Thay đổi Cán cân Rủi ro An ninh Mạng: Các Nguyên tắc và Phương pháp Tiếp cận Bảo mật theo Thiết kế và Mặc định

Xuất bản: ngày 13 tháng 4 năm 2023

Cơ quan An ninh Mạng và Hạ tầng Cơ sở

NSA | FBI | ACSC | NCSC-UK | CCCS | BSI | NCSC-NL | CERT NZ | NCSC-NZ

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. Các hệ thống sử dụng mạng internet được kết nối 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 quản lý danh tính cá nhân đến chăm sóc y tế. Lấy một ví dụ, các cuộc tấn công mạng đã dẫn đến việc bệnh viện phải hủy bỏ các ca phẫu thuật và chuyển hướng chăm sóc bệnh nhân trên toàn cầu. Công nghệ không an toàn và các lỗ hổng trong các hệ thống quan trọng có thể là 'mồi nhử' cho các cuộc xâm nhập mạng độc hại, dẫn đến những rủi ro an ninh[1] tiềm ẩn nghiêm trọng.

Hiện nay, hơn bao giờ hết, các nhà sản xuất công nghệ phải đặt trọng tâm cho tính Bảo mật theo Thiết kế và Bảo mật theo Mặc định trong quá trình thiết kế và phát triển sản phẩm. Một số nhà cung cấp đã có những tiến bộ đáng kể trong việc thúc đẩy ngành công nghiệp trong việc bảo đảm phần mềm, trong khi một số khác lại đang chậm lại phía sau. Các cơ quan tác giả mạnh mẽ khuyến khích các nhà sản xuất công nghệ nên thiết kế sản phẩm của mình một cách thật an toàn, để khách hàng không cần phải liên tục thực hiện việc giám sát, cập nhật định kỳ và kiểm soát thiệt hại trên hệ thống của họ để giảm thiểu các cuộc xâm nhập mạng. Các nhà sản xuất được khuyến khích đảm nhận trách nhiệm cải thiện kết quả an ninh cho khách hàng của họ. Trong quá khứ, các nhà sản xuất công nghệ đã phụ thuộc vào việc sửa các lỗ hổng được tìm thấy sau khi khách hàng triển khai sản phẩm, đòi hỏi khách hàng phải tốn công sức, thời gian 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 và cài đặt các bản vá.

Để đạt được các tiêu chuẩn cao cho an ninh phần mềm, các cơ quan tác giả khuyến khích các nhà sản xuất nên ưu tiên tích hợp an ninh 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 làm việc mới, trong đó vấn đề an ninh 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 an ninh sản phẩm trong Đạo luật Khả năng Thích ứng Mạng (Cyber-Resilience-Act), nhấn mạnh rằng các nhà sản xuất nên triển khai an ninh trong suốt vòng đời 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 cho công nghệ và các sản phẩm liên quan an toàn hơn cho khách hàng, các cơ quan tác giả thúc đẩy các nhà sản xuất cải tiến 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 (Secure-by-Design and Secure-by-Default) được chuyển giao đến khách hàng. Các sản phẩm Bảo mật theo Thiết kế là những sản phẩm mà sự an toàn của khách hàng là mục tiêu kinh doanh chính, không chỉ là một tính năng kỹ thuật. Các sản phẩm Bảo mật theo Thiết kế được bắt nguồn với mục tiêu đó trước khi giai đoạn phát triển bắt đầu. 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 chi phí. Hai nguyên tắc này cùng nhau giúp chuyển phần lớn gánh nặng bảo mật đến nhà sản xuất, đồng thời giảm thiểu tỷ lệ khách hàng trở

[1] Các cơ quan tác giả nhận thấy rằng thuật ngữ "an toàn" có nhiều ý nghĩa khác nhau tùy thuộc vào ngữ cảnh sử dụng. Đối với mục đích của hướng dẫn này, "an toàn" sẽ đề cập đến việc nâng cao tiêu chuẩn an ninh công nghệ để bảo vệ khách hàng khỏi các hoạt động tấn công mạng độc hại.

thành nạn nhân của các vụ vi phạm an ninh mạng do cấu hình sai, hay quá chậm trong việc cập nhật bản vá hoặc nhiều vấn đề thông thường khác.

