Yêu cầu Bảo mật (SR) nhấn mạnh việc chủ động xác định các yêu cầu bảo mật của phần mềm, dựa trên mục tiêu kinh doanh cấp cao. Ban đầu, các yêu cầu bảo mật được thu thập qua phân tích cấp độ dự án. Khi tổ chức phát triển, các kỹ thuật nâng cao như kiểm soát truy cập được áp dụng để phát hiện thêm yêu cầu bảo mật mới. Ở mức phức tạp, tổ chức mở rộng các yêu cầu bảo mật này vào quan hệ với nhà cung cấp và tiến hành kiểm tra để đảm bảo mọi dự án đều tuân thủ các yêu cầu bảo mật đã xác định. Ba mục tiêu chính về yêu cầu bảo mật (SR 1, SR 2 và SR 3) cùng với các hoạt động liên quan để đảm bảo bảo mật được tích hợp trong vòng đời phát triển phần mềm:

**SR 1:** Tập trung vào việc xem xét bảo mật trong quá trình xác định yêu cầu phần mềm. Các hoạt động gồm:

(A) xác định yêu cầu bảo mật từ chức năng kinh doanh của phần mềm

(B) đánh giá hướng dẫn bảo mật và tuân thủ để đảm bảo đáp ứng tiêu chuẩn ngành.

**SR 2:** Tăng độ chi tiết của yêu cầu bảo mật dựa trên logic kinh doanh và các rủi ro đã biết. Các hoạt động gồm:

(A) xây dựng ma trận kiểm soát truy cập cho các tài nguyên và khả năng

(B) xác định yêu cầu bảo mật để giảm thiểu các rủi ro bảo mật đã xác định.

**SR 3:** Đặt ra quy trình yêu cầu bảo mật bắt buộc cho tất cả dự án, bao gồm các phụ thuộc bên thứ ba. Các hoạt động gồm:

(A) tích hợp yêu cầu bảo mật vào hợp đồng với nhà cung cấp

(B) mở rộng chương trình kiểm toán để đánh giá liên tục yêu cầu bảo mật.

Đánh giá Yêu cầu Bảo mật tập trung vào mức độ tuân thủ của các nhóm dự án và bên liên quan trong việc thực hiện các yêu cầu bảo mật trong phát triển phần mềm. Mỗi câu hỏi được chấm điểm từ 0.0 đến 1.0, phản ánh mức độ đáp ứng từ "Không" đến "Hầu hết".

* **Yêu cầu bảo mật của nhóm dự án**: Đo lường xem các nhóm dự án có xác định yêu cầu bảo mật từ giai đoạn đầu không, và xác định yêu cầu bảo mật trong quá trình phát triển không (SR 1).
* **Xem xét ma trận kiểm soát truy cập**: Xác định liệu các bên liên quan có xem xét quyền truy cập vào tài nguyên và dữ liệu nhạy cảm thông qua ma trận kiểm soát truy cập (SR 2).
* **Điều chỉnh yêu cầu bảo mật dựa trên phản hồi**: Đánh giá mức độ các nhóm dự án điều chỉnh yêu cầu bảo mật dựa trên phản hồi từ các hoạt động bảo mật khác (SR 2).
* **Xem xét hợp đồng với nhà cung cấp**: Đo lường mức độ xem xét các điều khoản bảo mật trong hợp đồng với nhà cung cấp để đảm bảo tuân thủ (SR 3).
* **Kiểm toán yêu cầu bảo mật**: Xác định tần suất thực hiện kiểm toán yêu cầu bảo mật, từ "Một lần" đến "Hàng năm" đảm bảo yêu cầu bảo mật được duy trì liên tục (SR 3).

**SR1:** **Xem xét bảo mật trong quá trình xác định yêu cầu phần mềm**

**1. Đánh giá yêu cầu bảo mật ban đầu:**

* Dự án có chỉ định các yêu cầu bảo mật trong quá trình phát triển không?
* Các nhóm dự án có lấy yêu cầu từ các thực tiễn tốt nhất và hướng dẫn tuân thủ không?

