1. TÓM TẮT QUY TRÌNH

1.1 Các hoạt động chính

1.1.1 Quy trình quản lý lỗ hổng gồm các hoạt động chính

1.1.1.1. Quy trình quản lý lỗ hổng rà quét

- Rà quét lỗ hổng;
- Lập kế hoạch xử lý lỗ hổng;
- Xử lý lỗ hổng;
- Trình ký báo cáo lỗ hổng ATTT và kết thúc.

1.1.1.2. Quy trình quản lý lỗ hổng pentest

- Kiểm tra đánh giá ATTT lỗ hổng-pentest;
- Tạo request trên ITSM;
- Lập kế hoạch xử lý lỗ hổng,
- Trường hợp cần xử lý lỗ hổng tạm thời cần theo dõi bảng rủi ro ATTT;
- Lập biên bản ATTT;
- Đóng request.

1.1.1.3. Quy trình quản lý lỗ hổng Threat Intelligence

- Thông tin nguy cơ ATTT từ nguồn Threat Intelligence;
- Kiểm tra sản phẩm, dịch vụ, IP;
- Tạo request trên ITSM;
- Trường hợp ảnh hưởng sản phẩm, dịch vụ, IP khách hàng thông báo khách hàng và kết thúc;
- Trường hợp ảnh hưởng sản phẩm, dịch vụ, IP nội bộ phân tích, đánh giá, lên
- phương án xử lý lỗ hổng;
- Lập kế hoạch xử lý lỗ hổng;
- Trường hợp cần xử lý lỗ hổng tạm thời cần theo dõi bảng rủi ro ATTT:

1.1.2 Quy trình cập nhật bản vá gồm các hoạt động chính:

- Thông tin về bản vá;
- Thông báo các bên liên quan;

- Lập kế hoạch cập nhật bản vá;
- Tiến hành cập nhật bản vá;
- Lập báo cáo và lưu thông tin.

2. VAI TRÒ THAM GIA

2.1 Quy trình quản lý lỗ hổng

2.1.1 Quy trình quản lý lỗ hổng và rà quét

Tên vai trò	Các nhiệm vụ trong quy trình
Team ATTT	Rà quét lỗ hổng
	Thông báo lỗ hổng cho SO
	Kiểm tra lại lỗ hổng
	Lập kế hoạch xử lý lỗ hổng
	Tổng hợp
SO	Lập kế hoạch xử lý lỗ hổng
	Tiến hành xử lý lỗ hổng
Ban lãnh đạo	Phê duyệt kế hoạch xử lý lỗ hổng

2.1.2 Quy trình quản lý lỗ hổng pentest

Tên vai trò	Các nhiệm vụ trong quy trình
Team ATTT	Lập kê hoạch trên ITSM
	Kiêm tra, đánh giá ATTT - Pentest
	Viêt báo cáo ATTT
	Tạo yêu cầu
	Kiểm tra lại lỗ hổng
	Biên bản ATTT
	Đóng request
SO	Phát triển hệ thống mới/tính năng mới

	Chuẩn bị môi trường thử nghiệm
	Lập kế hoạch xử lý lỗ hổng
	Cập nhật tiến độ request
	Tiến hành xử lý lỗ hổng
	Theo dõi rủi ro ATTT
Ban lãnh đạo	Phê duyệt kế hoạch xử lý lỗ hổng

2.1.3 Quy trình quản lý lỗ hổng threat intelligence

Tên vai trò	**Các nhiệm vụ trong quy trình**
Team ATTT	Nguy cơ ATTT từ các nguồn TI
	Kiểm tra sản phẩm, dịch vụ, IP
	Phân tích đánh giá lên phương án xử lý lỗ hổng
	Tạo yêu cầu
	Kiểm tra lại lỗ hổng
	Đóng request
SO	Lập kế hoạch xử lý lỗ hổng tạm thời
	Tiến hành xử lý lỗ hổng tạm thời
	Lập kế hoạch xử lý lỗ hổng
	Cập nhật tiến độ request
	Tiến hành xử lý lỗ hổng
Ban lãnh đạo	Phê duyệt kế hoạch xử lý lỗ hổng
Chăm sóc KH	Thông báo cho khách hàng

2.1.4 Quy trình cập nhật bản vá

Tên vai trò	**Các nhiệm vụ trong quy trình**
Team ATTT	Tiếp nhận thông tin về bản vá ATTT

