Health-ISAC™
SHARING SINCE 2010
Collaborating for Resilience in Healthcare

Health-ISAC Weekly Blog -- Hacking Healthcare™

Hacking Healthcare™ ○ TLP:WHITE Alert ID : 0231ca63 Feb 23, 2024, 04:15 PM

This week, *Hacking Healthcare*TM explores how the EU's Digital Markets Act may have a negative effect on healthcare cybersecurity. Specifically, we examine how provisions relating to mobile apps and app stores could unintentionally lead to increased risk for the EU's mobile ecosystem and organizations that take advantage of bring your own device (BYOD) policies. We also consider actions Health-ISAC members may want to take to limit this risk.

Welcome back to *Hacking Healthcare*TM.

EU Digital Markets Act May Raise Mobile Cybersecurity Risk

The EU has pursued several significant legal and regulatory efforts with cybersecurity and privacy implications over the past few years. While many of you will be familiar with the revision to the Network and Information Security (NIS) Directive and the Cyber Resilience Act (CRA), fewer are probably as familiar with the Digital Markets Act (DMA). While not directly aimed at healthcare organizations, certain provisions within the text could negatively impact healthcare entity cybersecurity and are worth exploring in more depth.

What is the DMA?

The DMA is described by the European Commission as a “law to make the markets in the digital sector fairer and more contestable.”[i] At face value, the DMA is an attempt to level the digital playing field in ways that may help drive marketplace innovation and competition while providing the benefits of competition, such as lower prices and product/service choice, to consumers.

How does the DMA Accomplish its Goals?

The primary mechanism at work is the identification and regulation of “Gatekeepers,” which the European Commission describes as “large digital platforms providing so called core platform services, such as for example online search engines, app stores, messenger services.”[ii] In practice, the DMA is scoped in such a way that it primarily targets US technology giants like Alphabet, Amazon, Apple, Meta, and Microsoft.[iii] However, the DMA also applies to ByteDance, and the list of Gatekeepers is subject to change.

A Blow to Mobile Cybersecurity?

The Core Platform Services and Gatekeepers ultimately puts the Apple App Store, Google Play Store, Google Android operating system, and Apple iOS operating system in scope for coverage by the DMA. This means that Apple and Google, whose mobile phones, operating systems, and app stores dominate the mobile market, must adhere to the various applicable provisions within the DMA.

For our purposes, we are going to focus on two provisions that seem all but certain to negatively impact the mobile cybersecurity ecosystem. Under Article 6, "Obligations for gatekeepers susceptible of being further specified under Article 8," are the following provisions:[iv]

- 6.4. The Gatekeeper shall allow and technically enable the installation and effective use of third-party software applications or software application stores using, or interoperating with, its operating system and allow those software applications or software application stores to be accessed by means other than the relevant core platform services of that Gatekeeper.
- 6.7 The Gatekeeper shall allow providers of services and providers of hardware, free of charge, effective interoperability with, and access for the purposes of interoperability to, the same hardware and software features accessed or controlled via the operating system or virtual assistant listed in the designation decision pursuant to Article 3(9) as are available to services or hardware provided by the gatekeeper.

These provisions essentially require Gatekeepers like Google and Apple to open up their mobile ecosystem to more easily allow mobile users to access third-party apps and app stores. They also require that third-party apps be able to access the same kinds of hardware and software features that might otherwise be reserved for trusted first-party apps.

Let's analyze the security ramifications of these provisions, put them in a broader policy context, and make some recommendations for how Health-ISAC members may be able to mitigate some level of risk created by these DMA provisions.

Action & Analysis
Included with Health-ISAC Membership

Congress
Tuesday, February 20
No relevant hearings

Wednesday, February 21
No relevant meetings

Thursday, February 22
No relevant meetings

International Hearings/Meetings

No relevant meetings

EU

[i] https://digital-markets-act.ec.europa.eu/about-dma_en

[ii] https://digital-markets-act.ec.europa.eu/index_en

[iii] https://digital-markets-act.ec.europa.eu/gatekeepers_en

[iv] https://eur-lex.europa.eu/eli/reg/2022/1925

[v] https://play.google/intl/en_au/developer-content-policy/

[vi] https://developer.apple.com/app-store/review/guidelines/

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

[viii] https://eur-lex.europa.eu/eli/reg/2022/1925

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

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

[xi] https://www.pymnts.com/news/regulation/2024/competitors-say-apples-plans-dont-comply-with-digital-markets-act/

[xii] https://arstechnica.com/security/2024/02/a-password-manager-lastpass-calls-fraudulent-booted-from-app-store/

Report Source(s)

Health-ISAC

Reference | References

Apple

Europa Analytics

Europa Analytics
PYMNTS
Europa Analytics
ArXiv
Ars Technica
Europa Analytics
play
Apple

Tags

BYOD, Digital Markets Act, Regulation, Hacking Healthcare, BYOD policy, mobile, DMA

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions and/or Comments:

Please email us at contact@h-isac.org

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Hacking Healthcare™:

Hacking Healthcare is co-written by John Banghart and Tim McGiff.

John Banghart has served as a primary advisor on cybersecurity incidents and preparedness and led the National Security Council’s efforts to address significant cybersecurity incidents, including those at OPM and the White House. John is currently the Senior Director of Cybersecurity Services at Venable. His background includes serving as the National Security Council’s Director for Federal Cybersecurity, as Senior Cybersecurity Advisor for the Centers for Medicare and Medicaid Services, as a cybersecurity researcher and policy expert at the National Institute of Standards and Technology (NIST), and in the Office of the Undersecretary of Commerce for Standards and Technology.

Tim McGiff is currently a Cybersecurity Services Program Manager at Venable, where he coordinates the Health-ISAC’s annual Hobby Exercise and provides legal and regulatory updates for the Health-ISAC’s monthly Threat Briefing.

- John can be reached at jbanghart@h-isac.org and jfbanghart@venable.com.
- Tim can be reached at tmcgiff@venable.com.

Access the Health-ISAC Intelligence Portal:

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Cyware.