TRƯỜNG ĐẠI HỌC KỸ THUẬT – CÔNG NGHỆ CẦN THƠ

AN TOÀN CÁC HỆ THỐNG THÔNG TIN

ThS. Nguyễn Văn Kha

dzokha1010@gmail.com

Chương 2
QUẢN LÝ RỦI RO VÀ ĐÁNH GIÁ LỖ HỔNG

2.1. Quản lý rủi ro

2.2. Đánh giá lỗ hổng

2.3. An ninh Vòng đời phát triển hệ thống (SDLC)

2.4. Kỹ thuật phát hiện Malware

2.1 Quản lý rủi ro

Rủi ro (Risk): là xác suất xảy ra sự cố không mong muốn, chẳng hạn như sự kiện xảy ra ảnh hưởng xấu đến an ninh thông tin hoặc thiệt hại tài sản thông tin. Các tổ chức phải giảm thiểu rủi ro để phù hợp với trạng thái rủi ro mà họ chấp nhận được, cả về số lượng và tính chất của rủi ro.

2.1 Quản lý rủi ro (tt)

Quản trị an ninh HTTT phải thiết lập một chương trình quản lý rủi ro (RM - Risk Management) hiệu quả. RM tập trung vào việc trả lời các câu hỏi quan trọng về rủi ro liên quan đến tài sản thông tin của tổ chức:

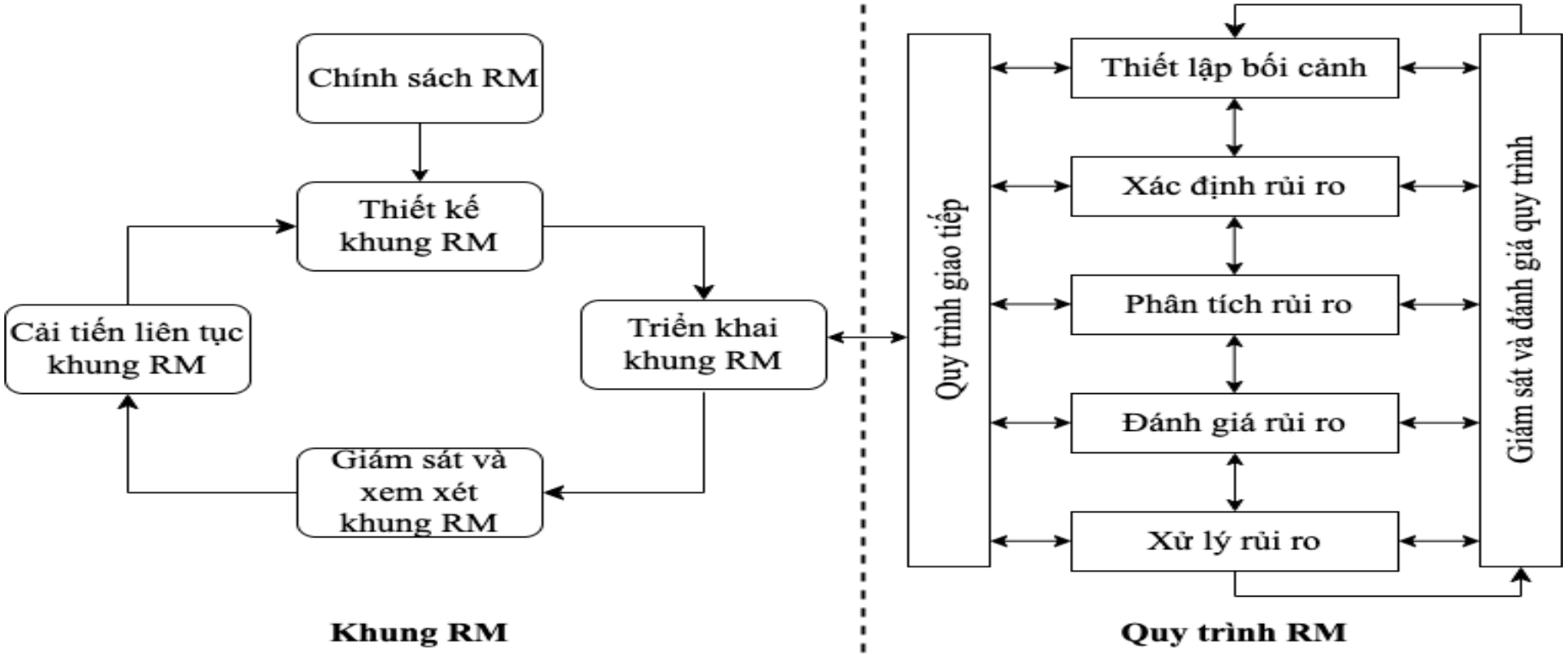
1. Rủi ro ở đâu và là gì (xác định rủi ro)?

2. Mức độ rủi ro hiện tại nghiêm trọng như thế nào (phân tích rủi ro)?

3. Mức độ rủi ro hiện tại có thể chấp nhận được không (đánh giá rủi ro)?

4. Cần làm gì để đưa rủi ro xuống mức có thể chấp nhận được (xử lý rủi ro)?

2.1 Quản lý rủi ro (tt)



Chương trình RM

2.1 Quản lý rủi ro
2.1.1. Khung quản lý rủi ro

Khung RM bao gồm năm giai đoạn chính:

1. Quản trị và hỗ trợ điều hành (Chính sách RM)
2. Thiết kế khung RM (xây dựng kế hoạch RM chi tiết)
3. Triển khai khung RM (thử nghiệm, từng phần, toàn bộ)
4. Giám sát và xem xét khung RM (RM thực tế)
5. Cải tiến liên tục (thiết kế lại khung RM)

2.1 Quản lý rủi ro
2.1.1. Khung quản lý rủi ro (tt)

Khung RM giống như chính sách an ninh thông tin doanh nghiệp (EISP - Enterprise Information Security Policy), là một tài liệu chiến lược chính thức hóa phần lớn ý định của nhóm quản trị. Bao gồm các phần sau:

- Mục đích và phạm vi
- Ý định và mục tiêu RM
- Vai trò và trách nhiệm
- Yêu cầu về nguồn lực
- Mức độ chấp nhận và khả năng chịu rủi ro
- Hướng dẫn phát triển chương trình RM
- Hướng dẫn sửa đổi chinh sách
- Tham chiếu đến các chính sách, kế hoạch, tiêu chuẩn và hướng dẫn quan trọng khác

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro

Các nhiệm vụ chính:

a) Thiết lập bối cảnh;

b) Xác định rủi ro;

c) Phân tích rủi ro;

d) Đánh giá rủi ro;

e) Xử lý rủi ro không thể chấp nhận được.

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
a) Thiết lập bối cảnh

Bối cảnh bên ngoài:

- Môi trường kinh doanh
- Môi trường pháp lý/quy định
- Môi trường đe dọa
- Môi trường hỗ trợ
- Có thể là các yếu tố khác

Bối cảnh nội bộ:

- Cấu trúc quản trị của tổ chức
- Các bên liên quan nội bộ
- Văn hóa của tổ chức
- Mức độ trưởng thành của chương trình an ninh thông tin của tổ chức
- Kinh nghiệm của tổ chức về chính sách, lập kế hoạch và quản lý rủi ro

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
b) Xác định rủi ro

(1) Xác định tài sản thông tin của tổ chức, phân lớp dựa trên độ nhạy cảm hoặc nhu cầu bảo mật, nhóm thành các danh mục hữu ích, ưu tiên theo tầm quan trọng

(2) Xếp hạng tài sản thông tin

(3) Đánh giá mối đe doạ: Xác định mối đe dọa; Đánh giá các mối đe dọa; Ưu tiên các mối đe dọa; Đánh giá lỗ hổng bảo mật.