Cơ quan An ninh Mạng và An ninh Hạ tầng Cơ sở (CISA), Cơ quan Tình báo Quốc gia (NSA), Cục Điều tra Liên bang (FBI) cùng với các đối tác quốc tế[2] sau đây đưa ra các khuyến nghị trong hướng dẫn này như một lộ trình cho các nhà sản xuất công nghệ nhằm bảo đảm an ninh cho sản phẩm của họ:

- Trung tâm An ninh Mạng Úc châu (ACSC)
- Trung tâm An ninh Mạng Gia Nã Đại (CCCS)
- Trung tâm An ninh Mạng Quốc gia Vương Quốc Anh (NCSC-UK)
- Cục An ninh Mạng Liên bang Đức (BSI)
- Trung tâm An ninh Mạng Quốc gia Hà Lan (NCSC-NL)
- Đội Phản ứng Khẩn cấp Máy tính Tân Tây Lan (CERT NZ) và Trung tâm An ninh Mạng Quốc gia Tân Tây Lan (NCSC-NZ).

Các cơ quan tác giả thừa nhận nhiều đóng góp của nhiều đối tác tư nhân trong việc thúc đẩy Bảo mật theo Thiết kế và Bảo mật theo Mặc định. Mục đích của tài liệu này nhằm thúc đẩy một cuộc đối thoại quốc tế về các ưu tiên cốt lõi, đầu tư và các quyết định 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 cơ quan tác giả mong muốn nhận được phản hồi 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, xác định rõ và nâng cao hướng dẫn của chúng tôi, nhằm đạt được mục đích chung của chúng ta.

Để biết thêm thông tin về tầm quan trọng của vấn đề bảo mật sản phẩm, xin xem bài viết của CISA, Tổn thất của Công nghệ Không An toàn và Những gì Chúng ta Có thể Làm về Điều này (The Cost of Unsafe Technology and What We Can Do About It.)

Bảo mật theo Thiết kế

"Bảo mật theo Thiết kế" có nghĩa là các sản phẩm công nghệ được thiết kế theo các phương pháp bảo vệ hợp lý để chống lại các hành động xâm nhập của những kẻ tấn công mạng độc hại nhằm truy cập vào các thiết bị, dữ liệu và hệ thống 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, sau đó đưa các biện pháp bảo vệ vào bản thiết kế sản phẩm nhằm đối đầu với bối cảnh các mối đe dọa mạng đang liên tục xảy ra.

Các phương pháp phát triển công nghệ thông tin an toàn (IT) và nhiều lớp phòng thủ – được gọi là phòng thủ sâu (defense-in-depth) – cũng được khuyến nghị để ngăn chặn các hoạt động của kẻ xâm nhập mạng độc hại, từ việc tấn công vào các hệ thống hoặc truy cập trái phép vào dữ liệu nhạy cảm. Các cơ quan tác giả khuyến nghị các nhà sản xuất sử dụng mô hình các mối đe dọa phù hợp trong giai đoạn phát triển sản phẩm,

[2] Sau đây sẽ được gọi là "các cơ quan tác giả".

để 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 cơ quan tác giả kêu gọi các nhà sản xuất thực hiện 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 sự đầu tư các nguồn lực đáng kể từ các nhà sản xuất phần mềm ở mỗi tầng trong quá trình thiết kế và phát triển sản phẩm vốn không thể được "gắn thêm vào" sau này. Điều này đòi hỏi sự lãnh đạo mạnh mẽ từ các nhà quản lý kinh doanh hàng đầu của nhà sản xuất để đưa việc bảo mật trở thành một ưu tiên trong kinh doanh, mà không chỉ là một tính năng kỹ thuật. Sự hợp tác giữa các nhà lãnh đạo kinh doanh và các nhóm kỹ thuật kéo dài từ giai đoạn ban đầu của thiết kế và phát triển, thông qua bước khách hàng triển khai và bảo trì. Các nhà sản xuất được khuyến khích đưa ra những sự đánh đổi và đầu tư khó khăn, bao gồm các đầu tư "vô hình" đối với khách hàng, chẳng hạn như chuyển sang ngôn ngữ lập trình có khả năng loại bỏ các lỗ hổng phổ biến. Họ nên ưu tiên cho các tính năng, cơ chế và cách triển khai các công cụ bảo vệ khách hàng thay vì các tính năng sản phẩm có vẻ hấp dẫn nhưng làm tăng diện tích tấn công.

Không có một giải pháp đơn lẻ nào để chấm dứt các mối đe dọa liên tục từ các kẻ tấn công mạng độc hại lợi dụng các lỗ hổng 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 viết tài liệu để đồng bộ hóa danh mục sản phẩm hiện có của họ với các phương pháp "Bảo mật theo Thiết kế", và chỉ sai lệch trong các trường hợp bất khả kháng mà thôi.

