Bài đăng dự kiến đăng trên vfossa.vn
Các bài đăng báo sử dụng nguồn tham chiếu này!

Rủi ro khi sử dụng mã nguồn mở hay là sự đánh tráo khái niệm để cạnh tranh không lành mạnh?

Tác giả: Ban chuyên môn VFOSSA

Gần đây một số doanh nghiệp sử dụng chiến dịch truyền thông phát đi thông điệp không đúng khi đánh giá về rủi ro khi sử dụng mã nguồn mở. Câu lạc bộ phần mềm tự do nguồn mở Việt Nam xin phản biện lại thông điệp này và cung cấp thông tin đầy đủ về các luận điểm được sử dụng trong các lập luận có liên quan trong các bài báo này để bạn đọc đánh giá chính xác thông tin, tránh việc sa vào hoặc tin theo những luận điểm sai lệch để đánh tráo khái niệm nhằm gây hoang mang trên truyền thông.

Ngày nay, đa số các sản phẩm công nghệ thông tin đều sử dụng ít hay nhiều phần mềm nguồn mở. Theo ước tính của tổ chức Linux Foundation, thành phần phần mềm nguồn mở chiếm khoảng 70-90% trong bất kỳ giải pháp phần mềm hiện đại nào [12]. Chính vì vậy việc hiểu biết đúng đắn về rủi ro an ninh đóng vai trò hết sức quan trọng trong bối cảnh sử dụng phần mềm nguồn mở trong chuyển đổi số hiện nay. Trong bài báo đăng ngày 24/05/2023 với tiêu đề *"Chuyển đổi số doanh nghiệp: Nhiều rủi ro khi sử dụng mã nguồn mở"*, tác giả nêu ra 7 rủi ro được cho là "điểm yếu" của phần mềm nguồn mở. Đáng ngại là bài báo này sau đó đã được một loạt báo điện tử khác đăng lại. Tuy nhiên các lập luận để đi đến kết luận là thiếu dẫn chứng, ngụy biện, thậm chí sai lệch, gây ra hiểu nhầm cho công chúng. Cụ thể như sau:

1. Đánh giá về rủi ro an ninh, bài báo này cho rằng "với mã nguồn mở - phần mềm được công khai trên mạng nên tin tặc có thể dễ dàng nghiên cứu, phân tích các lỗ hổng và phát tán nhanh chóng". Điều này là một lập luận sai trái đã được các chuyên gia phần mềm phân tích trong các báo cáo [1], [2], [3].

Một luận điểm khác được sử dụng trong bài này là "khi gặp sự cố an toàn thông tin mức hệ thống sẽ rất khó có thể cập nhật và sửa lỗi". Nhiều bằng chứng cho thấy tốc độ vá lỗi của các phần mềm nguồn mở thường sẽ nhanh hơn phần mềm nguồn đóng cùng loại (ví dụ so sánh hệ điều hành nguồn mở Linux với Windows), lý do cho việc này là bởi vì phần mềm nguồn mở thường được nhiều nhà phát triển cùng phát triển, và do kho mã nguồn được công khai cho nên nhiều đơn vị có thể tham gia sửa lỗi (chứ không chỉ riêng nhà phát hành phần mềm). Lỗ hổng HeartBleed của OpenSSL là một ví dụ điển hình (lỗi được sửa chỉ sau 6 ngày) [2]

Ngoài ra nếu phần mềm nguồn mở có lỗi, thông thường các nhà phát triển sẽ phải chịu sức ép nhanh chóng tìm cách vá lỗi nhanh hơn phần mềm nguồn đóng do các hệ thống báo lỗi cũng được công khai thay vì bí mật như phần mềm nguồn đóng. Do yếu tố độc quyền nên nhiều nhà phát triển nguồn đóng "giấu nhẹm" các lỗi được phát hiện, nhiều trường hợp nhận được báo lỗi còn không chịu phát hành bản vá và để lỗi tồn tại dai dẳng nhiều năm sau đó cho đến khi sự cố lớn xảy ra.