(4) Bảng tính (TVA - Threats-Vulnerabilities-Assets)

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
b) Xác định rủi ro (tt)

Tài sản thông tin	Phân lớp dữ liệu	Tác động đến lợi nhuận
Thông tin được truyền trên mạng		
Đơn đặt hàng	Confidential	High
Lời khuyên thực hiện đơn hàng	Confidential	Medium
Dịch vụ khách hàng qua Email	Private	
Tài sản vùng DMZ		
Router	Public	Critical
Website	Public	Critical
Ứng dụng Server	Private	Critical

Bảng tài sản thông tin và phân loại

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
b) Xác định rủi ro (tt)

#	Tiêu chí	Tác động đến				Tầm quan trọng
		Doanh thu	Lợi nhuận	Danh tiếng	Tổng	
	Trọng số	**0,3**	**0,4**	**0,3**	**1,0**	
1.	Đơn đặt hàng					
2.	Lời khuyên thực hiện đơn hàng					
3.	Dịch vụ khách hàng qua Email					
4.	Router					
5.	Website					
6.	Ứng dụng Server					

Bảng phân tích trọng số của tài sản thông tin

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
b) Xác định rủi ro (tt)

#	Mối đe doạ	Câu hỏi quan trọng				Tầm quan trọng
		Câu 1	Câu 2	...	Tổng	
		0,3	0,4	0,3	1,0	
1.	Phần mềm độc hại					
2.	Tống tiền thông tin					
3.	Gián điệp hoặc đăng nhập					
4.	Lỗi hoặc sai sót do con người					
5.	Lỗi hoặc sự cố phần cứng					
6.	Lỗi hoặc sự cố phần mềm					
7.	Sự lỗi thời của công nghệ					
8.	Sai lệch về chất lượng dịch vụ					
9.	Tấn công phá huỷ hoặc phá hoại					
10.	Trộm					
11.	Sự xâm phạm đến Sở hữu trí tuệ					
12.	Sức mạnh của thiên nhiên					

Bảng phân tích trọng số mức độ nghiêm trọng của mối đe dọa

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
b) Xác định rủi ro (tt)

Bảng TVA

	Asset 1	Asset 2	Asset 3
Threat 1	T1V1A1 T1V2A1 T1V3A1 . . .	T1V1A2 T1V2A2 . . .	T1V1A3 . . .
Threat 2	T2V1A1 T2V2A1 . . .	T2V1A2 . . .	T2V1A3 . . .
Threat 3	T3V1A1 . . .	T3V1A2 . . .	

- Xác định rủi ro: Tập trung vào việc xem xét liệu tài sản có gặp phải rủi ro từ mối đe dọa hay không và xác định các lỗ hổng hiện có.
- Phân tích rủi ro: Mở rộng hơn, bao gồm việc đánh giá mức độ nghiêm trọng của rủi ro đối với tài sản, xét đến các biện pháp kiểm soát hiện có.

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
c) Phân tích rủi ro

(1) Giảm thiểu các biện pháp kiểm soát áp dụng

(2) Xác định khả năng xảy ra sự kiện đe dọa

(3) Đánh giá tác động tiềm tàng đến giá trị tài sản

(4) Tổng hợp

(5) Sự không chắc chắn (Không thể biết mọi thứ về mọi lỗ hổng)

(6) Xác định rủi ro (Bảng xếp hạng rủi ro)

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
c) Phân tích rủi ro (tt)

Tài sản	Lỗ hổng bảo mật	Khả năng xảy ra	Tác động	Điểm xếp hạng
		(1)	(2)	(1) x (2)
Đơn đặt hàng				
Lời khuyên thực hiện đơn hàng				
Dịch vụ khách hàng qua Email				
Router				
Website				
Ứng dụng Server				

Bảng xếp hạng rủi ro

2.1 Quản lý rủi ro
2.1.2. Quy trình quản lý rủi ro
c) Đánh giá rủi ro

Sản phẩm	Mục đích
Bảng tài sản thông tin và phân loại	Tổng hợp thông tin về tài sản thông tin, mức độ nhạy cảm của chúng và giá trị của chúng đối với tổ chức
Bảng phân tích trọng số của tài sản thông tin	Xếp hạng thứ tự từng tài sản thông tin theo các tiêu chí do tổ chức phát triển
Bảng phân tích trọng số mức độ nghiêm trọng của mối đe dọa	Xếp hạng thứ tự từng mối đe dọa đối với tài sản thông tin của tổ chức theo các tiêu chí do tổ chức phát triển
Bảng TVA	Kết hợp đầu ra từ việc xác định và ưu tiên tài sản thông tin với việc xác định và ưu tiên mối đe dọa, xác định các lỗ hổng tiềm ẩn trong "bộ ba" và kết hợp các biện pháp kiểm soát hiện có và đã lên kế hoạch
Bảng xếp hạng rủi ro	Chỉ định giá trị xếp hạng rủi ro cho mỗi bộ ba TVA, kết hợp khả năng xảy ra, tác động và có thể là thước đo mức độ không chắc chắn

Sản phẩm đánh giá rủi ro

- Nếu chấp nhận rủi ro thì tiến hành giám sát và đánh giá

- Nếu không chấp nhận thì tiến hành xử lý rủi ro

2.1 Quản lý rủi ro
2.1.3. Xử lý rủi ro

a) Giảm thiểu rủi ro (cố gắng ngăn chặn việc khai thác lỗ hổng)

b) Chuyển giao rủi ro (thuê ngoài cho các tổ chức khác, mua bảo hiểm hoặc triển khai hợp đồng dịch vụ với các nhà cung cấp)

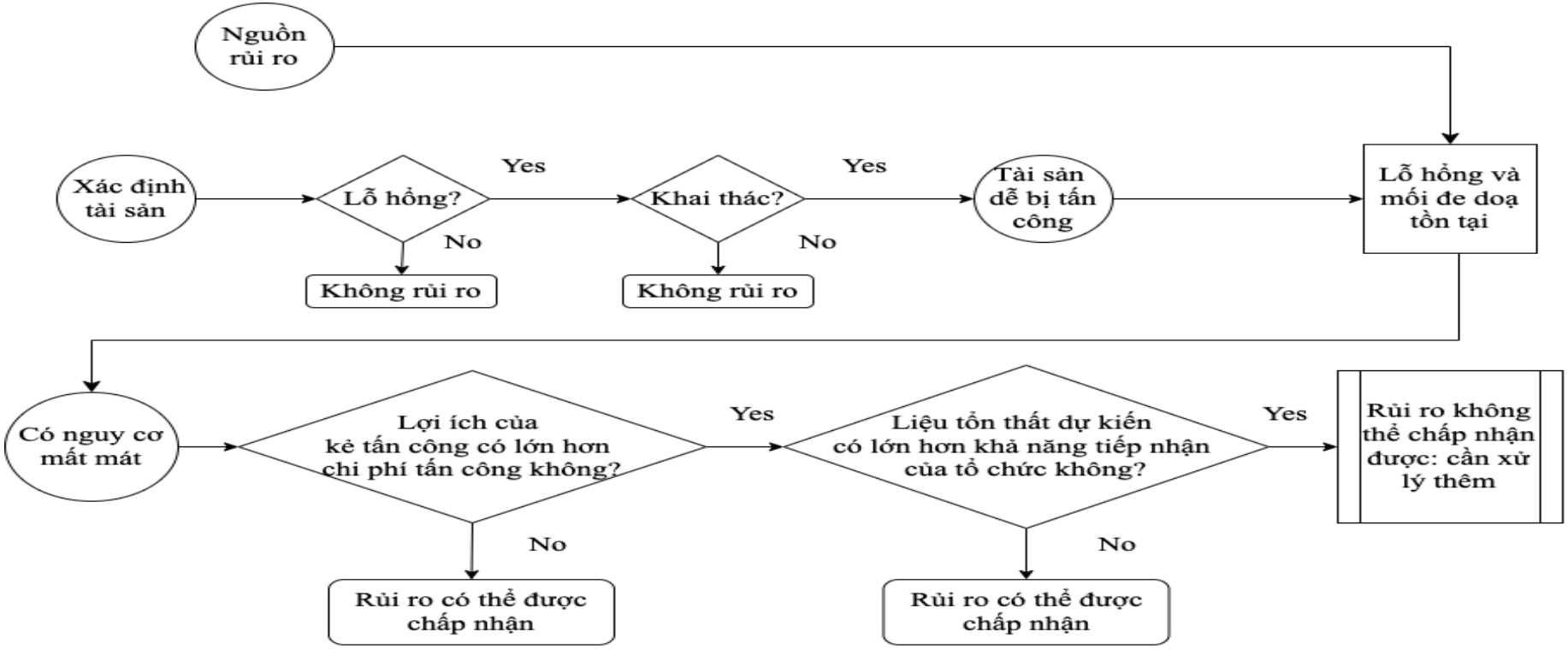
c) Chấp nhận rủi ro (là quyết định không làm gì ngoài mức bảo vệ hiện tại để bảo vệ tài sản thông tin khỏi rủi ro và chấp nhận kết quả từ bất kỳ hành vi khai thác nào phát sinh)

d) Chấm dứt rủi ro (vô hiệu hóa các chức năng chương trình hoặc ngắt kết nối hệ thống máy chủ khỏi mạng)