**A) Xác định yêu cầu bảo mật từ chức năng kinh doanh:**

* **Quy trình**: Xem xét các yêu cầu chức năng của phần mềm để xác định các yêu cầu bảo mật tương ứng. Nếu phần mềm do bên thứ ba phát triển, các yêu cầu này cũng cần được chia sẻ với nhà cung cấp.
* **Vai trò của chuyên viên bảo mật**: Một chuyên viên bảo mật nên dẫn dắt các bên liên quan xác định rõ các yêu cầu bảo mật cho từng yêu cầu chức năng, bao gồm bảo mật dữ liệu, kiểm soát truy cập, tính toàn vẹn giao dịch, mức độ quan trọng của chức năng kinh doanh, phân tách nhiệm vụ, và thời gian hoạt động.
* **Yêu cầu**: Yêu cầu bảo mật phải cụ thể, đo lường được và hợp lý, tuân theo các nguyên tắc chung của việc viết yêu cầu tốt.
* **Ứng dụng**: Áp dụng quy trình này cho tất cả các yêu cầu mới trong các dự án hiện tại. Đối với các tính năng đã có, khuyến nghị thực hiện phân tích lỗ hổng để hỗ trợ nâng cấp bảo mật trong tương lai.

**B) Đánh giá hướng dẫn bảo mật và tuân thủ yêu cầu:**

* **Xác định thực tiễn tốt nhất**: Xác định các thực tiễn tốt nhất của ngành mà các nhóm dự án nên coi như là yêu cầu, có thể lấy từ các hướng dẫn công khai, tiêu chuẩn nội bộ/ngoại bộ, hoặc các quy định tuân thủ hiện hành.
* **Phương pháp tiếp cận**: Không nên đưa quá nhiều yêu cầu thực tiễn tốt nhất vào mỗi chu kỳ phát triển do sẽ ảnh hưởng đến thiết kế và triển khai. Thay vào đó, khuyến nghị bổ sung từ từ các thực tiễn này qua các chu kỳ phát triển kế tiếp để cải thiện dần dần hồ sơ bảo đảm tổng thể của phần mềm.
* **Hệ thống hiện có**: Việc cải thiện bảo mật theo thực tiễn tốt nhất cho hệ thống đã có thể phức tạp. Nên bổ sung các yêu cầu bảo mật khi thêm tính năng mới. Ít nhất, cần phân tích để xác định các thực tiễn tốt nhất có thể áp dụng nhằm hỗ trợ lập kế hoạch cho tương lai.
* **Đội ngũ tham gia**: Đánh giá nên được thực hiện bởi chuyên viên bảo mật với sự tham gia của các bên liên quan kinh doanh. Các lập trình viên cao cấp, kiến trúc sư, và các bên liên quan kỹ thuật khác cũng nên tham gia để đóng góp kiến thức chuyên môn về thiết kế và triển khai vào quá trình ra quyết định.

**Kết quả (Results):**

1. **Liên kết với rủi ro kinh doanh:** Phát triển phần mềm được đồng bộ hóa với các rủi ro kinh doanh tổng thể, thiết lập yêu cầu bảo mật dựa trên mức độ ưu tiên và rủi ro.
2. **Thực tiễn tốt nhất của ngành:** Yêu cầu bảo mật rõ ràng được xác định dựa trên các thực tiễn tốt nhất, đảm bảo tuân thủ các tiêu chuẩn bảo mật hàng đầu.
3. **Nhận thức của các bên liên quan:** Tăng cường nhận thức và cam kết của các bên liên quan về các biện pháp giảm thiểu rủi ro phần mềm.

**Tỷ lệ thành công (Success Metrics):**

* Hơn 50% nhóm dự án có yêu cầu bảo mật rõ ràng, cho thấy tỷ lệ cao các dự án được triển khai với tiêu chuẩn bảo mật cụ thể.

**Chi phí (Costs):**

* Việc bổ sung yêu cầu bảo mật vào chu kỳ phát triển dẫn đến chi phí gia tăng do đầu tư thời gian và nguồn lực cho kiểm tra và đảm bảo tuân thủ.

**Nhân sự tham gia (Personnel):**

* **Chuyên viên bảo mật**
* **Chủ sở hữu doanh nghiệp**
* **Quản lý và Kiến trúc sư**

**Các cấp độ liên quan (Related Levels):**

1. **Đào tạo & Hướng dẫn:** Cung cấp đào tạo về bảo mật cho đội ngũ.
2. **Chính sách & Tuân thủ:** Xây dựng và đảm bảo tuân thủ các chính sách bảo mật.
3. **Đánh giá Thiết kế và Triển khai:** Đánh giá bảo mật trong thiết kế và triển khai.
4. **Kiểm tra Bảo mật:** Thực hiện kiểm tra bảo mật cho sản phẩm cuối để đảm bảo tuân thủ yêu cầu bảo mật.