Riêng lập luận rằng “phần mềm mã nguồn mở là việc khó kiểm soát đánh giá được mức độ an toàn bảo mật do các mã nguồn được phát triển bởi quá nhiều người dùng khác nhau. Thậm chí tiềm ẩn các đoạn mã gián điệp chứa virus để cố tình thu thập thông tin với mục đích xấu” thì điều này cũng hoàn toàn không chính xác. Phần mềm dù đóng hay mở thì vẫn có thể có nhiều nhà phát triển khác nhau và có thể bị kẻ xấu cài mã độc. Tuy nhiên, sử dụng phần mềm nguồn mở thì người dùng có cơ hội để kiểm tra mã nguồn và phát hiện các phần mềm gián điệp hay đoạn mã dạng “cửa hậu”, còn với phần mềm nguồn đóng thì việc này khó khăn hơi rất nhiều. Chưa kể tình trạng nhà phát hành cố tình đưa mã độc vào phần mềm nguồn đóng hoặc đặt “cửa hậu” để thực hiện các mục đích xấu. Trong khi đó, những phần mềm nguồn mở được phát hành chuẩn chưa từng có trường hợp nào được phát hiện nhà sản xuất phần mềm cố ý cài mã độc hoặc “cửa hậu”, các trường hợp cố tình có ý đồ xấu đều bị phát hiện kịp thời trong quá trình phát triển, với quy trình peer-review chặt chẽ. Đấy cũng là lý do mà chính quyền các nước tránh dùng phần mềm nguồn đóng của các quốc gia khác nhưng sẵn sàng sử dụng phần mềm nguồn mở có nguồn gốc cũng từ các quốc gia đó. [4], [5]

Nói về việc đóng hay mở an ninh hơn thì việc này đã được các chuyên gia công nghệ trong nước tranh luận và ngã ngũ cách đây gần 24 năm trên tạp chí Tin học và Đời sống [14]. Thực tế sau đó nhiều năm chứng minh qua việc Mỹ lệnh cấm ZTE - nhà sản xuất các thiết bị viễn thông lớn thứ 2 của Trung Quốc, sau Huawei - mua vi chip, hệ điều hành và các phần mềm ứng dụng trong kho phần mềm đi với hệ điều hành đó từ các công ty của Mỹ trong vòng 7 năm - có hiệu lực từ ngày 15/04/2018. Sau đó là bài học tương tự cho Huawei khi ngày 15/05/2019 Mỹ đã ban hành sắc lệnh mà sau đó khiến Huawei không thể mua được chip cũng như tiếp cận các phần mềm từ các công ty của Mỹ. Về điều này, Tổng biên tập Nhật báo Khoa học và Công nghệ, cơ quan ngôn luận của Bộ Khoa học và Công nghệ Trung Quốc, nói tại một hội thảo ở Bắc Kinh hôm 21/6/2018: “Căn nhà của chúng ta được xây trên nền móng của người khác nhưng một số người cứ cho rằng chúng ta có các quyền sở hữu tài sản vĩnh cửu và tuyệt đối. Điều đáng lo ngại là những người có quan điểm này đang lừa dối các lãnh đạo, công chúng và ngay chính họ” (Nguồn: Tạp chí Kinh tế Sài Gòn Online ngày 14/7/2018 [13]). Việc ZTE, Huawei không làm chủ được các công nghệ sản xuất các con vi chip, hệ điều hành và các ứng dụng phần mềm đi với hệ điều hành đó mà phải đi mua các phần mềm và công nghệ độc quyền giống như xây nhà trên nền móng của người khác, nó khiến cho họ dễ bị tổn thương, đồng thời cho thấy an ninh của ZTE và Huawei là bằng 0 khi phụ thuộc vào các công nghệ độc quyền.

2. Đánh giá rủi ro trong triển khai và vận hành, bài viết cho rằng “Không phải phần mềm nguồn mở nào cũng có tài liệu hướng dẫn cài đặt và vận hành chi tiết và đầy đủ như phần mềm thương mại nên sẽ gây khó khăn trong quá trình triển khai và vận hành”. Đây cũng là đánh giá rất phiến diện và chủ quan, việc này hoàn toàn không liên quan đến việc phần mềm là nguồn đóng hay nguồn mở mà chủ yếu liên quan đến việc nhà phát triển có cung cấp đầy đủ tài liệu hay không, và nếu là doanh nghiệp đặt hàng sử dụng phần mềm thì bạn có quyền yêu cầu nhà cung cấp cung cấp tài liệu theo hợp đồng cho dù phần mềm được yêu cầu theo hợp đồng là phần mềm nguồn đóng hay nguồn mở.

