkarmışlardır.[36] Hem kamu sektörü hem de özel sektördeki birçok kuruluş da hassas verilere veya uygulamalara da erişimi olan cihazlarda yalnızca onaylı uygulamaların yüklendiğinden emin olmak üzere Mobil Cihaz Yönetimi'nden (MDM) yararlanmaktadır ve bu araçlar gelecekte yöneticilerin hangi uygulama mağazalarına izin verildiğini kararlaştırmasına olanak tanıyacaktır.

Yukarıda belirtilen risklerin kapsamı ve karmaşıklığı göz önünde bulundurulduğunda, nihai kullanıcıların bir anda, kendilerini katmanlı güvenlik ile nasıl koruyacakları, kabul edilir riskler için optimum kombinasyonu nasıl yapılandıracakları dahil mobil güvenlik ve gizliliğe yönelik gerekli farkındalık ve algıya sahip olmasını beklemek mantıklı değildir ve başka yöntemlerin kullanımı geniş ölçekli olarak uygun değildir. Nihai kullanıcıların evrensel nitelikli uygulama mağazalarının güvenli olduğunu varsayacağı muhtemeldir. Başka yaklaşımlar da bulunsa da, bunlar, denetçilerin kendi uygulama mağazalarında halihazırda yürürlüğe koyduklarına benzer korumalar gerektirmektedir.

Google ve Apple Bu Tehditlerle Nasıl Mücadele Ediyor?

Apple App Store ve Google Play Store gibi birçok birinci taraf uygulama mağazası ile DMA tarafından denetçi tanımlamasını almayan başka uygulama mağazaları, yukarıda bahsedilen riskleri azaltmak amacıyla, yeni ve güncellenen uygulamaları kötü amaçlı yazılımlar veya orijinal uygulama işlevselliği bakımından taramak için tasarlanan politika ve süreçler aracılığıyla geniş kapsamlı önlemler almaktadır. Hem Apple hem de Google, geliştiriciden resmi uygulama mağazalarına giden ve buradan tüketicilere ulaşan politika ve süreçler oluşturmuştur. Hiçbir uygulama mağazası tamamen güvenli olmasa da, bu çabalar Google Play Store ve Apple App Store'un, kullanıcıları korumaya yönelik yaklaşımlarına destek olmak üzere yıllarca yapılan yatırım ve kazanılan deneyimler aracılığıyla tüketicilerin güvenini kazanmasına ve güvenilir bir itibar elde etmesine neden olmuştur.

Apple App Store ve Google Play Store gibi önde gelen birinci taraf uygulama mağazaları, temel gereklilikler ve rehber ilkeler oluşturmak, öz onaylar sağlamak gibi süreçlerin uygulanması ve uygulamaların incelenmesi yoluyla güvenlik sağlamaktadır.[37] Uygulama geliştiricilerinin bu uygulama mağazalarının birinde yer alabilmek için çeşitli güvenlik, gizlilik ve şeffaflık gerekliliklerini başarıyla karşılaması gerekmektedir. Buna, uygulamanın tanıtımında belirttiği şeyi yaptığından, yalnızca uygun izinleri istediğinden ve yürürlükte işlevsel gizlilik politikaları bulunduğundan emin olmak dahil olabilir. Apple ve Google'ın uygulama

[35] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[36] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[37] https://developer.apple.com/app-store/review/guidelines/, https://play.google.com/about/developer-content-policy/

mağazaları, aynı zamanda uygulama mağazası ilanlarında, uygulamanın kullandığı izinler ve veri toplama hakkında bilgiler dahil şeffaflığı da gerektirmektedir.[38],[39]

Birinci taraf uygulama mağazalarında ayrıca uygulamanın incelenmesine ek olarak geliştirici hesaplarının güvenlik incelemeleri gibi ek korumalar da bulunabilir. Örneğin, Google Play Store, potansiyel tehditleri belirlemek için "geliştiricinin Google hesabını, hareketlerini, geçmişini, fatura bilgilerini, cihaz bilgilerini ve daha fazlasını" incelemektedir.[40]