Các cơ quan tác giả thừa nhận rằng nhận phần trách nhiệm về việc bảo đảm kết quả an ninh cho khách hàng và bảo đảm mức độ bảo mật này có thể làm tăng chi phí phát triển. Tuy nhiên, đầu tư vào các phương pháp "Bảo mật theoThiết 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 tư thế an ninh của khách hàng và giảm xác suất bị tấn công. Nguyên tắc Bảo mật theo Thiết kế không chỉ làm vững tư thế bảo mật cho khách hàng và tăng cường uy tín thương hiệu cho các nhà phát triển, 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 được đề nghị để các nhà sản xuất có thể xem xét.

Bảo mật theo Mặc định

"Bảo mật theo Mặc định" có nghĩa là sản phẩm được thiết kế để chống chịu các kỹ thuật lợi dụng lỗ hổng phổ biến ngay khi được đưa vào sử dụng mà không cần phải trả thêm chi phí. Những sản phẩm này được bảo vệ từ những mối đe dọa và các lỗ hổng phổ biến mà người dùng không cần phải thực hiện thêm bất kỳ bước nào để bảo vệ chúng. Các sản phẩm Bảo mật theo Mặc định được thiết kế nhằm giúp cho khách hàng hiểu rõ rằng, khi họ đi chệch khỏi mặc định an toàn, họ đang làm tăng khả năng bị tấn công trừ khi họ triển khai các biện pháp khác để bù vào.

- Cấu hình bảo mật nên là cơ sở mặc định an toàn căn bản. Các sản phẩm Bảo mật theo Mặc định tự động kích hoạt các biện pháp kiểm soát bảo mật quan trọng cần thiết nhất để bảo vệ doanh nghiệp

từ những kẻ đột nhập mạng độc hại, cũng như cung cấp khả năng sử dụng và thiết lập thêm các biện pháp kiểm soát bảo mật mà không phải trả thêm chi phí.

• Mức độ phức tạp của cấu hình bảo mật không nên là vấn đề của khách hàng. Các nhân viên 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 triển khai các biện pháp giảm thiểu cần thiết để có một hệ thống an ninh mạng mạnh mẽ. Qua việc tối ưu hóa cấu hình sản phẩm bảo mật – bảo mật "lộ trình mặc định" – các nhà sản xuất có thể giúp đỡ khách hàng của họ bằng cách bảo đảm các sản phẩm của họ được sản xuất, phân phối và sử dụng an toàn theo tiêu chuẩn "Bảo mật theo Mặc định".

Các nhà sản xuất sản phẩm "Bảo mật theo Mặc định" không tính thêm lệ phí để triển khai các cấu hình bảo mật bổ sung. Thay vào đó, họ bao gồm chúng trong sản phẩm cơ bản như những dây an toàn được bao gồm trong tất cả các chiếc ô tô mới. Bảo mật không phải là một tùy chọn sang trọng mà là tiêu chuẩn mà mọi khách hàng nên mong đợi mà không cần phải thương lượng hoặc trả thêm tiền.

KHUYẾN NGHỊ CHO CÁC NHÀ SẢN XUẤT PHẦN MỀM

Hướng dẫn liên danh này đưa ra các khuyến nghị cho các nhà sản xuất về việc phát triển một lộ trình viết tài liệu để thực hiện, và bảo đảm an ninh công nghệ thông tin. Các cơ quan tác giả khuyến nghị các nhà sản xuất phần mềm thực hiện các chiến lược được trình bày trong các phần sau đây để đảm nhận trách nhiệm cho các kết quả an ninh của khách hàng thông qua các 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 trọng tâm chiến lược để ưu tiên cho an ninh phần mềm. Các cơ quan tác giả đã thiết kế ba nguyên tắc cốt lõi dưới đây để hướng dẫn các nhà sản xuất phần mềm tích hợp tính an ninh phần mềm vào quá trình thiết kế của họ trước khi phát triển, thiết lập cấu hình và chuyển giao sản phẩm.

1. Trách nhiệm về bảo mật không nên chỉ thuộc về khách hàng. Các nhà sản xuất phần mềm nên chịu trách nhiệm về kết quả bảo mật cho các sản phẩm mà khách hàng mua của họ và phát triển sản phẩm của mình sao cho phù hợp.
2. Nâng cao tính minh bạch và trách nhiệm cấp tiến. Các nhà sản xuất phần mềm nên tự hào về việc cung cấp sản phẩm an toàn và bảo mật, đồng thời tạo sự khác biệt giữa họ với cộng đồng các nhà sản xuất khác dựa trên khả năng của họ. Điều này có thể bao gồm việc chia sẻ thông tin mà họ học 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 các tư vấn về lỗ hổng và các hồ sơ lưu về lỗ hổng và mức độ phơi nhiễm phổ biến (CVE) liên quan là đầy đủ và chính xác. Tuy nhiên, cần cẩn trọng và không nên xem số lượng CVE như là một chỉ số tiêu cực, vì những con số đó cũng là dấu hiệu của một cộng đồng phân tích mã và kiểm tra mã mạnh mẽ.

