TLP:CLEAR

BẢO MẬT THEO THIẾT KẾ

THAY ĐỔI CÁN CÂN
RỦI RO AN NINH MẠNG:

CÁC NGUYÊN TẮC VÀ PHƯƠNG PHÁP CHO
PHẦN MỀM BẢO MẬT THEO THIẾT KẾ

CISA | NSA | FBI | ACSC | CCCS | CERT NZ | NCSC-NZ | NCSC-UK | BSI | NCSC-NL
NCSC-NO | NÚKIB | INCD | KISA | NISC JP | JPCERT/CC | CSA | CSIRTAMERICAS

TLP:CLEAR

Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité

Mục lục

KHÁI QUÁT: DỄ BỊ TẤN CÔNG THEO THIẾT KẾ

Công nghệ được kết hợp vào hầu hết trong mọi khía cạnh của cuộc sống hàng ngày, khi các hệ thống sử dụng internet ngày càng kết nối chúng ta với các hệ thống quan trọng trực tiếp ảnh hưởng đến sự thịnh vượng kinh tế, đời sống và thậm chí sức khỏe của chúng ta, từ việc quản lý danh tính cá nhân đến y tế. Một ví dụ về nhược điểm của những tiện lợi như vậy là các vụ vi phạm mạng toàn cầu dẫn đến việc các bệnh viện phải hủy bỏ các ca phẫu thuật và chuyển hướng chăm sóc bệnh nhân. Công nghệ không an toàn và các lỗ hổng bảo mật trong các hệ thống quan trọng có thể tạo cơ hội 'mời gọi' các cuộc xâm nhập mạng độc hại, dẫn đến các rủi ro an ninh[1] tiềm ẩn.

Do đó, điều tối cần thiết đối với các nhà sản xuất phần mềm là làm cho bảo mật theo thiết kế và bảo mật theo mặc định trở thành các tâm điểm của quá trình thiết kế sản phẩm và tạo sản phẩm. Một số nhà cung cấp đã có những tiến bộ đáng kể trong việc thúc đẩy kỹ nghệ này tiến lên trong việc bảo đảm phần mềm, trong khi một số khác lại đang chậm lại phía sau. Các tổ chức tác giả mạnh mẽ khuyến khích các nhà sản xuất công nghệ xây dựng sản phẩm trên cơ sở giảm bớt gánh nặng đối với an ninh mạng cho khách hàng, để họ không cần phải liên tục thực hiện việc theo dõi, cập nhật định kỳ và kiểm soát thiệt hại trên hệ thống của mình hầu giảm thiểu các cuộc xâm nhập mạng. Chúng tôi cũng kêu gọi các nhà sản xuất phần mềm xây dựng sản phẩm của họ theo cách tạo điều kiện thuận lợi cho việc tự động hóa cấu hình, theo dõi và cập nhật định kỳ. Các nhà sản xuất được khuyến khích để đảm nhận trách nhiệm trong việc cải thiện kết quả bảo mật cho khách hàng của họ. Trong quá khứ, các nhà sản xuất công nghệ đã trông cậy vào việc sửa các lỗ hổng bảo mật được tìm thấy sau khi khách hàng triển khai sản phẩm, đòi hỏi khách hàng phải tốn công sức để áp dụng các bản vá đó. Chỉ bằng việc tích hợp các thực hành bảo mật theo thiết kế, chúng ta mới có thể phá vỡ vòng lẩn quẩn của việc tạo ra rồi cài đặt các bản vá. **Lưu ý:** Thuật ngữ "bảo mật theo thiết kế" bao gồm cả bảo mật theo thiết kế và bảo mật theo mặc định.

Để đạt được các tiêu chuẩn cao về bảo mật phần mềm, các tổ chức tác giả khuyến khích các nhà sản xuất nên ưu tiên tích hợp bảo mật sản phẩm như một điều kiện tiên quyết quan trọng trước các tính năng và tốc độ đưa sản phẩm ra thị trường. Theo thời gian, các nhóm kỹ sư sẽ tạo cho mình một nhịp độ ở trạng thái ổn định mới, trong đó vấn đề bảo mật sẽ thực sự được tích hợp vào thiết kế và không tốn nhiều công sức để bảo trì.

Phản ánh quan điểm này, Liên minh châu Âu củng cố tầm quan trọng của bảo mật sản phẩm trong Đạo luật Khả năng Thích ứng Mạng, nhấn mạnh rằng các nhà sản xuất nên triển khai bảo mật trong suốt vòng đời của sản phẩm, nhằm ngăn ngừa các nhà sản xuất đưa ra thị trường các sản phẩm dễ bị tấn công.

Để tạo ra một tương lai theo đó công nghệ và các sản phẩm liên quan an toàn hơn cho khách hàng, các tổ chức tác giả kêu gọi các nhà sản xuất cải thiện chương trình thiết kế và phát triển của họ, để chỉ cho phép các sản phẩm được bảo mật theo thiết kế và bảo mật theo mặc định mới được chuyển giao. Một thời gian dài trước khi đi đến giai đoạn phát triển, các sản phẩm được bảo mật theo thiết kế đã được khái niệm hóa với tính an toàn của khách hàng là mục tiêu kinh doanh cốt lõi, chứ không chỉ là một tính năng kỹ thuật. Các

[1] Các tổ chức tác giả thừa nhận rằng thuật ngữ "an toàn" mang nhiều ý nghĩa tùy thuộc vào ngữ cảnh được sử dụng. Đối với mục đích của hướng dẫn này, thuật ngữ "an toàn" sẽ nói đến việc nâng cao các tiêu chuẩn bảo mật công nghệ, để bảo vệ khách hàng khỏi các hoạt động tấn công mạng độc hại.

sản phẩm được bảo mật theo thiết kế bắt đầu với mục tiêu đó trước khi đi đến giai đoạn phát triển. Các sản phẩm hiện tại có thể được nâng cao để đạt được trạng thái bảo mật theo thiết kế qua nhiều phiên bản. Các sản phẩm bảo mật theo mặc định là những sản phẩm an toàn để sử dụng "ngay sau khi mở hộp" mà không cần thay đổi cấu hình nhiều, và tính năng bảo mật đã có sẵn mà không cần phải trả thêm lệ phí. Hai triết lý này, cùng nhau giúp chuyển phần lớn trách nhiệm bảo mật sang nhà sản xuất, đồng thời giảm bớt nguy cơ khách hàng trở thành nạn nhân của các vụ vi phạm an ninh mạng do cấu hình sai, hay quá chậm trong việc cập nhật bản vá cho khách hàng hoặc nhiều vấn đề thường gặp khác.

Cơ quan An ninh Mạng và An ninh Hạ tầng Cơ sở (Cybersecurity and Infrastructure Security Agency - CISA), Cơ quan An ninh Quốc gia (National Security Agency - NSA), Cục Điều tra Liên bang (Federal Bureau of Investigation - FBI) cùng với các đối tác quốc sau đây[2] đưa ra các khuyến nghị trong hướng dẫn này như một lộ trình cho các nhà sản xuất phần mềm nhằm bảo đảm an ninh cho sản phẩm của họ:

- Trung tâm An ninh Mạng Úc châu (Australian Cyber Security Centre - ACSC)
- Trung tâm An ninh Mạng Gia Nã Đại (Canadian Centre for Cyber Security - CCCS)
- Trung tâm An ninh Mạng Quốc gia Vương Quốc Anh (United Kingdom's National Cyber Security Centre - NCSC-UK)
- Cục An ninh Mạng Liên bang Đức (Germany's Federal Office for Information Security - BSI)
- Trung tâm An ninh Mạng Quốc gia Hà Lan (Netherlands' National Cyber Security Centre - NCSC-NL)
- Trung tâm An ninh Mạng Quốc gia Na Uy (Norway's National Cyber Security Center - NCSC-NO)
- Đội Ứng phó với Tình trạng Khẩn cấp Máy vi tính Tân Tây Lan (Computer Emergency Response Team New Zealand - CERT NZ) và Trung tâm An ninh Mạng Quốc gia Tân Tây Lan (New Zealand's National Cyber Security Centre - NCSC-NZ).
- Cơ quan An ninh và Internet Hàn Quốc (Korea Internet & Security Agency - KISA)
- Tổng cục Mạng Quốc gia Do Thái (Israel's National Cyber Directorate - INCD)
- Trung tâm Quốc gia về Tình trạng Sẵn sàng và Chiến lược cho An ninh Mạng Nhật Bản (Japan's National Center of Incident Readiness and Strategy for Cybersecurity - NISC) và Trung tâm Phối hợp Đội Ứng phó Khẩn cấp Máy vi tính Nhật Bản (Japan Computer Emergency Response Team Coordination Center - JPCERT/CC).
- OAS/CICTE (Các Tổ chức của các Quốc gia châu Mỹ/Ủy ban Liên châu Mỹ Chống Khủng bố) Mạng lưới Đội Ứng phó Vấn đề Mạng của Chính phủ (CSIRT) Châu Mỹ (Cyber Incident Response Teams - CSIRT) châu Mỹ
- Cơ quan An ninh Mạng Tân Gia Ba (Cyber Security Agency of Singapore CSA)
- Cơ quan An ninh và Thông tin Mạng Quốc gia của Cộng hòa Séc (Czech Republic's National Cyber and Information Security Agency - NÚKIB)

Các tổ chức tác giả ghi nhận nhiều đóng góp của nhiều đối tác thuộc các khu vực tư nhân trong việc thúc đẩy bảo mật theo thiết kế và bảo mật theo mặc định Mục đích của tài liệu này là nhằm thúc đẩy một cuộc đối thoại tầm vóc quốc tế về các ưu tiên, đầu tư và các quyết định quan trọng cần thiết để đạt được một tương lai, trong đó công nghệ an toàn, bảo mật và linh hoạt theo thiết kế và mặc định. Nhằm đạt được mục tiêu đó, các tổ chức tác giả mong nhận được ý kiến đóng góp từ các bên liên quan về tài liệu này và có ý định triệu tập một loạt các phiên họp để tiếp tục hoàn thiện, định nghĩa rõ và nâng cao hướng dẫn của chúng tôi nhằm đạt được mục đích chung của chúng ta.

Muốn biết thêm thông tin về tầm quan trọng của an toàn sản phẩm, hãy xem bài viết của CISA, Cái Giá phải Trả do Công nghệ Không An toàn và Chúng ta Có Thể Làm Gì Về Điều Này.

[2] Sau đây sẽ được gọi là "các tổ chức tác giả."

CÓ GÌ MỚI

Lần xuất bản đầu tiên của phúc trình này đã tạo ra nhiều cuộc thảo luận trong ngành công nghiệp phần mềm. Tin tức hàng ngày về các tổ chức và cá nhân bị xâm phạm nêu bật nhu cầu cần có nhiều cuộc trao đổi hơn về cách giải quyết các vấn đề lâu đời và được hệ thống hoá trong các sản phẩm phần mềm.

Sau khi công bố vào tháng 4 năm 2023, các tổ chức tác giả (kể từ đây được gọi là "chúng tôi" và "của chúng tôi") đã nhận được nhiều ý kiến đóng góp hữu ích từ hàng trăm cá nhân, công ty và hiệp hội thương mại. Yêu cầu thường thấy nhất qua các ý kiến góp ý là yêu cầu cung cấp thêm chi tiết về ba nguyên tắc khi chúng áp dụng với cả nhà sản xuất phần mềm cũng như với các khách hàng của họ. Trong tài liệu này, chúng tôi mở rộng bản phúc trình gốc và đề cập đến các chủ đề khác như tầm quy mô của nhà sản xuất và khách hàng, mức độ am tường của khách hàng và phạm vi của các nguyên tắc.

Phần mềm hiện diện ở khắp mọi nơi và không có một bản phúc trình nào sẽ có thể trình bày đầy đủ toàn bộ các loại hệ thống phần mềm, quá trình phát triển sản phẩm phần mềm, triển khai và bảo trì của khách hàng, cũng như tích hợp với các hệ thống khác. Đối với các hướng dẫn bên dưới mặc dù không áp dụng rõ ràng cho môi trường cụ thể nào, nhưng chúng tôi mong nhận được ý kiến từ cộng đồng về cách những phương pháp được mô tả trong tài liệu này đã đưa đến những cải thiện cụ thể về an ninh.

Phúc trình này áp dụng với các nhà sản xuất hệ thống và mô hình phần mềm trí tuệ nhân tạo (artificial intelligence - AI). Mặc dù có thể khác biệt so với các dạng phần mềm truyền thống, nhưng các biện pháp bảo mật cơ bản vẫn áp dụng với các hệ thống và mô hình AI. Một số phương pháp bảo mật theo thiết kế có thể cần được điều chỉnh để tính đến các yếu tố cụ thể cho AI, nhưng ba nguyên tắc bao quát về bảo mật theo thiết kế áp dụng với tất cả các hệ thống AI.

Chúng tôi thừa nhận rằng việc chuyển đổi vòng đời phát triển phần mềm (software development lifecycle - SDLC) để phù hợp với các nguyên tắc bảo mật theo thiết kế này không phải là một công việc đơn giản và có thể mất nhiều thời gian. Hơn nữa, các nhà sản xuất phần mềm nhỏ hơn có thể gặp khó khăn trong việc thực hiện các gợi ý này. Chúng tôi tin rằng ngành công nghiệp phần mềm cần phải cung cấp rộng rãi các công cụ và quy trình giúp làm cho các sản phẩm trở nên an toàn hơn. Khi ngày càng nhiều người và tổ chức tập trung chú ý vào việc cải thiện an ninh phần mềm, chúng tôi tin rằng vẫn còn có thể có những thay đổi để thu hẹp khoảng cách giữa các nhà sản xuất phần mềm lớn và nhỏ vì lợi ích của tất cả khách hàng.

Phần cập nhật này cho bản phúc trình gốc về bảo mật theo thiết kế là một phần trong cam kết của chúng tôi về việc xây dựng mối quan hệ đối tác với nhiều cộng đồng bên liên quan được kết nối với nhau làm nền tảng cho hệ sinh thái công nghệ của chúng ta. Đây là kết quả của các ý kiến đóng góp từ nhiều phần của hệ sinh thái đó và chúng tôi sẽ tiếp tục lắng nghe và học hỏi từ các quan điểm khác nhau. Mặc dù còn rất nhiều thử thách phía trước, nhưng chúng tôi rất lạc quan khi tìm hiểu thêm về những cá nhân và tổ chức đã áp dụng triết lý bảo mật theo thiết kế và thường thành công.

CÁCH SỬ DỤNG TÀI LIỆU NÀY

Chúng tôi kêu gọi các nhà sản xuất phần mềm tuân thủ các nguyên tắc trong tài liệu này. Các nhà sản xuất phần mềm có thể chứng minh sự quyết tâm của mình bằng cách công khai chứng minh bằng tài liệu về các hành động mà họ đã thực hiện, phù hợp với các bước được liệt kê bên dưới. Chúng tôi khuyến khích các nhà sản xuất phần mềm tìm ra các chiến thuật đáp ứng tinh thần của nguyên tắc này và tạo ra các sản phẩm có khả năng thuyết phục ngay cả những khách hàng hiện tại và tiềm năng còn đang hoài nghi, để họ hiểu rằng quý vị đang thể hiện triết lý bảo mật theo thiết kế.

Ngoài những hành động mà nhà sản xuất phần mềm nên thực hiện, khách hàng cũng có thể tận dụng tài liệu này. Các công ty mua phần mềm nên đặt những câu hỏi hóc búa cho nhà cung cấp của mình, lấy nguồn cảm hứng từ các ví dụ về việc tuân thủ các nguyên tắc được liệt kê trong tài liệu này. Bằng cách làm như vậy, khách hàng có thể giúp chuyển hướng thị trường về phía các sản phẩm được bảo mật theo thiết kế hơn. Có ví dụ về các câu hỏi mà khách hàng có thể hỏi nhà cung cấp được nêu trong Hướng dẫn Mua sắm Công nghệ K-12 của CISA.

