BỘ THÔNG TIN VÀ TRUYỀN THÔNG	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
-------	Độc lập - Tự do - Hạnh phúc

Số: 1126/QĐ-BTTTT	*Hà Nội, ngày 30 tháng 07 năm 2021*

QUYẾT ĐỊNH

BAN HÀNH YÊU CẦU KỸ THUẬT CƠ BẢN ĐỐI VỚI SẢN PHẨM TƯỜNG LỬA ỨNG DỤNG WEB

BỘ TRƯỞNG BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Theo đề nghị của Cục trưởng Cục An toàn thông tin.

QUYẾT ĐỊNH:

Điều 1. Ban hành kèm theo Quyết định này Yêu cầu kỹ thuật cơ bản đối với sản phẩm Tường lửa ứng dụng web (WAF).

Điều 2. Khuyến nghị cơ quan, tổ chức nghiên cứu, phát triển, lựa chọn, sử dụng sản phẩm WAF đáp ứng các yêu cầu kỹ thuật cơ bản theo Điều 1 Quyết định này.

Điều 3. Cục An toàn thông tin chủ trì, phối hợp với các cơ quan, tổ chức liên quan hướng dẫn việc áp dụng các yêu cầu trong Yêu cầu kỹ thuật cơ bản đối với sản phẩm WAF tại Điều 1 Quyết định này.

Điều 4. Quyết định này có hiệu lực thi hành kể từ ngày ký.

Điều 5. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Thủ trưởng các đơn vị thuộc Bộ, các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

KT. BỘ TRƯỞNG
THỨ TRƯỞNG

Nơi nhận:
- Như Điều 5;
- Bộ trưởng (để b/c);
- Các Thứ trưởng;
- Cổng thông tin điện tử của Bộ;
- Lưu: VT, CATTT.

Nguyễn Huy Dũng

YÊU CẦU KỸ THUẬT CƠ BẢN

ĐỐI VỚI SẢN PHẨM TƯỜNG LỬA ỨNG DỤNG WEB

(Kèm theo Quyết định số 1126/QĐ-BTTTT ngày 30 tháng 07 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

I. THÔNG TIN CHUNG

1. Phạm vi áp dụng

Tài liệu này đưa ra các yêu cầu kỹ thuật cơ bản với sản phẩm Tường lửa ứng dụng web (WAF), bao gồm các nhóm yêu cầu là Yêu cầu về tài liệu, Yêu cầu về quản trị hệ thống, Yêu cầu về kiểm soát lỗi, Yêu cầu về log, Yêu cầu về hiệu năng xử lý, Yêu cầu về chức năng tự bảo vệ, Yêu cầu về chức năng bảo vệ ứng dụng web.

2. Đối tượng áp dụng

Các cơ quan, tổ chức có liên quan đến hoạt động nghiên cứu, phát triển; đánh giá, lựa chọn sản phẩm Tường lửa ứng dụng web khi đưa vào sử dụng trong các hệ thống thông tin.

3. Khái niệm và thuật ngữ

3.1. Tập luật bảo vệ

Danh sách các luật bao gồm các tham số, quy tắc được định nghĩa và thiết lập bởi quản trị viên dùng, cho phép sản phẩm phát hiện, cảnh báo những sự kiện, nguy cơ, sự cố và các hành vi gây mất an toàn thông tin khác đối với các đối tượng, hệ thống được bảo vệ.

3.2. Nhật ký hệ thống (log)

Sự kiện an toàn thông tin được hệ thống ghi lại liên quan đến trạng thái hoạt động, thông báo, cảnh báo, sự cố, cuộc tấn công và các thông tin khác liên quan đến hoạt động của hệ thống (nếu có).

3.3. Thời gian duy trì phiên kết nối (session timeout)

Khoảng thời gian được thiết lập để cho phép hệ thống hủy phiên kết nối đối với một máy khách, nếu trong khoảng thời gian này mà hệ thống không nhận được yêu cầu mới từ máy khách đó.

3.3. Mã hóa/giải mã ký tự (character encoding/decoding)

Việc phiên dịch bộ ký tự của ngôn ngữ tự nhiên được sử dụng bởi con người sang dạng ký tự nhị phân của máy tính và ngược lại.

3.4. Chức năng bỏ qua kiểm soát (fail open)

Chức năng cho phép WAF bỏ qua các biện pháp kiểm soát theo tập luật bảo vệ khi có sự cố xảy ra.