Uygulama başvuruları içinse, birinci taraf uygulama mağazaları, uygulamanın işlevinden emin olmak üzere birçok adım atabilmektedir. Örneğin, mağaza, uygulama geliştiricinin onaylarını inceleyebilir, çeşitli otomatik incelemeler uygulayabilir ve bir kişiden uygulamayı manuel olarak incelemesini isteyebilir. Bu incelemeler, kötü amaçlı yazılımları ve diğer potansiyel olarak zararlı veya istenmeyen özellikleri saptamak amacıyla statik ve dinamik incelemelerin gerçekleştirilmesi için çeşitli araç ve tekniklerden yararlanabilir. Ayrıca, başvurusu yeni yapılan uygulamaların rutin denetimlerine ek olarak, Apple'ınki gibi birinci taraf uygulama mağazaları, tüm yeni işlevlerin güvenli olmaya devam ettiğinden emin olmak üzere uygulama güncellemelerini incelemektedir. Son olarak, birinci taraf uygulama mağazaları, uygulamaların istenmeyen davranışlar gösterdiğine ilişkin tüketici veya güvenlik araştırmacılarından alınan şikayet veya bildirimleri temel alan incelemeler de başlatmaktadır.

Bir uygulama, uygulama mağazasında yer almaya yönelik gerekli standart ve rehber ilkeleri karşılayıp sürdüremiyorsa, uygulama mağazasından tamamen kaldırılır. Apple, 2022 yılında 1,5 milyonun üzerinde uygulama başvurusunu reddettiğini ve uygulama mağazasından 186.000'in üzerinde uygulamayı kaldırdığını açıklamıştır.[41] Uygulamaların bu şekilde kaldırılması, güvenli ve güvenilir bir uygulama ortamını desteklemekte, nihai kullanıcılara zarar gelmesini önlemekte ve kötü amaçlı oyuncuları cihazlara zarar vermek üzere daha verimli başka yollar aramaya teşvik etmektedir.

Apple ve Google, tüketici düzeyinde güvenlik ve politika korumaları ve gerekliliklerini, uygulama mağazalarını kullanan kullanıcılar için kolay erişilebilir ve anlaşılabilir hale getirmek için önemli çaba sarf etmiştir. Ayrıca, her iki şirket de, tüketicilerin resmi uygulama mağazası standartlarının ötesinde talep edebileceği gizlilik ve güvenlik düzeyi hakkında bilgiye dayalı karar alabilmesi için güvenlik incelemesinden geçmiş uygulamaların istediği izinlere yönelik daha fazla şeffaflık oluşturmaya çalışmaktadır. Hatta, Google Play Store, bağımsız bir güvenlik incelemesini tamamlamış olan uygulamaları bir rozetle sınıflandırmaya başlamıştır.[42] Bu süreç ve politikaların etkin olduğu kanıtlanmıştır, ancak önemli düzeyde yatırım gerektirmektedirler.

Mobil Uygulama Mağazalarında Güvenlik Yatırım Demektir

Yukarıda belirtildiği gibi, güvenlik sorumluluğunu kullanıcılara yüklemek etkin değildir ve kullanıcının standart olarak korunduğundan emin olmak üzere giderek daha fazla politika ve süreci destekleyen siber güvenlik en iyi uygulama kriterlerine

---

[38] https://support.google.com/googleplay/android-developer/answer/10144311?hl=en

[39] https://developer.apple.com/app-store/user-privacy-and-data-use/#:~:text=In%20order%20to%20submit%20new,websites%20owned%20by%20other%20companies

[40] https://developers.google.com/android/play-protect/cloud-based-protections

[41] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

[42] https://security.googleblog.com/2022/12/app-defense-alliance-expansion.html

uymamaktadır. Büyük ve kaynak bakımından zengin Google ve Apple gibi kurumların bunu yapabilecek uzmanlığı, kaynakları ve isteğibulunsa da, aynı durumda olan başka kurumların sayısı çok azdır.