	Gửi yêu cầu cập nhật bản vá cho SO
	Kiêm tra lại sau khi cập nhật bản vá
	Báo cáo và lưu thông tin
SO	Lập kế hoạch cập nhật bản vá
	Tiến hành cập nhật bản vá
Ban lãnh đạo	Phê duyệt kế hoạch xử lý lỗ hổng
Chăm sóc KH	Thông báo cho khách hàng

3. Ranh giới quy trình

3.1 Sự kiện bắt đầu và sự kiện kết thúc quy trình

- **Sự kiện bắt đầu:** Khi có lỗ hổng ATTT được cảnh bảo hoặc được nhận diện trên các hệ thống thông tin, hệ thống mạng, thiết bị, ứng dụng, nghiệp vụ, người dùng có thể dẫn đến các nguy cơ gây ra sự cố ATTT
- **Sự kiện kết thúc: Khi** lỗ hổng ATTT được xử lý tạm thời hoặc triệt để.

3.2 Đầu vào và đầu ra của quy trình

3.2.1 Quy trình quản lý lỗ hổng

a. Đầu vào: Khi có lỗ hổng ATTT được nhận diện theo các tình huống sau:

Các dấu hiệu bất thường xác định là các lỗ hổng ATTT thông qua kiểm tra trực tiếp hoặc các cảnh báo từ công cụ giám sát hay công cụ rà quét lỗ hổng.

Kết quả của việc rà quét, đánh giá ATTT các thiết bị, HTTT.

b. Đầu ra: Lỗ hổng ATTT được xử lý, kèm theo các yêu cầu ầu sau khi xử lý gồm:

Thông tin xử lý chuyển sang QT quản lý rủi ro nếu lỗ hổng chưa được fix hay chưa được xử lý triệt để. chr

Kết quả của việc thay đổi, tác động hệ thống nhằm khắc phục lỗ hổng ATTT.

3.2.2 Quy trình cập nhật bản vá

a. Đầu vào: Khi có thông tin về bản vá cần cập nhật

b. Đầu ra: Các hệ thống, ứng dụng được cập nhật bản vá mới nhất.

4. Giải thích thuật ngữ, định nghĩa, khái niệm và từ viết tắt

4.1 Giải thích thuật ngữ, định nghĩa, khái niệm

- Lỗ hổng bảo mật: Là điểm yếu có thể bị sử dụng để thực hiện khai thác, tấn công đe dọa an toàn thông tin (ATTT) của hệ thống thông tin.
- Lỗ hổng mức NGHIÊM TRỌNG (critical): Là các lỗ hổng được các tổ chức, các nhà phát triển hệ thống đánh giá ở mức nghiêm trọng. Các lỗ hổng mức nghiêm trọng có thể dẫn tới mất mát dữ liệu, có khả năng gây thiệt hại lớn, có ảnh hưởng trên diện rộng, tạo điều kiện thuận lợi cho tin tặc chiếm quyền điều khiển xâm nhập trái phép vào hệ thống.
- Lỗ hổng mức CAO (high): Là các lỗ hổng được các tổ chức, các nhà phát triển hệ thống đánh giá ở mức cao. Các lỗ hổng mức cao có thể dẫn tới mất mát dữ liệu, ngưng hoạt động, có khả năng gây thiệt hại, tạo điều kiện cho tin tặc chiếm quyền điều kiển máy chủ.
- Lỗ hổng mức TRUNG BÌNH (medium) và mức THẤP (low): Là các lỗ hổng được các tổ chức, các nhà phát triển hệ th thông đánh 9:5-ở mức trung bình và xay ra, khả năng gây thiệt hại và ảnh mức thấp. Các lỗ hổng này ít có khả năng xảy ra, khả hưởng không đáng kể, không có khả năng tạo điều kiện cho tin tặc chiếm quyền điều khiển máy chủ.
- SO): cá nhân hoặc một nhóm được - Người quản trị hệ thông (System Ownerky, giao trách nhiệm quản lí hệ thống, bao gồm: phát triển, triển khai, duy trì, VHKT, nâng cấp, mở rộng và bảo vệ hệ thống.
- Hệ thống thông tin: Hệ thống thông tin là tập hợp phần cứng, phần mềm và cơ sở dữ liệu được thiết lập phục vụ mục đích tạo lập, cung cấp, truyền đưa, thu thập, xửlý, lưu trữ và trao đổi thông tin trên mạng (Theo khoản 3 Điều 3 Luật An toàn Thông tin mạng số 86/2015/QH13).