신뢰할 수 있는 앱 스토어: 보안 및 무결성 보호

2024 년 2 월

편집자:

Heather West | 수석 이사

+1 202.344.4597

HEWest@Venable.com

Tim McGiff | 프로젝트 매니저

+1 202.344.4365

TCMcGiff@Venable.com

CENTER FOR CYBERSECURITY POLICY AND LAW

목차

경영진 요약

유럽연합(EU)은 디지털 시장을 위한 새로운 정책과 규정을 시행함에 있어 접근성, 개인 정보 보호, 보안과 함께 경제적 고려 사항을 신중하게 균형 있게 고려해야 합니다.

안타깝게도 디지털 시장법(DMA)의 모바일 앱 스토어 조항은 휴대폰 생태계를 신뢰할 수 있고 탄력적으로 만들어온 기본적인 보안 통제를 약화시킬 수 있습니다. 사이버보안 정책 및 법률 센터는 앱을 설치하는 방법이 급증하면 사용자에게 압도적인 부담을 주고 악의적인 행위자가 이를 악용할 수 있는 수많은 길이 열릴 것을 우려하고 있습니다.

그렇다고 해서 사용자를 보호하기 위해 할 수 있는 일이 전혀 없다는 것은 아니지만, 과거에는 필요하지 않았던 방식으로 사용자를 보호하기 위해 기업과 사용자 스스로가 조치를 취해야 할 것입니다. 이 백서에서는 EU 시민, 디바이스 및 데이터에 대한 잠재적 위험과 이러한 위험을 완화하기 위한 접근 방식을 간략하게 설명합니다. 마지막으로 규제 당국과 정책 입안자들이 사용자가 모바일 생태계를 계속 신뢰할 수 있도록 하기 위한 권장 사항과 사용자와 기업에 미칠 수 있는 잠재적인 보안 영향을 완화하는 방법을 제시합니다. 이 백서가 자국민의 보안과 개인정보를 보호하는 동시에 자국 디지털 시장의 경쟁을 촉진하고자 하는 다른 국가들에게도 인사이트를 제공할 수 있기를 바랍니다.

사이버 보안 및 법률 센터 소개

사이버보안 정책 및 법률 센터는 정부, 민간 업계, 시민 사회에 보안 위협을 더 잘 관리할 수 있는 사례와 정책을 제공함으로써 전 세계 사이버 보안을 강화하는 데 전념하는 독립적인 조직입니다. 2017 년 Venable LLP의 사이버보안 서비스 그룹 내 501(c)(6) 비영리단체로 설립된 이 센터는 정책 전문성과 글로벌, 국가, 지역 차원의 소집력을 결합하여 업계 리더와 정책 입안자가 함께 연합을 구성하고 실제 성과를 창출하는 이니셔티브를 출범하도록 지원합니다. 합의 중심의 위험 관리 기반 접근 방식을 적용하는 이 센터는 디지털 인프라와 정보 시스템 보안의 최전선에 있는 사람들의 관점과 관행에서 도출된 실용적인 솔루션과 정책 권장 사항을 홍보함으로써 사이버 보안에 대한 복잡성을 해소하고 혼란을 없애고자 노력합니다.

소개

점점 더 연결되는 세상에서 우리는 종종 휴대폰의 앱을 사용하여 다양한 서비스, 정보 및 리소스로 구성된 생태계와 상호 작용합니다. 휴대폰의 장점은 널리 알려져 있습니다[1]:

휴대폰은 세상을 향한 창문이며, 건강을 추적하고, 친구들과 공유하고, 상품을 구매하고, 서비스를 관리합니다. 따라서 우리는 하루에 4~5 시간 이상 모바일 앱을 사용하는 데 많은 시간을 소비합니다.[2] 그러므로 디바이스와 앱의 보안과 신뢰성을 유지하는 것이 중요합니다.

연구에 따르면 미국 내 18~34 세 소비자의 81%는 자신이 소유한 커넥티드 디바이스가 안전하다고 생각하는 것으로 나타났습니다.[3] 이러한 생태계를 보호하기 위한 운영 체제 개발자와 앱 스토어의 노력 덕분에 사람들은 모바일 디바이스와 앱을 신뢰할 수 있는 충분한 이유가 있습니다.

2021년 보고서 *모바일의 미래: 모바일 보안 및 개인정보 보호의 지속적인 개선*[4]에 대한 경로에서 업계, 학계, 시민 사회의 사이버 보안 전문가 23 명과 모바일 보안에 대해 논의한 결과 "모바일 디바이스에 대한 새로운 위협이 계속 발생하고 있지만, 다른 사이버 보안 영역에 비해 일반적으로 보호 기능이 더 잘 작동하고 있다"[5]는 사실을 발견했습니다. 포커스 그룹의 공통된 의견은 모바일 환경은 운영 체제(OS) 및 앱 스토어 수준에서 보안 및 개인정보 보호 기능이 내장되어 있어 사용자가 스스로를 보호해야 하는 부담이 크게 줄어든다는 것이었습니다.