Yukarıda belirtilen ve üçüncü taraf uygulama mağazalarınca uygulandığında dahi çok nadir uygulanan bu koruma türleri, kötü amaçlı, düşük kaliteli ve yanıltıcı uygulamaların büyük çoğunluğunu elemektedir. Üçüncü taraf uygulama mağazalarının platform ve işletim sistemine yönelik aynı düzeyde kaynakları, deneyimi ve bilgi birikimi bulunmamaktadır ve uygulama mağazalarını korumak veya barındırdıkları uygulamaları birinci taraf uygulama mağazalarının yaptığı gibi güvenlik incelemesinden geçirmek için gerekli teşviğe sahip değildirler. Ayrıca, üçüncü taraf uygulama mağazaları, aksi halde onaylanmayacak uygulamalara karşı daha esnek olarak kendilerini daha büyük ve köklü mağazalardan ayırmayı amaçlamaktadır. Madalyonun diğer yüzünde ise, pazarlarındaki uygulamaların güvenliğini artırmak üzere kayda değer kaynak harcaması yapan birinci taraf uygulama mağazaları bulunmaktadır.

DMA'nın Uygulanmasına Yönelik Yol Haritası

Mobil işletim sistemlerinin gerekli kılınması, mobil ekosistemin gizlilik ve güvenliği üzerinde engellenemeyecek olumsuz etkiler doğuracak olsa da bir yandan kullanıcılara üçüncü taraf uygulama ve uygulama mağazaları için daha geniş kapsamlı, güvenli erişim sağlarken diğer yandan üçüncü taraf uygulama geliştiricilerine işletim sistemi düzeyinde işlevsellik için daha fazla erişim sunmanın yolları vardır. Yukarıda belirttiğimiz gibi ve Apple gibi birinci tarafların onayladığı üzere, DMA'ya uyum, "kötü amaçlı yazılım, dolandırıcılık ve sahtekarlıkların, yasa dışı ve zararlı içeriğin ve gizlilik ve güvenlikle ilgili başka tehditlerin" yaygınlığını artıracağı hemen hemen kesindir.[43] Ancak, kanun koyucular ve politika belirleyiciler, bu sorunları, geçit bekçisi olarak belirlenmiş şirketlerin tüketicilerini korumasına olanak tanıyan yapıcı uygulama rehberliği ile hafifletebilir.

AB'ye üye devletlerin, hem birinci taraf uygulama mağazaları ve mobil işletim sistemi sahipleri hem de mobil cihaz kullanıcılarına, aşağıdakileri destekleyerek yardımcı olmaya istekli olması gereklidir:

- Geçit bekçisi olarak belirlemiş şirketler, dağıtım kanalından bağımsız olarak temel uygulama incelemeleri gerçekleştirmelidir. Bunun için işletim sistemlerine entegre yeni mekanizmalar veya uygulama mağazaları ile sözleşmeler gerekli olabilir. Aynı zamanda, uygulamaların güvenli olduğunu göstermek için sertifikalardan ve üçüncü taraf değerlendirmelerden yararlanmanın bir yolu olabilir.
- Politika belirleyiciler, kullanıcıların ve başkalarının uygulamaların nasıl çalıştığını ve ne yapmayı amaçladıklarını anlamasına yardımcı olmak üzere uygulama açıklamasında temel işlevler ve gerekli bilgilerle ilgili bildirimleri değerlendirmelidir.
- İşletim sistemleri, kötü amaçlı yazılımların mobil cihazın güvenliği ve bütünlüğüne zarar vermesine engel olmak üzere artırılmış mobil korumalardan yararlanabilir. Bunlara, uygulamaların elenmesi ve birbirinden korunması ve işletim sisteminin, kullanıcı verilerinin ve cihaz donanımının kötü amaçlı uygulamalardan korunması için ek araçlar dahildir. Bu araçlar arasında, kurum yöneticileri için MDM(Mobil Cihaz Yönetimi= araçları yer alabilir.
- Geçit bekçisi olarak belirlemiş şirketler , güvenilir olduklarından emin olmak üzere üçüncü taraf uygulama mağazaları için teknik ve sözleşmeye dayalı denetimler getirmelidir. Her bir denetçinin farklı hafifletme stratejileri arasında farklı bir