2.1.4. Quản lý rủi ro

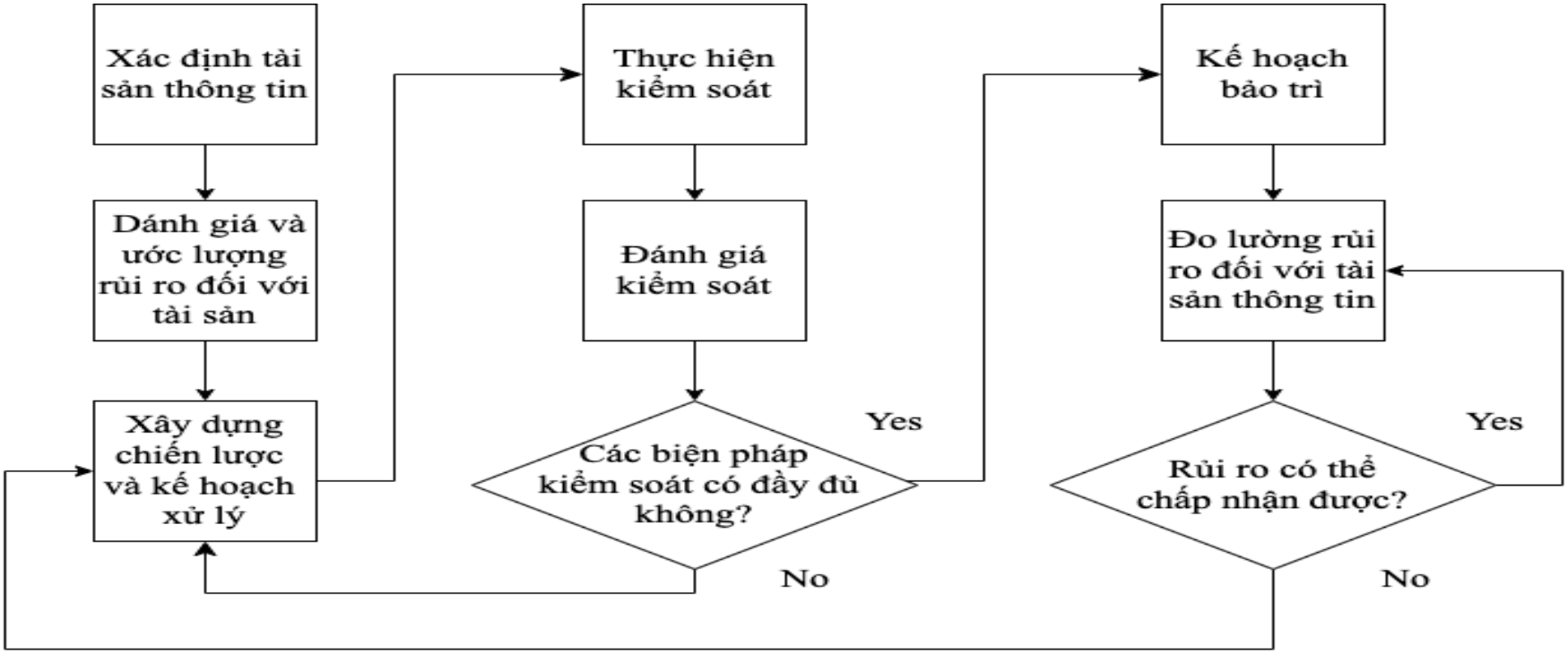
Mục tiêu không phải là đưa rủi ro còn sót lại về mức bằng không; thay vào đó, mục tiêu của InfoSec là đưa rủi ro còn sót lại phù hợp với mức độ chấp nhận rủi ro của tổ chức

2.1.4. Quản lý rủi ro (tt)



Điểm hành động xử lý rủi ro

2.1.4. Quản lý rủi ro (tt)



Chu kỳ xử lý rủi ro

2.1.4. Quản lý rủi ro (tt)

Trước khi chúng ta dành thêm thời gian, tiền bạc hoặc nguồn lực cho các cơ chế bổ sung để bảo vệ tài sản này, liệu có đáng không?

Phân tích khả thi và chi phí-lợi ích (CBA - Cost-Benefit Analysis)

Lợi ích từ một giải pháp kiểm soát thay thế

CBA = ALE(pre-control) - ALE(post-control) – ACS

- ALE Kỳ vọng tổn thất hàng năm, trước và sau khi kiểm soát thay thế được áp dụng
- ACS là chi phí bảo vệ hàng năm

2.1.4. Quản lý rủi ro (tt)

Chi phí

- Chi phí phát triển hoặc mua lại phần cứng, phần mềm và dịch vụ
- Phí đào tạo—Chi phí đào tạo nhân sự
- Chi phí triển khai
- Chi phí dịch vụ
- Chi phí bảo trì
- Chi phí tiềm ẩn do mất tài sản

Lợi ích

Lợi ích là giá trị mà tổ chức thu được khi áp dụng các biện pháp kiểm soát để ngăn ngừa tổn thất do một lỗ hổng bảo mật gây ra. Kết quả này được thể hiện dưới dạng kỳ vọng tổn thất hàng năm (ALE).

2.1.4. Quản lý rủi ro (tt)

Kỳ vọng tổn thất hàng năm (ALE)

ALE = SLE x ARO

- **SLE là Kỳ vọng tổn thất đơn**
- ARO là tỷ lệ xảy ra mối đe doạ hàng năm

Ví dụ: 2 năm xảy ra 1 lần thì ARO = 0.5.

Kỳ vọng tổn thất đơn (SLE)

SLE = AV x EF

- AV là giá trị tài sản
- EF là phần trăm tổn thất xảy ra do một lỗ hổng nhất định bị khai thác

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm

Lỗ hổng (Vulnerability) là điểm yếu hoặc lỗi trong IS, cho phép kẻ tấn công khai thác và xâm phạm tính bảo mật, toàn vẹn hoặc khả dụng của hệ thống.

Lỗ hổng có thể phát sinh từ nhiều nguyên nhân như lỗi phần mềm, cấu hình hệ thống không chính xác, mật khẩu yếu, Malware, dữ liệu người dùng không được kiểm tra hoặc căn phòng chứa server không được khóa.

Lỗ hổng an ninh chia làm hai loại:

- Lỗ hổng đã biết
- Lỗ hổng Zero-day

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Rủi ro an ninh được xem là lỗ hổng khi nó được xác định là một điểm yếu có thể bị kẻ tấn công khai thác. Khi lỗ hổng đã có ít nhất một cuộc tấn công thực tế hoặc đang hoạt động, nó được coi là khai thác (Exploit). Chỉ cần phát hiện ra một lỗ hổng nghiêm trọng, toàn bộ hệ thống mạng đều có nguy cơ bị tấn công.