Chúng tôi khuyến khích khách hàng doanh nghiệp kết hợp các phương pháp này vào quy trình mua sắm, thẩm định độ tin cậy của nhà cung cấp, các quyết định về việc chấp nhận rủi ro doanh nghiệp và các bước khác cần thực hiện khi đánh giá nhà cung cấp. Khách hàng cũng nên thúc đẩy các nhà cung cấp của mình công khai chứng minh bằng tài liệu về các hành động bảo mật theo thiết kế mà mỗi nhà cung cấp thực hiện. Nói chung, điều này có thể tạo ra tín hiệu nhu cầu mạnh mẽ về việc bảo mật, đồng thời có thể khuyến khích và giúp các nhà sản xuất phần mềm thực hiện các bước hướng tới mức độ an ninh cao hơn. Nói cách khác, giống như chúng ta tìm cách tạo ra triết lý bảo mật theo thiết kế toàn diện trong các nhà sản xuất phần mềm, chúng ta cần tạo ra một văn hóa "bảo mật theo yêu cầu" đối với khách hàng của họ.

Bảo mật theo Thiết kế

"Bảo mật theo Thiết kế" nghĩa là các sản phẩm công nghệ được thiết kế theo cách bảo vệ hợp lý để những kẻ tấn công mạng độc hại không truy cập được vào các thiết bị, dữ liệu và hạ tầng cơ sở được kết nối. Các nhà sản xuất phần mềm nên thực hiện đánh giá rủi ro để xác định và liệt kê các mối đe dọa mạng phổ biến đối với các hệ thống quan trọng và rồi bao gồm biện pháp bảo vệ vào bản thiết kế sản phẩm có tính đến bối cảnh mối đe dọa mạng luôn phát triển.

Các phương pháp phát triển công nghệ thông tin (information technology - IT) an toàn và nhiều lớp phòng thủ – được gọi là phòng thủ sâu (defense-in-depth) – cũng được khuyến nghị để ngăn chặn những kẻ xâm nhập mạng độc hại tấn công vào các hệ thống hoặc truy cập trái phép vào dữ liệu nhạy cảm. Các tổ chức tác giả cũng khuyến nghị các nhà sản xuất sử dụng mô hình các mối đe dọa phù hợp trong suốt giai đoạn phát triển sản phẩm nhằm giải quyết tất cả các mối đe dọa tiềm ẩn đối với hệ thống và tính đến quy trình triển khai của từng hệ thống.

Các tổ chức tác giả kêu gọi các nhà sản xuất áp dụng phương pháp bảo mật toàn diện cho các sản phẩm và nền tảng của họ. Việc phát triển bảo mật theo thiết kế đòi hỏi các nhà sản xuất phầm mềm có những chiến lược đầu tư về các nguồn lực được dành riêng, tại mỗi tầng trong quá trình thiết kế và phát triển sản phẩm vốn không thể "gắn thêm vào" sau này. Điều này đòi hỏi vai trò lãnh đạo mạnh mẽ từ các nhà điều hành doanh nghiệp hàng đầu của nhà sản xuất, để việc bảo mật trở thành một ưu tiên trong kinh doanh, chứ không chỉ là một tính năng kỹ thuật. Sự hợp tác giữa các nhà lãnh đạo kinh doanh và các nhóm kỹ thuật mở rộng từ giai đoạn sơ khởi của thiết kế và phát triển, cho tới giai đoạn khách hàng triển khai và bảo trì. Các nhà sản xuất được khuyến khích thực hiện những đánh đổi và đầu tư khó khăn, bao gồm các đầu tư "vô hình" đối với khách hàng (ví dụ: chuyển sang ngôn ngữ lập trình có khả năng loại bỏ các lỗ hổng bảo mật phổ biến). Họ nên ưu tiên các tính năng, cơ chế và việc triển khai các công cụ bảo vệ khách hàng hơn là các tính năng của sản phẩm trông có vẻ hấp dẫn nhưng làm tăng bề mặt tấn công.

Không có một giải pháp duy nhất nào để chấm dứt được các mối đe dọa liên tục từ các kẻ tấn công mạng độc hại lợi dụng các lỗ hổng bảo mật công nghệ và các sản phẩm "bảo mật theo thiết kế" sẽ tiếp tục mắc phải các nhược điểm; tuy nhiên, một tập hợp lớn các nhược điểm là do sự tập hợp tương đối nhỏ của nhiều nguyên nhân gốc. Các nhà sản xuất nên phát triển các lộ trình bằng văn bản để đồng bộ hóa danh mục sản phẩm hiện có của họ tuân thủ theo các phương pháp bảo mật cao hơn theo thiết kế và bảo đảm là chỉ sai lệch trong các tình huống bất khả kháng mà thôi.

Các tổ chức tác giả thừa nhận rằng đã nhận trách nhiệm cho kết quả an ninh của khách hàng và việc bảo đảm mức độ bảo mật này có thể làm tăng chi phí phát triển. Tuy nhiên, việc đầu tư vào các phương pháp bảo mật theo thiết kế trong quá trình phát triển sản phẩm công nghệ mới và duy trì các sản phẩm hiện có, có thể cải thiện đáng kể tình trạng an ninh của khách hàng và giảm khả năng bị tấn công. Nguyên tắc bảo mật theo thiết kế không chỉ làm vững chắc tình trạng an ninh cho khách hàng và tăng cường uy tín thương hiệu cho các nhà phát triển sản phẩm, mà còn giảm các chi phí bảo trì và vá lỗi cho các nhà sản xuất về lâu dài.

Phần Khuyến nghị cho các Nhà Sản xuất Phần mềm được liệt kê dưới đây, bao gồm một danh sách các phương pháp và chính sách phát triển sản phẩm để các nhà sản xuất xem xét.

Bảo mật theo Mặc định

"Bảo mật theo mặc định" nghĩa là sản phẩm được thiết kế để chống chịu các kỹ thuật lợi dụng lỗ hổng bảo mật phổ biến ngay khi được đưa vào sử dụng mà không bị tính thêm lệ phí. Những sản phẩm này được bảo vệ khỏi những mối đe dọa và các lỗ hổng bảo mật phổ biến nhất mà người dùng không cần phải thực hiện thêm các bước để bảo mật chúng. Các sản phẩm bảo mật theo mặc định được thiết kế để khách hàng biết rõ rằng khi họ lệch khỏi các mặc định an toàn, thì họ đang làm tăng khả năng bị tấn công, trừ khi họ thực hiện các biện pháp kiểm soát bổ sung để đền bù vào. Bảo mật theo mặc định là một hình thức của bảo mật theo thiết kế.

- Một cấu hình an toàn nên là mốc điểm cơ sở mặc định. Các sản phẩm bảo mật theo mặc định tự động kích hoạt các biện pháp kiểm soát quan trọng cần thiết nhất để bảo vệ doanh nghiệp khỏi những kẻ tấn công mạng độc hại, cũng như cung cấp khả năng sử dụng và cấu hình thêm các biện pháp kiểm soát bảo mật mà không bị tính thêm lệ phí.
- Mức độ phức tạp của cấu hình bảo mật không nên là vấn đề của khách hàng. Các nhân viên IT (Công nghệ Thông tin) của các tổ chức thường xuyên bị quá tải với các trách nhiệm bảo mật và vận hành, do đó dẫn đến việc họ không có đủ thời gian để tìm hiểu và thực hiện các hành động an ninh và biện pháp giảm thiểu cần thiết để có một tình trạng an ninh mạng mạnh mẽ. Các nhà sản xuất có thể trợ giúp khách hàng của mình bằng cách tối ưu hóa cấu hình sản phẩm bảo mật – bảo mật "lộ trình mặc định" –bảo đảm là các sản phẩm của họ được sản xuất, phân phối và sử dụng an toàn tuân theo các tiêu chuẩn "bảo mật theo mặc định".

Các nhà sản xuất sản phẩm "bảo mật theo mặc định" không tính thêm lệ phí đối với việc cung cấp các cấu hình bảo mật bổ sung. Thay vào đó, họ bao gồm chúng trong sản phẩm cơ bản, giống như những dây an toàn ở ghế ngồi được bao gồm trong tất cả các chiếc xe hơi mới.

Bảo mật không phải là một tùy chọn xa xỉ, mà nên coi là quyền lợi mà mọi khách hàng đều nhận được mà không cần phải thương lượng hoặc trả thêm tiền.

CÁC KHUYẾN NGHỊ ĐỐI VỚI NHÀ SẢN XUẤT PHẦN MỀM

Hướng dẫn liên danh này đưa ra các khuyến nghị cho các nhà sản xuất để phát triển lộ trình bằng văn bản nhằm thực hiện và bảo đảm an ninh IT. Các tổ chức tác giả khuyến nghị các nhà sản xuất phần mềm thực hiện các chiến lược được nêu ra trong các phần dưới đây và đảm nhận trách nhiệm về kết quả an ninh của khách hàng nhờ nguyên tắc bảo mật theo thiết kế và bảo mật theo mặc định.

CÁC NGUYÊN TẮC BẢO MẬT SẢN PHẨM PHẦN MỀM

Các nhà sản xuất công nghệ được khuyến khích áp dụng một chiến lược ưu tiên về an toàn phần mềm. Các tổ chức tác giả đã soạn thảo ba nguyên tắc cốt lõi dưới đây để hướng dẫn các nhà sản xuất phần mềm tích hợp tính bảo mật của phần mềm vào quá trình thiết kế của họ trước khi đi đến giai đoạn phát triển, cấu hình và chuyển giao sản phẩm.

1 **Chịu trách nhiệm về kết quả bảo mật của khách hàng** và phát triển sản phẩm sao cho phù hợp. Gánh nặng bảo mật không nên chỉ đặt hoàn toàn vào khách hàng.

2 **Chấp nhận tính minh bạch và chịu trách nhiệm cấp tiến.**
Các nhà sản xuất phần mềm nên tự hào về việc cung cấp các sản phẩm an toàn và bảo mật, cũng như tạo sự khác biệt với phần còn lại của cộng đồng nhà sản xuất dựa trên khả năng của họ để làm điều đó. Việc này có thể bao gồm việc chia sẻ thông tin mà họ thu thập được từ quá trình triển khai của khách hàng, chẳng hạn như việc sử dụng các cơ chế xác thực mạnh theo mặc định. Điều này cũng bao gồm một cam kết mạnh mẽ để bảo đảm là các thông báo về lỗ hổng bảo mật và các hồ sơ lưu về lỗ hổng bảo mật và mức độ phơi nhiễm phổ biến (common vulnerability and exposure - CVE) có liên quan luôn đầy đủ và chính xác. Tuy nhiên, hãy cẩn trọng khi coi CVE là số liệu tiêu cực, vì những con số như vậy cũng là dấu hiệu của một cộng đồng kiểm chứng và phân tích mã lành mạnh.

3 **Xây dựng cơ cấu tổ chức và lãnh đạo để đạt được những mục tiêu này.**
Trong khi khả năng chuyên môn về kỹ thuật là điều quan trọng đối với tính bảo mật sản phẩm, nhưng trong các tổ chức, cấp lãnh đạo thâm niên là những người đưa ra quyết định chính về việc thực hiện các thay đổi trong một tổ chức. Cấp lãnh đạo cần ưu tiên bảo mật như một yếu tố quan trọng trong quá trình phát triển sản phẩm trong toàn tổ chức và trong quan hệ đối tác với khách hàng.

Để thực hiện ba nguyên tắc này, các nhà sản xuất nên xem xét một số chiến thuật hoạt động để cải thiện quá trình phát triển sản phẩm của họ.

Tổ chức các cuộc họp định kỳ với cấp lãnh đạo điều hành công ty để thúc đẩy tầm quan trọng của việc bảo mật theo thiết kế và bảo mật theo mặc định trong tổ chức của mình. Nên thành lập các chính sách và phương pháp tặng thưởng cho các nhóm sản xuất phát triển tạo được những sản phẩm tuân thủ các nguyên tắc này, có thể bao gồm việc trao giải thưởng cho việc thực hiện các phương pháp bảo mật phần mềm xuất sắc hoặc những khích lệ về các tiêu chuẩn thăng tiến và thăng chức.

Hoạt động xoay quanh tầm quan trọng của việc bảo mật phần mềm đối với sự thành công của doanh nghiệp. Ví dụ: hãy xem xét đến việc phân công một "người lãnh đạo về bảo mật phần mềm" hoặc một "nhóm về bảo mật phần mềm" có nhiệm vụ thực hiện các hoạt động kinh doanh và IT liên quan trực tiếp với các tiêu chuẩn về bảo mật phần mềm và tính trách nhiệm của nhà sản xuất. Các nhà sản xuất nên bảo đảm rằng họ có các chương trình thẩm định và đánh giá an ninh sản phẩm một cách độc lập và mạnh mẽ.

Sử dụng một mô hình mối đe dọa phù hợp trong suốt quá trình phân bổ nguồn lực và phát triển để ưu tiên các tính năng thiết yếu và có tác động cao nhất. Mô hình mối đe dọa xem xét từng trường hợp sử dụng cụ thể của sản phẩm nhằm giúp cho các nhóm phát triển củng cố sản phẩm. Cuối cùng, cấp lãnh đạo thâm niên nên buộc các nhóm phải chịu trách nhiệm đối với việc cung cấp các sản phẩm an toàn như một yếu tố then chốt của tính xuất sắc và phẩm chất cao của sản phẩm.

Một phần của bản cập nhật vào tháng 10 năm 2023 cho hướng dẫn này, ba nguyên tắc này được mở rộng qua các phần giải thích, minh họa và bằng chứng sau đây.

NGUYÊN TẮC 1: Đảm nhận Trách nhiệm về Kết quả An ninh của Khách hàng

GIẢI THÍCH

Các phương pháp tốt nhất hiện đại đòi hỏi các nhà sản xuất phần mềm đầu tư vào các nỗ lực bảo mật sản phẩm bao gồm **củng cố ứng dụng, các tính năng của ứng dụng** và ứng dụng **chế độ cài đặt mặc định.**

Các nhà sản xuất phần mềm cần thực hiện **củng cố ứng dụng** bằng cách sử dụng các quy trình và công nghệ nhằm làm tăng phí tổn cho những kẻ xâm nhập mạng độc hại muốn xâm phạm ứng dụng. Các giao thức và quy trình củng cố ứng dụng giúp sản phẩm chống chọi với các cuộc tấn công của những kẻ xâm nhập mạng độc hại xảo quyệt. Các thuật ngữ như "củng cố", "tính bảo mật của sản phẩm" và "khả năng thích ứng" đều liên quan chặt chẽ đến phẩm chất của sản phẩm. Ý tưởng là bảo mật phải là "vốn có" chứ không phải "gắn thêm vào." [1] Bằng cách bao gồm tính bảo mật, các nhà sản xuất phần mềm có thể không chỉ tăng cường bảo mật cho khách hàng mà còn nâng cao phẩm chất sản phẩm của họ. Các chiến thuật mẫu bao gồm bảo đảm đầu vào của người dùng được xác thực và không có lỗi và không được nhập trực tiếp vào mã nguồn (tức là bằng cách sử dụng các truy vấn được tham số hóa), sử dụng ngôn ngữ lập trình an toàn bộ nhớ, quản lý nghiêm ngặt vòng đời phát triển phần mềm (software development life cycle - SDLC) và sử dụng cách quản lý khóa mật mã được hỗ trợ bởi phần cứng.

Các ứng dụng cần hỗ trợ **các tính năng của ứng dụng** liên quan đến an ninh mạng. Đôi khi được gọi là "khả năng", những tính năng này mở rộng chức năng của sản phẩm hoặc dịch vụ theo cách giúp duy trì hoặc tăng cường tình trạng bảo mật của khách hàng. Các tính

năng mẫu liên quan đến an ninh bao gồm hỗ trợ bảo mật lớp vận chuyển (transport layer security – TLS) cho tất cả các kết nối mạng, hỗ trợ đăng nhập một lần (single sign on - SSO), hỗ trợ xác thực đa yếu tố (multi-factor authentication - MFA), nhật ký ghi chép kiểm tra sự kiện bảo mật, kiểm soát truy cập dựa trên vai trò (role-based access control - RBAC) và kiểm soát truy cập dựa trên đặc điểm (attribute-based access control - ABAC).

