**Bài kiểm tra** – môn ATTT

SV được phép tham khảo tài liệu

**Họ tên: Bùi Lê Thủy Tiên**

**Mssv: 22162048**

**Câu 1.** (3 điểm) Malware là gì? Trình bày đặc điểm của một số loại malware phổ biến. Giải pháp phòng chống malware trong một hệ thống CNTT?

- Malware là một tập các câu lệnh chạy trên máy tính của bạn và làm cho hệ thống máy tính thực hiện việc gì đó mà người tấn công mong muốn.

- Một số loại malware nổi tiếng và đặc điểm của chúng là:

*Virus*: là một malware human-assisted propagation, tức là một malware nhân rộng dưới sự trợ giúp của con người (tức là chúng ta tự tay khởi động nó); nó là một đoạn mã tự chèn vào máy chủ, bao gồm cả hệ điều hành, để lây lan. Nó không thể chạy độc lập. Nó yêu cầu chương trình máy chủ của nó phải được chạy để kích hoạt nó. Bốn giai đoạn của virus: dormant phase, propagation phase, triggering phase, triggering phase, excution phase.

*Worms*: là một malware có thể tự động nhân bản mà không cần đến sự trợ giúp của con người; sâu máy tính là một chương trình phần mềm độc hại phát tán các bản sao của chính nó mà không cần phải tiêm vào các chương trình khác và thường không có sự tương tác của con người. Trong phần lớn các trường hợp, sâu sẽ mang cac malicous payload, như là xóa file or installing backdoor. Sâu thường sử dụng kết nối Internet hoặc mạng cục bộ (LAN) của tổ chức nạn nhân để phát tán. Một số cách lây lan sâu máy tính phổ biến nhất bao gồm: email, mạng, lỗ hổng hệ thống, chia sẻ tệp (peer-to-peer) ,nhắn tin ….

*Trojan Horse:* là một malware khiến người dùng lầm tưởng đây là một đoạn chương trình có ích nhưng lại tiềm tàng 1 số chức năng mà người dùng không thấy (something malicous).

*Spyware*: Là phần mềm gián điệp, được thiết kế để thu thập thông tin người dùng mà không được sự đồng ý, chẳng hạn như số tài khoản, mật khẩu và bán lên chợ đen.

*Ransomware:* là một loại malware dùng để khóa và mã hóa dự liệu của người dùng, người tấn công ransomware sẽ yêu cầu thanh toán để mở khóa và giải mã dữ liệu, giúp nạn nhân lấy lại quyền truy cập. Vòng đời của ransomware có sáu giai đoạn chung: phân phối và lây nhiễm phần mềm độc hại; chỉ huy và kiểm soát; khám phá và chuyển động bên; trộm cắp độc hại và mã hóa tập tin; tống tiền; và độ phân giải.

\* Giải pháp phòng chống malware trong một hệ thống CNTT:

- Sử dụng phần mềm diệt virus/phần mềm bảo mật: Cài đặt và duy trì một phần mềm diệt virus/phần mềm bảo mật tin cậy trên tất cả các thiết bị và máy chủ trong hệ thống. Đảm bảo phần mềm này được cập nhật thường xuyên để phòng chống các mối đe dọa mới nhất.

- Cập nhật phần mềm và hệ điều hành: Luôn giữ cho tất cả các phần mềm, ứng dụng và hệ điều hành được cập nhật mới nhất. Các bản cập nhật thường bao gồm các bản vá lỗi bảo mật quan trọng để ngăn chặn các lỗ hổng bảo mật mà malware có thể lợi dụng.

- Đào tạo nhận thức về bảo mật: Đào tạo và nâng cao nhận thức về bảo mật cho nhân viên, giúp họ nhận biết và tránh các mối đe dọa malware như email lừa đảo, tệp đính kèm nguy hiểm, v.v.

- Quản lý quyền truy cập: Áp dụng các chính sách quản lý quyền truy cập phù hợp, chỉ cấp quyền cần thiết cho từng người dùng và giới hạn quyền đặc biệt để giảm thiểu rủi ro.

