**Information Security Integration with Agile Software Development: Systematic Literature Review and Expert Judgement**

Tengku Chavia Zagita, Teguh Raharjo - Faculty of Computer Science, Universitas Indonesia, Jakarta, Indonesia, Indonesian Journal of Computer Science Vol. 12, No. 6, Ed. 2023 | page 3487 - 3487

Dưới đây là một tóm tắt chi tiết hơn về việc tích hợp bảo mật thông tin vào phát triển phần mềm Agile:

Giới thiệu

Nhiều doanh nghiệp ngày nay đang sử dụng phương pháp Agile để phát triển phần mềm nhằm đáp ứng nhu cầu thay đổi nhanh chóng và giao hàng giá trị chức năng sớm hơn. Tuy nhiên, bảo mật thông tin thường bị coi là yêu cầu phi chức năng và thường bị đặt ở ưu tiên thấp hơn so với các yêu cầu chức năng trong phát triển phần mềm Agile. Sự không tích hợp bảo mật có thể dẫn đến nhiều rủi ro nghiêm trọng như mất dữ liệu, thiệt hại tài chính và danh tiếng. Do đó, việc tích hợp bảo mật thông tin vào quy trình phát triển phần mềm Agile là rất cần thiết. Nghiên cứu này tập trung vào việc cung cấp cái nhìn tổng thể về cách các nhà nghiên cứu đã tiếp cận vấn đề tích hợp bảo mật thông tin vào phát triển phần mềm Agile.

Phương pháp nghiên cứu

Nghiên cứu này sử dụng phương pháp Tổng quan Tài liệu Có hệ thống (SLR) với các bước quy trình chuẩn bao gồm lập kế hoạch, thực hiện và báo cáo. Quá trình tìm kiếm bài báo khoa học đã được thực hiện trên các cơ sở dữ liệu lớn như ACM, IEEE, ScienceDirect và Scopus với chuỗi tìm kiếm liên quan đến "Tích hợp Bảo mật Thông tin vào Phát triển Phần mềm Agile". Sau khi áp dụng các tiêu chí lọc về ngôn ngữ, năm xuất bản, sự đánh giá ngang hàng, tính đầy đủ và liên quan, 15 nghiên cứu đã được chọn để phân tích.

Kết quả và thảo luận

Phương pháp Agile được sử dụng

Kết quả cho thấy hầu hết các nghiên cứu (8/15) đã sử dụng phương pháp Scrum trong nghiên cứu, phù hợp với xu hướng Scrum là phương pháp Agile phổ biến nhất hiện nay. Một số nghiên cứu khác kết hợp Scrum với các phương pháp Agile khác như FDD. Các nghiên cứu còn lại tuyên bố rằng kết quả nghiên cứu có thể áp dụng cho tất cả các phương pháp Agile.

Tích hợp bảo mật vào các công đoạn Agile

- Khởi tạo Backlog sản phẩm: Một số nghiên cứu đề xuất thêm các câu chuyện người dùng liên quan đến bảo mật trong giai đoạn này để xem xét bảo mật ngay từ đầu.

- Grooming Backlog: Đây là công đoạn được nhiều nghiên cứu tập trung nhất vào việc tích hợp bảo mật. Các hoạt động như phân tích rủi ro, đánh giá mức độ nghiêm trọng của các mối đe dọa bảo mật cho từng hạng mục backlog được đưa vào giai đoạn này.

- Lập kế hoạch Sprint: Một số nghiên cứu đề xuất việc thêm các tác vụ, câu chuyện người dùng liên quan đến bảo mật vào backlog của sprint. Ngoài ra, các tiêu chí chấp nhận liên quan đến bảo mật cũng được xem xét tại giai đoạn này.

- Trong Sprint: Hầu hết các nghiên cứu (12/15) có đề xuất việc tích hợp các hoạt động liên quan đến bảo mật vào trong giai đoạn thực hiện sprint. Các hoạt động này bao gồm kiểm tra mã, đánh giá rủi ro, rà soát thiết kế, v.v. Một số nghiên cứu thậm chí đề xuất thêm vai trò mới như chuyên gia bảo mật vào nhóm phát triển.