Một số tính năng này của sản phẩm có thể cấu hình được, cho phép khách hàng tích hợp sản phẩm dễ dàng hơn vào môi trường và quy trình làm việc hiện tại của họ. Những cấu hình đó có nghĩa là các ứng dụng phải có các **chế độ cài đặt mặc định** cho đến khi khách hàng cấu hình chúng. Những chế độ cài đặt mặc định đó cần được cài đặt một cách an toàn "ngay từ khi mở hộp" để khách hàng không phải tốn nhiều nguồn lực để làm cho các sản phẩm công nghệ của họ trở nên an toàn hơn.

Từng yếu tố này – củng cố ứng dụng, tính năng bảo mật của ứng dụng và các chế độ cài đặt mặc định của ứng dụng – đều đóng một vai trò trong tính bảo mật của ứng dụng và tình trạng bảo mật của khách hàng. Nhà sản xuất phần mềm nên suy nghĩ về từng yếu tố này và cách chúng liên quan với nhau. Các nhà sản xuất nên suy nghĩ không chỉ về việc đầu tư để kết hợp những yếu tố này vào sản phẩm của mình mà còn hơn thế nữa. Các nhà sản xuất nên tiến thêm bước nữa và xem xét xem những yếu tố đó làm thay đổi tình trạng bảo mật trong thế giới thực của khách hàng như thế nào, theo chiều hướng tốt hơn hay tồi tệ hơn.

Các nhà sản xuất nên đãm nhận trách nhiệm về kết quả bảo mật của khách hàng, hơn là chỉ đo lường bản thân dựa trên nỗ lực và đầu tư của mình. Trách nhiệm nên được đặt ở vị trí 'thượng nguồn' với các nhà sản xuất, nơi có nhiều khả năng nhất để giảm thiểu cơ hội bị xâm phạm.

Thật đáng tiếc, hiện giờ đang không phải là như vậy. Có quá nhiều nhà sản xuất đặt gánh nặng bảo mật lên khách hàng, hơn là đầu tư vào việc **củng cố ứng dụng toàn diện.** Ví dụ: khi nhà sản xuất vá một lỗ hổng bảo mật, chúng ta thường thấy các lỗ hổng bảo mật tương tự khác lộ ra, vì họ chỉ giải quyết được triệu chứng chứ không phải nguyên nhân gốc rễ của lỗi đó. Sản phẩm có thể thực hiện các biện pháp giảm thiểu khác trong các phần khác nhau của mã nguồn cho cùng một loại lỗ hổng bảo mật. Lấy một ví dụ, sau khi nhà sản xuất khắc phục một lỗ hổng bảo mật xác nhận đầu vào, các nhà nghiên cứu hoặc kẻ tấn công mạng phát hiện ra các đường mã không được làm cho hoàn hảo từ việc cải thiện xác nhận đầu vào. Nhà sản xuất áp dụng các bản vá cho từng lỗi một, hơn là đồng nhất mã nguồn để loại bỏ loại lỗ hổng bảo mật đó trên toàn bộ ứng dụng.

Các tính năng của ứng dụng có thể tạo ra cả lợi ích và rủi ro cho khách hàng. Các tính năng cho phép tích hợp với nhiều hệ thống và phiên bản bên ngoài có thể làm tăng đáng kể giá trị của sản phẩm. Tuy nhiên, việc hỗ trợ các tính năng mà không có kế hoạch ngừng sử dụng, chẳng hạn như giao thức mạng, có thể khiến khách hàng dễ bị tấn công nếu họ thiếu hiểu biết về những hệ lụy của việc liên tục sử dụng tính năng đó. Ví dụ: một số sản phẩm vẫn tiếp tục sử dụng các giao thức mạng có nguồn gốc từ những năm 1990 hoặc 2000 và hiện được biết là không an toàn. Có nhiều yếu tố có thể làm chậm tốc độ khách hàng nâng cấp và triển khai các biện pháp bảo mật hiện đại. Họ có thể sử dụng các sản phẩm tích hợp với phần còn lại của mạng lưới của tổ chức, nhưng thiếu các biện pháp bảo mật hiện đại, do đó gây cản trở việc hiện đại hóa của đội ngũ IT. Dẫu vậy, các nhà sản xuất phần mềm có thể tính đến những khuôn mẫu này vào quy trình lập kế hoạch của họ để khuyến khích khách hàng luôn cập nhật.

Chế độ cài đặt mặc định của ứng dụng là thêm một lĩnh vực nhiều rủi ro tiềm ẩn đối với khách hàng. Các nhà sản xuất thường chọn một số chế độ cài đặt mặc định nhất định, giúp khách hàng dễ dàng hơn trong việc sử dụng các tính năng ứng dụng mà họ muốn. Nhược điểm là phương pháp này làm tăng bề mặt tấn công cho những khách hàng có thể không cần một số tính năng và giao thức nhất định được kích hoạt mặc định. Ngoài ra, nhiều biện pháp kiểm soát bảo mật được tắt theo mặc định hoặc đòi hỏi khách hàng phải dành thời gian để cấu hình chế độ cài đặt của mình hầu tăng cường bảo mật. Lập mô hình mối đe dọa rõ ràng là một chiến thuật có thể giúp quyết định xem nên bật tính năng nào theo mặc định hoặc chế độ cài đặt nào cần được bảo mật theo mặc định. Một chiến thuật khác là nghiên cứu cách làm cho các tính năng trở nên dễ khám phá hơn cho quản trị viên.

Một số nhà sản xuất giao sản phẩm với các chế độ cài đặt mặc định mà có thể tạo ra rủi ro cho một số hoặc tất cả khách hàng của họ. Thay vì cài đặt các mặc định an toàn hơn, họ thường chọn tạo ra một **hướng dẫn tăng cường** mà khách hàng phải phải bỏ công của để thực hiện. Hướng dẫn tăng cường bị một số vấn đề thường gặp. Một số hướng dẫn tăng cường khó tìm thấy và không được hỗ trợ tốt. Một số khác rất phức tạp để thực hiện, đôi khi đòi hỏi phát triển phần mềm để viết mô-đun (là phần mở rộng của chương trình chính dành riêng cho một chức năng cụ thể) mở rộng. Vậy mà một số hướng dẫn tăng cường phức tạp lại cho rằng đọc giả có nhiều kinh nghiệm về an ninh mạng để hiểu cách thức theo đó các chế độ cài đặt khác nhau làm thay đổi bề mặt tấn công. Những người thực hành thiếu hiểu biết về cách thức hoạt động của kẻ tấn công có thể không thực hiện đúng hướng dẫn tăng cường, đặc biệt nếu các hướng dẫn không cho thấy rõ ràng về sự đánh đổi. Hơn nữa, không phải tất cả các hướng dẫn tăng cường đều được viết bởi các kỹ sư quen thuộc với chiến thuật và kinh tế của kẻ tấn công, khiến họ tạo ra các hướng dẫn tăng cường không hiệu quả ngay cả khi được thực hiện đúng. Hàng triệu khách hàng đang đảm nhận trách nhiệm củng cố nhiều phiên bản phần mềm hoặc hệ thống, thường là trong môi trường eo hẹp về nguồn lực. Việc dựa vào các hướng dẫn tăng cường đơn giản là không thể đo lường được.

Các chế độ cài đặt của ứng dụng phải được đánh giá liên tục xem chế độ đó là mặc định hay do khách hàng đặt dựa trên hiểu biết hiện tại của nhà sản xuất về bối cảnh mối đe dọa. Các ứng dụng phải được làm với các dấu chỉ rõ ràng về những rủi ro tiềm ẩn có thể do chế độ cài đặt đó và nên cho biết rõ về các dấu chỉ đó. Giống như một chiếc xe hơi hiện đại có tín hiệu báo về dây an toàn và thể hiện tín hiệu đó bằng cách phát ra âm thanh cảnh báo nếu quý vị cố lái xe mà không thắt dây an toàn, phần mềm nên hiển thị các tín hiệu về trạng thái an ninh của hệ thống. Nếu một ứng dụng được cấu hình để không cần MFA (Xác thực đa Yếu tố) cho các tài khoản quản trị viên, thì ứng dụng đó nên đều đặn thông báo cho quản trị viên biết rằng họ và toàn bộ tổ chức của họ đang nằm trong tình trạng nguy hiểm nếu họ không cấu hình MFA. Ngoài ra, nếu một ứng dụng được cấu hình để hỗ trợ các giao thức cũ hơn hiện được biết là thực hiện mã hóa yếu, thì ứng dụng đó nên đều đặn thông báo rõ ràng cho quản trị viên rằng tổ chức đang nằm trong tình trạng nguy hiểm và cung cấp nguồn lực để giải quyết tình huống này. Chúng tôi kêu gọi các nhà sản xuất thực hiện các nhắc nhở định kỳ được tích hợp trong sản phẩm, hơn là dựa vào quản trị viên để có thời gian, kiến thức chuyên môn và nhận thức để diễn giải các hướng dẫn tăng cường. Rõ ràng là có nhiều cơ hội cho sự đổi mới để quân bình giữa những cân nhắc về bảo mật và tính tiện lợi cho việc sử dụng.

Mỗi yếu tố trên tạo ra một tình huống không thể giải quyết được, trong đó khách hàng cần nghiên cứu, cấp vốn, mua sắm, sắp xếp nhân viên, triển khai và theo dõi các **sản phẩm bảo mật** bổ sung để giảm nguy cơ bị xâm phạm. Các tổ chức nhỏ và trung bình (Small and Medium Sized Organizations - SMO) thường không thể tạo điều kiện thuận lợi cho các lựa chọn này. Họ đối mặt với tình trạng khan hiếm về chuyên môn, tài chính và thời gian, tạo áp lực lên băng thông và chức năng, khiến bảo mật bị xếp xuống hàng thứ yếu và tổng thể, làm trầm trọng thêm rủi ro chung. Ngược lại, đầu tư vào an ninh của một số ít nhà sản xuất sẽ đo lường được. Một câu thành ngữ tóm tắt vấn đề này là, ngành công nghiệp phần mềm cần nhiều sản phẩm được bảo mật hơn, chứ không phải nhiều sản phẩm về bảo mật. Các nhà sản xuất phần mềm nên dẫn đầu sự chuyển đổi đó.

> ***Ngành công nghiệp phần mềm cần nhiều sản phẩm được bảo mật hơn, chứ không phải nhiều sản phẩm về bảo mật. Các nhà sản xuất phần mềm nên dẫn đầu sự chuyển đổi đó.***

Ngày nay, đôi khi chúng ta đọc thấy nhận xét từ các nhà sản xuất giải thích rằng, khách hàng đã bị xâm phạm là do họ không bật một tính năng bảo mật cụ thể hoặc không tuân theo hướng dẫn tăng cường cụ thể nào đó. Thay vào đó, sau một vụ xâm phạm, các nhà sản xuất nên giải thích liệu một tính năng bảo mật hoặc hướng dẫn tăng cường cụ thể nào đó lẽ ra đã ngăn chặn được vụ xâm phạm hay không và xem xét đến việc làm cho tính năng đó trở thành mặc định mà không tính lệ phí. Trong những trường hợp mà chính sản phẩm cũng không đủ cứng cáp trong giai đoạn thiết kế và triển khai, nhà sản xuất nên giải thích cách họ đang nỗ lực để loại bỏ loại lỗ hổng bảo mật đó khỏi dòng sản phẩm của mình.

Các nhà sản xuất phần mềm có trách nhiệm bảo đảm rằng sản phẩm của họ được thiết kế và phát triển với bảo mật là ưu tiên hàng đầu. Để đạt được mục tiêu đó, họ nên **đo lường một cách khách quan kết quả** từ những nỗ lực của mình trong lĩnh vực này. Chúng tôi yêu cầu các nhà sản xuất không chỉ tập trung vào nỗ lực nội bộ của họ, mà còn đo lường một cách khách quan và phúc trình đều đặn về kết quả cũng như tính hiệu quả của các nỗ lực và cấu hình bảo mật của sản phẩm, đồng thời thiết lập vòng phản hồi để tạo ra những thay đổi trong SDLC (Vòng đời Phát triển Phần mềm) để đưa đến những cải tiến về an toàn cho khách hàng mà có thể đo lường được và các sản phẩm an toàn hơn. Phúc trình nên bao gồm dữ liệu ẩn danh mà cộng đồng giới học thuật và nghiên cứu bảo mật có thể sử dụng để theo dõi các xu hướng cấp cao và đo lường tiến triển trên toàn hệ sinh thái.

CHỨNG MINH NGUYÊN TẮC NÀY

Các nhà sản xuất phần mềm và dịch vụ trực tuyến nên tìm cách chứng minh sự thành công trong việc thực hiện nguyên tắc này. Họ nên tìm cách cung cấp bằng chứng dưới dạng những tài liệu mà bên ngoài có thể kiểm chứng. Không có một sản phẩm đơn lẻ nào tự nó sẽ chứng minh rằng một nhà sản xuất đang thực hiện một chương trình bảo mật theo thiết kế mạnh mẽ, nhưng bằng cách cung cấp nhiều sản phẩm khác nhau, họ sẽ chứng minh cho thấy sự cam kết của mình đối với việc phát triển sản phẩm an toàn. Phương pháp này dựa trên tinh thần "cho thấy, hơn là kể."

Để chứng minh nguyên tắc này, những nhà sản xuất phần mềm nên xem xét các bước như trong danh sách sau đây. Các tổ chức tác giả nhận ra rằng, ít nhà sản xuất phần mềm sẽ có khả năng thực hiện ngay lập tức những phương pháp này và tạo ra các sản phẩm tương ứng từ khi bắt đầu hành trình bảo mật theo thiết kế của họ. Hơn nữa, nhà sản xuất phần mềm sẽ cần ưu tiên danh sách này tùy thuộc vào cách khách hàng triển khai sản phẩm trong thực tế để đạt được lợi ích bảo mật lớn nhất.

PHƯƠNG PHÁP BẢO MẬT THEO MẶC ĐỊNH

1. **Loại bỏ mật mã mặc định.** Mật mã mặc định tiếp tục được coi là nguyên nhân của nhiều cuộc tấn công hàng năm. Cam kết để loại bỏ vấn đề kinh niên này sẽ khiến những kẻ tấn công không dễ dàng truy cập được. Tương tự, các nhà sản xuất nên xem xét những biện pháp về mật mã nào nên được thực hiện, như độ dài tối thiểu của mật mã và không cho phép sử dụng lại những mật mã bị xâm phạm đã biết.

2. **Tiến hành kiểm tra thực tế.** Khi công nghệ tiếp tục phát triển và trở nên phức tạp hơn, điều quan trọng hơn đối với các nhà sản xuất phần mềm, là tiến hành kiểm tra người dùng tập trung vào bảo mật để hiểu rõ tình trạng bảo mật của sản phẩm của họ trên thực tế. Tương tự như cách các nghiên cứu người dùng cung cấp thông tin cho những đòi hỏi về phát triển phần mềm, nhà sản xuất phần mềm cũng nên tiến hành nghiên cứu người dùng, tập trung vào tính bảo mật để hiểu xem trải nghiệm của người dùng về tính bảo mật (user experience - UX) còn thiếu sót ở đâu. Qua quan sát cách thức khách hàng triển khai và sử dụng sản phẩm của mình trong môi trường thực, các nhà sản xuất phần mềm có thể thu lượm được sự hiểu biết quý giá về tính dễ sử dụng và hiệu quả của các tính năng và kiểm soát bảo mật của sản phẩm. Những hiểu biết sâu sắc này có thể giúp xác định các lĩnh vực cần cải thiện và vi chỉnh sản phẩm của mình để đáp ứng tốt hơn nhu cầu bảo mật của khách hàng. Ví dụ, các kiểm tra thực tế có thể gợi ý cho biết những thay đổi về luồng trải nghiệm người dùng (UX), giá trị mặc định, hệ thống cảnh báo và theo dõi. Các kiểm tra thực tế cũng có thể cho thấy những cải thiện trước đây trong thiết kế của sản phẩm làm giảm tốc độ của các bản vá bảo mật, giảm lỗi cấu hình và giảm thiểu bề mặt tấn công.

Các nhà sản xuất nên xem xét những điều sau đây:

- Khách hàng có thực hiện đúng hướng dẫn tăng cường không?
- Các tính năng bảo mật hiện có của sản phẩm, trên thực tế, có hoạt động như mong đợi không?
- Những tính năng đó có thực sự chống lại được các cuộc tấn công trong thế giới thực không?
- Các tính năng nào sẽ giúp làm giảm khả năng bị xâm phạm một cách hiệu quả hơn?