- Sao lưu dữ liệu: Thực hiện sao lưu dữ liệu thường xuyên để đảm bảo khả năng phục hồi trong trường hợp bị tấn công malware.

- Tường lửa và bảo mật mạng: Triển khai và duy trì tường lửa, hệ thống phát hiện xâm nhập (IDS/IPS) và các biện pháp bảo mật mạng khác để ngăn chặn malware xâm nhập vào hệ thống.

- Kiểm soát truy cập Web và email: Sử dụng các công cụ lọc nội dung để kiểm soát truy cập các trang web và email nguy hiểm, giảm nguy cơ lây nhiễm malware.

- Giám sát và phân tích: Thường xuyên giám sát và phân tích các hoạt động của hệ thống để phát hiện sớm các dấu hiệu của malware và can thiệp kịp thời.

- Cập nhật chính sách bảo mật: Định kỳ đánh giá và cập nhật chính sách bảo mật để đảm bảo phù hợp với các mối đe dọa mới và thực tiễn tốt nhất.

**Câu 2.** (4 điểm) Trình bày đặc điểm của Firewall. Giải pháp triển khai Firewall trong hệ thống CNTT?

**\* Đặc điểm của Firewall:**

- Về cơ bản chức năng của firewall là chống lại truy cập trái phép vào máy chủ.

- Chi tiết hơn thì firewall là:

+ Một phần của hệ thống máy tính hoặc mạng được thiết kế để ngăn chặn lưu lượng truy cập trái phép từ mạng này sang mạng khác.

+ Tách biệt các thành phần đáng tin cậy và không đáng tin cậy của mạng.

+ Phân biệt các mạng trong một mạng đáng tin cậy.

+ Các chức năng chính là lọc dữ liệu, chuyển hướng lưu lượng và bảo vệ khỏi các cuộc tấn công mạng

Một số yêu cầu của firewall:

+ Tất cả lưu lượng giữa các vùng tin cậy phải đi qua tường lửa.

+ Chỉ những lưu lượng được ủy quyền, như được xác định bởi chính sách bảo mật, mới được phép đi qua.

+ Bản thân tường lửa phải có khả năng miễn nhiễm với sự xâm nhập, nghĩa là sử dụng một hệ thống cứng với Hệ điều hành được bảo mật.

- Các chính sách của firewall:

+ User control: Kiểm soát truy cập vào dữ liệu dựa trên vai trò của người đang cố gắng truy cập vào nó.

+ Service controll: Kiểm soát các truy cập thông qua các dịch vụ được gởi bởi host.

+ Direction control: Xác định đường đi của gói tin như nó được gửi từ đâu và có được cho phép đi qua tường lửa không.

- Hành động của firewall:

+ Accepted: Được phép vào mạng/máy chủ được kết nối thông qua tường lửa.

+ Denied: Không được phép vào mạng/máy chủ được kết nối thông qua tường lửa (không có bất kì thông tin gì trả về)

+ Rejected: có thể hiểu sang nghĩa tiếng việt là từ chối và phản hồi. Firewall sẽ chặn và không cho phép gói tin đi qua. Tuy nhiên, nó sẽ gửi một gói tin ICMP (Internet Control Message Protocol) phản hồi lại cho người gửi, thông báo rằng kết nối hoặc yêu cầu truy cập đã bị từ chối. Điều này giúp người gửi biết rằng yêu cầu của họ đã bị tường lửa chặn lại.

VD: Giả sử một máy tính client cố gắng kết nối với một máy chủ web (web server) đang được bảo vệ bởi Firewall. Máy chủ web này chỉ cho phép kết nối từ một số địa chỉ IP hoặc mạng cụ thể.

B1: Client gửi một gói tin TCP SYN (yêu cầu thiết lập kết nối) đến cổng 80 (cổng web) của máy chủ web.