[43] https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

- Yönetmelik belirleyicilerin de hem uygulama hem de uygulama mağazalarında güvenlik ve bütünsellik kaygılarını göz önünde bulundurmaları ve tüm uygulama ve mağazaların eşit olmadığını anlamaları önemlidir. Uygulama ve uygulama mağazası geliştiricilerinin sorumlu şekilde hareket ettiğini değerlendirip garanti altına almak ve aksi takdirde sorumlu tutulmalarını sağlayacak mekanizmaların geliştirilmesini desteklemeleri gereklidir.
- Mobil işletim sistemleri geliştirenşirketlerin, geliştiricilerin değişen ekosistemden çıkar sağlamadığından emin olmak üzere izinleri, güvenlik modellerini ve çalışma şekillerini ayarlamaya yönelik esneklik sahibi olması gereklidir. Politika belirleyicilerin, uygulama mağazaları ve cihaz işletim sistemlerinin ekosistemlerine entegre edilebilecek güvenlik mekanizmaları ve sınırlama türlerini geliştirme yetisini koruması gereklidir.
- Mobil ekosistemleri ele alan politikalar, bu ekosistemlerin güvenliğini zayıflatmamalıdır. Politika belirleyiciler, mobil platformların güvenliği ve gizliliğinin gelişmeye devam ettiğinden emin olmalı ve bu özelliklerin platform ve uygulamalara başından entegre edilmesini sağlamalıdır. Gerçekleştirilen ilerlemeyi tehdit eden teklifler yeniden değerlendirilmelidir.
- Politika belirleyiciler, kullanıcıların üstlenmeye gönüllü ve hazır oldukları güvenlik sorumlulukları konusunda gerçekçi olmalıdır. Araştırmalar, güvenlik konusunda farkındalığın iyi güvenlik kararlarının alınması ile ilişkili olmadığını göstermektedir.[44]
- Politika belirleyiciler, mobil cihazların nasıl çalışabileceği ve ne tür uygulamaların yüklenebileceği hakkında özel uygulamalar kararlaştırmak yerine mobil cihazlara yönelik risk temelli uygulamaları desteklemelidir.

Sonuç

DMA'nın yasa olarak onaylanması ve geçit bekçisi olarak belirlenmiş şirketlerin uymak üzere çalışmalarını sürdürmesiyle, mobil ekosistem için önemli bir geçiş sürecine girmekteyiz. Siber Güvenlik Politika ve Hukuk Merkezi, politika belirleyicilerin, şirketlerin ve mobil ekosistemin geri kalanının kullanıcıların ve mobil cihazlarının güvende kalmaya devam etmesi için işbirliği yapabileceğini ümit etmektedir. Politika belirleyiciler, şirketler, ekosistem ve tüketiciler üzerindeki güvenlik etkilerini değerlendirmelidir. Mevcut uygulama mağazası inceleme ve gözetim unsurlarının birçoğunun etkisinin ne miktarda olduğunu söylemek güç olsa da, uygulama mağazası geliştiricilerinin kullanıcılarını korumak için yaptığı yatırımların görülmesi ve ödüllendirilmesi gereklidir. Uygulama mağazası sahipleri ve geliştiriciler güvenlik ve gizliliği artırıcı adımlar attığında, kullanıcılar bundan farkında olmadıkları şekilde yarar sağlamaktadır.

Kullanıcıları mobil ortamdaki tüm kötü amaçlı yazılımlardan koruyan mükemmel bir sistem bulunmasa da kullanıcıların göz önünde bulundurması gereken istenmeyen veya kötü amaçlı etkinliklerin sayısının önemli ölçüde nasıl azaltabileceğimizi biliyoruz.

[44] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/