이제 겨우 3년이 지난 이 백서는 평판이 좋은 운영 체제 개발자와 신뢰할 수 있는 공식 앱스토어의 최신 모바일 아키텍처와 보안 기능을 바탕으로 작성되었습니다. 지난 10년 동안 모바일 생태계는 점진적으로 더 안전해졌지만, 유럽연합의 경쟁 중심적인 DMA[6]의 앱 설치 조항은 이러한 보안 발전을 지속하는 대신 생태계를 후퇴시킬 수 있습니다. 우

---

[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] Techcrunch를 통해 Data.ai는 모바일 사용자가 하루에 4~5시간을 앱에서 보낸다고 보고합니다 – 링크

[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] Text of the Digital Markets Act can be found at https://eur-lex.europa.eu/eli/reg/2022/1925

리는 이러한 보안의 진전을 유지하기 위해 함께 노력해야 합니다.

운영체제가 추가 소스의 앱 설치를 허용하도록 요구하는 DMA 조항은 사용자에게 부담을 주고 모바일 디바이스 관리를 구현하는 기업 관리자에게 어려움을 줄 수 있으며, 악의적인 행위자에게 새로운 길을 열어줄 수 있습니다. 이러한 위험을 완화하려면 모바일 운영 체제 게이트키퍼를 지원하여 DMA의 의도와 균형을 맞추는 동시에 보다 개방적인 에코시스템에 수반되는 위험을 완화할 수 있는 합리적인 접근 방식을 취해야 합니다.

이 백서에서는 DMA 내의 앱 스토어 조항과 이러한 조항으로 인해 악화되는 모바일 생태계 위협에 대해 간략히 설명하고, 퍼스트 파티 앱 스토어 및 모바일 OS 소유자가 역사적으로 이러한 위협에 어떻게 대처해왔는지 간략하게 살펴볼 것입니다. 이 백서에서는 준비되지 않은 최종 사용자가 갑자기 모바일 생태계와 디바이스의 보안을 위협받지 않도록 하기 위해 EU 회원국이 지원해야 하는 DMA 구현 접근 방식의 종류에 대한 사례를 제시합니다.

DMA 본문은 기술 및 계약 메커니즘을 포함하여 사용자를 보호할 수 있는 잠재적인 방법을 언급하고 있으며, 입법자와 규제 당국은 앱 검토, 멀웨어 보호 강화, 투명성 요건, 모바일 기기 운영체제에 내장된 권한 및 보안 모델 조정 등을 통해 운영체제 개발자의 역할을 지원하여 사용자를 보호해야 합니다. 활기차고 혁신적인 모바일 생태계를 보장하기 위해 함께 노력하는 것이 중요합니다. 정책 입안자들이 DMA의 시행법에서 보안의 중요성을 강조하고 게이트키퍼가 규정 준수를 확립하기 위해 노력할 것을 촉구합니다.

DMA 앱 스토어 조항

2024 년 3월까지 '핵심 플랫폼 서비스'를 운영하는 '게이트키퍼'의 정의에 해당하는 기업은 앱 스토어 및 타사 앱 스토어 및 앱과의 모바일 OS 상호 작용과 관련된 DMA 조항의 적용을 받게 됩니다. 게이트키퍼는 유럽 위원회가 지정한 대로 유럽 시장에 중대한 영향을 미치고 기업(예: 앱 개발자)과 최종 사용자(예: 앱을 설치하는 휴대폰 사용자) 간의 관계를 중개하는 서비스를 제공하는 기업입니다. [7]DMA의 목적은 유럽의 소규모 기업들이 시장에서 보다 '확고한' 위치를 점하고 있는 기업들과 보다 쉽게 경쟁할 수 있도록 하는 것입니다.

DMA 조항은 모바일 운영 체제가 게이트키퍼가 아닌 앱 스토어 또는 기타 방법을 통해 앱을 설치할 수 있도록 허용하고 운영 체제가 자사 및 타사 앱에 동일한 시스템 액세스

[7] As of publication, Apple's iOS operating system and Google's Android operating system are considered core platform services. Microsoft's Windows desktop PC operating system is also considered a core platform service but is outside the scope of this paper. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

및 툴링을 허용하도록 요구합니다.