B2: Firewall nhận được gói tin này và kiểm tra với các quy tắc đã được cấu hình. Nếu địa chỉ IP của client không nằm trong danh sách được phép kết nối, Firewall sẽ đưa ra hành động "rejected".

B3: Firewall sẽ gửi một gói tin ICMP "Destination Unreachable" (Đích không thể đạt được) với mã lỗi "Communication Administratively Prohibited" (Kết nối bị cấm bởi quản trị viên) trở lại cho client.

B4: Client nhận được gói tin ICMP này và biết rằng yêu cầu kết nối đã bị từ chối bởi Firewall, thay vì chỉ đơn giản là bị dropped (dropped có nghĩa là gói tin bị hủy mà không có phản hồi).

**\* Giải pháp triển khai Firewall trong hệ thống CNTT:**

+ Hạn chế truy cập VPN: Chỉ cho phép truy cập VPN từ các địa chỉ IP hoặc mạng được xác định trước, giúp kiểm soát và giới hạn khả năng truy cập từ bên ngoài.

+ Giám sát quyền truy cập của người dùng: Theo dõi và kiểm soát chặt chẽ quyền truy cập của người dùng, đảm bảo chỉ những người được ủy quyền mới có thể truy cập vào các tài nguyên nhất định.

+ Tắt các dịch vụ mạng không sử dụng: Vô hiệu hóa các dịch vụ mạng không cần thiết để giảm thiểu các lỗ hổng và điểm yếu có thể bị tấn công.

+ Cập nhật phần mềm firewall: Luôn cập nhật phần mềm Firewall mới nhất để vá các lỗ hổng bảo mật và tăng cường khả năng phòng thủ.

+ Sử dụng nhiều lớp Firewall: Triển khai nhiều lớp firewall để tăng cường bảo mật, ví dụ: firewall mạng để kiểm soát lưu lượng mạng, firewall ứng dụng để kiểm soát nội dung ứng dụng.

+ Thiết lập chính sách kiểm soát truy cập: Xây dựng chính sách kiểm soát truy cập chi tiết, quy định rõ ràng những giao thức, cổng, địa chỉ IP nào được phép truy cập và từ đâu.

**Câu 3.** (3 điểm) Trình bày giải pháp bảo vệ toàn diện cho một hệ thống CNTT doanh nghiệp.

Đề bảo vệ toàn diện cho một hệ thống CNTT doanh nghiệp thì ta phải tuân thủ theo các bước sau:

- Áp dụng mô hình CIA Triad (Confidentiality - Tính bảo mật, Integrity - Tính toàn vẹn, Availability - Tính sẵn sàng):

+ Confidentiality: Đảm bảo chỉ những người được ủy quyền mới có quyền truy cập vào thông tin.

+ Integrity: Đảm bảo thông tin và dữ liệu không bị sửa đổi hoặc hủy hoại bởi những người không được ủy quyền.

+ Availability: Đảm bảo thông tin và dữ liệu luôn sẵn sàng cho người dùng được ủy quyền khi cần thiết.

- Phát triển 3 yếu tố cốt lõi hình thành nên một doanh nghiệp mạnh:

+ People (Con người): Đảm bảo nhân viên có đủ kiến thức, kỹ năng và ý thức về an ninh thông tin.

+ Process (Quy trình): Xây dựng và tuân thủ các quy trình, chính sách về an ninh thông tin.

+ Technology (Công nghệ): Áp dụng các công nghệ an ninh thông tin như tường lửa, phần mềm diệt virus, mã hóa dữ liệu, v.v.

- Thực hiện quản trị doanh nghiệp thông qua:

+ Policies (Chính sách): Xây dựng và triển khai các chính sách an ninh thông tin rõ ràng cho toàn bộ doanh nghiệp.

+ Audit (Kiểm toán): Thực hiện kiểm toán an ninh thông tin định kỳ để đánh giá hiệu quả của các chính sách và biện pháp an ninh.

+ Awareness (Nâng cao nhận thức): Tổ chức các khóa đào tạo, hội thảo để nâng cao nhận thức về an ninh thông tin cho nhân viên.