Các lỗ hổng cần được sắp xếp theo mức độ nghiêm trọng, sau đó phân loại theo máy chủ hoặc dịch vụ bị ảnh hưởng. Các lỗ hổng nghiêm trọng nên ở đầu báo cáo và nên được liệt kê theo thứ tự giảm dần: nghĩa là nghiêm trọng, sau đó là cao, trung bình và thấp.

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Đánh giá lỗ hổng (Vulnerability Assessment) là quá trình kiểm tra và đánh giá các hệ thống, dịch vụ hoặc cơ sở vật chất nhằm phát hiện các điểm yếu, vấn đề an ninh tiềm ẩn có thể bị kẻ tấn công khai thác. Quá trình này không chỉ giới hạn ở các hệ thống máy tính hay mạng, mà còn bao gồm các yếu tố vật lý.

Đánh giá lỗ hổng là một thành phần thiết yếu trong chính sách an ninh của mọi tổ chức. Quá trình này nhằm xác định và đánh giá mức độ nghiêm trọng của các điểm yếu trong hệ thống.

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Quá trình đánh giá lỗ hổng thường bao gồm các bước sau:

1. Lập danh mục tài sản và nguồn lực trong hệ thống.

2. Xác định giá trị định lượng và tầm quan trọng của từng tài sản.

3. Xác định các lỗ hổng hoặc mối đe dọa tiềm ẩn đối với từng tài sản.

4. Giảm thiểu hoặc loại bỏ các lỗ hổng nghiêm trọng nhất đối với các tài sản có giá trị nhất.

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Thông thường, một công ty bảo mật sẽ được thuê để thực hiện quá trình này, tập trung vào việc đánh giá và ghi nhận các lỗ hổng tiềm năng, thay vì thực hiện các cuộc tấn công xâm nhập. Kết quả sẽ là các đề xuất cụ thể về biện pháp giảm thiểu rủi ro và cải thiện bảo mật.

Quy trình gồm các bước: Scan hệ thống để xác định các lỗ hổng tiềm năng; Phân tích và đánh giá các lỗ hổng theo mức độ nghiêm trọng; Đưa ra khuyến nghị và thực hiện các biện pháp để khắc phục hoặc giảm thiểu rủi ro.

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Đánh giá lỗ hổng và kiểm thử xâm nhập (Penetration Test) là khác nhau trong quản lý an ninh mạng.

- Đánh giá lỗ hổng là quá trình xem xét các dịch vụ và hệ thống để phát hiện các vấn đề bảo mật tiềm ẩn. Mục tiêu là nhận diện và phân tích các điểm yếu mà không thực hiện bất kỳ cuộc tấn công nào.
- Kiểm thử xâm nhập, ngược lại, thực sự tiến hành các cuộc tấn công mô phỏng và khai thác các lỗ hổng để chứng minh rằng những vấn đề bảo mật này là có thật. Kiểm thử xâm nhập đi xa hơn so với đánh giá lỗ hổng vì nó không chỉ phát hiện các điểm yếu mà còn thể hiện khả năng khai thác chúng.

2.2. Đánh giá lỗ hổng
2.2.1. Khái niệm (tt)

Kiểm thử xâm nhập có thể được định nghĩa là một nỗ lực hợp pháp và được ủy quyền để xác định và khai thác các lỗ hổng trong hệ thống máy tính, nhằm mục tiêu làm cho các hệ thống an toàn hơn.

Quá trình này bao gồm việc thăm dò các lỗ hổng cũng như cung cấp các cuộc tấn công theo bằng chứng khái niệm (PoC - Proof of Concept) để chứng minh các lỗ hổng là có thật.

2.2. Đánh giá lỗ hổng
2.2.2. Báo cáo đánh giá lỗ hổng

Đánh giá lỗ hổng cần phải đi kèm với một báo cáo toàn diện, nếu không, kết quả sẻ trở nên vô ích. Báo cáo đánh giá lỗ hổng phải bao gồm:

- Xác định các lỗ hổng

- Xếp hạng mức độ nghiệm trọng của từng lỗ hổng: nghiêm trọng (Critical), cao (High), trung bình (Medium), thấp (low).

- Số lượng lỗ hổng

2.2. Đánh giá lỗ hổng
2.2.2. Báo cáo đánh giá lỗ hổng (tt)

Một báo cáo toàn diện, linh hoạt và có thể tùy chỉnh không chỉ cung cấp hướng dẫn về các bước kỹ thuật cần thực hiện mà còn giúp bạn biện minh với ban quản lý về chi phí triển khai các biện pháp an ninh.

Báo cáo tốt sẽ là "đạn dược" cần thiết để thuyết phục các bên liên quan về tầm quan trọng của các biện pháp bảo vệ an ninh mạng.

2.2. Đánh giá lỗ hổng
2.3.2. Quét mạng

Mục tiêu lý thuyết của quét mạng (Scan) là nâng cao tính an ninh trên tất cả các hệ thống hoặc thiết lập một tiêu chuẩn hoạt động tối thiểu trên toàn mạng.

Quét mạng là quá trình xác định các hệ thống đang hoạt động và các dịch vụ đang chạy trên những hệ thống đó.

2.2. Đánh giá lỗ hổng
2.3.2. Quét mạng
a) Ping

Ping là một loại gói mạng đặc biệt được gọi là gói Giao thức tin nhắn điều khiển Internet (ICMP - Internet Control Message Protocol)

ping target_ip

fping -a -g 192.168.1.1 192.168.1.254 > hosts.txt

2.2. Đánh giá lỗ hổng
2.2.2. Quét mạng
a) Quét cổng

Mục tiêu của việc quét cổng là xác định các cổng đang mở và các dịch vụ khả dụng trên hệ thống mục tiêu.

Mỗi dịch vụ đại diện cho một công việc cụ thể mà máy tính thực hiện, như email hay web. Mỗi máy tính có 65.536 cổng, sử dụng giao thức TCP hoặc UDP tùy thuộc vào dịch vụ.

Việc quét cổng giúp chúng ta hiểu rõ hơn về mục đích của máy và lập kế hoạch tấn công. Nmap là công cụ quét cổng tốt nhất, miễn phí và có sẵn trên nhiều hệ điều hành, bao gồm Kali Linux.

2.2. Đánh giá lỗ hổng
2.2.3. Quét mạng
a) Quét cổng (tt)

Nmap là tiện ích mã nguồn mở, giúp khám phá, quản trị và kiểm tra an ninh mạng. Nó sử dụng gói IP thô để xác định máy chủ khả dụng, dịch vụ cung cấp, hệ điều hành, và tường lửa đang sử dụng. Nmap có giao diện dòng lệnh truyền thống và Zenmap là giao diện người dùng đồ hoạ (GUI - Graphical User Interface) chính thức. Kết quả quét có thể được lưu, so sánh và tìm kiếm trong cơ sở dữ liệu.

2.2. Đánh giá lỗ hổng
2.2.3. Quét mạng
a) Quét cổng (tt)

Chỉ sử dụng một máy quét không đủ để giải quyết vấn đề an ninh mạng. Một máy quét tốt sẽ giúp giải quyết một phần vấn đề, nhưng tốt hơn là sử dụng nhiều máy quét. Bằng cách này, bạn có thể so sánh kết quả và nhận diện các lỗ hổng từ nhiều góc độ. Một số máy quét tập trung vào các dịch vụ cụ thể, giúp bạn kiểm tra kỹ lưỡng hơn. Kiến trúc máy quét điển hình: Scan theo từng mục tiêu hoặc nhiều mục tiêu, Scan lỗ hổng đã biết, Scan lỗ hổng Database.

2.2.3. Quét mạng
b) Quét cổng
Quét TCP Connect

nmap -sT -p- -Pn 192.168.1.1-254

Trong đó:

- sT: quét TCP connect
- -p-: quét tất cả các cổng chứ không phải 1000 cổng mặc định.
- Pn: vô hiệu hoá chức năng phát hiện Host.