Ghi chú: Để có những hiểu biết sâu sắc hơn về các yếu tố này, các nhà sản xuất phần mềm có thể muốn hợp tác với khách hàng để tiến hành các bài tập của 'đội màu đỏ' để xem sản phẩm đối đầu như thế nào trước các cuộc tấn công. Những kiểm tra trên thực tế có thể diễn ra tại địa điểm của khách hàng, theo cách ảo hoặc qua dữ liệu từ ứng dụng theo dõi theo cách bảo đảm tính riêng tư.

3. **Giảm kích cỡ cho hướng dẫn tăng cường.** Các nhà sản xuất có thể cải thiện tình trạng bảo mật của khách hàng bằng cách đơn giản hóa hoặc thậm chí loại bỏ các hướng dẫn tăng cường sản phẩm và tập trung vào các biện pháp bảo mật quan trọng nhất mà khách hàng nên ưu tiên khi triển khai sản phẩm của mình. Thay vì khiến khách hàng choáng ngợp với một danh sách dài các biện pháp bảo mật, nhà sản xuất nên xác định các rủi ro bảo mật hàng đầu mà sản phẩm của họ dễ gặp phải và đưa ra hướng dẫn rõ ràng và ngắn gọn về cách giảm thiểu những rủi ro này. Ngoài ra, nhà sản xuất nên cung cấp cho khách hàng các công cụ và cơ chế tự động hóa giúp đơn giản hóa quá trình thực hiện các kiểm soát bảo mật, chẳng hạn như các tập lệnh có thể dễ dàng triển khai trong môi trường của họ. Các công cụ này nên có khả năng xác minh và hiển thị rõ ràng các thay đổi được thực hiện so với điểm cơ bản ban đầu. Bằng cách đơn giản hóa các hướng dẫn tăng cường và cung cấp cho khách hàng các công cụ dễ sử dụng

và tự động hóa, các nhà sản xuất có thể giảm bớt gánh nặng cho khách hàng và giúp bảo đảm rằng sản phẩm của họ được triển khai một cách an toàn. Một chiến thuật có thể là xem xét việc thực hiện nguyên tắc Pareto (Nguyên tắc Pareto mô tả 80% hậu quả đến từ 20% nguyên nhân, khẳng định mối quan hệ không bình đẳng giữa đầu vào và đầu ra) để giảm thiểu số bước cho các trường hợp sử dụng phổ biến (80%) và sau đó cung cấp hướng dẫn và công cụ theo ngữ cảnh cho các trường hợp ít phổ biến hơn (20%). Bằng cách này, các nhà sản xuất phần mềm sẽ làm cho những điều đơn giản thành đơn giản, và những điều khó khăn trở thành khả thi. Kiểm tra thực tế sẽ là một công cụ mạnh mẽ trong việc đo lường xem khách hàng phải mất bao lâu để khám phá, hiểu và thực hiện các hướng dẫn tăng cường. Các nhà sản xuất nên xem xét làm thế nào để sản phẩm có thể nhắc nhở quản trị viên thực hiện hành động ngay trong chính sản phẩm, hơn là dựa vào họ để thực hiện các công việc từ một hướng dẫn tăng cường.

4. **Chủ động ngăn cản việc sử dụng các tính năng cũ không an toàn.** Ưu tiên bảo mật qua đường dẫn nâng cấp rõ ràng, hơn là khả năng tương thích ngược. Công bố các bài đăng trên blog cho thấy việc áp dụng các tính năng và giao thức an toàn và thông báo về việc loại bỏ các tính năng không an toàn, có thể là từ nội trong chính sản phẩm. Một số lượng đáng kể khách hàng đã chứng minh rằng họ sẽ không cập nhật hệ thống của mình với mạng, danh tính và các tính năng bảo mật quan trọng hiện đại khác. Trong một số trường hợp, khách hàng lo ngại rằng các chức năng hiện tại có thể gặp trục trặc sau khi nâng cấp. Bằng cách làm cho việc nâng cấp trở nên dễ dàng nhất có thể, khách hàng có thể sẽ nâng cấp và nhận được các bản sửa lỗi bảo mật thường xuyên và nhanh chóng hơn. Các nhà sản xuất phần mềm nên tích cực thúc đẩy khách hàng theo các lộ trình nâng cấp để giảm rủi ro cho họ.

5. **Thực hiện cảnh báo nhằm thu hút sự chú ý.**
Tương tự như chuông báo thắt dây an toàn trong xe hơi liên tục kêu khi dây an toàn chưa được cài, các nhà sản xuất nên thực hiện cảnh báo kịp thời và lặp đi lặp lại khi người dùng hoặc quản trị viên đang ở trong tình trạng thực sự không an toàn, cảnh báo quản trị viên rằng họ đang sử dụng các giao thức đã lạc hậu trong môi trường của họ và gợi ý các lộ trình nâng cấp. Thực hiện cảnh báo kịp thời và lặp đi lặp lại khi người dùng, quản trị viên, hoặc cấu hình ứng dụng, đang trong trạng thái không an toàn. Thông báo rõ ràng về chế độ không an toàn cho quản trị viên một cách đều đặn. Một tính năng bổ sung có thể yêu cầu quản trị viên cấp cao thừa nhận việc thiếu MFA (Xác thực Đa Yếu tố) trên tài khoản của họ mỗi khi đăng nhập hoặc thậm chí tắt một số tính năng chính nào đó cho đến khi họ bật MFA. Vẫn còn có thể có những đổi mới để đạt được những mục tiêu này mà không tạo ra sự mệt mỏi do quá cảnh giác.

6. **Tạo mẫu cấu hình an toàn.**
Các mẫu này có thể thiết lập trước một số cấu hình nhất định vào các chế độ cài đặt an toàn dựa trên mức độ chấp nhận rủi ro của tổ chức. Mặc dù việc có các mẫu bảo mật ở mức độ thấp/trung bình/cao có thể là quá đơn giản, nhưng ví dụ đó minh họa số lượng chế độ cài đặt có thể được cập nhật để quản lý rủi ro cho tổ chức. Mẫu có thể được hỗ trợ bằng các hướng dẫn tăng cường về những rủi ro mà nhà sản xuất đã xác định.

CÁC PHƯƠNG PHÁP PHÁT TRIỂN SẢN PHẨM AN TOÀN

1. **Chứng minh bằng tài liệu về việc tuân thủ khuôn khổ SDLC (Vòng đời Phát triển Phần mềm) an toàn.** Các khuôn khổ SDLC bảo mật cung cấp các mục tiêu và ví dụ cho toàn bộ nhân sự, quy trình và công nghệ. Hãy xem xét đến việc công bố chi tiết về các biện pháp kiểm soát khuôn khổ SDLC bảo mật đã được thực hiện và mô tả các biện pháp kiểm soát thay thế đã được sử dụng. Trong lãnh thổ Hoa Kỳ, hãy xem xét đến việc sử dụng Khuôn khổ Phát triển Phần mềm An toàn (Secure Software Development Framework – SSDF) của NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia). Mặc dù không phải là danh mục kiểm tra, nhưng SSDF "mô tả một bộ các phương pháp căn bản đúng đắn để phát triển phần mềm an toàn."
2. **Chứng minh bằng Tài liệu các Mục tiêu Hiệu suất An ninh mạng (Cybersecurity Performance Goals - CPG) hoặc sự tuân thủ tương đương.** Khi một tổ chức chứng nhận rằng họ tuân thủ tiêu chuẩn Khuôn khổ Phát triển Phần mềm An toàn (SSDF) của NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia), họ đang khẳng định rằng SDLC (Vòng đời Phát triển Phần mềm) của họ dựa trên các phương pháp tốt nhất được hiểu rõ. Tuy nhiên, việc họ chỉ có SDLC mạnh mẽ là chưa đủ. Họ còn cần phải bảo vệ doanh nghiệp và môi trường phát triển của chính mình khỏi những kẻ xâm nhập mạng độc hại, những kẻ sẽ tìm cách thao túng tính bảo mật của sản phẩm trong khi nó vẫn đang trong quá trình phát triển. Đây không phải là loại tấn công trên lý thuyết, mà là chiến lược tấn công được thực hiện với những ảnh hưởng bất lợi đối với khách hàng và nói rộng ra là vấn đề an ninh quốc gia. Các tổ chức nên xem xét đến việc công bố thông tin chi tiết về việc tổ chức tuân thủ CPG (Mục tiêu Hiệu suất An ninh mạng) của CISA (Kiểm Toán viên Hệ thống Thông tin được Chứng nhận), Khuôn khổ An ninh Mạng (CSF) của NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia) hoặc các khuôn khổ chương trình an ninh mạng khác.
3. **Quản lý lỗ hổng bảo mật.** Một số nhà sản xuất có chương trình quản lý lỗ hổng bảo mật mà chỉ tập trung vào việc vá những lỗ hổng bảo mật được phát hiện trong nội bộ hoặc từ bên ngoài và hơn thế chút xíu. Các chương trình hoàn thiện hơn kết hợp phân tích sâu rộng về các lỗ hổng bảo mật và nguyên nhân gốc rễ của chúng dựa trên dữ liệu, thực hiện các bước để loại bỏ toàn bộ các loại lỗ hổng bảo mật một cách có hệ thống[3]. Họ thực hiện các chương trình chính thức xung quanh việc lập kế hoạch để bảo đảm phẩm chất, kiểm soát phẩm chất, cải tiến và đo lường phẩm chất. Họ xem việc quản lý khuyết điểm là một vấn đề kinh doanh, chứ không chỉ đơn thuần là vấn đề bảo mật. Các chương trình này không khác biệt nhiều so với các chương trình bảo đảm phẩm chất và an toàn trong các ngành công nghiệp khác.
4. **Sử dụng phần mềm mã nguồn mở rộng một cách có trách nhiệm.** Khi sử dụng phần mềm nguồn mở rộng, hãy có trách nhiệm bằng cách kiểm tra các gói mã nguồn mở, khuyến khích việc đóng góp mã trở lại các phần phụ thuộc và giúp duy trì sự phát triển cũng như bảo trì các thành phần quan trọng. Để tham khảo, Bộ Kinh tế, Thương mại và Công nghiệp (Ministry of Economy, Trade, and Industry - METI) Nhật Bản đã xuất bản "Bộ Sưu tập các Ví dụ về Trường hợp Sử dụng các Phương pháp Quản lý đối với việc Sử dụng OSS (Hệ thống Hỗ trợ Hoạt động) và Bảo đảm An ninh của Nó."
5. **Cung cấp các giá trị mặc định an toàn cho nhà phát triển.** Làm cho lộ trình mặc định trong quá trình phát triển phần mềm trở thành lộ trình an toàn bằng cách cung cấp các thành phần xây dựng an toàn cho nhà phát triển. Ví dụ, xét đến mức độ phổ biến của các lỗ hổng bảo mật SQL injection (SQL injection là một kỹ thuật mà kẻ tấn công sử dụng để truy cập trái phép vào cơ sở dữ liệu ứng dụng web bằng cách thêm một chuỗi mã độc vào truy vấn cơ sở dữ liệu) gây hại thực tế, hãy bảo đảm rằng nhà thiết kế sử dụng một thư viện được duy trì tốt để ngăn chặn loại lỗ hổng bảo mật đó. Còn được gọi là "đường trải nhựa" hoặc "đường được thắp sáng tốt", phương pháp này bảo đảm cả tốc độ lẫn an ninh, đồng thời giảm thiểu lỗi do con người gây ra.
6. **Tạo ra một lực lượng phát triển phần mềm hiểu biết về an ninh.** Để bảo đảm rằng các nhà phát triển phần mềm của quý vị hiểu về an ninh, bằng cách huấn luyện họ về các phương pháp viết mã bảo mật tốt nhất. Hơn nữa, giúp chuyển đổi lực lượng lao động rộng hơn bằng cách cập nhật các phương pháp tuyển dụng để đánh giá kiến thức về bảo mật và hợp tác với các trường đại học, cao đẳng cộng đồng, chương trình đào tạo và các nhà giáo dục khác để đưa bảo mật vào chương trình giảng dạy phát triển phần mềm và khoa học máy vi tính.

[3] NIST (Viện Tiêu chuẩn và Công nghệ Quốc gia) SSDF (Khuôn khổ Phát triển Phần mềm An toàn), PO 1.2, Ví dụ 2: "Xác định các chính sách có quy định rõ các yêu cầu về bảo mật cho phần mềm của tổ chức và xác minh sự tuân thủ tại các điểm chính trong SDLC (Vòng đời Phát triển Phần mềm) (ví dụ: các loại lỗi phần mềm được xác minh qua cổng, ứng phó với các lỗ hổng bảo mật được phát hiện trong phần mềm đã phát hành)."

7. **Kiểm tra quản lý sự kiện vấn đề an ninh (security incident event management - SIEM) và kết hợp phối hợp bảo mật, tự động hóa và ứng phó (security orchestration, automation, and response - SOAR).** Ngoài việc tiến hành kiểm tra trên môi trường thực tế, hãy hợp tác cùng với các nhà cung cấp SIEM và SOAR nổi tiếng, cùng với các khách hàng được chọn để hiểu cách các nhóm ứng phó với vấn đề sử dụng nhật ký ghi chép để điều tra các vấn đề bảo mật thực sự hoặc đáng ngờ. Rất ít nhà phát triển phần mềm có kinh nghiệm ứng phó với vấn đề và vì vậy họ có thể tạo các mục nhật ký ghi chép mà không giúp ích cho những chuyên gia ứng phó như họ kỳ vọng. Bằng cách làm việc với cả công nghệ SIEM và SOAR cũng như các chuyên gia ứng phó với vấn đề thực tế, nhóm phát triển có thể tạo nhật ký ghi chép để trình bày sự việc thật chính xác và đầy đủ, tiết kiệm thời gian và giảm bớt sự không chắc chắn khi xảy ra vấn đề.
8. **Phù hợp với Kiến trúc Không Tin cậy (Zero Trust Architecture - ZTA).** Làm cho các hướng dẫn triển khai sản phẩm phù hợp với, ví dụ như, mô hình NIST ZTA và Mô hình Khôn ngoan Không Tin cậy của CISA. Khuyến khích khách hàng kết hợp những nguyên tắc này vào môi trường của họ.

CÁC HOẠT ĐỘNG KINH DOANH CHỦ ĐỘNG VỀ AN NINH

1. **Cung cấp tính năng nhật ký ghi chép (logging) miễn phí.** Các dịch vụ đám mây nên cam kết tạo ra và lưu trữ các bản nhật ký liên quan đến bảo mật mà không phải trả thêm lệ phí. Tương tự, các sản phẩm được sử dụng tại cơ sở cũng nên tạo ra các bản nhật ký liên quan đến bảo mật miễn phí mà không tính thêm lệ phí. Hơn nữa, sản phẩm nên ghi lại các sự kiện bảo mật theo mặc định, vì nhiều khách hàng có thể không hiểu giá trị của việc này cho đến khi vấn đề đã xảy ra. Các chiến thuật này có thể đòi hỏi xem xét kỹ lưỡng về những sự kiện bảo mật nào nên được ghi vào nhật ký để cung cấp nhận thức về trạng thái an ninh mạng, cách khách hàng có thể cấu hình nhật ký, được lưu giữ trong thời gian bao lâu, cách bảo vệ tính toàn vẹn và lưu trữ của nhật ký cũng như cách phân tích nhật ký. Trong một số trường hợp, quá trình đánh giá có thể gợi ý nhu cầu tái cấu trúc kiến trúc quản lý nhật ký của ứng dụng, để có thể sử dụng nhằm thực hiện biện pháp khắc phục và có chi phí phù hợp với nhà sản xuất. Làm việc với các chuyên gia ứng phó vấn đề (incident response - IR) có thể làm tăng cơ hội nhật ký sẽ hữu ích cho các nhà điều tra tại hiện trường. Xem phần về SIEM (quản lý sự kiện vấn đề an ninh).