이러한 조항의 핵심은 다음과 같습니다:

- *섹션 6.4: 게이트키퍼는 운영 체제를 사용하거나 상호 운용하는 타사 소프트웨어 애플리케이션 또는 소프트웨어 애플리케이션 스토어의 설치 및 효과적인 사용을 허용하고 기술적으로 가능하게 해야 하며 해당 소프트웨어 애플리케이션 또는 소프트웨어 애플리케이션 스토어가 해당 게이트키퍼의 관련 핵심 플랫폼 서비스 이외의 방법으로 액세스할 수 있도록 허용해야 합니다.*
- *섹션 6.7: 게이트키퍼는 서비스 제공자부 하드웨어 제공자가 운영 체제 또는 가상 비서를 통해 액세스하거나 제어하는[...] 동일한 하드웨어 및 소프트웨어 기능과의 효과적인 상호 운용성을 무료로 허용하고 상호 운용성을 위한 목적으로 액세스하도록 허용해야 합니다. 또한, 게이트키퍼는[...] 해당 서비스를 제공할 때 해당 게이트키퍼가 사용할 수 있거나 사용하는 기능이 운영 체제의 일부인지 여부에 관계없이 동일한 운영 체제, 하드웨어 또는 소프트웨어 기능과의 효과적인 상호 운용성 및 상호 운용성 목적의 액세스를 허용해야 합니다.*

이러한 DMA 조항을 다른 유럽연합 법률과 결합하면 게이트키퍼는 타사 앱과 앱 스토어를 모바일 디바이스에 쉽게 설치하고, 모바일 사용자가 타사 앱 스토어에 쉽게 액세스할 수 있도록 하며, 타사 개발자 및 앱에 현재 게이트키퍼가 누리고 있는 모바일 OS 와의 동일한 액세스, 상호운용성 및 기능을 부여할 수 있습니다.

이러한 조항과 더불어 모바일 생태계의 '개방'으로 인한 보안 및 개인정보 보호 위험에 대한 경각심을 강조하는 것 외에도 강조되지 않은 보안 주의 사항이 있습니다. DMA의 제 50 조는 타사 앱과 앱 스토어에 대한 추가 액세스가 사용자 및 디바이스 보안을 약화시켜서는 안 된다고 명시하고 있습니다. 그러나 운영 체제가 앱에 대한 액세스를 차별화하거나 축소할 수 있는 방법에 대한 제한을 고려할 때 운영 체제가 모바일 디바이스와 사용자를 어떻게 보호할 것으로 기대하는지는 DMA에 명시되어 있지 않습니다. 신중한 고려 없이 시행될 경우 위의 DMA 조항은 현재의 모바일 위협 생태계를 더욱 악화시킬 수 있습니다.

모바일 위협 생태계

모바일 멀웨어를 퇴치하는 것은 모바일 OS 개발자와 전 세계 조직의 최우선 과제입니다. 성공적인 보안 아키텍처에도 불구하고 모바일 디바이스는 어디에나 있고, 하루 종일 함께하며, 우리 생활의 핵심 부분이고 수많은 디지털 상호 작용의 한가운데에 있기 때문에 매력적인 공격 대상입니다.

운영 체제가 폐쇄적인 생태계가 아닌 진정한 플랫폼이 되면서 모바일 위협도 증가했으

며, 모바일 OS 개발자와 유명 앱 스토어 운영자는 앱과 데이터를 샌드박싱하는 OS 아키텍처 설계 선택, 앱 조정, 앱 기능 및 품질 검사, 점점 더 세분화된 권한 모델을 통해 위협을 억제하기 위해 노력해 왔습니다. CrowdStrike의 2019 모바일 위협 환경 보고서에 따르면 모바일 플랫폼이 범죄자들의 표적이 되고 있으며, 숙련도가 낮은 공격자들은 이제 개념 증명 모바일 멀웨어에 액세스하여 모바일 디바이스에 쉽게 접근을 시도할 수 있게 되었습니다.[8]

주요 모바일 위협

악의적인 공격자와 기회주의적인 공격자 모두 이 엄청나게 인기 있는 플랫폼을 활용할 방법을 찾고 있기 때문에 모바일 생태계에 대한 위협은 무수히 많습니다. 게이트키퍼와 정책 입안자는 DMA를 구현할 때 이러한 위협을 최소화할 수 있는 방법을 염두에 두어야 합니다.