2.2.3. Quét mạng
b) Quét cổng
Quét SYN

Quét SYN còn gọi là quét tàng hình (Stealth Scan)

nmap -sS -p- -Pn 192.168.1.132

Trong đó:

- sS: quét SYN thày vì quét TCP connect
- -p-: quét tất cả các cổng chứ không phải 1000 cổng mặc định.
- Pn: vô hiệu hoá chức năng phát hiện Host.

2.2.3. Quét mạng
b) Quét cổng
Quét UDP

Điều quan trọng cần nhớ là không phải mọi dịch vụ đều sử dụng TCP, nên sẻ thiếu sót dịch vụ nếu không quét UDP.

nmap -sUV 192.168.18.132

Trong đó:

- sU: quét UDP
- sV: quét phiên bản

2.2.3. Quét mạng
b) Quét cổng
Quét XMAS

XMAS sẻ trả về chi tiết mô tả các ghi chú, các kỹ thuật của hệ thống (không hiệu quả khi quét Windows).

nmap -sX -p- -Pn 192.168.18.132

Trong đó:

- sX: quét XMAS
- -p-: quét tất cả các cổng chứ không phải 1000 cổng mặc định.
- Pn: vô hiệu hoá chức năng phát hiện Host.

2.2.3. Quét mạng
b) Quét cổng
Quét NULL

Quét NULL giống như quét XMAS

nmap -sN -p- -Pn 192.168.18.132

Trong đó:

- sN: quét NULL
- -p-: quét tất cả các cổng chứ không phải 1000 cổng mặc định.
- Pn: vô hiệu hoá chức năng phát hiện Host.

2.2.3. Quét mạng
b) Quét cổng
Nmap Scripting Engine (NSE)

NSE cho phép Nmap hoàn thành nhiều tác vụ khác nhau bao gồm quét lỗ hổng, khám phá mạng nâng cao, phát hiện Backdoor và trong một số trường hợp thậm chí thực hiện khai thác!

Tài liệu hướng dẫn: https://nmap.org/nsedoc/

2.2.3. Quét mạng
b) Quét cổng
Nmap Scripting Engine (NSE)

nmap --script category_name 192.168.18.132

- script: gọi NSE

- category_name được thay thế bằng :

+ banner: in bất kỳ đầu ra nào được gửi từ hệ thống đích đến thiết bị đầu cuối cục bộ.

+ vuln: tìm kiếm các sự cố đã biết trên hệ thống mục tiêu.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng

Lỗ hổng là điểm yếu trong cấu hình phần mềm hoặc hệ thống thường có thể bị khai thác. Lỗ hổng có thể xuất hiện dưới nhiều hình thức nhưng thường liên quan đến việc thiếu bản vá. Các nhà cung cấp thường phát hành bản vá để khắc phục sự cố hoặc lỗ hổng đã biết.

Phần mềm và hệ thống chưa vá thường dẫn đến các cuộc kiểm tra thâm nhập nhanh vì một số lỗ hổng cho phép thực thi mã từ xa.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

Máy quét lỗ hổng có thể tiêu tốn nhiều băng thông, vì vậy quá trình quét cần được hoàn thành nhanh chóng. Quét càng toàn diện thì thời gian càng lâu, tạo ra sự đánh đổi giữa tốc độ và độ sâu.

Để tăng hiệu suất, bạn có thể sử dụng nhiều máy quét và hệ thống tổng hợp kết quả. Sử dụng nhiều công cụ quét khác nhau để so sánh kết quả là thực hành tốt nhất.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

Có nhiều công cụ đánh giá lỗ hổng có thể tìm hiểu trên trang https://sectools.org/

a) Nessus

Nessus liên tục được cập nhật, với hơn 46.000 plug-in. Các tính năng chính bao gồm kiểm tra bảo mật từ xa và cục bộ (đã xác thực), kiến trúc Client-Server với giao diện Web và ngôn ngữ kịch bản nhúng để viết các plug-in của riêng bạn hoặc hiểu các plug-in hiện có. Phiên bản mã nguồn mở của Nessus đã được phân nhánh bởi một nhóm người dùng vẫn đang phát triển nó dưới tên OpenVAS.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

b) GFI LANguard

Đây là trình quét lỗ hổng và bảo mật mạng được thiết kế để hỗ trợ quản lý bản vá, kiểm tra mạng và phần mềm, cũng như đánh giá lỗ hổng. Giá dựa trên số lượng địa chỉ IP bạn muốn quét. Có phiên bản dùng thử miễn phí cho tối đa năm địa chỉ IP.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

c) Retina

Retina là một máy quét đánh giá lỗ hổng thương mại của eEye. Giống như Nessus, chức năng của Retina là quét tất cả các máy chủ trên mạng và báo cáo về bất kỳ lỗ hổng nào được tìm thấy. Nó được viết bởi eEye, một công ty nổi tiếng về nghiên cứu bảo mật.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

d) Core Impact

Core Impact không hề rẻ (hãy chuẩn bị chi ít nhất 30.000 đô la), nhưng nó được coi là công cụ khai thác mạnh mẽ nhất hiện có. Nó có cơ sở dữ liệu lớn, được cập nhật thường xuyên về các khai thác chuyên nghiệp và có thể thực hiện các thủ thuật khéo léo như khai thác một máy và sau đó thiết lập một đường hầm được mã hóa thông qua máy đó để tiếp cận và khai thác các hộp khác. Các lựa chọn tốt khác bao gồm Metasploit và Canvas.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

e) Internet Security Systems Internet Scanner

Đánh giá lỗ hổng cấp ứng dụng Internet Scanner bắt đầu vào năm 1992 như một máy quét mã nguồn mở nhỏ của Christopher Klaus. Hiện nay, ông đã phát triển Internet Security Systems (ISS) thành một công ty trị giá hàng tỷ đô la với vô số sản phẩm bảo mật.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

f) X-Scan

Một trình quét chung để quét các lỗ hổng mạng, X-Scan là trình quét lỗ hổng đa luồng, được hỗ trợ bởi plug-in. X-Scan bao gồm nhiều tính năng, bao gồm hỗ trợ đầy đủ Ngôn ngữ tập lệnh tấn công Nessus, phát hiện các loại dịch vụ, phát hiện loại/phiên bản hệ điều hành từ xa, cặp mật khẩu người dùng yếu và nhiều tính năng khác. Bạn có thể tìm thấy các phiên bản mới hơn có sẵn tại trang web X-Scan nếu bạn có thể xử lý hầu hết các trang được viết bằng tiếng Trung.

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

g) QualysGuard

Một trình quét lỗ hổng dựa trên Web được cung cấp dưới dạng dịch vụ qua Web, QualysGuard loại bỏ gánh nặng triển khai, bảo trì và cập nhật phần mềm quản lý lỗ hổng hoặc triển khai các ứng dụng bảo mật tùy ý. Khách hàng truy cập QualysGuard một cách an toàn thông qua giao diện Web dễ sử dụng. QualysGuard có hơn 5000 lần kiểm tra lỗ hổng duy nhất, một công cụ quét dựa trên suy luận và các bản cập nhật hàng ngày tự động cho cơ sở kiến thức về lỗ hổng QualysGuard

2.2. Đánh giá lỗ hổng
2.2.4. Quét lỗ hổng (tt)

h) Microsoft Baseline Security Analyzer (MBSA)

MBSA là một công cụ dễ sử dụng được thiết kế cho chuyên gia CNTT giúp các doanh nghiệp vừa và nhỏ xác định trạng thái bảo mật của họ theo các khuyến nghị bảo mật của Microsoft và cung cấp hướng dẫn khắc phục cụ thể. Được xây dựng trên cơ sở hạ tầng Windows Update Agent và Microsoft Update, MBSA đảm bảo tính nhất quán với các sản phẩm quản lý khác của Microsoft, bao gồm Microsoft Update, Windows Server Update Services, Systems Management Server và Microsoft Operations Manager. Rõ ràng, trung bình, MBSA quét hơn ba triệu máy tính mỗi tuần.