2. **Xóa bỏ các khoản thuế ẩn.** Công bố cam kết không bao giờ tính lệ phí đối với các tính năng bảo mật hoặc quyền riêng tư hoặc tính tích hợp. Ví dụ, trong phạm vi lớn hơn của quản lý danh tính và quyền truy cập (identity and access management - IAM), có các dịch vụ được gọi là dịch vụ đăng nhập một lần (single sign-on - SSO). Một số nhà sản xuất tính lệ phí nhiều hơn để kết nối hệ thống của họ với dịch vụ SSO (đôi khi được gọi là nhà cung cấp danh tính). "Thuế SSO" này có nghĩa là việc quản lý danh tính và quyền truy cập tốt nằm ngoài tầm với của nhiều SMO (Văn phòng Quản lý Dịch vụ), khiến họ không thể đạt được tư thế bảo mật mạnh mẽ. Một số dịch vụ tính lệ phí nhiều hơn để kích hoạt MFA (Xác thực đa Yếu tố) cho người dùng. **Không nên định giá bảo mật như hàng hóa xa xỉ , mà nên coi đó là quyền lợi của khách hàng.** Một số nhà sản xuất lập luận rằng, có rất ít khách hàng yêu cầu những tính năng này và phải tốn kém nhiều hơn để bảo trì chúng. Những lập luận này bỏ qua thực tế là rất ít khách hàng sẽ gọi để phàn nàn hoặc mặc cả, không phải tất cả khách hàng đều thực sự hiểu rõ lợi ích của những tính năng này và tất cả các tính năng đều tốn kém để được bảo trì. Tuy nhiên, chúng tôi không thấy nhiều nhà sản xuất tính lệ phí thêm cho tính sẵn có hoặc cho tính toàn vẹn của dữ liệu. Chi phí để hỗ trợ những thuộc tính quan trọng đó đã được tính sẵn vào giá cả mà tất cả khách hàng phải trả, giống như chi phí bao gồm dây an toàn, cột tay lái có thể gập lại và túi khí giúp cứu mạng sống trong các vụ tai nạn xe.

3. **Thúc đẩy các tiêu chuẩn mở rộng.** Thực hiện các tiêu chuẩn mở rộng, đặc biệt là về các giao thức nhận dạng và mạng thường gặp. Tránh các giao thức độc quyền khi mà các tiêu chuẩn mở rộng đang có sẵn.

4. **Cung cấp công cụ nâng cấp.** Nhiều khách hàng cảm thấy miễn cưỡng khi áp dụng phiên bản mới nhất của sản phẩm, bao gồm việc triển khai các tính năng mới và an toàn hơn như kết nối mạng an toàn. Các nhà sản xuất phần mềm có thể tăng cường sự chấp nhận của khách hàng đối với các bản nâng cấp mới bằng cách cung cấp các công cụ giúp giảm bớt sự không chắc chắn và rủi ro. Cung cấp giấy phép miễn phí để khách hàng kiểm tra các bản nâng cấp và bản vá trong môi trường kiểm tra như là một cách để khuyến khích khách hàng.

NGUYÊN TẮC 2: Chấp nhận Tính Minh bạch và Chịu Trách nhiệm Cấp tiến

GIẢI THÍCH

Các nhà sản xuất phần mềm nên tự hào về việc cung cấp các sản phẩm an toàn và bảo mật, cũng như tạo sự khác biệt với phần còn lại của cộng đồng nhà sản xuất dựa trên khả năng của họ để làm điều đó.

Hãy giải quyết mối quan ngại thường gặp về tính minh bạch. Khi những người thực hiện thảo luận về tính minh bạch cấp tiến, cuộc trò chuyện có xu hướng 'sa lầy' vào mối lo ngại rằng họ đang đưa ra "lộ trình cho những kẻ tấn công." Tuy nhiên, bằng chứng rõ ràng cho thấy rằng những kẻ tấn công đang hoạt động rất tốt mà không cần đến những lộ trình như vậy và những lo ngại này nên được đặt ở mức ưu tiên thấp hơn so với tính minh bạch vì nó mang lại nhiều lợi ích cho khách hàng trực tiếp, khách hàng gián tiếp, chuỗi cung ứng và toàn bộ ngành công nghiệp phần mềm.

Tính minh bạch giúp ngành công nghiệp này thành lập các quy ước—nói cách khác, thế nào là "tốt". Nó giúp những quy ước đó thay đổi theo thời gian để đáp ứng nhu cầu của khách hàng, những thay đổi về chiến thuật hoặc kinh tế của những kẻ gây hại đe dọa hoặc sự tiến triển công nghệ. Tính minh bạch giúp các nhà sản xuất có ít nguồn lực hơn học hỏi từ những nhà sản xuất có các nguồn lực dồi dào và có năng lực hơn. Các cuộc đối thoại về việc chia sẻ thông tin nên mở rộng ra ngoài các dấu chỉ báo mối đe dọa theo thời gian thực, để bao gồm các yếu tố dưới đây.

Tính minh bạch thúc ép các quyết định về bảo mật phải được đưa ra sớm trong quá trình phát triển và là hoạt động liên tục của các nhà lãnh đạo doanh nghiệp cũng như các kỹ sư và chuyên gia bảo mật. Tính minh bạch quy phần trách nhiệm vào sản phẩm.

Xin lưu ý về việc lựa chọn tính từ "cấp tiến" trước "minh bạch". Ngày nay, hiếm khi các nhà sản xuất phần mềm công bố thông tin chi tiết về cách họ phát triển và bảo trì phần mềm, cũng như cách họ hoàn thiện các chương trình bằng cách sử dụng dữ liệu qua thời gian. Trong ngành công nghiệp phần mềm, ít nhà sản xuất cung cấp hướng dẫn chi tiết về cách họ thiết kế phần mềm của họ. Có rất ít cơ hội để các nhà sản xuất phần mềm xem cách các tổ chức đồng nghiệp cấu trúc các chương trình SDLC (vòng đời phát triển phần mềm) của họ và cách những chương trình này tồn tại trong môi trường của khách hàng khi phải đối mặt với những kẻ tấn công thực sự. Ngành công nghiệp tập thể sẽ được hưởng lợi từ việc chia sẻ nhiều thông tin hơn về các chủ đề như: chiến lược đo lường chi phí của các lỗi bảo mật và loại bỏ các các loại lỗ hổng bảo mật. Do những thực hành phổ biến này, tất cả các nhà sản xuất phần mềm phải tự học cách giải quyết vấn đề bảo mật cho sản phẩm của họ. Có lẽ bằng cách không đánh thuế xa xỉ đối với các tính năng an ninh, do vậy, an toàn và bảo mật trở thành trung tâm của chi phí hơn là trung tâm của lợi nhuận và các công ty sẽ được hưởng lợi bằng cách giảm bớt gánh nặng nhờ sự hợp tác và tính minh bạch.

Chúng ta muốn tập trung vào các chiến lược có thể đẩy nhanh sự phát triển của ngành công nghiệp phần mềm. Chúng ta không thể chỉ thực hiện những cải tiến mang tính cơ hội và gia tăng từng bước một nữa. Nếu chúng ta muốn cùng nhau vượt qua các mối đe dọa do những kẽ gây hại đầy xảo quyệt và giỏi thích ứng gây ra, chúng ta phải chấp nhận mức độ minh bạch mà hôm nay có thể làm cho chúng ta cảm thấy khó chịu, nhưng điều đó sẽ thúc đẩy ngành công nghiệp tiến tới. Hiện nay có những nhà sản xuất đang áp dụng một số nguyên tắc bảo mật theo thiết kế này. Như ông William Gibson nói, "tương lai là đây rồi, chỉ là nó không được phân phối đồng đều mà thôi." **Sự minh bạch cấp tiến sẽ giúp phổ biến thông tin đó và mang lại lợi ích nhiều hơn cho những người 'bảo vệ nhà' so với những kẻ muốn hại chúng ta.**

Tính minh bạch có thể làm được nhiều việc hơn là chỉ thuần tuý giúp các tổ chức đồng nghiệp hoàn thiện SDLC (Vòng đời Phát triển Phần mềm) của họ. Các khách hàng và nhà đầu tư tương lai có thể tìm hiểu thêm về các khoản đầu tư và sự đánh đổi mà các nhà sản xuất đã thực hiện, cũng như tình trạng an toàn mà các khoản đầu tư đó đã tạo ra cho khách hàng. Những nhà sản xuất nào ủng hộ sự minh bạch cấp tiến sẽ cung cấp cho khách hàng thông tin để giúp họ đưa ra quyết định mua sắm không chỉ dựa trên giá cả và tính năng, mà còn dựa trên tính bảo mật.

Trong khi các tổ chức nỗ lực hết sức để bảo đảm chuỗi cung ứng và SDLC của họ, các công ty đã gặp phải tình trạng các quy trình xây dựng của họ bị xâm phạm trong thời gian gần đây. Việc thúc đẩy tính minh bạch cấp tiến sẽ đưa đến việc tiết lộ công khai về các cuộc tấn công, cũng như những cải tiến mà công ty đã thực hiện để ngăn chặn và phát hiện các cuộc tấn công trong tương lai. Hình thức chia sẻ thông tin đó sẽ giúp các tổ chức khác học hỏi mà không phải cùng chịu chung số phận.

CHỨNG MINH NGUYÊN TẮC NÀY

Để chứng minh nguyên tắc này, nhà sản xuất phần mềm nên thực hiện các bước sau:

CÁC PHƯƠNG PHÁP BẢO MẬT THEO MẶC ĐỊNH

1. **Công bố số liệu thống kê và xu hướng tổng hợp liên quan đến bảo mật.** Các chủ đề ví dụ bao gồm việc khách hàng và quản trị viên áp dụng MFA (Xác thực đa Yếu tố) cũng như việc sử dụng các giao thức cũ không an toàn.
2. **Công bố số liệu thống kê về bản vá.** Cho biết chi tiết có bao nhiêu phần trăm khách hàng sử dụng phiên bản mới nhất của sản phẩm và những gì quý vị đang làm để giúp việc cập nhật trở nên dễ dàng và đáng tin cậy hơn.
3. **Công bố dữ liệu về các đặc quyền chưa sử dụng.** Công bố thông tin tổng hợp về các quyền hạn quá mức trên toàn bộ cơ sở khách hàng của quý vị, cũng như các nhắc nhở và các thay đổi khác đối với sản phẩm mà quý vị đang thực hiện để giảm thiểu bề mặt tấn công của khách hàng. Những đặc quyền chưa được sử dụng này có thể là các dấu hiệu tốt cho các cảnh báo từ quản trị viên, chẳng hạn như chuông nhắc thắt dây an toàn.

PHƯƠNG PHÁP PHÁT TRIỂN SẢN PHẨM AN TOÀN

1. **Thành lập các biện pháp kiểm soát an ninh nội bộ.** Nhiều công ty đã nhận thấy nhiều lợi ích của việc chuyển dữ liệu của họ sang các nhà cung cấp dịch vụ đám mây. Giờ đây những nhà cung cấp dịch vụ đám mây đó trở thành mục tiêu của các kẻ tấn công. Các nhà cung cấp Phần mềm dưới dạng Dịch vụ (SaaS) phải công bố số liệu thống kê về các biện pháp kiểm soát nội bộ của họ. Ví dụ: nhà cung cấp SaaS nên công bố số liệu thống kê về việc triển khai nội bộ tính năng MFA (Xác thực đa Yếu tố) chống lừa đảo, như Xác thực Nhận dạng Nhanh Trực tuyến (Fast Identity Online - FIDO). Lý tưởng nhất là họ có thể nói rằng, không nhân viên nào có thể truy cập dữ liệu khách hàng hoặc các dữ liệu nhạy cảm khác mà không thông qua tính năng MFA xác thực chống lừa đảo.

2. **Công bố các mô hình mối đe dọa cấp cao.** Các sản phẩm được bảo mật theo thiết kế bắt đầu bằng các mô hình mối đe dọa bằng văn bản, mô tả những gì nhà tạo ra sản phẩm đang cố gắng bảo vệ và các mối đe doạ là từ đâu. Các mô hình mối đe dọa hiệu quả được xác định dựa trên cách thức các hành vi xâm nhập xảy ra trong môi trường thực tế và nên bao gồm cả môi trường doanh nghiệp và phát triển, cũng như cách các nhà sản xuất phần mềm dự định sử dụng nó trong môi trường của khách hàng.

3. **Công bố các bản tiết tự chứng nhận về SDLC (Vòng đời Phát triển Phần mềm) an toàn với đầy đủ chi tiết.** Các nhà sản xuất tuân theo NIST SSDF (Viện Tiêu chuẩn và Công nghệ - Khung Làm việc Phát triển Phần mềm An toàn) hoặc các khuôn khổ làm việc tương tự khác, đều đang tích cực nỗ lực hướng tới một vòng đời phát triển phần mềm hoàn thiện. Việc công bố bản tự chứng nhận về các biện pháp kiểm soát mà nhà sản xuất đã thực thi và áp dụng đối với sản phẩm nào, sẽ cho thấy cam kết về việc tuân thủ các phương pháp tốt nhất này và mang lại mức độ tin cậy ngày càng cao cho khách hàng của họ. Các chương trình chứng nhận khác bao gồm Phương thức cho Chuỗi Cung ứng Mạng của Do Thái chẳng hạn.

4. **Chấp nhận tính minh bạch về lỗ hổng bảo mật.** Công bố cam kết bảo đảm rằng các lỗ hổng bảo mật của sản phẩm được xác định sẽ được công bố dưới dạng mục CVE (Các Lỗ hổng Bảo mật và Phơi nhiễm Phổ biến) đầy đủ và chính xác. Điều đó đặc biệt đúng đối với lĩnh vực liệt kê điểm yếu Chung giúp xác định nguyên nhân gốc rễ của các lỗ hổng bảo mật. Cơ sở dữ liệu CVE công khai càng chính xác và đầy đủ thì ngành công nghiệp càng có thể theo dõi cách các sản phẩm trở nên an toàn hơn và loại lỗ hổng bảo mật nào phổ biến nhất. Tuy nhiên, hãy cẩn trọng khi coi CVE là số liệu tiêu cực, vì những con số như vậy cũng là dấu hiệu của một cộng đồng kiểm chứng và phân tích mã lành mạnh. Khi các nhà sản xuất thực hiện triết lý bảo mật theo thiết kế, có thể lúc ban đầu số lượng CVE thô của họ sẽ tăng lên do quá trình phát hiện và khắc phục toàn diện hơn các lỗ hổng bảo mật trong mã hiện có. Các nhà sản xuất nên công bố phân tích về các lỗ hổng bảo mật trong quá khứ, bao gồm bất kỳ mô hình và biện pháp nào đã được thực hiện để giải quyết toàn bộ loại lỗ hổng bảo mật đó. Ví dụ: nếu phần lớn CVE của công ty có liên quan đến tập lệnh chéo trang (cross-site scripting XSS), việc ghi lại phân tích nguyên nhân gốc rễ, ứng phó (chẳng hạn như chuyển sang các khuôn khổ mẫu về web ngăn chặn được XSS) và kết quả sẽ báo hiệu cho khách hàng rằng họ sẽ không trở thành nạn nhân của một loại loại lỗ hổng bảo mật mà các biện pháp giảm thiểu đã được hiểu rõ qua nhiều thập niên.

5. **Công bố Danh sách Vật liệu Phần mềm (Software Bills of Materials - SBOMs).** Các nhà sản xuất nên nắm quyền kiểm soát chuỗi cung ứng của mình. Các tổ chức nên xây dựng và duy trì SBOM [2] cho từng sản phẩm, yêu cầu dữ liệu từ nhà cung cấp của họ và cung cấp SBOM cho khách hàng và người dùng ở hạ nguồn. Việc này sẽ giúp thể hiện sự tỉ mỉ của họ trong việc hiểu rõ các thành phần họ sử dụng để tạo ra sản phẩm, khả năng ứng phó với những rủi ro mới được xác định và có thể giúp khách hàng hiểu cách ứng phó nếu một trong các mô-đun trong chuỗi cung ứng có lỗ hổng bảo mật mới được phát hiện. Để tham khảo, Bộ Kinh tế, Thương mại và Công nghiệp Nhật Bản (METI) đã xuất bản "Hướng dẫn Giới thiệu Danh sách Vật liệu Phần mềm (SBOM) về Quản lý Phần mềm" Tính minh bạch nên mở rộng đến firmware (là một dạng vi mã hoặc chương trình được cài vào các thiết bị phần cứng để giúp chúng hoạt động hiệu quả) chèn trong các thiết bị cũng như dữ liệu và mô hình được sử dụng trong trí tuệ nhân tạo AI/học máy (ML). Ngoài việc hỗ trợ các quyết định mua sắmvà khả năng vận hành, SBOM còn đóng một vai trò quan trọng trong hạ tầng cơ sở để phát hiện và ứng phó với các cuộc tấn công độc hại nhắm vào chuỗi cung ứng.