3. Xây dựng cơ cấu tổ chức và lãnh đạo để đạt được những mục tiêu này. Trong khi chuyên môn kỹ thuật là điều quan trọng đối với việc bảo mật sản phẩm, các nhà lãnh đạo cao cấp là những người quyết định chính để thực hiện các thay đổi trong một tổ chức. Sự cam kết của các nhà lãnh đạo cao cấp dành cho các nhà sản xuất phần mềm đặt ưu tiên bảo mật như một yếu tố quan trọng trong quá trình phát triển sản phẩm, đòi hỏi sự phát triển quan hệ đối tác với khách hàng của tổ chức để hiểu:
    a. Hướng dẫn khuôn khổ triển khai sản phẩm cùng với mô hình đe dọa tùy chỉnh
    b. Đề xuất triển khai các biện pháp kiểm soát bảo mật để phù hợp với các nguyên tắc Bảo mật theo Mặc định
    c. Các chiến lược phân bổ nguồn lực phù hợp với mức độ quy mô của công ty và khả năng thay thế các phương pháp phát triển cũ bằng các phương pháp Bảo mật theo Thiết kế
    d. Cần duy trì một đường dây liên lạc mở rộng cho cho những ý kiến đóng góp nội bộ và bên ngoài (ví dụ: ý kiến đóng góp của nhân viên và khách hàng) liên quan đến các vấn đề bảo mật sản phẩm. An ninh phần mềm nên được nhấn mạnh trong các diễn đàn nội bộ (ví dụ: tất cả các thành viên hoặc các cuộc họp nhỏ không chính thức), cũng như tiếp thị sản phẩm bên ngoài và tương tác với khách hàng.
    e. Đánh giá hiệu quả trong việc triển khai của khách hàng. Các nhà lãnh đạo cao cấp sẽ muốn biết các khoản đầu tư vào bảo mật theo thiết kế và mặc định đang giúp ích gì cho khách hàng bằng cách giảm tốc độ các bản vá bảo mật, giảm lỗi cấu hình và giảm thiểu diện tích tấn công.

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 của họ.

Tổ chức các cuộc họp thường xuyên với lãnh đạo cao cấp của công ty để thúc đẩy tầm quan trọng của việc Bảo mật theo Thiết kế và Bảo mật theo Mặc định trong tổ chức. Nên thiết lập chính sách và phương pháp để động viên các nhóm sản xuất phát triển sản phẩm tuân thủ các nguyên tắc này, bao gồm việc trao giải thưởng cho các nhóm thực hiện các phương pháp bảo mật phần mềm xuất sắc, hoặc khuyến khích về các tiêu chuẩn thăng tiến và đánh giá nâng bậc.

Hoạt động xoay quanh tầm quan trọng của việc bảo mật phần mềm đối với sự thành công của doanh nghiệp. Ví dụ, cân nhắc phân công một “người đứng đầu an ninh phần mềm” hoặc một “nhóm an ninh phần mềm” nhằm bảo đảm các tiêu chuẩn an ninh phần mềm và trách nhiệm của nhà sản xuất được liên kết trực tiếp với các phương pháp kinh doanh và công nghệ thông tin. Các nhà sản xuất nên bảo đảm rằng họ có các chương trình thẩm định và đánh giá bảo mật sản phẩm mạnh mẽ, độc lập cho các sản phẩm của mình.

Sử dụng một mô hình mối đe dọa phù hợp trong quá trình phát triển để ưu tiên xác định các sản phẩm quan trọng nhất và có tác động lớn 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, lãnh đạo cao cấp nên

quy trách nhiệm cho các nhóm về việc cung cấp các sản phẩm an toàn, như một yếu tố chính của sản phẩm đạt phẩm chất cao, và sự xuất sắc của sản phẩm.

Các Chiến thuật Bảo mật theo Thiết kế

Khung Phát triển Phần mềm An toàn (SSDF), còn được gọi là NIST SP 800-218, của Viện Tiêu chuẩn và Công nghệ Quốc gia, là một tập hợp cốt lõi của các phương pháp phát triển phần mềm bảo mật cao cấp có thể được tích hợp vào từng giai đoạn của vòng đời phát triển phần mềm (SDLC). Làm theo các phương pháp này có thể giúp nhà sản xuất phần mềm trở nên hiệu quả hơn trong việc tìm và loại bỏ các lỗ hổng trong phần mềm đã phát hành, giảm thiểu tác động tiềm ẩn của việc khai thác các lỗ hổng và giải quyết nguyên nhân gốc rễ của các điểm yếu để ngăn chặn sự tái diễn trong tương lai.