악성 앱은 저장된 민감한 데이터와 모바일 디바이스의 핵심 기능에 직접 액세스할 수 있다는 점에서 오랫동안 모바일 디바이스의 가장 큰 위협이었습니다. 노키아[9]와 카스퍼스키 연구[10]에 따르면 대부분의 모바일 멀웨어는 트로이 목마 앱을 통해 모바일 디바이스에 침투합니다. 이러한 앱은 손전등 앱부터 고가의 소프트웨어 무료 버전까지 사람들이 실제로 설치하고 싶어하는 것처럼 위장하지만 트로이 목마 앱은 민감한 정보나 자격 증명 수집과 같은 원치 않는 동작을 숨기고 있습니다.[11] 이는 휴대폰에 저장된 위치 데이터나 연락처를 요청하는 손전등 앱과 같이 표면적인 기능에는 필요하지 않은 권한을 요청하기 때문에 가능합니다.[12] 사용자는 일반적으로 무료로 제공되는 정상적인 앱이나 게임을 설치하지만, 악성 공격자에게 자신의 디바이스와 데이터를 공개하게 됩니다. Check Point는 이러한 앱, 특히 무료 평가판이나 추가 기능을 제공하려는 목적의 앱이 증가하고 있다고 보고했습니다.[13] 이러한 앱 중 상당수가 익숙한 브랜드 및 제품 이름을 활용하지만 데이터, 자격 증명을 훔치거나 봇넷에 디바이스를 추가하기 때문에 익숙한 것을 신뢰하는 것은 위험하다고 지적합니다.[14]

---

[8] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

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

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

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

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

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

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

해킹 툴, 액세스웨어, 스파이웨어, 애드웨어, 다이얼러, 장난 프로그램 등 사용자가 원하지 않는 성가시거나 유해한 동작을 하는 트로이 목마 앱이 급증하고 있습니다.[15] 심지어 계정을 탈취하고 모바일 디바이스를 봇넷에 연결하는 앱을 만드는 서비스형 멀웨어 제공업체도 있습니다.[16]

이러한 앱 중 일부는 고도로 표적화된 앱이기도 합니다. 예를 들어, 인도와 아시아, 아프리카, 라틴 아메리카의 다른 국가에서 여러 인스턴트 대출 앱 사기가 유포되고 있습니다. 이 앱은 설치 후 대출을 제공하기도 하지만, 사용자에 대한 정보와 누드 사진을 포함한 휴대폰의 기타 데이터를 수집하여 괴롭힘, 협박, 갈취에 이용하기도 합니다.[17]

주요 모바일 위협이 확인되었으니 자연스럽게 "그렇다면 이러한 악성 앱은 어떻게 설치될까요?"라는 질문이 생깁니다. 구글 플레이 스토어와 애플 앱 스토어와 같은 퍼스트 파티 앱 스토어는 악성 앱을 완벽하게 차단하지는 못하지만, 스토어를 안전하게 유지하기 위한 노력으로 인해 스토어에 있는 대부분의 앱은 양성 앱입니다. 멀웨어의 가장 위험한 경로는 타사 앱 스토어와 사이드로딩입니다. 각 방법의 위험 정도를 정확하게 정량화하는 것은 매우 어렵지만 일부 연구에 따르면 사용자에게 상당한 위험을 초래할 수 있는 것으로 나타났습니다.

타사 앱 스토어

일부 연구에서는 주요 타사 앱 스토어가 Google Play 스토어와 같은 자사 앱 스토어에 비해 안전할 수 있다고 주장하지만, 타사 스토어가 모바일 사용자의 보안 및 개인정보 보호 위험을 증가시킨다는 증거가 있지만 이는 운영 체제와 관련이 없기 때문이 아닙니다. 대신, 타사 앱 스토어는 일반적으로 앱 보안을 위해 동일한 노력을 기울이지 않거나 할 수 없기 때문에 주요 모바일 OS 가 역사적으로 타사 앱 스토어를 기본적으로 허용하지 않은 이유 중 하나라고 할 수 있습니다.[18] 또한 앱 스토어 자체가 악성 앱을 설치하기 위한 목적이 있는 앱 스토어의 에도 있습니다.[19] 2021 년 포커스 그룹에서 CrowdStrike 는 대부분의 모바일 멀웨어가 제공하는 애플리케이션에 대한 포괄적인 검사를 수행하지

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

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

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

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

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

않는 타사 소스에서 배포된다는 점에 주목했습니다.[20]

정확한 위험도를 정량화하기는 어렵지만, 2020년 한 연구에 따르면 '기타 상위 대체 마켓'의 Android 사용자는 Google Play 스토어를 사용하는 사용자보다 멀웨어 또는 악성 앱을 발견할 가능성이 평균 5배, 최대 19배 더 높은 것으로 나타났습니다.[21] 또한 사이버 보안 업체인 시만텍은 2018년에 발견한 모바일 멀웨어의 99.9%가 타사 앱 스토어에서 호스팅되었다고 보고했습니다.[22]