6. **Công bố chính sách tiết lộ lỗ hổng bảo mật.** Công bố một chính sách tiết lộ lỗ hổng bảo mật bao gồm (1) ủy quyền kiểm tra đối với tất cả các sản phẩm do nhà sản xuất cung cấp và các điều kiện cho các thử nghiệm đó, (2) được miễn trách nhiệm pháp lý cho các hành động thực hiện phù hợp với chính sách và (3) cho phép tiết lộ công khai các lỗ hổng bảo mật sau một khoảng thời gian đã ấn định. Các nhà sản xuất nên thực hiện việc phân tích nguyên nhân gốc rễ của các lỗ hổng bảo mật được phát hiện và ở mức độ khả thi cao nhất, thực hiện các biện pháp để loại bỏ toàn bộ các loại lỗ hổng bảo mật. Hãy xem Mẫu Chính sách Tiết lộ Lỗ hổng Bảo mật của CISA để tham khảo ngôn ngữ.

CÁC HOẠT ĐỘNG KINH DOANH CHỦ ĐỘNG VỀ AN NINH

1. **Công khai nêu tên một nhà tài trợ điều hành cấp cao ủng hộ triết lý "bảo mật theo thiết kế".** Trong nhiều tổ chức, vấn đề bảo mật (cũng như phẩm chất) được giao cho các nhóm kỹ thuật có khả năng hạn chế trong việc thực hiện các thay đổi về cấu trúc nhằm cải thiện đáng kể tính bảo mật của sản phẩm. Việc công khai chỉ định một giám đốc điều hành kinh doanh hàng đầu để giám sát chương trình bảo mật theo thiết kế sẽ biến tính bảo mật của sản phẩm thành mối quan tâm kinh doanh ở cấp cao nhất.

2. **Công bố lộ trình bảo mật theo thiết kế.** Các nhà sản xuất nên có văn bản cho những thay đổi được thực hiện đối với SDLC (Vòng đời Phát triển Phần mềm) của mình để cải thiện tính bảo mật cho khách hàng, bao gồm thông tin chi tiết về phúc trình kiểm tra thực tế, các biện pháp được thực hiện để loại bỏ toàn bộ loại lỗ hổng bảo mật và các mục khác được liệt kê trong các nguyên tắc khác. Như trong trường hợp của các nỗ lực nhằm cải thiện phẩm chất, các chương trình cải thiện an ninh cũng có giai đoạn lập kế hoạch, kiểm soát và cải thiện riêng biệt. Trên tinh thần thực hiện thay vì chỉ nói suông, việc công bố lộ trình và chi tiết của những giai đoạn này, sẽ tạo dựng sự tin tưởng rằng các sản phẩm được bảo mật theo thiết kế. Sau khi đạt được những tiến bộ đáng kể, các nhà sản xuất có thể trình bày chi tiết về những giai đoạn này trong các phúc trình về tính minh bạch. Hành động này không chỉ cho thấy sự cam kết với nguyên tắc bảo mật theo thiết kế mà còn có thể truyền nguồn cảm hứng cho các nhà sản xuất khác để áp dụng các chương trình tương tự bằng cách đưa ra bằng chứng hiện hữu.

3. **Công bố một lộ trình về an toàn bộ nhớ.** Các nhà sản xuất có thể thực hiện các bước để loại bỏ một trong những loại lỗ hổng bảo mật lớn nhất bằng cách di chuyển các sản phẩm hiện có và tạo dựng sản phẩm mới bằng cách sử dụng ngôn ngữ an toàn cho bộ nhớ. Mặc dù có thể không thực hiện được điều này cho mọi trường hợp, nhưng các nhà sản xuất có thể xem xét phát triển chương trình bao bọc ứng dụng (application wrappers) bằng ngôn ngữ an toàn cho bộ nhớ thay vì viết lại toàn bộ ứng dụng. Điều này cũng có thể bao gồm cách các nhà sản xuất cập nhật quy trình tuyển dụng, đào tạo, đánh giá mã và các quy trình nội bộ khác, cũng như các cách họ đang giúp cộng đồng nguồn mở rộng thực hiện những điều tương tự.

4. **Công bố kết quả.** Trong khi cập nhật SDLC (Vòng đời Phát triển Phần mềm) để thể hiện triết lý bảo mật theo thiết kế, các tổ chức sẽ đạt được những thành quả nhanh chóng, những thành quả đòi hỏi nhiều nguồn lực hơn và một số trở ngại bất ngờ. Bằng cách trình bày những thành công và trở ngại nội bộ, toàn bộ ngành công nghiệp có thể học hỏi từ những thành quả đó.

NGUYÊN TẮC 3: Lãnh đạo từ Trên xuống

GIẢI THÍCH

Mặc dù triết lý tổng quát được gọi là "bảo mật theo thiết kế", nhưng động cơ cho sự an toàn của khách hàng bắt đầu từ trước giai đoạn thiết kế sản phẩm. Động cơ bắt đầu với các mục tiêu kinh doanh, các mục tiêu tiềm ẩn và rõ ràng cũng như các thành quả mong muốn. Chỉ khi các nhà lãnh đạo cấp cao coi bảo mật là điều ưu tiên hàng đầu của kinh doanh, tạo ra các khích lệ nội bộ và thúc đẩy một 'văn hóa' toàn diện để biến bảo mật thành một yêu cầu trong thiết kế, thì họ mới đạt được những kết quả tốt nhất.

Mặc dù kiến thức chuyên môn về chủ đề kỹ thuật là điều rất quan trọng đối với bảo mật sản phẩm, nhưng đó không phải là vấn đề chỉ được giao hoàn toàn cho nhân viên kỹ thuật. Đó là ưu tiên kinh doanh phải được bắt đầu từ trên.

Một số người thắc mắc liệu một nhà sản xuất phần mềm có áp dụng hai nguyên tắc đầu tiên và tạo ra những sản phẩm có ý nghĩa hay không? Liệu nguyên tắc thứ ba có cần thiết không? Cách thức một công ty thành lập tầm nhìn, sứ mệnh, giá trị và văn hóa sẽ ảnh hưởng đến sản phẩm và những yếu tố đó có thành phần nặng nề ở phía trên. Chúng tôi thấy điều này ở các ngành công nghiệp khác đã có những cải thiện đáng kể về an toàn và phẩm chất. Chuyên gia nổi tiếng về phẩm chất J.M. Juran đã viết:

> ***Để đạt được sự lãnh đạo về phẩm chất đòi hỏi các nhà quản lý cấp cao phải đích thân phụ trách về quản lý phẩm chất. Ở những công ty đã đạt được lãnh đạo về phẩm chất, các nhà quản lý cấp cao đích thân hướng dẫn sáng kiến này. Tôi không biết về bất kỳ trường hợp ngoại lệ nào. [3]***

Chúng tôi tin rằng bảo mật là tiểu loại của phẩm chất sản phẩm. Khi bảo mật và phẩm chất trở thành những yếu tố không thể thiếu trong kinh doanh, hơn là chức năng kỹ thuật chỉ được giao hoàn toàn cho nhân viên kỹ thuật, thì các tổ chức sẽ có thể đáp ứng nhu cầu bảo mật của khách hàng một cách nhanh chóng và hiệu quả hơn. Hơn nữa, việc đầu tư các nguồn lực cần thiết để bảo đảm rằng bảo mật phần mềm là ưu tiên kinh doanh cốt lõi ngay từ đầu, nó sẽ giúp giảm bớt các chi phí dài hạn cho việc giải quyết các lỗi phần mềm và từ đó, hạ giảm các nguy cơ đến an ninh quốc gia.

Tương tự như cách các nhóm lãnh đạo đã thực hiện các chương trình trách nhiệm xã hội của doanh nghiệp (corporate social responsibility - CSR), càng ngày càng có nhiều sự nhận thức rằng, các hội đồng quản trị doanh nghiệp, bao gồm cả các nhà sản xuất phần mềm nên đóng một vai trò tích cực hơn trong việc hướng dẫn các chương trình an ninh mạng. Thuật ngữ trách nhiệm mạng của doanh nghiệp (corporate cyber responsibility - CCR) đôi khi được sử dụng để mô tả ý tưởng mới nổi này.

CHỨNG MINH NGUYÊN TẮC NÀY

Để chứng minh nguyên tắc này, các nhà sản xuất phần mềm nên thực hiện các bước sau đây:

1. **Bao gồm các chi tiết về chương trình bảo mật theo thiết kế trong các phúc trình tài chính của doanh nghiệp.** Nếu nhà sản xuất là một công ty giao dịch trên thị trường chứng khoán, thì hãy cho thêm một phần trong mỗi phúc trình hàng năm dành riêng cho nỗ lực bảo mật theo thiết kế. Thông thường, các phúc trình tài chính hàng năm của các công ty sản xuất xe hơi thường bao gồm các phần về an toàn cho người lái và hành khách, kể cả thông tin về các ủy ban an toàn và phẩm chất được tập trung hóa và phân bổ. Việc trình bày chi tiết chương trình bảo mật theo thiết kế trong phúc trình tài chính sẽ chứng minh rằng tổ chức đang liên kết kết quả bảo mật của khách hàng với kết quả tài chính của doanh nghiệp, chứ không chỉ đơn giản là áp dụng một thuật ngữ trong tài liệu tiếp thị vì nó đang thịnh hành.
2. **Phúc trình đều đặn với hội đồng quản trị của quý vị.** Giám đốc an ninh thông tin (Chief information security officer - CISO) phúc trình với hội đồng quản trị doanh nghiệp thường bao gồm thông tin về các chương trình bảo mật hiện tại và theo kế hoạch, các mối đe dọa, các vấn đề về bảo mật bị nghi ngờ và đã xác nhận, cũng như các cập nhật khác tập trung vào tư thế và tình trạng bảo mật của công ty. Ngoài việc nhận được thông tin về tư thế bảo mật của doanh nghiệp, hội đồng quản trị nên yêu cầu thông tin về bảo mật sản phẩm và tác động của nó đối với vấn đề bảo mật của khách hàng. Hội đồng quản trị không nên chỉ trông cậy vào CISO, mà chủ yếu trông cậy vào các thành viên khác trong ban quản trị công ty để hạ giảm rủi ro cho khách hàng.
3. **Trao quyền cho người điều hành chịu trách nhiệm về bảo mật theo thiết kế.** Có sự khác biệt đáng kể giữa một tổ chức trong đó các nhóm kỹ thuật có "sự chấp thuận của ban điều hành" và những tổ chức mà các lãnh đạo doanh nghiệp đích thân quản lý quy trình cải thiện bảo mật của khách hàng bằng cách sử dụng các quy trình kinh doanh tiêu chuẩn. Thuật ngữ "sự chấp thuận của ban điều hành"ngụ ý rằng ai đó phải 'chào bán' ý tưởng về một chương trình an toàn cho khách hàng, thay vì là mục tiêu kinh doanh ưu tiên nhất. Người điều hành này phải được trao quyền để tạo ảnh hưởng đến việc đầu tư vào sản phẩm nhằm đạt được kết quả về bảo mật cho khách hàng.
4. **Tạo ra các khích lệ nội bộ có ý nghĩa.** Trong khi cẩn thận để tránh tạo ra các khích lệ sai trái, hãy điều chỉnh hệ thống khen thưởng để cải thiện sự an toàn của khách hàng nhằm phù hợp với các hành vi và những kết quả có giá trị khác. Từ người điều hành chịu trách nhiệm về bảo mật theo thiết kế, đến quản lý sản phẩm, phát triển phần mềm, hỗ trợ, bán hàng, pháp lý và các tổ chức khác, hãy đưa các khích lệ về bảo mật của khách hàng vào việc tuyển dụng, thăng chức, lương, thưởng, lựa chọn cổ phiếu và các quy trình thường gặp khác vào quá trình điều hành doanh nghiệp. Ví dụ: khi đặt ra các tiêu chuẩn để thăng chức cho các nhà phát triển phần mềm, hãy bao gồm việc cân nhắc để cải thiện tính bảo mật của sản phẩm cùng với các tiêu chuẩn khác như, thời gian hoạt động, thành tích và cải thiện tính năng.
5. **Thành lập một hội đồng bảo mật theo thiết kế.** Trong một số ngành công nghiệp, các tổ chức thường thành lập một hội đồng trung ương về phẩm chất và 'cấy' các đại diện đảm trách về phẩm chất vào các bộ phận hoặc đơn vị kinh doanh chủ chốt. Bằng cách bao gồm cả thành viên của nhóm được tập trung hóa và nhóm được phân bổ, các nhóm này hoạt động để cải thiện phẩm chất theo các mục tiêu ưu tiên hàng đầu, đồng thời nhận được dữ liệu từ sâu bên trong tổ chức. Tương tự, một hội đồng bảo mật theo thiết kế sẽ cải thiện tính bảo mật theo các mục tiêu bảo mật theo thiết kế trong toàn bộ tổ chức.
6. **Thành lập và phát triển hội đồng khách hàng.** Nhiều nhà sản xuất phần mềm có hội đồng khách hàng bao gồm khách hàng từ các khu vực, ngành công nghiệp và thuộc các quy mô khác nhau. Các hội đồng này có thể cung cấp rất nhiều thông tin về những thành công và thử thách của khách hàng trong quá trình triển khai các sản phẩm của công ty. Sắp xếp chương trình nghị sự của hội đồng với các chủ đề riêng biệt nhằm giải quyết vấn đề an toàn của khách hàng, ngay cả khi vấn đề đó hiện không được những thành viên quan tâm cho lắm. Xem xét xem hội đồng khách hàng sẽ phúc trình với ai và làm cách nào để tận dụng khai thác các thành viên để hiểu rõ hơn về tính bảo mật của sản phẩm khi được triển khai. Ví dụ: hội đồng có thiên vị về mục đích tiếp thị và bán hàng hay quản lý sản phẩm không? Người điều hành chịu trách nhiệm về bảo mật theo thiết kế sẽ giúp định hướng những tương tác với khách hàng và nên liên kết những tương tác này với các yếu tố khác trong bài viết này, chẳng hạn như nghiên cứu trên thực tế.

CHIẾN THUẬT BẢO MẬT THEO THIẾT KẾ

Khuôn khổ Phát triển Phần mềm Bảo mật (Secure Software Development Framework - SSDF), còn được gọi là Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) SP 800-218, là một bộ chính của các cách phương pháp về phát triển phần mềm có mức độ bảo mật cao mà có thể được tích hợp vào mỗi giai đoạn của vòng đời phát triển phần mềm (SDLC). Việc tuân theo các cách phương pháp này có thể giúp các nhà sản xuất phần mềm trở nên hiệu quả hơn trong việc tìm kiếm và loại bỏ các lỗ hổng bảo mật trong phần mềm đã phát hành, giảm thiểu tác động có thể có của việc lợi dụng các lỗ hổng bảo mật và giải quyết được các nguyên nhân gốc rễ của lỗ hổng bảo mật nhằm ngăn chặn sự tái diễn trong tương lai.