2.2. Đánh giá lỗ hổng
2.2.5. Các biện pháp đối phó quét mạng

1. Lọc các loại tin nhắn ICMP tại các bộ định tuyến và tường lửa biên.

2. Lọc tất cả các tin nhắn ICMP không thể truy cập (Destination Unreachable).

3. Cấu hình tường lửa Internet để chúng có thể xác định các lần quét cổng và điều tiết các kết nối cho phù hợp.

4. Đánh giá cách tường lửa mạng và các thiết bị IDS của bạn xử lý các gói tin IP bị phân mảnh.

5. Đảm bảo rằng các cơ chế định tuyến và lọc không thể bị bỏ qua qua các cổng nguồn.

2.2. Đánh giá lỗ hổng
2.2.5. Các biện pháp đối phó quét mạng (tt)

6. Bảo mật FTP công khai trước các lệnh PORT và PASV bị định dạng sai.

7. Cập nhật chương trình cơ sở và gói dịch vụ mới nhất cho tường lửa.

8. Các quy tắc chống giả mạo đã được xác định chính xác để thiết bị không chấp nhận các gói tin có địa chỉ nguồn bị giả mạo.

9. Sử dụng Proxy để chặn gói tin bị phân mảnh hoặc bị định dạng sai.

10. Khởi chạy quét cổng TCP và UDP cùng với các đầu dò ICMP trên không gian địa chỉ IP của riêng bạn.

2.3. An ninh SDLC

An ninh thông tin cần được tích hợp vào hệ thống ngay từ bước đầu và duy trì trong suốt quá trình phát triển và triển khai.

Để đảm bảo an toàn thông tin, tổ chức nên coi an ninh như một yếu tố cốt lõi của toàn bộ **vòng đời phát triển hệ thống** (SDLC - Systems Development Life Cycle). Điều này bao gồm việc xem xét và tích hợp các biện pháp an ninh ở mọi giai đoạn: từ thiết kế, phát triển, thử nghiệm, cho đến triển khai và bảo trì.

2.3. An ninh SDLC

Phương pháp phát triển truyền thống:

- JAD (Joint Application Development): nhiều bộ phận cùng tham gia phát triển.

- RAD (Rapid Application Development): tạo nguyên mẫu nhanh chóng, phiên bản thử nghiệm trước khi phát triển phiên bản hoàn chỉnh.

- Agile: cải tiến liên tục và phản hồi nhanh từ người dùng và hợp tác chặc chẽ giữa các thành viên.

- DevOps: kết hợp chặt chẽ giữa phát triển và vận hành để tối ưu hóa quy trình phát triển và triển khai hệ thống.

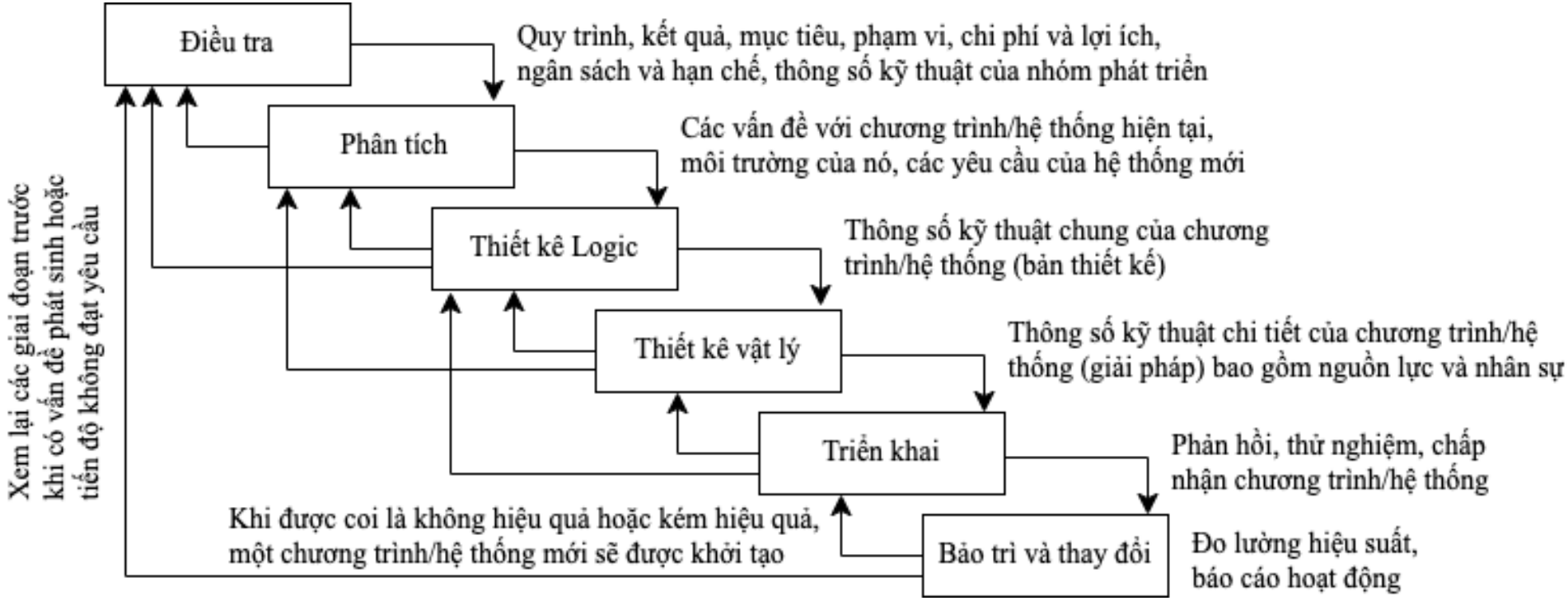
- DevSecOps: kết hợp bảo mật vào quy trình DevOps

2.3. An ninh SDLC

SDLC là một phương pháp luận nhằm thiết kế và triển khai các HTTT. Đảm bảo quy trình phát triển diễn ra một cách chặt chẽ, với các mục tiêu được xác định rõ ràng, từ đó tăng cường khả năng thành công của dự án.

Các mốc quan trọng sẽ được thiết lập, và một nhóm chuyên trách sẽ được lựa chọn để thực hiện và hoàn thành các mục tiêu đã đề ra của dự án.

2.3. An ninh SDLC
2.3.1. Phương pháp phát triển truyền thống



Mô hình thác nước của SDLC

2.3. An ninh SDLC
2.5.2. Đảm bảo phần mềm

Phần mềm không chỉ cần hoạt động đúng theo chức năng mà còn phải bảo đảm an toàn thông tin. Những nguyên tắc an ninh trong thiết kế phần mềm:

- Tiết kiệm cơ chế (thiết kế đơn giản)
- Mặc định an toàn (cơ chế cho phép thay vì cấm không được phép)
- Hoàn thành trung gian (kiểm tra quyền)
- Thiết kế mở (không nên dựa vào việc giữ bí mật mà phải dựa vào các yếu tố như khóa hoặc mật khẩu)
- Phân tách đặc quyền (nhiều yếu tố xác thực)
- Đặc quyền ít nhất (người dùng hoạt động với đặc quyền ít nhất)
- Cơ chế ít chung nhất (giảm thiểu số lượng cơ chế hoặc biến số chung)
- Khả năng chấp nhận về mặt tâm lý

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC

Phương pháp tiếp cận an ninh SDLC có năm giai đoạn chính: Khởi tạo, Phát triển/Mua lại, Triển khai/Đánh giá, Vận hành/Bảo trì và Xử lý.

Trong mỗi giai đoạn, cần đảm bảo tính an ninh cho cả hệ thống và thông tin mà nó xử lý. Tổ chức triển khai hệ thống có trách nhiệm đảm bảo rằng hệ thống được sử dụng một cách an toàn, không gây rủi ro cho tính bảo mật, tính toàn vẹn, và tính khả dụng của các tài sản thông tin.