이로 인해 보안 전문가와 규제 당국은 대부분의 타사 앱 스토어에서 앱을 다운로드하는 것이 신뢰할 수 있는 퍼스트 파티보다 훨씬 위험하다는 데 공감대를 형성했습니다. 주요 정부 및 민간 기관에서는 비공식적이고 신뢰할 수 없는 출처에서 앱을 다운로드하지 말 것을 권고하고 있으며, ENISA, 유로폴,[23] 미국 NSA,[24] 소비자 보호를 담당하는 미국 FTC, 영국 국가 사이버 보안 센터,[25] 인도 CERTIn,[26] 미국 DHS의 CISA27,[27] 상무부의 NIST,[28] 뉴질랜드의 CERT NZ,[29] 등이 여러 차례 경고를 보낸 바 있습니다. 그럼에도 불구하고 연구에 따르면 소비자들은 앱이 무료이거나 잘 알려진 게임 및 앱의 수정 버전이 있는 경우 타사 앱 스토어를 사용하는 것으로 나타났습니다.[30] 사용자들은 보안을 염두에 두지 않고 그저 너무 좋아 보이는 앱을 빨리, 가급적이면 무료로 받고 싶어 합니다.

사이드 로딩

이에 비해 사이드로딩은 기존의 앱 스토어가 필요하지 않으며, 사이드로딩된 앱은 배경

---

[20] 2021 Center paper

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

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

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

[24] 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

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

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

[27] 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

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

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

정보가 거의 없고 검증되지 않은 채 배포되거나 광고될 수 있으며 보안 및 신뢰성과 관련하여 허위 또는 오해의 소지가 있는 주장을 할 수 있습니다. 사이드로드는 웹사이트, 메시지 첨부 파일 또는 가려진 링크 등 어디에서나 발생할 수 있기 때문에 이러한 실사를 수행할 중개자가 없습니다.

사이드 로딩은 평판, 경험 또는 앱이 변조되지 않았는지 확인할 수단이 없는 제 3자를 신뢰해야 하지만, 사용자는 새로운 게임을 시도할 때 이러한 점을 고려하지 않습니다.

많은 타사 웹사이트와 스토어가 안전할 수 있지만, 앱이 어떻게 심사되었는지, 어떤 권한을 요청할 수 있는지에 대해 사용자가 동일한 수준의 투명성을 기대하기는 어렵고 평판이 좋은 앱스토어의 인프라가 없다면 그렇지 않은 척하는 것이 훨씬 더 간단합니다.

사이드 로딩은 사용자가 모바일 앱을 다운로드하는 가장 위험한 방법입니다. 사이드 로딩에는 많은 최종 사용자가 보유하지 못한 수준의 기술적 전문 지식이 필요한 경우가 많기 때문에 이러한 위험이 상쇄되어 왔지만, 모바일 운영 체제에서 기본적으로 사이드 로딩을 허용하면 이러한 마찰이 사라질 것입니다. 정보를 잘 알고 있는 최종 사용자도 결국에는 잘 알려지지 않았거나 의심스러운 개발자와 앱 스토어를 신뢰하는 경우가 많으며, 잘 알려진 회사에서 직접 다운로드하지 않는 한 기술 지식이 아무리 많아도 위험을 확실하게 낮출 수 없습니다.

최종 사용자 책임의 실패

연구에 따르면 사용자의 보안 결정이 보안 위협에 대한 지식과 반드시 상관관계가 있는 것은 아닙니다.[31] 악성 앱이 초래할 수 있는 실질적인 피해에도 불구하고 모바일 사용자는 앱이 요청하는 권한을 자세히 살펴보는 데 상당한 시간을 할애하는 경우가 드물고, 살펴보려고 해도 그 의미를 이해하지 못하는 경우가 많습니다.[32] 또한 사용자는 보안 경고가 표시되면 압도적으로 이를 무시합니다.[33]

예를 들어, 한 연구에 따르면 사용자의 40%는 편리하지 않으면 운영체제와 앱을 업데이트하지 않고, 28%는 화면 잠금 기능을 사용하지 않는다고 답했습니다.[34] 또 다른 연구에 따르면 스마트폰 사용자의 4 분의 3이 앱 스토어에서 다운로드하는 앱이 본질적으로 안

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

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

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

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

전하다고 믿고 있으며,[35] 이러한 앱에 대해 회의적인 태도를 보이는 것으로 나타났습니다. 이 연구에서는 심지어 앱 사용자가 다양한 앱 스토어에서 제공하는 보안 수준을 구분할 수 없거나 구분하는 데 관심이 없다는 사실도 발견했습니다. 최근의 또 다른 연구에 따르면 사용자들은 보안 위험에 대해 관심을 갖고 있지만 효과적으로 자신을 보호할 수 있는 지식과 기술이 부족하며, 심지어 시도조차 하지 않는 경우가 많다고 합니다.[36]