Các tổ chức tác giả khuyến khích việc sử dụng các chiến thuật bảo mật theo thiết kế, bao gồm các nguyên tắc tham khảo các phương pháp SSDF. Các nhà sản xuất phần mềm nên soạn thảo một lộ trình bằng văn bản để áp dụng các phương pháp phát triển phần mềm bảo mật theo thiết kế trong toàn bộ danh mục sản phẩm của họ. Sau đây là danh sách minh họa không đầy đủ các phương pháp tốt nhất về lộ trình:

- **Ngôn ngữ lập trình an toàn bộ nhớ (SSDF PW.6.1).** Ưu tiên cho việc sử dụng các ngôn ngữ lập trình an toàn bộ nhớ những khi có thể. Các tổ chức tác giả thừa nhận rằng các biện pháp giảm nhẹ dành riêng cho bộ nhớ, có thể là các chiến thuật hữu ích ngắn hạn cho các cơ sở mã nguồn cũ. Các ví dụ bao gồm cải tiến ngôn ngữ C/C++, giảm thiểu phần cứng, ngẫu nhiên hóa bố cục không gian địa chỉ (address space layout randomization - ASLR), tính toàn vẹn của luồng điều khiển (control-flow integrity - CFI) và kiểm thử lỗ hổng qua phương pháp fuzzing. Tuy nhiên, ngày càng có nhiều sự đồng thuận rằng, việc áp dụng ngôn ngữ lập trình an toàn về bộ nhớ có thể loại bỏ loại khiếm khuyết này và các nhà sản xuất phần mềm nên nghiên cứu cách để áp dụng chúng. Một số ví dụ về ngôn ngữ an toàn bộ nhớ hiện đại bao gồm C#, Rust, Ruby, Java, Go và Swift. Đọc tờ thông tin về an toàn bộ nhớ của NSA để biết thêm chi tiết.
- **Nền tảng Phần cứng An toàn.** Tích hợp các tính năng kiến trúc tạo điều kiện cho việc bảo vệ bộ nhớ có độ tinh vi, chẳng hạn như các tính năng được mô tả trong Hướng dẫn RISC Nâng cao Khả năng Phần cứng (Capability Hardware Enhanced RISC Instructions - CHERI) có thể mở rộng Kiến trúc Tập lệnh (Instruction-Set Architectures - ISA) phần cứng thông thường, cũng như các tính năng khác như Mô-đun Nền tảng Đáng Tin cậy và Mô-đun Bảo mật Phần cứng. Để biết thêm thông tin, truy cập trang mạng CHERI của Đại học Cambridge.
- **Thành phần Phần mềm an toàn (SSDF PW 4.1).** Mua và bảo trì các thành phần của phần mềm được bảo mật tốt (ví dụ: thư viện phần mềm, một đơn vị mã tự chứa (Mô-đun), phần mềm nằm giữa các ứng dụng (middleware), khuôn khổ làm việc mạng (frameworks)) từ các nhà phát triển thương mại, mã nguồn mở rộng và các bên thứ ba khác đã được xác minh để bảo đảm tính an toàn về bảo mật trong các sản phẩm phần mềm cho người tiêu dùng.
- **Khuôn khổ mẫu mạng (SSDF PW.5.1).** Sử dụng khuôn khổ mẫu mạng thực hiện tự động thoát đầu vào của người dùng để tránh các cuộc tấn công mạng chẳng hạn như tập lệnh chéo trang.
- **Truy vấn có tham số hóa (SSDF PW 5.1).** Sử dụng các truy vấn được tham số hóa hơn là bao gồm đầu vào của người dùng trong các truy vấn, để tránh các cuộc tấn công mạng nhắm vào các cơ sở dữ liệu và ứng dụng mạng sử dụng ngôn ngữ SQL (SQL injection).
- **Kiểm tra an ninh ứng dụng tĩnh và động (Static and dynamic application security testing - SAST/DAST)** (SSDF PW.7.2, PW.8.2). Sử dụng các công cụ này để phân tích mã nguồn của sản phẩm và cách thức ứng dụng để phát hiện các phương pháp dễ gây lỗi. Các công cụ này giải quyết các vấn đề từ việc quản lý bộ nhớ không đúng cách đến các phương pháp tạo truy vấn cơ sở dữ liệu dễ gây lỗi (ví dụ: đầu vào người dùng không tránh được, dẫn đến tấn công SQL). Các công cụ SAST và DAST có thể được tích hợp vào quy trình phát triển phần mềm và chạy tự động như một phần của quá trình phát

triển phần mềm. Các công cụ SAST và DAST nên bổ sung cho các phương pháp kiểm tra khác, chẳng hạn như kiểm tra đơn vị và kiểm tra tích hợp để bảo đảm sản phẩm tuân thủ các yêu cầu bảo mật dự kiến. Khi phát hiện vấn đề, các nhà sản xuất nên thực hiện phân tích nguyên nhân gốc rễ để giải quyết các lỗ hổng bảo mật một cách có hệ thống.

- **Đánh giá mã nguồn** (SSDF PW.7.1, PW.7.2). Luôn nỗ lực để bảo đảm rằng mã nguồn đưa vào sản phẩm phải trải qua các cách kiểm tra phẩm chất chẳng hạn như đánh giá của đồng nghiệp là các nhà phát triển khác hoặc phương pháp "gieo lỗi."

- Danh sách Vật liệu Phần mềm (SBOM) (SSDF PS.3.2, PW.4.1). Kết hợp việc tạo SBOM[4] để cung cấp khả năng hiển thị trong bộ phần mềm được đưa vào sản phẩm.

- **Chương trình tiết lộ lỗ hổng bảo mật** (SSDF RV.1.3). Thành lập chương trình tiết lộ lỗ hổng bảo mật cho phép các nhà nghiên cứu bảo mật trình báo các lỗ hổng bảo mật và được miễn trách nhiệm pháp lý. Là một phần của việc này, các nhà cung cấp phải thành lập quy trình để xác định nguyên nhân gốc rễ của các lỗ hổng bảo mật được phát hiện. Quy trình này nên bao gồm việc xác định xem áp dụng bất kỳ phương pháp bảo mật theo thiết kế nào trong tài liệu này (hoặc các phương pháp tương tự khác) có thể ngăn chặn sự xuất hiện của lỗ hổng bảo mật hay không.

- **Tính hoàn chỉnh của CVE (Các Lỗ hổng và Phơi nhiễm Phổbiến).** Phải chắc chắn rằng các CVE được công bố bao gồm nguyên nhân gốc rễ hoặc mã lỗi phổ biến (common weakness enumeration - CWE) nhằm giúp cho việc phân tích toàn diện về các khuyết điểm thiết kế bảo mật phần mềm trên toàn ngành công nghiệp. Mặc dù việc bảo đảm rằng mỗi CVE đều chính xác và đầy đủ, có thể tốn thêm thời gian, nhưng nó cho phép các thực thể khác nhau phát hiện ra các xu hướng trong ngành công nghiệp mà có lợi cho tất cả các nhà sản xuất và khách hàng. Để biết thêm thông tin về cách quản lý lỗ hổng bảo mật, hãy xem Hướng dẫn Phân loại Lỗ hổng Bảo mật Dành riêng cho các Bên Liên quan (SSVC) của CISA.

- **Phòng thủ Sâu.** Thiết kế hạ tầng cơ sở sao cho việc vi phạm một bảo mật đơn lẻ không dẫn đến tình trạng đe dọa toàn bộ hệ thống Ví dụ, phải bảo đảm các đặc quyền dành cho người dùng được cung cấp trong phạm vi hẹp và danh sách kiểm soát truy cập được sử dụng có thể làm giảm tác động của tài khoản bị xâm phạm. Ngoài ra, sử dụng kỹ thuật phần mềm sandboxing để cô lập một một lỗ hổng bảo mật nhằm hạn chế sự xâm phạm của toàn bộ ứng dụng.

- **Đáp ứng các Mục tiêu Hiệu suất An ninh Mạng (Cybersecurity Performance Goals - CPG).** Thiết kế các sản phẩm đáp ứng các phương pháp bảo mật cơ bản. Các Mục tiêu Hiệu suất về An ninh Mạng của CISA phác thảo các biện pháp an ninh mạng cơ bản, nền tảng mà các tổ chức nên thực hiện. Ngoài ra, muốn biết thêm các cách để củng cố tư thế an ninh mạng của tổ chức của quý vị, hãy xem Khuôn khổ Đánh giá An ninh Mạng của Vương quốc Anh có các điểm tương đồng với các Mục tiêu Hiệu suất về An ninh Mạng (CPG) của CISA. Nếu một nhà sản xuất không đáp ứng CPG — chẳng hạn như không yêu cầu xác thực đa yếu tố chống lừa đảo đối với tất cả nhân viên—thì họ không thể được coi là đang cung cấp các sản phẩm bảo mật theo thiết kế.

Các cơ quan tổ chức nhận thấy rằng những thay đổi này là những bước chuyển đổi đáng kể đối với vị thế của một tổ chức. Do đó, việc đưa những thay đổi này vào nên được ưu tiên dựa trên mô hình mối đe dọa phù hợp, mức độ nghiêm trọng, độ phức tạp và tác động kinh doanh. Những phương pháp này có thể được áp dụng cho phần mềm mới và dần dần mở rộng để bao gồm các trường hợp sử dụng và sản phẩm khác. Trong một số trường hợp, mức độ nghiêm trọng và tình trạng rủi ro của một số sản phẩm nhất định có thể đòi hỏi một lịch trình được tăng tốc để áp dụng những phương pháp này. Trong các trường hợp khác, các phương pháp có thể được đưa vào một mã nguồn cũ và khắc phục theo thời gian.

[4] Một số tổ chức tác giả đang tìm kiếm các phương pháp thay thế để đạt được sự bảo đảm an ninh xung quanh chuỗi cung ứng phần mềm.

CÁC CHIẾN THUẬT BẢO MẬT THEO MẶC ĐỊNH

Ngoài việc áp dụng các phương pháp phát triển bảo mật theo thiết kế, các cơ quan tổ chức khuyến nghị các nhà sản xuất phần mềm nên ưu tiên cấu hình bảo mật theo mặc định trong sản phẩm của họ. Các nhà sản xuất nên cố gắng cập nhật sản phẩm để tuân thủ các phương pháp này khi chúng được khôi phục. Ví dụ:

- **Loại bỏ các mật mã mặc định.** Các sản phẩm không nên có sẵn các mật mã mặc định được chia sẻ rộng rãi. Để loại bỏ mật mã mặc định, các tổ chức tác giả khuyến nghị các sản phẩm yêu cầu quản trị viên phải đặt một mật mã mạnh trong quá trình cài đặt và cấu hình hoặc để sản phẩm được gởi đi kèm với một mật mã mạnh, duy nhất cho từng thiết bị.

- **Xác thực đa yếu tố (MFA) trở thành bắt buộc đối với người dùng có đặc quyền.** Chúng tôi quan sát thấy rằng việc triển khai của nhiều doanh nghiệp do các quản trị viên quản lý mà chưa bảo vệ tài khoản của họ bằng MFA (Xác thực Đa Yếu tố). Vì trên thực tế quản trị viên là mục tiêu có giá trị cao, các sản phẩm nên làm cho MFA trở thành tùy chọn mặc định thay vì tùy chọn tham gia. Hơn nữa, hệ thống nên đều đặn nhắc nhở quản trị viên đăng ký MFA cho tài khoản của họ cho đến khi họ đã kích hoạt nó thành công trên tài khoản đó. NCSC (Trung tâm An ninh mạng Quốc gia) của Hà Lan có các hướng dẫn tương đương với CISA, hãy truy cập Tờ Thông tin Hệ thống Xác thực đã được Phát triển và Hoàn thiện của họ để biết thêm chi tiết.

- **Đăng nhập một lần (SSO).** Các ứng dụng Công nghệ Thông tin (IT) nên thực hiện hỗ trợ đăng nhập một lần qua các tiêu chuẩn mở rộng hiện đại. Các ví dụ bao gồm Ngôn ngữ Đánh dấu Xác nhận Bảo mật (Security Assertion Markup Language - SAML) hoặc Kết nối OpenID (OpenID Connect - OIDC.) Năng lực này nên được cung cấp theo mặc định mà không phải mất thêm chi phí.

- **Đăng nhập An toàn.** Cung cấp nhật ký ghi chép kiểm toán phẩm chất cao cho khách hàng mà không tính thêm lệ phí hoặc cấu hình bổ sung. Nhật ký ghi chép kiểm toán rất quan trọng để phát hiện và tăng cường giải quyết các vấn đề bảo mật có thể xảy ra. Chúng cũng rất quan trọng trong quá trình điều tra một vấn đề an ninh đáng nghi ngờ hoặc đã được xác nhận. Xem xét các phương pháp tốt nhất chẳng hạn như cung cấp khả năng tích hợp dễ dàng với hệ thống quản lý sự kiện và thông tin bảo mật (security information and event management) với quyền truy cập giao diện lập trình ứng dụng (application programming interface - API) sử dụng thời gian quốc tế phối hợp (coordinated universal time - UTC), định dạng múi giờ tiêu chuẩn và các kỹ thuật tài liệu mạnh mẽ.

- **Hồ sơ Ủy quyền Phần mềm.** Các nhà cung cấp phần mềm nên đưa ra các khuyến nghị về các vai trò ủy quyền được phê duyệt và các trường hợp sử dụng được chỉ định của chúng. Các nhà sản xuất nên bao gồm một cảnh báo rõ ràng để thông báo cho khách hàng về rủi ro gia tăng nếu họ đi lệch khỏi hồ sơ ủy quyền được đề xuất. Ví dụ: Bác sĩ có thể xem tất cả hồ sơ bệnh nhân, nhưng người lập lịch hẹn khám chỉ có quyền truy cập vào một số thông tin nhất định cần thiết để lên lịch hẹn mà thôi.

- **Bảo mật Tiên tiến hơn khả năng tương thích ngược.** Quá nhiều tính năng cũ tương thích ngược với các phiên bản cũ được bao gồm và thường được cho phép trong các sản phẩm mặc dù điều này gây ra các rủi ro cho việc bảo mật sản phẩm. Hãy chọn ưu tiên bảo mật hơn là tương thích ngược, trao quyền các nhóm bảo mật để họ loại bỏ các tính năng không an toàn ngay cả khi việc loại bỏ này gây ra các sự thay đổi không tương thích.

- **Theo dõi và giảm kích cỡ của "hướng dẫn tăng cường bảo mật".** Giảm kích cỡ của "hướng dẫn tăng cường bảo mật" được bao gồm với các sản phẩm và nỗ lực để bảo đảm rằng kích cỡ giảm đi theo thời gian khi các phiên bản mới của phần mềm được phát hành. Tích hợp các thành phần của "hướng dẫn tăng cường bảo mật" như là cấu hình mặc định của sản phẩm. Các tổ chức tác giả nhận thấy rằng việc rút ngắn hướng dẫn tăng cường bảo mật là kết quả của mối

quan hệ đối tác liên tục với các khách hàng hiện có và bao gồm các nỗ lực của nhiều nhóm sản phẩm, kể cả trải nghiệm cuả người dùng (UX).

- **Xem xét các hậu quả qua trải nghiệm của người dùng đối với chế độ cài đặt bảo mật:** Mỗi chế độ cài đặt mới đều tăng gánh nặng nhận thức cho người dùng và nên được đánh giá kết hợp với lợi ích kinh doanh mà nó đem lại. Điều lý tưởng nhất là không có chế độ cài đặt nào cả; thay vào đó, chế độ cài đặt bảo mật nhất sẽ được tích hợp vào sản phẩm theo mặc định. Khi cấu hình là điều cần thiết, tùy chọn mặc định nên được bảo đảm an toàn rộng rãi đối với các mối đe dọa thường gặp.

Các tổ chức tác giả nhận thức rằng những thay đổi này có thể ảnh hưởng đến cách phần mềm được triển khai và sử dụng trong hoạt động. Do đó, ý kiến đóng góp của khách hàng là điều rất quan trọng trong việc cân nhắc giữa hoạt động và yếu tố bảo mật. Chúng tôi tin rằng soạn thảo các lộ trình bằng văn bản và thành lập sự hỗ trợ của ban điều hành dành ưu tiên cho những ý tưởng này cho các sản phẩm quan trọng nhất của tổ chức, là bước đầu tiên để chuyển hướng sang các phương pháp phát triển phần mềm an toàn. Mặc dù ý kiến của khách hàng rất quan trọng, chúng tôi đã quan sát thấy những trường hợp quan trọng khi khách hàng không sẵn lòng hoặc không thể áp dụng các tiêu chuẩn cải tiến, thường là các giao thức mạng. Điều quan trọng là nhà sản xuất nên đưa ra các khích lệ có ý nghĩa, để khách hàng luôn cập nhật và không để họ phải tiếp tục nằm trong tình trạng dễ tấn công một cách vô thời hạn.