Các cơ quan 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 phát triển một lộ trình viết tài liệu để áp dụng thêm các phương pháp phát triển phần mềm được Bảo mật theo Thiết kế cho toàn bộ danh mục sản phẩm của mình. Sau đây là một danh sách minh họa không đầy đủ bao gồm các phương pháp tốt nhất của lộ trình viết tài liệu:

• 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 bất cứ khi nào có thể. Các cơ quan tác giả công nhận rằng những phương pháp cụ thể khác để bảo vệ bộ nhớ, chẳng hạn như ngẫu nhiên hóa bố cục không gian địa chỉ (ASLR), tính toàn vẹn luồng điều khiển (CFI) và kỹ thuật kiểm thử phần mềm được để tìm kiếm các lỗ hổng (fuzzing) có ích cho các mã nguồn cũ, nhưng chưa đủ để được xem là Bảo mật theo Thiết kế vì chúng không đủ để ngăn chặn việc khai thác. 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 (information sheet) 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 cung cấp phương tiện để 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 (**CHERI**) có thể mở rộng Kiến trúc tập lệnh phần cứng thông thường (**ISA**). Để biết thêm thông tin, truy cập trang mạng CHERI của Đại học Cambridge.

• Bảo mật các Thành phần của Phần mềm (SSDF PW 4.1): Thu thập 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 (module), phần mềm nằm giữa các ứng dụng (middleware), một bộ sưu tập các đơn vị mã tự chứa và công cụ cung cấp một cấu trúc cho việc xây dựng các ứng dụng phần mềm (framework)) 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.

• Khung mẫu Mạng (SSDF PW.5.1): Sử dụng khung mẫu mạng được triển khai 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 thay vì 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 (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 để giải quyết các lỗ hổng 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 quá trình đánh giá bởi các nhà phát triển khác để bảo đảm phẩm chất cao hơn.

• Danh sách Vật liệu Phần mềm (Software Bill of Materials (SBOM)) (SBOM) (SSDF PS.3.2, PW.4.1): Kết hợp việc tạo SBOM[3] để cung cấp khả năng hiển thị trong bộ phần mềm được đưa vào sản phẩm.

• Chương trình tiết lộ lỗ hổng (SSDF RV.1.3): Thiết lập chương trình tiết lộ lỗ hổng cho phép nhà nghiên cứu bảo mật trình báo các lỗ hổng và được miễn trách nhiệm pháp lý. Các nhà cung cấp phải thiết lập quy trình để xác định nguyên nhân gốc rễ của các lỗ hổng được phát hiện. Quy trình này nên bao gồm việc xác định xem việc 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 hay không.

• Hoàn chỉnh CVE (Các Lỗ hổng và Phơi nhiễm Phổ biến): Phải chắc chắn rằng các CVE được công bố bao gồm nguyên nhân gốc rễ hoặc Mã Lỗi Phổ biến (CWE) nhằm giúp cho việc phân tích nguyên nhân đối với các vấn đề về 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 có lợi cho tất cả các nhà sản xuất và khách hàng. Để biết thêm thông tin về quản lý lỗ hổng, xem hướng dẫn SVCC dành riêng cho các bên liên quan của CISA (CISA's Stakeholder- specific SVCC guidance)

• Phòng thủ Sâu (Defense-in-Depth): 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 ứng dụng, quy trình hoặc hệ thống có thể cách ly một lỗ hổng để hạn chế sự xâm phạm của toàn bộ ứng dụng.

• Đáp ứng các Mục tiêu Hiệu suất An ninh Mạng (CPGs): 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 (CISA's Cybersecurity Performance Goals) phác thảo các biện pháp an ninh mạng cơ bản mà các tổ chức nên thực hiện.

[3] Một số cơ quan tác giả đang khám phá các phương pháp thay thế để bảo đảm an ninh cho chuỗi cung ứng phần mềm.

Ngoài ra, để củng cố vị thế an ninh mạng của tổ chức của bạn, hãy xem Khung Đánh giá An ninh Mạng của Vương quốc Anh (UK's Cyber Assessment Framework), có các điểm tương đồng với các Mục tiêu Hiệu suất về An ninh Mạng của CISA. Nếu một nhà sản xuất không đáp ứng các Mục tiêu Hiệu suất về An ninh Mạng (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 tác giả nhận thấy rằng những thay đổi này là những bước chuyển đổi đáng kể đối với quan điểm của một tổ chức. Do đó, việc đưa những thay đổi này vào nên được ưu tiên dựa trên mức độ quan trọng, mức 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 sản phẩm nào đó có thể đòi hỏi một lịch trình được tăng tốc để áp dụng những phương pháp này. Trong các trường hợp khác, các ứng dụng có thể được đưa vào một mã nguồn cũ và khắc phục theo thời gian.