사용자가 온라인에서 자신을 보호하기 위해 보다 적극적인 역할을 수행하기를 바라지만, 모범 사례에서는 이러한 부담을 가능한 한 많이 덜어주는 것이 점점 더 중요해지고 있습니다. 국가 사이버 전략과 정부의 모범 사례는 점점 더 균형을 사용자에서 벗어나 디바이스, 데이터, 사람을 보호할 책임을 디바이스를 배포하는 기업에 부여하는 방향으로 나아가고 있습니다. 2023년 미국(CISA), 체코, 이스라엘, 싱가포르, 한국, 노르웨이, OAS/CICTE CSIRTAmericas 네트워크, 일본(JPCERT/CC 및 NISC)의 국가 사이버 보안 기관은 공동으로 최종 사용자로부터 위험의 균형을 전환하기 위한 지침을 발표했습니다.[37] 또한 공공 및 민간 부문의 많은 조직에서는 민감한 데이터나 앱에 액세스할 수 있는 디바이스에 승인된 앱만 설치되도록 하기 위해 모바일 디바이스 관리(MDM)를 사용하고 있으며, 향후에는 이러한 도구를 통해 관리자가 허용되는 앱 스토어를 결정할 수 있게 될 것입니다.

위의 위험의 범위와 복잡성을 고려할 때, 최종 사용자가 갑자기 계층화된 보안을 통해 자신을 보호하는 방법, 허용되는 위험에 대한 최적의 설정 조합을 구성하는 방법 등 모바일 보안 및 개인정보 보호에 대해 필요한 인식과 이해를 갖추기를 기대하는 것은 비합리적이며, 다른 방법은 대규모로 실행할 수 없습니다. 최종 사용자는 보편적으로 제공되는 앱 스토어가 안전하다고 생각할 가능성이 높습니다. 다른 접근 방식도 있지만 게이트키퍼가 이미 자체 앱 스토어에 적용하고 있는 것과 같은 보호 조치가 필요합니다.

구글과 애플이 이러한 위협에 대처하는 방법

Apple 앱 스토어, Google Play 스토어 등 많은 퍼스트 파티 앱 스토어와 DMA에 따라 게이트키퍼로 지정되지 않은 다른 앱 스토어는 신규 및 업데이트된 앱에서 멀웨어 또는 원래 앱 기능의 중대한 변경을 선별하도록 설계된 정책과 프로세스를 통해 위에서 식별된 위험을 완화하기 위한 광범위한 조치를 취하고 있습니다. Apple 과 Google 은 개발자로부터 공식 앱 스토어를 거쳐 소비자에게까지 확장되는 정책과 프로세스를 만들었습니다. 완벽한 보안을 갖춘 앱 스토어는 없지만, 이러한 노력의 결과로 구글 플레이 스토어와

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

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

[37] https://www.cisa.gov/resources-tools/resources/secure-by-design

애플 앱 스토어는 사용자 보호에 대한 접근 방식을 알리기 위해 수년간의 투자와 학습을 통해 소비자의 신뢰와 안전에 대한 명성을 얻게 되었습니다.

Apple App Store 및 Google Play 스토어와 같은 주요 퍼스트 파티 앱 스토어는 기본 요건 및 가이드라인 설정, 자체 인증 요구, 앱 검토와 같은 프로세스를 구현하여 보안을 확보하고 있습니다.[38] 앱 개발자가 이러한 앱 스토어에 등록하려면 앱에 대한 다양한 보안, 개인정보 보호 및 투명성 요건을 성공적으로 충족해야 합니다. 여기에는 앱이 광고된 대로 작동하는지, 적절한 권한만 요청하는지, 제대로 작동하는 개인정보 보호정책을 갖추고 있는지 등이 포함됩니다. 또한 Apple 과 Google의 앱 스토어는 앱이 사용하는 권한과 데이터 수집에 대한 정보를 포함하여 앱 스토어 목록에 투명성을 요구합니다.[39],[40]

퍼스트 파티 앱 스토어는 앱 자체를 검토하는 것 외에 개발자 계정을 심사하는 등 추가적인 보호 조치를 시행할 수도 있습니다. 예를 들어 Google Play 스토어는 "개발자의 Google 계정, 활동, 기록, 청구 세부 정보, 기기 정보 등"을 분석하여 잠재적인 위험 신호를 식별합니다.[41]

앱 제출을 검토할 때 퍼스트 파티 앱 스토어는 앱 개발자의 증명을 검토하고, 다양한 자동 검토를 적용하고, 사람 검토자가 앱을 수동으로 검토하는 등 앱의 기능을 보장하기 위해 여러 가지 조치를 취할 수 있습니다. 이러한 검토는 다양한 도구와 기법을 사용하여 멀웨어 또는 기타 잠재적으로 유해하거나 원치 않는 측면을 검색하는 정적 및 동적 검토를 수행할 수 있습니다. 또한 Apple 과 같은 퍼스트 파티 앱 스토어는 새로 제출된 앱에 대한 일상적인 검사 외에도 앱 업데이트를 검토하여 새로운 기능이 안전하게 유지되는지 확인합니다. 마지막으로, 퍼스트 파티 앱 스토어는 소비자 또는 보안 연구원의 불만 사항이나 앱이 원치 않는 동작을 수행한다는 알림을 기반으로 검토를 시작하는 경향이 있습니다.