Hơn thế nữa, với phần mềm nguồn mở, khi sử dụng thì doanh nghiệp cần chú ý tới việc đánh giá độ chín của phần mềm là dễ dàng giảm thiểu rủi ro trong triển khai và vận hành. Trong tất cả các tiêu chí đánh giá phần mềm nguồn mở theo điểm thất bại PoF hay điểm mô

hình độ chín nguồn mở OSMM đều có đánh giá về việc phần mềm có đầy đủ tài liệu hay không. Đây cũng là lý do mà Thông tư 20/2014/TT-BTTTT quy định về các sản phẩm phần mềm nguồn mở được ưu tiên mua sắm, sử dụng trong cơ quan, tổ chức nhà nước [6] lựa chọn các phần mềm nguồn mở có điểm ngưỡng thất bại PoF từ 50 điểm trở xuống và điểm mô hình độ chín nguồn mở OSMM từ 60 điểm trở lên (thang điểm 100). Các đơn vị lựa chọn phần mềm nguồn mở để sử dụng có thể sử dụng các công cụ này để đánh giá và lựa chọn phần mềm nguồn mở để dễ dàng giảm thiểu rủi ro trong triển khai và vận hành tương tự như việc lựa chọn các phần mềm nguồn đóng đạt các chứng chỉ CMMI, SSMM, RRR, SPICE...

3. Cho rằng phần mềm nguồn mở có khả năng tương thích kém và có thể gặp sự cố bất cứ lúc nào là đánh giá hoàn toàn sai trái. Phần mềm nguồn mở thường hỗ trợ các chuẩn mở, với mã nguồn công khai, việc giúp cho phần mềm tương thích là dễ dàng hơn đối với các phần mềm độc quyền. Việc này không chỉ liên quan đến yếu tố công nghệ mà còn liên quan đến giấy phép của phần mềm. Cụ thể: phần mềm nguồn mở thường cung cấp quyền sửa đổi mã nguồn, vì vậy nếu một phần mềm nguồn mở thiếu tương thích, đội kỹ thuật của doanh nghiệp có thể chủ động can thiệp và làm cho nó tương thích. Ngược lại, với phần mềm nguồn đóng, hầu hết doanh nghiệp không có mã nguồn phần mềm hoặc nếu có thì giấy phép thường ghi “khách hàng không có quyền can thiệp hoặc sửa đổi phần mềm”.

Bài viết lấy ví dụ trang https://healthcare.gov của chính phủ Mỹ sử dụng phần mềm nguồn mở và phải ngừng hoạt động để làm ví dụ là một trường hợp không điển hình và không có tính phổ quát để kết luận rằng sử dụng phần mềm nguồn mở. Hàng ngàn hệ thống sử dụng phần mềm nguồn đóng cũng xảy ra các sự cố nghiêm trọng và phải đóng cửa. Và bất cứ trường hợp nào đội ngũ kỹ thuật vận hành các hệ thống cụ thể cũng có thể để xảy ra các rủi ro tương tự nếu họ thiếu kinh nghiệm vận hành và xử lý sự cố.

4. Đánh giá phần mềm nguồn mở “khó nâng cấp và mở rộng theo nhu cầu” tiếp tục là một luận điểm sai hoàn toàn. Kiến trúc hệ thống là yếu tố ảnh hưởng hàng đầu tới vấn đề dễ dàng mở rộng và nâng cấp. Phần mềm nguồn mở được thiết kế với kiến trúc mở ngay từ trong ý tưởng; với những người có đủ năng lực thiết kế kiến trúc hoặc tìm tới đúng một kiến trúc sư trưởng, một nhà cung cấp dịch vụ giàu kinh nghiệm, luôn có thể đảm bảo cho một bản thiết kế kiến trúc có tính toán đầy đủ đến các vấn đề dễ dàng nâng cấp, mở rộng cũng như nhiều vấn đề trọng yếu khác về hiệu năng, an toàn, an ninh... Hơn nữa, với phần mềm nguồn mở, bất kỳ nhà cung cấp nào có năng lực cũng có thể can thiệp vào bất cứ phần nào trong mã nguồn để hỗ trợ khách hàng nâng cấp, phát triển (thậm chí tìm lại kho mã nguồn cũ của phần mềm để khôi phục lại một phiên bản cũ nếu cần). Ngược lại, với các phần mềm nguồn đóng, nếu nhà phát triển ngừng phát triển và hỗ trợ thì thậm chí các doanh nghiệp cung cấp dịch vụ cũng không có mã nguồn để tìm hiểu, việc can thiệp và chỉnh sửa, vá lỗi trở nên khó khăn hơn gấp nhiều lần.