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 tác giả 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 thông lệ này khi chúng được khôi phục. Ví dụ:

• Loại bỏ các mật khẩu mặc định: Các sản phẩm không nên có mật khẩu mặc định được chia sẻ rộng rãi. Để loại bỏ mật khẩu mặc định, các cơ quan tác giả khuyến nghị các quản trị viên phải được yêu cầu đặt mật khẩu mạnh trong quá trình cài đặt và cấu hình sản phẩm.

- Xác thực Đa Yếu tố Bắt buộc (MFA)cho người dùng có đặc quyền. Chúng tôi nhận thấy rằng có nhiều doanh nghiệp do các quản trị viên quản lý chưa bảo vệ tài khoản của họ bằng MFA. Vì quản trị viên là mục tiêu có giá trị cao, các sản phẩm phải làm cho MFA trở thành tùy chọn mặc định thay vì tùy chọn tham gia. Hơn nữa, hệ thống phải thường xuyên 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 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 (Mature Authentication Factsheet) để biết thêm thông tin.

• Đăng nhập một lần (SSO): Các ứng dụng Công nghệ Thông tin nên triển khai công nghệ đăng nhập một lần thông qua các tiêu chuẩn mở rộng hiện đại. Các ví dụ bao gồm Ngôn ngữ Đánh dấu Xác nhận Bảo mật (SAML) hoặc Kết nối OpenID (OIDC.) Kỹ năng này nên được cung cấp theo mặc định mà không phải mất thêm chi phí.

• Đăng nhập an toàn: Cung cấp nhật ký kiểm toán tốt nhất cho khách hàng mà không tính thêm chi phí. Nhật ký kiểm toán rất quan trọng để phát hiện và tăng cường giải quyết các vấn đề bảo mật tiềm tàng. 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 (SIEM) với quyền truy cập giao diện lập trình ứng dụng (API) sử dụng thời gian quốc tế phối hợp (UTC), định dạng múi giờ tiêu chuẩn và các kỹ thuật tài liệu mạnh mẽ.

• Hồ sơ Ủy quyền Phần mềm: Nhà cung cấp phần mềm nên cung cấp các khuyến nghị về các vai trò ủy quyền được phê duyệt và các trường hợp sử dụng đề xuất 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 chệch 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 thông tin địa chỉ 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 điều này gây ra các sự thay đổi không tương thích.

• Theo dõi và giảm kích thước của "hướng dẫn tăng cường bảo mật": Giảm kích cỡ của "hướng dẫn tăng cường bảo mật" được thiết kế cho các sản phẩm nhằm cố gắng để bảo đảm rằng kích cỡ giảm 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 cơ quan 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 người dùng (UX).

• Xem xét các hậu quả qua trải nghiệm của người dùng đối với cài đặt bảo mật: Mỗi cài đặt mới đều tăng gánh nặng nhận thức cho người dùng và nên được đánh giá kết hợp với lợi ích kinh doanh nó đem lại. Điều lý tưởng nhất là không có cài đặt nào cả, thay vào đó, 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 thông thường.

Các cơ quan tác giả công nhận rằng những thay đổi này có thể ảnh hưởng đến hoạt động của việc sử dụng phần mềm. Do đó, ý kiến đóng góp của khách hàng là điều rất quan trọng để cân bằng giữa các yếu tố hoạt động và bảo mật. Các cơ quan tác giả tin rằng việc phát triển các lộ trình viết tài liệu và 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, các cơ quan tác giả đã quan sát thấy những trường hợp quan trọng khi khách hàng không sẵn sàng 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 đối đầu với các lỗ hổng một cách vô hạn định.

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

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. Do đó, 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. Thông thường, nhiều tổ chức không biết về các hướng dẫn tăng cường, do đó họ để cài đặt cấu hình thiết bị của mình ở tư thế không an toàn. Một mô hình đảo ngược được gọi là hướng dẫn nới lỏng sẽ thay thế các hướng dẫn tăng cường và giải thích những thay đổi mà người dùng nên thực hiện, đồng thời liệt kê các rủi ro có thể phát sinh từ việc thực hiện các thay đổi đối với hệ thống hoặc ứng dụng.