II. YÊU CẦU CƠ BẢN

1. Yêu cầu về tài liệu

WAF có tài liệu bao gồm các nội dung sau:

a) Hướng dẫn cài đặt và thiết lập cấu hình;

b) Hướng dẫn sử dụng và quản trị.

2. Yêu cầu về quản trị hệ thống

2.1. Quản lý vận hành

WAF cho phép quản lý vận hành đáp ứng các yêu cầu sau:

a) Cho phép thiết lập, thay đổi, áp dụng và hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

b) Cho phép thay đổi thời gian hệ thống;

c) Cho phép thay đổi thời gian duy trì phiên kết nối;

d) Cho phép thiết lập, thay đổi các tham số giới hạn đối với kết nối quản trị từ xa (ví dụ: giới hạn địa chỉ IP, giới hạn số phiên kết nối quản trị từ xa đồng thời,…);

đ) Cho phép đăng xuất tài khoản người dùng có phiên kết nối còn hiệu lực;

e) Cho phép tìm kiếm dữ liệu log bằng từ khóa để xem lại;

g) Cho phép xóa log;

h) Cho phép xem thời gian hệ thống chạy tính từ lần khởi động gần nhất.

2.2. Quản trị từ xa

WAF cho phép quản trị từ xa an toàn đáp ứng các yêu cầu sau:

a) Sử dụng giao thức có mã hóa như TLS hoặc tương đương;

b) Tự động đăng xuất tài khoản và hủy bỏ phiên kết nối quản trị từ xa khi hết thời gian duy trì phiên kết nối.

2.3. Quản lý xác thực và phân quyền

WAF cho phép quản lý cấu hình tài khoản xác thực và phân quyền người dùng đáp ứng các yêu cầu sau:

a) Hỗ trợ phương thức xác thực bằng tài khoản - mật khẩu, trong đó, quản trị viên có thể thiết lập và thay đổi được độ phức tạp của mật khẩu;

b) Hỗ trợ phân nhóm tài khoản tối thiểu theo 02 nhóm là quản trị viên và người dùng thường với những quyền hạn cụ thể đối với từng nhóm.

2.4. Quản lý báo cáo

WAF cho phép quản lý báo cáo thông qua giao diện đồ họa đáp ứng các yêu cầu sau:

a) Cho phép tạo mới, xem lại và xóa báo cáo đã được tạo;

b) Cho phép tạo báo cáo mới theo các mẫu báo cáo đã được định nghĩa trước;

c) Cho phép áp dụng các quy tắc tìm kiếm thông tin, dữ liệu log để thêm, lọc, tinh chỉnh nội dung cho báo cáo;

d) Cho phép lựa chọn định dạng tệp tin báo cáo xuất ra đáp ứng tối thiểu 02 trong các định dạng sau: WORD, EXCEL, PDF, HTML, XML;

đ) Cho phép tải về tệp tin báo cáo đã được xuất ra.

2.5. Quản lý tập luật bảo vệ

WAF cho phép quản lý tập luật bảo vệ bao gồm các thao tác sau:

a) Thêm luật mới;

b) Tinh chỉnh luật;

c) Tìm kiếm luật;

d) Xóa luật;

đ) Kích hoạt/vô hiệu hóa luật;

e) Xuất tập luật ra tệp tin;

g) Khôi phục tập luật từ tệp tin;

h) Cập nhật tập luật được phát hành bởi nhà sản xuất.

2.6. Cập nhật tập luật bảo vệ

WAF cho phép cập nhật tập luật bảo vệ đáp ứng các yêu cầu sau:

a) Cho phép tự động thông báo có bản cập nhật mới cho quản trị viên;

b) Cho phép tải về trực tuyến và áp dụng thủ công bản cập nhật mới.

3. Yêu cầu về kiểm soát lỗi

3.1. Bảo vệ cấu hình

Trong trường hợp WAF phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), WAF đảm bảo các loại cấu hình sau mà đang được áp dụng phải được lưu lại và không bị thay đổi trong lần khởi động kế tiếp:

a) Cấu hình hệ thống;

b) Cấu hình quản trị từ xa;

c) Cấu hình tài khoản xác thực và phân quyền người dùng;

d) Cấu hình tập luật bảo vệ.

3.2. Bảo vệ dữ liệu log

Trong trường hợp WAF phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), WAF đảm bảo dữ liệu log đã được lưu lại phải không bị thay đổi trong lần khởi động kế tiếp.