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC
a) Khởi tạo

Ở thời điểm này, an ninh được xem xét không chỉ ở khía cạnh kỹ thuật mà còn là rủi ro đối với hoạt động kinh doanh, với sự tham gia của bộ phận an ninh thông tin.

Các hoạt động an ninh chính cho giai đoạn này bao gồm:

- Xác định ban đầu các yêu cầu kinh doanh về tính bảo mật, tính toàn vẹn và tính khả dụng;

- Xác định phân loại thông tin và nhận dạng các yêu cầu xử lý đặc biệt đã biết để truyền, lưu trữ hoặc tạo thông tin như thông tin nhận dạng cá nhân; và

- Xác định bất kỳ yêu cầu nào về quyền riêng tư.

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC
b) Phát triển hoặc mua lại

Phần này tập trung vào các yếu tố an ninh trong giai đoạn thứ hai của SDLC, với các hoạt động chính bao gồm:

- Thực hiện đánh giá rủi ro và sử dụng kết quả để cải thiện các biện pháp kiểm soát an ninh cơ bản;

- Phân tích các yêu cầu an ninh;

- Thực hiện thử nghiệm chức năng và an ninh;

- Chuẩn bị các tài liệu ban đầu để chứng nhận và công nhận hệ thống;

- Thiết kế kiến trúc an ninh.

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC
c) Triển khai hoặc Đánh giá

Trong giai đoạn này, hệ thống sẽ được cài đặt và đánh giá trong môi trường hoạt động của tổ chức.

Các hoạt động an ninh chính cho giai đoạn này bao gồm:

- Tích hợp hệ thống thông tin vào môi trường của nó;

- Lên kế hoạch và tiến hành các hoạt động chứng nhận hệ thống đồng bộ với việc thử nghiệm các biện pháp kiểm soát an ninh;

- Hoàn tất các hoạt động cấp phép cho hệ thống.

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC
d) Vận hành và Bảo trì

Trong giai đoạn này, hệ thống được vận hành, cải tiến và điều chỉnh nếu cần, bao gồm việc bổ sung hoặc thay thế phần cứng và phần mềm. Hệ thống được giám sát để đảm bảo tuân thủ các yêu cầu an ninh và duy trì hoạt động hiệu quả.

Các hoạt động an ninh chính cho giai đoạn này bao gồm:

- Đánh giá khả năng hoạt động: Đảm bảo HT hoạt động tốt

- Quản lý cấu hình của hệ thống;

- Thiết lập các quy trình và thủ tục để đảm bảo hoạt động và giám sát liên tục các biện pháp kiểm soát an ninh của hệ thống thông tin;

- Thực hiện việc cấp phép lại cho HT khi có các thay đổi ảnh hưởng đến mức độ an ninh.

2.3. An ninh SDLC
2.5.3. Phương pháp tiếp cận an ninh SDLC
e) Xử lý

Xử lý, quy định về việc xử lý hệ thống và đóng bất kỳ hợp đồng nào đang có. Khi các hệ thống thông tin được chuyển giao, trở nên lỗi thời hoặc không còn sử dụng được nữa, phải đảm bảo rằng các nguồn lực và tài sản được bảo vệ.

Các hoạt động an ninh chính cho giai đoạn này bao gồm:

- Xây dựng và thực hiện kế hoạch xử lý/chuyển đổi;
- Lưu trữ thông tin quan trọng;
- Vệ sinh phương tiện;
- Xử lý phần cứng và phần mềm.

2.4. Kỹ thuật phát hiện Malware
2.4.1. Đặc điểm Malware

Bốn đặc điểm đơn giản của phần mềm độc hại có thể được sử dụng để hiểu, phản hồi và xóa bỏ phần mềm độc hại, cũng như trả lời các câu hỏi của người dùng:

1. Vectơ lây nhiễm ban đầu (Malware xâm nhập vào hệ thống như thế nào).

2. Cơ chế lan truyền (Malware di chuyển giữa các hệ thống như thế nào).

3. Cơ chế tồn tại dai dẳng (Malware vẫn tồn tại trên hệ thống như thế nào, và tồn tại sau khi khởi động lại và khi người dùng đăng xuất).

4. Các hiện vật (những dấu vết mà Malware để lại trên hệ thống do kết quả thực thi của nó) mà bạn có thể tìm kiếm trong quá trình kiểm tra.

2.4. Kỹ thuật phát hiện Malware
2.4.1. Đặc điểm Malware
a) Vectơ lây nhiễm ban đầu

- Người dùng mở hoặc nhấp đúp vào tệp đính kèm email thực sự là tài liệu độc hại, người dùng nhấp vào liên kết đến trang web độc hại hoặc bị nhiễm, các "lượt truy cập" của trình duyệt khác.
- Hệ thống cũng có thể bị nhiễm khi các thiết bị lưu trữ di động (ví dụ: ổ đĩa USB, iPod, v.v.) bị nhiễm được kết nối với hệ thống.
- Cơ sở hạ tầng chia sẻ tệp ngang hàng (P2P) là một phương tiện phổ biến khác mà hệ thống có thể bị nhiễm.

2.4. Kỹ thuật phát hiện Malware
2.4.1. Đặc điểm Malware
b) Cơ chế lan truyền

- Khai thác lỗ hổng dựa trên mạng.
- Sử dụng chức năng kinh doanh hoạt động bằng cách ghi vào các thư mục hoặc chia sẻ trên mạng mà mọi người có thể truy cập
- Gửi bản sao của chính nó hoặc phần mềm độc hại khác cho mọi người có địa chỉ email trong danh sách liên lạc.

2.4. Kỹ thuật phát hiện Malware
2.4.1. Đặc điểm Malware
c) Cơ chế duy trì

- Sử dụng Registry với cơ chế tự động khởi động. Malware có thể chạy mà không cần người dùng phải làm gì, chỉ cần khởi động máy tính hoặc đăng nhập vào tài khoản.
- Lây nhiễm vào các tệp chương trình hoặc tệp dữ liệu. Khi bạn mở hoặc truy cập những tệp này, Malware sẽ tự động khởi động cùng với chúng.
- Một cơ chế duy trì thông qua chức năng tác vụ theo lịch trình của Windows. Tự khởi động vào những thời điểm được chỉ định.
- Malware vẫn duy trì bằng cách đặt một tệp thực thi vào thư mục Start Menu\ Programs\Startup, khiến tệp được khởi chạy khi người dùng đăng nhập vào hệ thống.
- Trong môi trường mạng, các hệ thống xung quanh có thể theo dõi và phát tán phần mềm độc hại sang các hệ thống khác

2.4. Kỹ thuật phát hiện Malware
2.4.1. Đặc điểm Malware
d) Hiện vật

Các hiện vật là những dấu hiệu cho thấy phần mềm độc hại đã tồn tại và hoạt động, nhưng chúng không phải là công cụ mà phần mềm độc hại sử dụng để duy trì sự hiện diện của nó.

Các cơ chế duy trì sự tồn tại của phần mềm độc hại được xem là một phần các hiện vật.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware

Có nhiều kỹ thuật mà tác giả Malware sử dụng để ẩn chương trình của chúng khỏi bị phát hiện, thậm chí còn làm cho chương trình của chúng trông giống một chương trình Windows bình thường nhất có thể. Đôi khi, họ thậm chí còn dựa vào những phương pháp mà các nhà phân tích sử dụng để phát hiện phần mềm độc hại nhằm tránh bị phát hiện.