**SR2: Đưa ra các yêu cầu bảo mật chi tiết hơn dựa trên yêu cầu doanh nghiệp và những rủi ro đã biết**

**Đánh giá yêu cầu bảo mật ban đầu**

* Các bên liên quan đã kiểm tra lại quyền kiểm soát truy cập của các dự án chưa?
* Các nhóm xây dựng dự án có xác định yêu cầu dựa trên phản hồi từ các hoạt động liên quan bảo mật khác hay không?

**A. Tạo ma trận kiểm soát truy cập cho tài nguyên và chức năng**

* Dựa trên mục tiêu kinh doanh của ứng dụng, xác định các vai trò của người dùng và người quản lý. Sau đó, lập danh sách các tài nguyên và chức năng của ứng dụng có áp dụng kiểm soát truy cập.
* Trong ma trận đơn giản có vai trò ở một trục và tài nguyên ở trục còn lại, xác định mối quan hệ giữa mỗi vai trò với từng tài nguyên. Tại mỗi điểm giao nhau, ghi chú cách hệ thống nên xử lý quyền truy cập theo yêu cầu của các bên liên quan. Đối với dữ liệu, ghi rõ quyền tạo, đọc, cập nhật và xóa. Đối với chức năng, ít nhất cần ghi nhận vai trò nào được phép sử dụng.
* Ma trận này sẽ là tài liệu xác nhận quyền truy cập phù hợp với logic kinh doanh của hệ thống. Nhóm dự án sẽ tạo ra ma trận này từ ý kiến của các bên liên quan và cập nhật trước mỗi lần phát hành, thường là vào đầu giai đoạn thiết kế.

**B. Xác định yêu cầu bảo mật dựa trên rủi ro đã biết**

* Xem xét kỹ các tài liệu hiện có để nắm rõ các rủi ro bảo mật đặc thù của tổ chức hoặc dự án, giúp hiểu rõ rủi ro tổng quan cho phần mềm. Nếu có thể, tham khảo các tài liệu như hồ sơ rủi ro kinh doanh, mô hình các mối đe dọa của ứng dụng, kết quả đánh giá thiết kế, đánh giá mã nguồn, kiểm thử bảo mật, v.v.
* Ngoài ra, sử dụng các kịch bản tấn công mẫu để xác định các yêu cầu bảo mật cụ thể, giúp giảm thiểu nguy cơ bị khai thác.
* Quy trình này nên được thực hiện bởi chủ sở hữu doanh nghiệp và kiểm toán viên bảo mật khi cần. Về lâu dài, việc xác định rủi ro và thêm yêu cầu bảo mật mới nên trở thành một phần của giai đoạn lập kế hoạch, để nhóm dự án có thể đánh giá kỹ càng các rủi ro mới phát hiện.

**Kết quả:**

* Hiểu rõ hơn về các tình huống tấn công vào logic kinh doanh.
* Ưu tiên phát triển các tính năng bảo mật dựa trên các mối đe dọa tiềm tang
* Quyết định tốt hơn khi cân nhắc giữa tính năng và bảo mật
* Các bên liên quan sẽ tránh được các yêu cầu chức năng có lỗ hổng bảo mật

**Tỷ lệ thành công**

* Hơn 75% các dự án có mô hình tình huống lạm dụng được cập nhật trong sáu tháng qua

**Chi phí**

* Chi phí phát sinh trong việc xây dựng và duy trì mô hình tình huống lạm dụng

**Nhân sự Tham gia**

* Kiểm toán viên bảo mật
* Quản lý
* Kiến trúc sư
* Chủ sở hữu doanh nghiệp

**Các cấp độ Liên quan**

* Đánh giá mối đe dọa - Cấp 1 & 3
* Chiến lược & Chỉ số - Cấp 1

**SR3: Yêu cầu quy trình bảo mật bắt buộc đối với tất cả các dự án phần mềm và các thành phần của bên thứ ba**

**1. Đánh giá yêu cầu bảo mật ban đầu:**

* Các bên liên quan có xem xét các thỏa thuận của nhà cung cấp về các yêu cầu bảo mật không?
* Có tiến hành kiểm toán theo các yêu cầu bảo mật do nhóm dự án chỉ định không?