3.3. Đồng bộ thời gian hệ thống

Trong trường hợp WAF phải khởi động lại do có lỗi phát sinh (ngoại trừ lỗi phần cứng), WAF đảm bảo thời gian hệ thống phải được đồng bộ tự động đến thời điểm hiện tại.

3.4. Khả năng chịu lỗi vận hành

Trong trường hợp WAF gặp lỗi trong quá trình thực thi tập luật bảo vệ mà không thể tự động khắc phục được, WAF phải cho phép tự động kích hoạt chức năng bỏ qua kiểm soát và cho phép quản trị viên kích hoạt thủ công chức năng này.

4. Yêu cầu về log

4.1. Log quản trị hệ thống

a) WAF cho phép ghi log quản trị hệ thống về các loại sự kiện sau:

i) Đăng nhập, đăng xuất tài khoản;

ii) Xác thực trước khi cho phép truy cập vào tài nguyên, sử dụng chức năng của hệ thống;

iii) Áp dụng, hoàn tác sự thay đổi trong cấu hình hệ thống, cấu hình quản trị từ xa, cấu hình tài khoản xác thực và phân quyền người dùng, cấu hình tập luật bảo vệ;

iv) Kích hoạt lệnh khởi động lại, tắt hệ thống;

v) Thay đổi thủ công thời gian hệ thống.

b) WAF cho phép ghi log quản trị hệ thống có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy trạm;

iii) Định danh của tác nhân (ví dụ: tài khoản người dùng, tên hệ thống,…);

iv) Thông tin về hành vi thực hiện (ví dụ: đăng nhập, đăng xuất, thêm, sửa, xóa, cập nhật, hoàn tác,…);

v) Kết quả thực hiện hành vi (thành công hoặc thất bại).

vi) Lý do giải trình đối với hành vi thất bại (ví dụ: không tìm thấy tài nguyên, không đủ quyền truy cập,…).

4.2. Log chức năng bảo vệ ứng dụng web

a) WAF cho phép ghi log chức năng bảo vệ ứng dụng web về các loại sự kiện sau:

i) Truy cập vào tài nguyên của ứng dụng web được bảo vệ;

ii) Cảnh báo được sinh ra bởi việc thực thi tập luật bảo vệ.

b) WAF cho phép ghi log chức năng bảo vệ ứng dụng web có các trường thông tin sau:

i) Thời gian sinh log (bao gồm năm, tháng, ngày, giờ, phút và giây);

ii) Địa chỉ IP hoặc định danh của máy nguồn;

iii) Địa chỉ IP hoặc định danh của máy đích;

iv) Số hiệu cổng nguồn;

v) Số hiệu cổng đích;

vi) Tên giao thức (HTTP hoặc HTTPS);

vii) Đường dẫn và danh sách tham số của URL;

viii) Phương thức truy vấn (ví dụ: GET, POST, HEAD,…);

ix) Mã trạng thái phản hồi (ví dụ: 200, 404,…);

x) Cách thức xử lý của luật bảo vệ khi có cảnh báo được sinh ra (ví dụ: từ chối khởi tạo kết nối, hủy kết nối hiện hành, điều hướng kết nối đến máy chủ khác,…).

xi) Lý do giải trình đối với cách thức xử lý của luật bảo vệ.

4.3. Định dạng log

WAF cho phép chuẩn hóa log theo tối thiểu 01 định dạng đã được định nghĩa trước để truyền dữ liệu log cho các phần mềm quản lý, phân tích, điều tra log.

4.4. Quản lý log

WAF cho phép quản lý log đáp ứng các yêu cầu sau:

a) Cho phép thiết lập và cấu hình các cài đặt liên quan đến lưu trữ và hủy bỏ log (ví dụ: ngưỡng giới hạn dung lượng lưu trữ, khoảng thời gian lưu trữ,…).

b) Cho phép tìm kiếm log theo từ khóa trên tất cả các trường thông tin bao gồm cả các trường thông tin cấp thấp hơn (nếu có);

c) Cho phép xuất dữ liệu log ra để phục vụ cho việc tích hợp các dữ liệu này vào SIEM hoặc giải pháp khác về quản lý, phân tích, điều tra log.

4.5. Kiểm soát thông tin trong log

WAF cho phép kiểm soát và che dấu các thông tin bí mật được thể hiện trong log như mật khẩu, mã xác thực một lần OTP và các loại giá trị bí mật khác dùng trong quá trình xác thực.