앱이 앱 스토어 등록에 필요한 요건과 가이드라인을 충족하지 못하면 일반적으로 앱이 삭제됩니다. Apple 은 2022 년에 150 만 개 이상의 앱 제출을 거부하고 186,000 개 이상의 앱을 앱 스토어에서 삭제했다고 밝힐 정도로 이러한 문제의 규모가 매우 큽니다.[42] 이러한 삭제는 안전하고 신뢰할 수 있는 앱 스토어 환경을 조성하고, 최종 사용자를 위

---

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

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

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

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

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

험으로부터 보호하며, 악의적인 행위자가 기기를 감염시킬 다른 더 유익한 수단을 찾도록 장려하는 역할을 합니다.

Apple 과 Google은 소비자 차원에서 보안 및 정책 보호와 요구 사항을 앱 스토어 사용자가 쉽게 접근하고 이해할 수 있도록 하기 위해 많은 노력을 기울여 왔습니다. 또한, 두 회사는 심사를 거친 앱이 요구하는 권한과 관련하여 더 많은 투명성을 확보하여 소비자가 공식 앱스토어 기준 이상의 개인정보 보호 및 보안 수준에 대해 정보에 입각한 결정을 내릴 수 있도록 노력해 왔습니다. Google Play 스토어는 독립적인 보안 검토를 완료한 앱에 배지를 표시하기 시작했습니다.[43] 이러한 프로세스와 정책은 효과가 입증되었지만 상당한 투자가 필요합니다.

모바일 앱 스토어를 위한 보안은 투자다

위에서 살펴본 바와 같이 최종 사용자에게 보안의 책임을 지우는 것은 비효율적이며, 기본적으로 사용자를 보호하기 위한 정책과 프로세스를 장려하는 사이버 보안 모범사례에도 어긋납니다. Google이나 Apple 과 같이 자원이 풍부한 대형 기업은 전문 지식과 자원, 그리고 이를 효과적으로 수행할 의지가 있지만, 다른 기업들도 마찬가지입니다.

위에서 언급한 보호 유형은 타사 앱 스토어에서 동일한 수준으로 구현되는 경우는 거의 없지만 대부분의 악성, 저품질 및 사기성 앱을 걸러냅니다. 타사 앱 스토어는 자사 앱 스토어를 보호하거나 호스팅된 앱을 심사할 수 있는 리소스, 경험, 플랫폼 및 OS에 대한 지식, 인센티브가 퍼스트파티 앱 스토어와 동일한 수준에 미치지 못합니다. 또한 타사 앱 스토어는 환영받지 못할 것으로 간주되는 앱을 더 관대하게 수용함으로써 기존 대형 스토어와 차별화하려고 할 수 있습니다. 반면에 퍼스트파티 앱 스토어는 마켓플레이스에서 앱의 보안을 개선하기 위해 상당한 리소스를 투자합니다.

DMA 구현을 위한 로드맵

모바일 운영체제를 의무화하면 모바일 생태계의 개인정보 보호와 보안에 부정적인 영향을 미칠 수밖에 없지만, 사용자가 타사 앱과 앱 스토어에 더 안전하게 액세스할 수 있도록 하는 동시에 타사 앱 개발자에게도 OS 수준의 기능에 대한 더 많은 액세스 권한을 부여할 수 있는 방법이 있습니다. 위에서 언급했듯이, 그리고 Apple 과 같은 퍼스트 파티가 증명했듯이, DMA 를 준수하면 "멀웨어, 사기 및 사기, 불법 및 유해 콘텐츠, 기타 개인정보 및 보안 위협"의 확산이 증가할 것이 거의 확실합니다. 그러나 입법자와 정책 입안자들은 게이트키퍼가 소비자를 보호할 수 있는 건설적인 이행 지침을 통해 이러한

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

문제를 완화할 수 있습니다.[44]

EU 회원국은 퍼스트 파티 앱 스토어 및 모바일 OS 소유자와 모바일 디바이스 사용자를 지원하여 기꺼이 지원해야 합니다:

- 게이트키퍼는 배포 채널에 관계없이 기본적인 앱 검토를 수행해야 합니다. 이를 위해서는 운영 체제에 내장된 새로운 메커니즘이나 앱 스토어와의 계약이 필요할 수 있습니다. 인증 및 제 3자 평가를 통해 앱이 안전하다는 것을 입증하는 방법도 있을 수 있습니다.
- 정책 입안자는 사용자와 다른 사람들이 앱의 작동 방식과 용도를 이해할 수 있도록 기본 기능 및 필수 정보에 관한 앱 설명 공지를 고려해야 합니다.
- 운영 체제는 악성 앱이 모바일 디바이스의 보안과 무결성을 해치는 것을 방지하기 위해 앱을 서로 샌드박스하고 보호하며 악성 앱으로부터 운영 체제, 사용자 데이터 및 디바이스 하드웨어를 보호하는 추가 도구를 포함하여 향상된 모바일 보호 기능을 구현할 수 있습니다. 이러한 도구에는 기업 관리자를 위한 MDM 도구가 포함될 수 있습니다.
- 게이트키퍼는 타사 앱 스토어를 신뢰할 수 있도록 기술적 및 계약적 통제 장치를 마련해야 합니다. 각 게이트키퍼는 서로 다른 완화 조치를 선택할 가능성이 높지만, DMA를 준수하기 위해 노력할 때 사용자를 보호하기 위해 사용할 수 있는 디바이스와 사용자를 보호할 수 있는 광범위한 옵션을 갖추고 있어야 합니다.
- 게이트키퍼 모바일 기업은 사용자를 보호할 수 있는 명확한 지침이 필요하며, 사용자 보호를 위해 새로운 시스템을 개념화, 구축, 테스트 및 입증할 수 있는 충분한 시간이 주어져야 합니다.
- 규제 당국은 앱과 앱스토어의 보안 및 무결성 문제에 주의를 기울이고 모든 앱과 스토어가 동일하게 만들어지는 것은 아니라는 점을 인식해야 합니다. 앱 및 앱 스토어 개발자가 책임감 있게 행동하도록 평가하고 보장하는 메커니즘의 개발을 지원해야 하며, 그렇지 않을 경우 책임을 물을 수 있도록 해야 합니다.
- 모바일 운영 체제를 개발하는 게이트키퍼는 개발자가 변화하는 생태계를 이용하지 못하도록 권한 및 보안 모델과 운영 방식을 유연하게 조정할 수 있어야 합니다. 정책 입안자는 앱 스토어와 디바이스 운영 체제가 생태계에 통합할 수 있는 보안 메커니즘과 제한 사항을 발전시킬 수 있는 능력을 보호해야 합니다.
- 모바일 생태계를 다루는 정책은 해당 생태계의 보안을 약화시켜서는 안 됩니다. 정책 입안자들은 모바일 플랫폼의 보안과 개인정보 보호가 지속적으로 개선되고, 이 두 가지가 처음부터 플랫폼과 앱에 내장되도록 해야 합니다. 지금까지의

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

진전을 위협하는 제안은 재고되어야 합니다.

- 정책 입안자는 사용자가 기꺼이 감당할 수 있는 보안 책임과 부담이 무엇인지 현실적으로 파악해야 합니다. 연구에 따르면 보안 인식과 올바른 보안 결정은 상관관계가 없다고 합니다.
- 정책 입안자들은 모바일 기기의 작동 방식과 설치 가능한 앱에 대한 특정 관행을 의무화하기보다는 모바일 기기에 대한 위험 기반 관행을 지원해야 합니다.[45]

결론

DMA 가 법으로 통과되고 게이트키퍼가 규정 준수를 위해 노력하면서 모바일 생태계는 중요한 전환기에 접어들고 있습니다. 사이버보안 정책 및 법률 센터는 정책 입안자와 게이트키퍼, 그리고 나머지 모바일 생태계가 사용자와 모바일 디바이스를 안전하게 보호하기 위해 함께 노력할 수 있기를 바랍니다. 정책 입안자들은 기업, 생태계, 소비자에 대한 보안 영향을 고려해야 합니다. 기존 앱스토어 심사 및 감독의 이러한 여러 요소의 영향을 정량화하기는 어렵지만, 앱스토어 개발자가 사용자를 보호하기 위해 투자하는 노력은 인정하고 보상해야 합니다. 앱 스토어 소유자와 개발자가 보안 및 개인정보 보호 강화 조치를 취하면 사용자들은 자신도 모르는 방식으로 혜택을 누릴 수 있습니다.

모든 모바일 멀웨어로부터 사용자를 보호하는 완벽한 시스템은 없지만, 사용자가 고려해야 하는 원치 않거나 악의적인 활동의 수를 크게 줄일 수 있는 방법을 알고 있습니다.

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