- Xem xét Sprint: Các nghiên cứu đề xuất việc thực hiện kiểm tra bảo mật sản phẩm đối với các tính năng được hoàn thành trong sprint và trình bày kết quả kiểm tra trong buổi xem xét.

- Retrospective Sprint: Một vài nghiên cứu nhấn mạnh đến việc đánh giá quy trình bảo mật, các vấn đề bảo mật gặp phải và đề xuất cải tiến trong giai đoạn này.

Lợi ích của việc tích hợp bảo mật

- Cải thiện tính năng động: Việc tích hợp bảo mật ngay từ đầu vào quy trình Agile giúp đảm bảo các yêu cầu bảo mật được xem xét đầy đủ, từ đó tránh việc phải sửa đổi nhiều ở cuối chu kỳ phát triển, giúp tăng tính năng động.

- Hiệu quả chi phí: Bằng cách giải quyết các vấn đề bảo mật ngay từ đầu và liên tục trong suốt dự án, việc tích hợp bảo mật giúp giảm chi phí điều chỉnh và sửa lỗi về sau, đem lại hiệu quả cao hơn về chi phí.

- Giảm phức tạp bảo mật: Việc tích hợp bảo mật một cách hệ thống và rõ ràng vào quy trình Agile sẽ giúp đơn giản hóa việc quản lý các yêu cầu bảo mật thay vì để chúng tồn tại phân tán.

- Cải thiện mức độ bảo mật: Đây là lợi ích quan trọng nhất, việc tích hợp bảo mật sẽ giúp nâng cao mức độ bảo mật, đáp ứng tốt hơn các yêu cầu pháp lý và quy định của tổ chức.

Vấn đề khi tích hợp bảo mật

- Làm chậm quá trình tạo chức năng: Do phải thực hiện nhiều hoạt động

**Semiotics: An Approach to Model Security Scenarios for IoT-Based Agriculture Software**

Julio Ariel Hurtado; Leandro Antonelli; Santiago López; Adriana Gómez; Juliana Delle Ville ; Giuliana Maltempo; Frey Giovanny Zambrano; Andrés Solis; Marta Cecilia Camacho Miguel Solinas; Gladys Kaplan; Freddy Muñoz - TecnoLógicas, Vol. 27, no. 59, e2923, 2024

Tài liệu này đề xuất một phương pháp xây dựng kịch bản bảo mật cho các ứng dụng Internet vạn vật (IoT) trong lĩnh vực nông nghiệp. Nó bắt đầu bằng việc mô tả các kịch bản sử dụng đúng đắn của phần mềm đã đề xuất, sau đó mô tả các kịch bản sử dụng không chính xác, trong đó hệ thống bị lạm dụng. Các kịch bản sử dụng không đúng này sau đó được chuyển đổi thành các kịch bản bảo mật bằng cách áp dụng một tập hợp các quy tắc. Cuối cùng, các kịch bản bảo mật được điều chỉnh và hoàn thiện thêm.

Mục đích là đảm bảo các yêu cầu phi chức năng quan trọng như bảo mật được đáp ứng khi phát triển các giải pháp IoT cho nông nghiệp. Kịch bản bảo mật giúp xác định các mối đe dọa và lỗ hổng bảo mật tiềm ẩn để các nhà phát triển có thể giải quyết chúng trong giai đoạn đầu. Phương pháp này sử dụng kịch bản theo cách phi chính thức, khuyến khích sự tương tác giữa các chuyên gia từ nhiều lĩnh vực khác nhau để đạt được sự hiểu biết sâu sắc hơn về vấn đề.