Thay vì thiết kế các hướng dẫn tăng cường bảo mật bao gồm các phương pháp để bảo vệ sản phẩm, các cơ quan tác giả khuyến khích các nhà sản xuất phần mềm chuyển sang phương pháp Bảo mật theo Thiết kế bằng cách 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 nhu cầu kinh doanh khác.

KHUYẾN NGHỊ CHO KHÁCH HÀNG

Các cơ quan tác giả khuyến nghị các tổ chức yêu cầu các nhà sản xuất cung cấp công nghệ của họ phải chịu trách nhiệm về kết quả bảo mật của sản phẩm của họ. Nhằm thực hiện điều này các cơ quan tác giả khuyến nghị rằng các giám đốc điều hành của tổ chức nên ưu tiên cho tầm quan trọng của việc mua các sản phẩm Bảo mật theo Thiết kế và Bảo mật theo Mặc định. Điều này có thể thể hiện thông qua việc thiết lập các chính sách yêu cầu bộ phận công nghệ thông tin đánh giá tính an toàn phần mềm của nhà sản xuất trước khi mua, cũng như cho phép bộ phận công nghệ thông tin phản kháng nếu cần thiết. Bộ phận công nghệ thông tin (IT) nên được trao quyền để phát triển các tiêu chuẩn mua hàng nhằm nhấn mạnh tầm quan trọng của các biện pháp Bảo mật theo Thiết kế và Bảo mật theo Mặc định (cả những biện pháp được nêu ra trong tài liệu này và các biện pháp khác do tổ chức khác thiết kế). Hơn nữa, bộ phận công nghệ thông tin (IT) cần được ban quản lý điều hành hỗ trợ khi thực thi các tiêu chuẩn này trong các quyết định mua hàng. Các quyết định của tổ chức về việc chấp nhận các rủi ro liên quan đến các sản phẩm công nghệ cụ thể, phải được lập thành văn bản chính thức, được giám đốc điều hành kinh doanh cao cấp phê duyệt và trình bày thường xuyên trước Hội đồng Quản trị.

Các dịch vụ công nghệ thông tin (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 phản hồi, 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 khả năng 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.

Nếu có thể, các tổ chức nên cố gắng tạo dựng mối quan hệ đối tác chiến lược với các nhà cung cấp công nghệ thông tin (IT) chính của họ. Những mối quan hệ này bao gồm sự tin tưởng ở nhiều cấp độ của tổ chức

và cung cấp các phương tiện để giải quyết vấn đề và xác định các ưu tiên chung. Bảo mật phải 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 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. Các tổ chức nên đòi hỏi 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 công nghệ thông tin cũng nên hợp tác với các đồng nghiệp trong ngành để hiểu rõ hơn về các sản phẩm và dịch vụ nào phù hợp 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 động lực để họ ưu tiên cho việc bảo mật.

Khi tận dụng các hệ thống đám mây, các tổ chức cần chắc chắn rằng họ hiểu rõ về mô hình chịu trách nhiệm chung với nhà cung cấp công nghệ của mình. Điều này có nghĩa là tổ chức cần phải rõ ràng về trách nhiệm an ninh của nhà cung cấp chứ không chỉ là trách nhiệm của khách hàng. Tổ chức nên ưu tiên chọn những nhà cung cấp đám mây có tính minh bạch về tư thế bảo mật, kiểm soát nội bộ và khả năng đáp ứng các nghĩa vụ của họ 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. 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 cụ thể, hoặc các sản phẩm, quy trình, hoặc dịch vụ thương mại bằng dịch vụ thương hiệu, thương hiệu, hoặc nhà sản xuất khác, không đại diện hoặc ngụ ý ủng hộ, khuyến nghị hoặc thiên vị bởi CISA và các cơ quan 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 (CISA's SBOM Guidance)
- Mục tiêu Hiệu suất An ninh mạng Chéo ngành của CISA (CISA's Cross-Sector Cybersecurity Performance Goals)
- Hướng dẫn về Tương tác Công nghệ của CISA (Guidelines on Technology Interoperability)
- CISA và NIST's Phòng thủ Chống lại các cuộc Tấn công Chuỗi Cung ứng Phần mềm (CISA and NIST's Defending Against Software Supply Chain Attacks)
- Chi phí của Công nghệ Không an toàn và Những gì Chúng ta Có thể Làm| CISA (The Cost of Unsafe Technology and What We Can Do About It | CISA)
- Hãy Ngừng Đổ lỗi Trách nhiệm về việc Bảo mật Mạng: Tại sao các Công ty Phải Thiết

kế tính An toàn cho Sản phẩm Công nghệ (foreignaffairs.com) (Stop Passing the Buck on Cybersecurity: Why Companies Must Build Safety Into Tech Products (foreignaffairs.com))