**A) Bổ sung các yêu cầu bảo mật vào thỏa thuận với nhà cung cấp**

**1. Khai thác lợi ích bảo mật từ thỏa thuận bên thứ ba:**

- Ngoài các yêu cầu bảo mật đã xác định từ trước, có thể khai thác thêm lợi ích bảo mật từ các thỏa thuận với bên thứ ba.

**2. Phân công công việc giữa nội bộ và nhà cung cấp:**

- Yêu cầu và thiết kế cấp cao thường được phát triển nội bộ.

- Thiết kế chi tiết và triển khai thường được giao cho nhà cung cấp.

**3. Xác định hoạt động bảo mật cụ thể:**

- Xác định các hoạt động bảo mật và tiêu chí đánh giá kỹ thuật cho từng thành phần do bên ngoài phát triển.

- **Các hoạt động bảo mật phổ biến:**

+ Đánh giá thiết kế

+ Đánh giá mã nguồn

+ Quy trình kiểm tra bảo mật.

**5. Điều chỉnh nội dung thỏa thuận cho từng nhà cung cấp:**

- Điều chỉnh nội dung trong thỏa thuận cho từng nhà cung cấp tùy vào tình huống cụ thể, vì việc thêm yêu cầu bảo mật sẽ tăng chi phí.

**6. Cân nhắc chi phí và lợi ích của hoạt động bảo mật:**

- Cân nhắc chi phí của mỗi hoạt động bảo mật so với lợi ích của hoạt động đó dựa trên thành phần hoặc hệ thống đang được sử dụng.

**B) Mở rộng chương trình kiểm toán cho các yêu cầu bảo mật:**

**1. Mở rộng chương trình kiểm toán bảo mật:**

- Tích hợp kiểm tra tính đầy đủ của các yêu cầu bảo mật vào các cuộc kiểm toán dự án định kỳ.

**2. Kiểm tra tài liệu dự án:**

- Kiểm tra các tài liệu như yêu cầu và thiết kế để xác minh rằng phân tích bảo mật phù hợp đã được thực hiện.

**3. Chú thích yêu cầu chức năng với bảo mật:**

- Mỗi yêu cầu chức năng cần có chú thích yêu cầu bảo mật dựa trên:

+ Động lực kinh doanh

+ Các kịch bản tấn công

**4. Yêu cầu bảo mật tổng thể của dự án**

- Yêu cầu tổng thể của dự án nên bao gồm danh sách các yêu cầu bảo mật từ hướng dẫn và tiêu chuẩn tốt nhất.

**5. Danh sách các yêu cầu bảo mật chưa hoàn thành**

- Lập danh sách các yêu cầu bảo mật chưa thực hiện và thời gian dự kiến hoàn thành trong các phiên bản tiếp theo.

**6. Thời điểm thực hiện kiểm toán**

- Kiểm toán bảo mật nên được thực hiện ở mỗi lần phát triển lặp lại, tốt nhất là cuối quá trình yêu cầu và trước khi phát hành sản phẩm.

**Kết quả (Results):**

1. Thiết lập mức chuẩn cho các yêu cầu bảo mật đối với mã nguồn từ bên ngoài.
2. Tập trung các thông tin về nỗ lực bảo mật do mỗi nhóm dự án thực hiện.
3. Khả năng phân bổ tài nguyên cho các dự án dựa trên rủi ro của ứng dụng và yêu cầu bảo mật mong muốn.

**Tỷ lệ thành công (Success Metrics):**

- Hơn 80% dự án vượt qua kiểm toán yêu cầu bảo mật trong 6 tháng qua.

- Hơn 80% thỏa thuận với nhà cung cấp được phân tích về các yêu cầu bảo mật trong hợp đồng trong 12 tháng qua.

**Chi phí (Costs):**

- Chi phí tăng thêm do phát triển bên ngoài với các yêu cầu bảo mật bổ sung.

- Chi phí phát sinh trong quá trình do các bước kiểm tra bảo mật trước khi phát hành.

**Nhân sự tham gia (Personnel):**

- Kiểm toán viên bảo mật

- Quản lý

- Chủ doanh nghiệp

**Các cấp độ liên quan**

- Đánh giá mối đe dọa - Cấp 3

- Chính sách & Tuân thủ - Cấp 2