Đầu tiên, phương pháp giới thiệu hai loại kịch bản: kịch bản tập trung vào chức năng của ứng dụng phần mềm và kịch bản tập trung vào các khía cạnh bảo mật trong kiến trúc. Kịch bản chức năng mô tả một tình huống cụ thể để đạt được một mục tiêu, bao gồm các bước, vai trò tham gia và tài nguyên được sử dụng. Ví dụ, kịch bản kích hoạt hệ thống tưới tiêu.

Kịch bản kiến trúc bảo mật tuân theo một khuôn mẫu khác, chỉ định các thành phần như nguồn kích hoạt, kích hoạt, môi trường, thực thể bị ảnh hưởng, phản ứng và đo lường phản ứng. Chúng xác định cách hệ thống phải phản ứng với các tình huống bảo mật như một cuộc tấn công.

Các công trình liên quan trước đây đã đề cập đến nhiều khía cạnh của phát triển phần mềm IoT và nhu cầu bảo mật, nhưng chưa giải quyết cách xác định các yêu cầu bảo mật một cách chính xác.

Bước đầu tiên của phương pháp là mô tả các kịch bản sử dụng chính xác của ứng dụng phần mềm dự kiến, bao gồm các khía cạnh bảo mật. Người phân tích yêu cầu nên tương tác với các chuyên gia trong lĩnh vực để thu thập yêu cầu và xây dựng kịch bản này.

Bước tiếp theo là phân tích kịch bản ở bước trước để xác định các vấn đề bảo mật tiềm ẩn và mô tả các kịch bản lạm dụng hệ thống để khai thác các lỗ hổng đó. Ví dụ, một người dùng không được phép truy cập để khởi động hệ thống tưới tiêu.

Sau đó, phương pháp áp dụng một tập hợp các quy tắc để ánh xạ các thuộc tính từ kịch bản lạm dụng sang kịch bản kiến trúc bảo mật. Nó sử dụng bốn thuộc tính từ kịch bản lạm dụng (tiêu đề, ngữ cảnh, vai trò và tài nguyên) để điền vào bốn thuộc tính của kịch bản bảo mật (kích hoạt, môi trường, nguồn kích hoạt và thực thể).

Bước cuối cùng là hoàn thiện kịch bản bảo mật thu được từ ánh xạ ở bước trước. Các điều chỉnh và bổ sung thông tin mới cần được thực hiện để nâng cao độ chính xác của kịch bản. Chuyên gia yêu cầu nên sử dụng kinh nghiệm và kiến thức của họ để bổ sung thông tin mới và sửa đổi thông tin đã có.

Cụ thể, kịch bản bảo mật cần được gán một ID để nhận dạng trong quá trình phát triển phần mềm. Các thuộc tính kích hoạt, môi trường, nguồn kích hoạt và thực thể cần được diễn đạt lại để phù hợp hơn. Hai thuộc tính phản ứng và đo lường phản ứng cần được xây dựng hoàn toàn mới, trong đó đo lường phản ứng cần được mô tả bằng các số đo lường định lượng.

Tài liệu cũng trình bày một đánh giá sơ bộ về phương pháp đề xuất. Một khảo sát với 5 chuyên gia an ninh cho thấy phương pháp được đánh giá là hữu ích nói chung, nhưng cần cải thiện ở một số khía cạnh khác nhau.

Các chuyên gia đề xuất rằng phương pháp cần cụ thể hơn về các khía cạnh an ninh mạng, lỗ hổng và rủi ro thường gặp trong hệ thống IoT. Nó cũng nên xem xét đến các loại người dùng và đối tượng tấn công khác nhau. Ngoài ra, phương pháp cần được tương tác nhiều hơn để người dùng có thể ghi nhớ các bước một cách dễ dàng.

Phần tiếp theo của tài liệu mô tả một nguyên mẫu công cụ hỗ trợ phương pháp đề xuất. Công cụ này sử dụng các kỹ thuật xử lý ngôn ngữ tự nhiên để tăng cường mức độ chi tiết của kịch bản sử dụng không chính xác dựa trên k