5. Về ý kiến rằng phần mềm nguồn mở hiệu năng chậm “vì trong bộ mã nguồn mở không tránh khỏi những đoạn code, chức năng dư thừa, chúng sẽ chiếm dụng nhiều tài nguyên hệ thống hơn bình thường và làm cho hệ thống chạy chậm” tiếp tục là một luận điểm đầy phiến diện. Bất cứ phần mềm dù nguồn đóng hay nguồn mở nếu không được tối ưu thì đều gặp vấn đề này. Nếu cùng một điều kiện như nhau, việc phát hành phần mềm dưới dạng phần mềm nguồn mở sẽ có nhiều động lực khiến nhà phát hành & các lập trình viên phải trau chuốt mã nguồn hơn là phần mềm nguồn đóng. Việc phát hành các đoạn

code “rác” trong phần mềm nguồn mở sẽ khiến cộng đồng và các doanh nghiệp khác dễ dàng phát hiện và chê cười, ngược lại, với phần mềm nguồn đóng thì cả lập trình viên và doanh nghiệp đều không bị động lực này thúc đẩy phải “làm đẹp” từng đoạn code.

Một thông tin thêm để bạn đọc dễ dàng so sánh: Theo thống kê năm 2016, có 498 trong tổng số 500 siêu máy tính với tốc độ nhanh nhất thế giới sử dụng hệ điều hành Linux, thay vì Windows [9]; thống kê năm 2023 cho thấy 100% máy tính trong Top 500 siêu máy tính trên thế giới sử dụng hệ điều hành nguồn mở Linux [10].

6. Đánh giá phần mềm nguồn mở thiếu hỗ trợ và phụ thuộc vào cộng đồng người dùng là một sự đánh tráo khái niệm, bởi vì phần mềm nguồn mở có cộng đồng người sử dụng và hay được nhắc đến yếu tố cộng đồng không có nghĩa là chỉ có cộng đồng người sử dụng hỗ trợ cho phần mềm. Phải hiểu chính xác rằng sự hỗ trợ từ cộng đồng người sử dụng phần mềm nguồn mở thông thường là hỗ trợ tình nguyện và miễn phí (việc này cũng xảy ra với một số ít các cộng đồng phần mềm nguồn đóng) và đương nhiên hỗ trợ miễn phí thì chủ yếu là tự nguyện, không có cam kết rõ ràng. Ngoài việc hỗ trợ miễn phí này, doanh nghiệp sử dụng phần mềm nguồn mở có thể thuê sự hỗ trợ chuyên nghiệp từ các nhà phát triển và các đơn vị cung cấp dịch vụ khác. Thị trường này cực kỳ đa dạng và rất linh hoạt chứ không bó buộc theo “khung” được các nhà phát triển phần mềm nguồn đóng ban hành. Đây chính là ưu điểm và là yếu tố khiến các chính phủ có chính sách ưu đãi cho phần mềm nguồn mở vì nó không bị “trói buộc” vào một nhà cung cấp hoặc đơn vị hỗ trợ nào cả.

Do đó, cũng trong đánh giá này, lập luận rằng “một số phần mềm mã nguồn mở phụ thuộc vào cộng đồng người dùng để duy trì và phát triển” là một lập luận sai. Riêng đánh giá “Nếu cộng đồng không phát triển hoặc bên cung cấp thay đổi chiến lược kinh doanh có thể chấm dứt dự án bất cứ lúc nào, người dùng có thể gặp phải các vấn đề liên quan đến tính năng, ổn định hoặc thậm chí không thể tiếp tục sử dụng phần mềm và phải tìm kiếm phần mềm khác thay thế” là sự đánh tráo khái niệm vì với phần mềm nguồn đóng, việc này vẫn xảy ra tương tự khi một nhà cung cấp bị đóng cửa hoặc phải thay đổi chiến lược kinh doanh do thị trường. Không có gì là trường tồn và một sản phẩm phần mềm cũng có chu kỳ phát triển và suy thoái của nó.