HƯỚNG DẪN TĂNG CƯỜNG BẢO MẬT SO VỚI HƯỚNG DẪN NỚI LỎNG BẢO MẬT

Các hướng dẫn tăng cường bảo mật có thể là kết quả của việc thiếu các biện pháp kiểm soát bảo mật sản phẩm được tích hợp vào kiến trúc của sản phẩm từ khi bắt đầu phát triển. Hậu quả là các hướng dẫn tăng cường cũng có thể là lộ trình để các kẻ tấn công mạng độc hại xác định và khai thác các tính năng không an toàn. Điều thường thấy là nhiều tổ chức không biết về các hướng dẫn tăng cường, do đó họ để chế độ cài đặt cấu hình thiết bị của mình ở tình trạng không an toàn. Một mô hình đảo ngược được gọi là hướng dẫn nới lỏng nên thay thế các hướng dẫn tăng cường và giải thích những thay đổi nào người dùng nên thực hiện, đồng thời liệt kê các rủi ro liên quan đến hướng dẫn nới lỏng đó. Những hướng dẫn này nên được viết bởi các chuyên gia an ninh, những người có thể giải thích các sự đánh đổi một cách rõ ràng bằng ngôn ngữ dễ hiểu, nhằm tăng cơ hội chúng được áp dụng đúng đắn.

Thay vì phát triển các hướng dẫn tăng cường bảo mật và liệt kê các phương pháp để bảo vệ sản phẩm, các tổ chức tác giả khuyến khích các nhà sản xuất phần mềm chuyển sang phương pháp bảo mật theo mặc định và cung cấp các "hướng dẫn nới lỏng." Những hướng dẫn này giải thích các rủi ro kinh doanh của các quyết định bằng ngôn ngữ đơn giản, dễ hiểu và có thể nâng cao nhận thức của tổ chức về rủi ro đối với các cuộc xâm nhập mạng độc hại. Sự đánh đổi về bảo mật nên được xác định bởi các giám đốc điều hành cao cấp của khách hàng, cân bằng giữa bảo mật với các đòi hỏi kinh doanh khác.

KHUYẾN NGHỊ CHO KHÁCH HÀNG

Các tổ chức tác giả khuyến nghị các tổ chức buộc các nhà sản xuất cung cấp phần mềm của họ phải chịu trách nhiệm về kết quả bảo mật cho sản phẩm của họ. Một phần của việc này là các tổ chức tác giả khuyến nghị rằng các giám đốc điều hành ưu tiên cho tầm quan trọng của việc mua sắm các sản phẩm bảo mật theo thiết kế và bảo mật theo mặc định. Điều này có thể thể hiện qua việc thành lập các chính sách đòi hỏi bộ phận IT đánh giá tính bảo mật của phần mềm trước khi mua sắm, cũng như cho phép bộ phận công nghệ thông tin từ chối nếu cần thiết. Bộ phận IT nên được trao quyền để soạn thảo các tiêu chuẩn mua hàng nhằm nhấn mạnh tầm quan trọng của các phương pháp bảo mật theo thiết kế và bảo mật theo mặc định (cả hai phương pháp được nêu ra trong tài liệu này và các phương pháp khác do tổ chức phát triển). Hơn nữa, bộ phận IT cần được ban quản lý điều hành hỗ trợ khi thực thi các tiêu chuẩn này trong các quyết định mua sắm. Các quyết định của tổ chức về việc chấp nhận các rủi ro liên quan đến các sản phẩm công nghệ cụ thể nào đó, phải được ghi chép chính thức thành văn bản, được giám đốc điều hành kinh doanh cao cấp phê duyệt và trình bày đều đặn trước hội đồng quản trị.

Các dịch vụ IT cốt lõi hỗ trợ tư thế bảo mật của tổ chức chẳng hạn như mạng lưới doanh nghiệp, danh tính doanh nghiệp và quản lý truy cập, cũng như các hoạt động bảo mật và khả năng ứng phó, nên được coi là các chức năng kinh doanh quan trọng và được tài trợ để phù hợp với tầm quan trọng của chúng đối với sự thành công trong sứ mệnh của tổ chức. Các tổ chức nên xây dựng kế hoạch nâng cấp các năng lực này để tận dụng các nhà sản xuất có xu hướng áp dụng các phương pháp bảo mật theo thiết kế và bảo mật theo mặc định.

Những khi có thể, các tổ chức nên cố gắng tạo dựng mối quan hệ đối tác chiến lược với các nhà cung cấp IT chính của họ. Những mối quan hệ này bao gồm sự tin tưởng ở nhiều tầng của tổ chức và cung cấp các phương tiện để giải quyết vấn đề và xác định các ưu tiên chung. Bảo mật nên là một yếu tố quan trọng của các mối quan hệ như vậy, và các tổ chức nên nỗ lực để củng cố tầm quan trọng của các cách phương pháp bảo mật theo thiết kế và bảo mật theo mặc định trong cả khía cạnh chính thức (ví dụ: hợp đồng hoặc thỏa thuận với nhà cung cấp) và khía cạnh không chính thức của mối quan hệ đó. Các tổ chức nên kỳ vọng sự minh bạch từ các nhà cung cấp công nghệ của họ về tình hình kiểm soát nội bộ cũng như lộ trình hướng tới việc áp dụng các phương pháp bảo mật theo thiết kế và bảo mật theo mặc định.

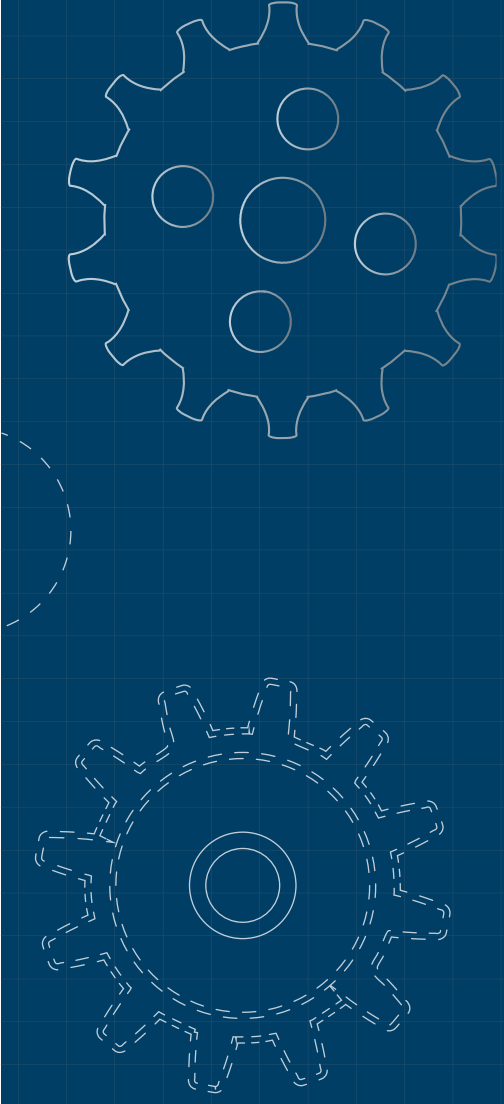
Ngoài việc đưa phương pháp bảo mật theo mặc định lên hàng ưu tiên trong tổ chức, các nhà lãnh đạo IT cũng nên hợp tác với các đồng nghiệp trong ngành để hiểu xem các sản phẩm và dịch vụ nào thể hiện với các nguyên tắc thiết kế này. Những nhà lãnh đạo này nên phối hợp các yêu cầu của họ để giúp các nhà sản xuất ưu tiên cho các sáng kiến bảo mật sắp tới của họ. Bằng cách cùng nhau làm việc, khách hàng có thể giúp đưa ra các ý kiến đóng góp có ý nghĩa cho nhà sản xuất và tạo khích lệ để họ ưu tiên các tính năng bảo mật.

Khi tận dụng các hệ thống đám mây, các tổ chức nên chắc chắn rằng họ hiểu về mô hình chịu trách nhiệm chung với nhà cung cấp công nghệ của mình. Điều này có nghĩa là tổ chức nên nắm rõ về trách nhiệm an ninh của nhà cung cấp, thay vì chỉ là trách nhiệm của khách hàng.

Tổ chức nên ưu tiên cho những nhà cung cấp đám mây nào minh bạch về tư thế bảo mật, kiểm soát nội bộ và khả năng của họ trong việc thực hiện đúng các bổn phận của mình theo mô hình chịu trách nhiệm chung.

TUYÊN BỐ MIỄN TRỪ TRÁCH NHIỆM

Thông tin trong phúc trình này được cung cấp “như đã trình bày” chỉ dành cho mục đích tham khảo mà thôi . CISA và các cơ quan tác giả không bảo trợ cho bất kỳ sản phẩm hoặc dịch vụ thương mại nào, bao gồm bất kỳ chủ đề nào được phân tích. Bất kỳ sự đề cập nào đến các tổ chức thương mại hoặc các sản phẩm, quy trình, hoặc dịch vụ thương mại bằng dịch vụ thương hiệu, thương hiệu, nhà sản xuất cụ thể nào hoặc khác đi, không đại diện hoặc ngụ ý ủng hộ, khuyến nghị, hoặc thiên vị bởi CISA và các tổ chức tác giả. Tài liệu này là một sáng kiến liên danh bởi CISA và không tự động trở thành tài liệu quy định.



Nguồn lực

CISA

- Hướng dẫn SBOM của CISA
- Mục tiêu Hiệu suất An ninh Mạng Chéo ngành của CISA
- Hướng dẫn về Tương tác Công nghệ
- Phòng thủ của CISA và NIST Chống lại các cuộc Tấn công Chuỗi Cung ứng Phần mềm
- Phí tổn của Công nghệ Không An toàn và Chúng ta Có thể Làm Gì về Điều đó| CISA
- Hãy Ngừng Đổ lỗi Trách nhiệm về việc Bảo mật Mạng: Tại sao các Công ty Phải Thiết kế tính An toàn cho các Sản phẩm Công nghệ (foreignaffairs.com)
- Hướng dẫn của CISA về Phân loại Lỗ hổng Bảo mật dành Riêng cho Các bên Liên quan (SSVC)
- Tờ Thông tin của CISA về MFA Chống Lừa đảo
- Hướng dẫn về An ninh Mạng cho các Doanh nghiệp Nhỏ | CISA

NSA

- Tờ Thông tin An ninh Mạng về An toàn Bộ nhớ của NSA
- ESF của NSA Bảo vệ Chuỗi Cung ứng Phần mềm: Các Phương pháp Tốt nhất cho các nhà Cung cấp

FBI

- Hiểu và Ứng phó với Cuộc Tấn Công Chuỗi Cung Ứng nguồn Năng lượng Gió: Quan Điểm của Liên Bang Mỹ
- Mối Đe dọa Mạng - Ứng phó và Trình báo
- Chiến lược An ninh Mạng của FBI

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST)

- Hướng dẫn Nhận dạng Kỹ thuật số của NIST
- Khuôn khổ Hướng dẫn An ninh Mạng của NIST
- Khuôn khổ về Phát triển Phần mềm An toàn của NIST (SSDF)

Trung tâm An ninh Mạng Úc (ACSC)

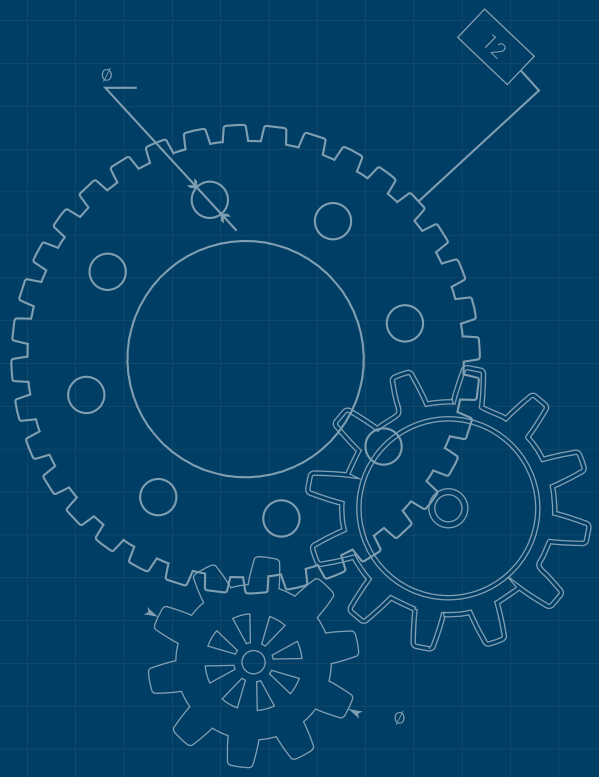
- Hướng dẫn của ACSC về Quy tắc Thực hành IoT dành cho các Nhà Sản xuất

Trung tâm An ninh Mạng Quốc gia của Vương quốc Anh (UK)

- Khuôn khổ Đánh giá An ninh Mạng của Vương quốc Anh
- Hướng dẫn Triển khai và Phát triển An toàn của NCSC Vương quốc Anh
- Hướng dẫn Quản lý Lỗ hổng Bảo mật của NCSC Vương quốc Anh
- Bộ Công cụ Tiết lộ Lỗ hổng Bảo mật của NCSC Vương quốc Anh
- CHERI của Đại học Cambridge
- Hẹn gặp lại và cám ơn quý vị đã cung cấp thông tin - NCSC.GOV.UK

Trung tâm An ninh Mạng Gia Nã Đại (CCCS)

- Hướng dẫn của CCCS về Bảo vệ Chống lại các cuộc Tấn công Chuỗi Cung ứng Phần mềm
- Chuỗi cung ứng mạng Phương pháp đánh giá các rủi ro
- Hướng dẫn về mã độc tống tiền CONTI của Trung tâm An ninh Mạng Gia Nã Đại



Văn phòng Liên bang Đức về An ninh Thông tin (BSI)

- » Bản tóm tắt tài liệu BSI Grundschutz (mô-đun CON.8)
- » Tiêu chuẩn quốc tế IEC 62443, phần 4-1
- » Trình Báo Tình trạng An ninh IT tại Đức, năm 2022
- » Phương pháp BSI về bảo mật ứng dụng mạng

Trung tâm An ninh Mạng Quốc gia Hà Lan

- » Tờ Thông tin Hệ thống Xác minh đã được Phát triển và Hoàn thiện của Trung tâm An ninh Mạng Quốc gia Hà Lan

Trung tâm Quốc gia về Tình trạng Sẵn sàng và Chiến lược cho An ninh Mạng Nhật Bản (NISC)

- » Chiến lược An ninh Mạng Quốc gia Nhật Bản

Bộ Kinh tế, Thương mại và Công nghiệp Nhật Bản (METI)

- » Hướng dẫn Giới thiệu Danh sách Vật liệu Phần mềm (SBOM) cho Quản lý Phần mềm
- » Bộ Sưu tập các Ví dụ về Trường hợp Sử dụng các Phương pháp Quản lý đối với việc Sử dụng OSS (Hệ thống Hỗ trợ Hoạt động) và Bảo đảm An ninh của Nó

Cơ quan An ninh Mạng Tân Gia Ba

- » Cố vấn Kỹ thuật về Phát triển Bảo mật API
- » Chính sách Tiết lộ Lỗ hổng Bảo mật CSA SingCERT
- » Danh mục Kiểm tra Ứng phó Vấn đề của CSA SingCERT
- » Sách Hướng dẫn Ứng phó Vấn đề của CSA SingCERT
- » Khuôn khổ Bảo mật theo Thiết kế của CSA
- » Danh mục Kiểm tra Khuôn khổ Bảo mật theo Thiết kế của CSA
- » Hướng dẫn của CSA về Mô hình Mối đe dọa Mạng
- » Chương trình Dán nhãn An toàn Mạng của CSA

Các nguồn lực khác

- » Làm thế nào mà các Hệ thống Phức tạp bị Lỗi
- » Giao diện Mới trong lỗi của hệ thống phức tạp

TÀI LIỆU THAM KHẢO

[1] https://csrc.nist.rip/publications/history/ande72.pdf

[2] https://www.cisa.gov/sbom và tài liệu tham khảo SBOM trong TR 03183-2 https://www.bsi.bund.de/dok/TR-03183

[3] Juran viết về Phẩm chất theo Thiết kế của J.M. Juran, 1992.