- Hướng dẫn Phân loại Lỗ hổng Bảo mật dành riêng cho các bên Liên quan (SSVC) của CISA (CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guidance)
- Tờ thông tin MFA chống lừa đảo của CISA (CISA's Phishing Resistant MFA Fact Sheets)
- Hướng dẫn về An ninh mạng cho Doanh nghiệp nhỏ | CISA (Cyber Guidance for Small Businesses | CISA)

NSA

- Tờ thông tin An ninh mạng về An toàn Bộ nhớ của NSA (NSA's Cybersecurity Information Sheet on Memory Safety)
- ESF của NSA Bảo vệ Chuỗi cung ứng Phần mềm: Các Phương pháp Thực hành Tốt nhất cho các nhà Cung cấp (NSA's ESF Securing the Software Supply Chain: Best Practices for Suppliers)

FBI

- Tìm hiểu và Phản Ứng với Cuộc Tấn Công Chuỗi Cung Ứng nguồn Năng lượng Gió: Quan Điểm của Liên Bang Mỹ (Understanding and Responding to the SolarWinds Supply Chain Attack: The Federal Perspective)
- Mối Đe dọa Mạng - Phản Ứng và Trình báo (The Cyber Threat - Response and Reporting)
- Chiến lược An ninh Mạng của FBI (FBI's Cyber Strategy)

Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST)

- Hướng dẫn Nhận dạng Kỹ thuật số của NIST (NIST's Digital Identity Guidelines)
- Khung Hướng dẫn An ninh Mạng của NIST (NIST's Cyber Security Framework)
- Khung Phát triển Phần mềm An toàn của NIST (SSDF) (NIST's Secure Software Development Framework (SSDF))

Trung tâm An ninh Mạng Úc châu (ACSC)

- Hướng dẫn của ACSC đối với các Quy tắc Thực hành IoT dành cho các Nhà sản xuất (ACSC's IoT Code of Practice Guidance for Manufacturers)

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

- Khung Đánh giá An ninh Mạng của Vương quốc Anh (The UK's Cyber Assessment Framework)
- Hướng dẫn Triển khai và Phát triển An toàn của NCSC Vương quốc Anh (The UK NCSC's Secure Development and Deployment guidance)
- Hướng dẫn Quản lý Lỗ hổng của NCSC Vương quốc Anh (The UK NCSC's Vulnerability Management guidance)
- Bộ Công cụ Tiết lộ Lỗ hổng của NCSC Vương quốc Anh (The UK NCSC's Vulnerability

Disclosure Toolkit)

- CHERI của Đại học Cambridge (University of Cambridge's CHERI)
- Hẹn gặp lại và cám ơn quý vị đã cung cấp thông tin - NCSC.GOV.UK (So long and thanks for all the bits - NCSC.GOV.UK)

Trung tâm An ninh Mạng Gia Nã Đại (CCS)

- Hướng dẫn của (CCCS) về việc Bảo vệ Chống lại các cuộc Tấn công Chuỗi Cung ứng Phần mềm (CCCS's Guidance on Protecting Against Software Supply Chain Attacks)
- Chuỗi Cung ứng Mạng : Một Phương pháp Đánh giá các Rủi ro (Cyber supply chain: An approach to assessing risks)
- Hướng dẫn về Mã độc Tống tiền CONTI của Trung tâm An ninh Mạng Gia Nã Đại (Canadian Centre for Cyber Security's CONTI ransomware guidance)

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

- Bản tóm tắt tài liệu BSI Grundschutz (mô-đun CON.8) (The BSI Grundschutz compendium (module CON.8))
- Tiêu chuẩn Quốc tế IEC 62443, phần 4-1 (The international standard IEC 62443, part 4-1)
- Trình Báo Tình trạng An ninh CNTT tại Đức, năm 2022 (State of IT-security in Germany report, 2022)
- Phương pháp BSI về Bảo mật Ứng dụng Mạng (BSI practices of web application security)

Trung tâm An ninh Mạng Quốc gia Hà Lan

- Tờ thông tin Hệ thống Xác đã được Phát triển và Hoàn thiện của Trung tâm An ninh Mạng Quốc gia Hà Lan (NCSC-NL) (NCSC-NL's Mature Authentication Factsheet)

Các Nguồn khác

- Làm thế nào Mà các Hệ thống Phức tạp Thất bại (How Complex Systems Fail)
- Một Góc nhìn Khác về sự Thất bại của các Hệ thống Phức tạp (The New Look in complex system failure)