Cách hiệu quả nhất mà một nhà phân tích có thể áp dụng là sử dụng một quy trình được ghi chép cẩn thận. Điều này sẽ giúp họ giảm số lượng tệp cần phải xem xét xuống mức có thể quản lý dễ dàng hơn.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware

a) Quét Virus

b) Phân tích Log

c) Phân tích chuyên sâu

- Tập tin được đóng gói
- Chữ ký số
- Windows File Protection (WFP)
- Alternate Data Streams (ADS)
- Thời gian biên dịch PE (Portable Executable)
- Lây nhiễm MBR
- Phân tích Registry
- Hoạt động Internet

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
a) Quét Virus

- Bkav
- Kaspersky
- Sophos Home
- ESET Smart Security
- MalwareBytes
- Comodo Antivius
- Windows Defender
- Avira Free Antivirus
- Avast Free Antivirus
- AVG Free Antivirus
- Bitdefender Free Antivirus
- FortiClient

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
b) Phân tích Log

- Kiểm tra Log của phần mềm diệt Virus
- Kiểm tra Log cuả MRT (Microsoft's Malicious Software Removal Tool)
- Kiểm tra Log của Windows Defender
- Kiểm tra Log của Debugging Tools for Windows

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Tập tin được đóng gói

Nén hoặc đóng gói (Packing) là một phương pháp giúp giảm kích thước tệp, nhưng quan trọng hơn, nó còn được sử dụng để ẩn bản chất thực sự của các tệp thực thi di động (PE - Portable Executable) nhằm tránh bị phát hiện bởi các công cụ quét phần mềm độc hại (AV).

Công cụ kiểm tra tệp đã đóng gói:

- PEiD (https://www.aldeid.com/wiki/PEiD), có sẵn miễn phí quét các tệp trong một thư mục, cũng như lặp lại qua các thư mục con và chỉ quét các tệp PE.
- YARA (https://virustotal.github.io/yara), trình quét dựa trên quy tắc, trong đó người dùng có thể xác định bộ quy tắc của riêng mình, dựa trên chuỗi, mẫu hướng dẫn, biểu thức chính quy, v.v., để phát hiện và phân loại phần mềm độc hại.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Chữ ký số

Kiểm tra các tệp thực thi để tìm chữ ký số hợp lệ là một cách tiếp cận có giá trị để phát hiện phần mềm độc hại.

- Sigcheck (https://learn.microsoft.com/en-us/sysinternals/downloads/sigcheck), Công cụ này cho phép nhà phân tích quét hệ thống để tìm các tệp thực thi không có chữ ký số.
- Autoruns (https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns), hỗ trợ để xem các hình ảnh tự động khởi động của bên thứ ba đã được thêm vào hệ thống.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Windows File Protection (WFP)

Windows File Protection (WFP) là một quy trình chạy ngầm trên Windows, ngăn các chương trình thay thế các File hệ thống Windows quan trọng.

Kẻ tấn công có thể vô hiệu hóa tạm thời WFP và thay thế hoặc lây nhiễm File được bảo vệ, sau đó WFP được bật lại. WFP không thăm dò hoặc quét, mà chỉ lắng nghe và chờ các sự kiện thay đổi File, do đó, sau khi được bật lại, File đã sửa đổi sẽ không bị phát hiện.

Sử dụng công cụ SFC (System File Checker) có trên Windows để sửa chữa các File hệ thống bị thiếu hoặc bị hỏng.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Alternate Data Streams (ADS)

ADS là một tính năng của hệ thống tệp NTFS, được thiết kế để cung cấp khả năng tương thích với Hệ thống tệp phân cấp Macintosh (HFS).

ADS cho phép lưu trữ dữ liệu bổ sung cho các tệp mà không làm thay đổi kích thước của tệp chính. Điều này có nghĩa là bạn có thể lưu trữ thông tin ẩn mà không ai có thể thấy chỉ bằng cách kiểm tra tệp bình thường.

ADS có thể không dễ phát hiện, ngay cả khi sử dụng các công cụ phân tích pháp y. Hàng nghìn File trên hệ thống có thể có ADS mà không được hiển thị rõ ràng.

Streams (https://learn.microsoft.com/en-us/sysinternals/downloads/streams), cho phép người dùng xem và quản lý ADS trên hệ thống.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Thời gian biên dịch PE (Portable Executable)

Thời gian biên dịch tệp PE (Portable Executable) là một yếu tố quan trọng trong việc phát hiện các tệp đáng ngờ, đặc biệt là phần mềm độc hại.

Các dấu thời gian trong siêu dữ liệu của tệp thường bị sửa đổi (timestomped) để ngụy trang cho File độc hại, giúp nó hòa lẫn với các File hợp lệ của ứng dụng và hệ điều hành.

Do đó, việc so sánh thời gian biên dịch từ tiêu đề PE với thời gian được tạo và sửa đổi từ siêu dữ liệu tệp và tìm kiếm các điểm bất thường có thể cho phép bạn xác định phần mềm độc hại.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Lây nhiễm MBR

Lây nhiễm MBR (Master Boot Record) là phần mềm độc hại lây nhiễm vào Bảng ghi khởi động của ổ cứng.

Để phát hiện trình lây nhiễm MBR, Bằng cách sử dụng công cụ mmls.exe từ Sleuthkit, có thể tìm ra vị trí bắt đầu của phân vùng, thường là sector 63. Sau đó, họ có thể kiểm tra từ sector 0 đến 63 để tìm các sector không chứa toàn số không, nếu các sector 0, 10 và 63 chứa dữ liệu khác ngoài số không, điều này có thể chỉ ra sự tồn tại của phần mềm độc hại.

Adwcleaner (https://www.malwarebytes.com/adwcleaner), Trình dọn dẹp adware, tìm và xóa các chương trình không mong muốn và phần mềm rác.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Lây nhiễm MBR

Lây nhiễm MBR (Master Boot Record) là phần mềm độc hại lây nhiễm vào Bảng ghi khởi động của ổ cứng.

Để phát hiện trình lây nhiễm MBR, Bằng cách sử dụng công cụ mmls.exe từ Sleuthkit, có thể tìm ra vị trí bắt đầu của phân vùng, thường là sector 63. Sau đó, họ có thể kiểm tra từ sector 0 đến 63 để tìm các sector không chứa toàn số không, nếu các sector 0, 10 và 63 chứa dữ liệu khác ngoài số không, điều này có thể chỉ ra sự tồn tại của phần mềm độc hại.

Adwcleaner (https://www.malwarebytes.com/adwcleaner), Trình dọn dẹp phần mềm quảng cáo, tìm và xóa các chương trình không mong muốn và phần mềm rác.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Phân tích Registry

Phân tích Registry là một kỹ thuật quan trọng và có thể mang lại nhiều thông tin khi tìm kiếm phần mềm độc hại. một đặc điểm chung của các phần mềm độc hại là sử dụng tên dịch vụ ngẫu nhiên và chạy dưới quy trình svchost.exe để duy trì sự tồn tại của chúng. Ngoài cơ chế duy trì, phần mềm độc hại còn có thể để lại nhiều dấu hiệu khác trong Registry.

Process Monitor (https://learn.microsoft.com/en-us/sysinternals/downloads/procmon), hiển thị hệ thống tệp, Registry và hoạt động của quy trình/luồng theo thời gian thực.

2.4. Kỹ thuật phát hiện Malware
2.4.2. Phát hiện Malware
c) Phân tích chuyên sâu

Hoạt động Internet

Nhiều nhà phân tích thường xem xét hoạt động Internet của người dùng để xác định các trang web mà họ đã truy cập, kỹ thuật này cũng có thể được áp dụng để phát hiện sự hiện diện của phần mềm độc hại và xác định nguồn gốc của nó.

Khi kẻ xâm nhập đưa phần mềm độc hại vào hệ thống, họ thường có quyền truy cập cao, như quyền Quản trị viên. Với quyền này, họ có thể tạo các tác vụ theo lịch trình hoặc dịch vụ Windows, cho phép phần mềm độc hại chạy với quyền cao hơn. Nếu phần mềm độc hại sử dụng API WinInet (cũng là API mà Internet Explorer sử dụng) để kết nối ra bên ngoài, bạn có thể tìm thấy dấu hiệu của hoạt động này trong hệ thống, chẳng hạn như các mục trong tệp index.dat nằm trong Thư mục Tệp Internet Tạm thời (TIF) của người dùng "User Default".

ProDiscover (https://prodiscover.com/), có thể hỗ trợ phân tích lịch sữ Internet.

Cảm ơn các bạn,

Chúc các bạn thành công!