5. Yêu cầu về hiệu năng xử lý

WAF được triển khai thỏa mãn cấu hình tối thiểu theo hướng dẫn cài đặt và thiết lập cấu hình của nhà sản xuất đảm bảo đáp ứng các yêu cầu sau:

5.1. Đối với giao thức HTTP

a) Duy trì lên đến 30.000 kết nối trung bình mỗi giây;

b) Duy trì lên đến 20.000 phiên kết nối liên tục đồng thời;

c) Duy trì độ trễ trung bình gửi yêu cầu không quá 3 mili giây.

5.2. Đối với giao thức HTTPS

a) Duy trì lên đến 20.000 kết nối TLS/SSL trung bình mỗi giây;

b) Duy trì lên đến 14.000 phiên kết nối TLS/SSL liên tục đồng thời;

c) Duy trì độ trễ trung bình gửi yêu cầu không quá 5 mili giây.

5.3. Đối với việc áp dụng các sự thay đổi trong cấu hình tập luật bảo vệ

WAF cho phép áp dụng các sự thay đổi trong cấu hình tập luật bảo vệ mà không làm gián đoạn hoạt động của các ứng dụng web được bảo vệ quá 10 giây.

6. Yêu cầu về chức năng tự bảo vệ

6.1. Phát hiện và ngăn chặn tấn công hệ thống

WAF có khả năng tự bảo vệ, ngăn chặn các dạng tấn công phổ biến sau vào giao diện ra bên ngoài của hệ thống, bao gồm tối thiểu các dạng sau:

a) SQL Injection;

b) OS Command Injection;

c) XPath Injection;

d) Remote File Inclusion (RFI);

đ) Local File Inclusion (LFI);

e) Cross-Site Scripting (XSS);

g) Cross-Site Request Forgery (CSRF).

6.2. Cập nhật bản vá hệ thống

WAF cho phép cập nhật bản vá để xử lý các điểm yếu, lỗ hổng bảo mật của hệ thống mà đã được công bố.

7. Yêu cầu về chức năng bảo vệ ứng dụng web

7.1. Phát hiện và ngăn chặn tấn công ứng dụng web được bảo vệ

WAF có khả năng ngăn chặn tối thiểu các dạng tấn công phổ biến sau vào các ứng dụng web được bảo vệ:

a) SQL Injection;

b) OS Command injection;

c) XPath Injection;

d) Brute-force;

e) Remote File Inclusion (RFI);

f) Local File Inclusion (LFI);

g) Cross-Site Scripting (XSS);

h) Cross-Site Request Forgery (CSRF).

7.2. Cơ chế thực thi bảo vệ

WAF cho phép phát hiện và ngăn chặn tấn công thông qua tối thiểu 02 trong các cơ chế thực thi sau:

a) Cơ chế dựa trên phân tích tập luật bảo vệ;

b) Cơ chế dựa trên phân tích thông tin về hành vi truy cập ứng dụng web;

c) Cơ chế dựa trên phát hiện và sửa đổi thông tin có nội dung độc hại trên URL của gói tin yêu cầu gửi đến ứng dụng web.

7.3. Che giấu thông tin về ứng dụng web được bảo vệ

WAF cho phép che giấu các thông tin về hệ điều hành máy chủ, kiến trúc nền tảng web,… của ứng dụng web được bảo vệ.

7.4. Hỗ trợ giao thức TLS/SSL

Đối với các giao dịch của ứng dụng web có sử dụng giao thức HTTPS, WAF cho phép sử dụng các phiên bản giao thức có mã hóa TLS/SSL.

7.5. Tùy biến cấu hình tập luật bảo vệ theo đối tượng

WAF cho phép tùy biến và áp dụng cấu hình tập luật bảo vệ theo từng ứng dụng web cụ thể được bảo vệ.

7.6. Thiết lập cấu hình giao thức

WAF cho phép thiết lập cấu hình giao thức đáp ứng các yêu cầu sau:

a) Cấu hình hỗ trợ giao thức ứng dụng web HTTP/HTTPS;

b) Cấu hình phương pháp mã hóa/giải mã ký tự;

c) Thiết lập các tham số của giao thức (ví dụ: giới hạn kích thước gói tin yêu cầu, giới hạn kích thước gói tin phản hồi, giới hạn độ dài phần tiêu đề của gói tin,…).