7. Đánh giá việc sử dụng phần mềm nguồn mở “dễ xảy ra tranh chấp bản quyền phần mềm” tiếp tục là một quan điểm mang tính ngụy biện. Nếu doanh nghiệp sử dụng sai giấy phép thì thì sử dụng phần mềm nguồn đóng càng gặp nhiều rủi ro hơn vì phần mềm nguồn đóng hạn chế nhiều quyền của người sử dụng hơn. Điển hình là các trường hợp sử dụng phần mềm vi phạm bản quyền bị khởi kiện, bị phạt chủ yếu do sử dụng các phần mềm nguồn đóng không có bản quyền.

Phần mềm nguồn mở mặc dù mang lại nhiều lợi ích cho cộng đồng và xã hội nhưng lại “lép vế” về mặt thương mại khi đứng trước phần mềm nguồn đóng vì nó giảm quyền lợi của nhà phát triển mà tăng quyền cho người sử dụng. Đó là lý do tại sao các chính phủ nhiều nước trên thế giới có chính sách khuyến khích sử dụng, phát triển phần mềm nguồn đóng. Việt Nam cũng không nằm ngoài xu hướng ấy mặc dù đóng góp của các nhà phát triển người Việt cho cộng đồng nguồn mở trên thế giới chưa nhiều nhưng chúng ta đã nhận được rất nhiều lợi ích từ phần mềm nguồn mở. Cộng đồng công nghệ thông tin nói riêng và chính

phủ Việt Nam nói chung đang từng bước nỗ lực để giúp thúc đẩy phát triển phần mềm nguồn mở.

Chú thích:

[1] Open Source Software Is More Secure Than Closed Source Softwarehttps://www.informit.com/articles/article.aspx?p=3172442&seqNum=9
[2] THE SECURITY OF OPEN SOURCE VS CLOSED SOURCE SOFTWAREhttps://www.simplerisk.com/blog/the-security-of-open-source-vs-closed-source-software
[3] Open Source vs Closed Source Security
https://www.netsec.news/open-source-vs-close-source-security/
[4] Nước Mỹ sử dụng phần mềm tự do nguồn mở (FOSS) như thế nào?
https://letrungnghia.mangvn.org/Author/Nuoc-My-su-dung-phan-mem-tu-do-nguon-mo-FOSS-nhu-the-nao-2994.html
[5] “Schneier nói về an toàn”
https://letrungnghia.mangvn.org/Philosophy/Schneier-noi-ve-an-toan-5119.html
[6] Thông tư 20/2014/TT-BTTTT Thông tư Quy định về các sản phẩm phần mềm nguồn mở được ưu tiên mua sắm, sử dụng trong cơ quan, tổ chức nhà nước
https://mic.gov.vn/Pages/VanBan/10139/20_2014_TT-BTTTT.html
[9] Các "siêu máy tính" nhanh nhất thế giới chạy hệ điều hành gì?
https://dantri.com.vn/suc-manh-so/cac-sieu-may-tinh-nhanh-nhat-the-gioi-chay-he-dieu-hanh-gi-20161116064655966.htm
[10] Thống kê về top 500 siêu máy tính
https://www.top500.org/statistics/list/
[11] Gartner: Mark Driver, Is Open Source Software More Secure Than Proprietary Software?
https://emtemp.gcom.cloud/ngw/globalassets/en/doc/documents/744611-is-open-source-software-secure.pdf
[12] A Summary of Census II: Open Source Software Application Libraries the World Depends On.
https://www.linuxfoundation.org/blog/blog/a-summary-of-census-ii-open-source-software-application-libraries-the-world-depends-on
[13] Chiến tranh thương mại, “nhát cửa” vào niềm tự hào công nghệ của Trung Quốc - Tạp chí Kinh tế Sài Gòn Online ngày 14/7/2018
[14] “Đóng” hay “mở” an ninh hơn - Tạp chí Tin học và Đời sống số tháng 12/2009, trang 68-70
https://vnfoss.blogspot.com/2009/12/ong-hay-mo-ninh-hon.html