

# Chương 3: Vấn đề an ninh trong TMĐT

---

# Nội dung

---

Nguyên tắc bảo mật

Một số khái niệm

NIST Cybersecurity Framework

# Nguyên tắc bảo mật

---

Tính sẵn sàng (Availability)

Tính toàn vẹn (Integrity)

Tính bí mật (Confidentiality)

Tính chống thoái thác (Non-repudiation)

# Tính sẵn sàng - Availability

---

Dữ liệu và tài nguyên

- Đảm bảo độ tin cậy và truy cập kịp thời cho người dùng hợp pháp

Các thiết bị mạng, máy tính và ứng dụng

- Cung cấp đầy đủ chức năng để hoạt động bình thường với hiệu suất có thể chấp nhận được
- Có thể phục hồi sau sự cố gián đoạn một cách an toàn và nhanh chóng, không ảnh hưởng đến hiệu suất
- Có các cơ chế bảo vệ cần thiết để bảo vệ khỏi các mối đe dọa bên trong và bên ngoài có thể ảnh hưởng đến tính sẵn sàng và hiệu suất

# Tính toàn vẹn - Integrity

---

Đảm bảo về tính chính xác và độ tin cậy của thông tin và hệ thống, ngăn chặn các thao tác sửa đổi trái phép.

Đảm bảo những kẻ tấn công, sai sót của người dùng không ảnh hưởng đến tính toàn vẹn của hệ thống hoặc dữ liệu.

Phần cứng, phần mềm và các cơ chế giao tiếp

- Hoạt động phối hợp để duy trì và xử lý dữ liệu chính xác,
- Truyền dữ liệu đến đích chính xác.

Hệ thống và mạng

- Được bảo vệ khỏi sự can thiệp từ bên ngoài

# Tính bí mật - Confidentiality

---

Đảm bảo bí mật được thực thi tại mỗi điểm giao trong quy trình xử lý dữ liệu, ngăn chặn việc tiết lộ trái phép.

- Dữ liệu nằm trên các hệ thống và thiết bị trong mạng
- Dữ liệu được truyền đi
- Dữ liệu đến đích.

Có thể được cung cấp bằng cách

- mã hóa dữ liệu được lưu trữ , truyền đi
- thực thi kiểm soát truy cập nghiêm ngặt và phân loại dữ liệu
- đào tạo nhân viên về các quy trình bảo vệ dữ liệu thích hợp.

# Tính chống thoái thác - Non-repudiation

---

## Đảm bảo

- Người gửi thông tin được cung cấp bằng chứng gửi
- Người nhận được cung cấp bằng chứng về danh tính của người gửi
- → Không thể phủ nhận việc đã xử lý thông tin

Bảo vệ chống lại một cá nhân từ chối đã thực hiện một hành động cụ thể.

- Cung cấp khả năng xác định một cá nhân nhất định có thực hiện một hành động cụ thể
  - tạo thông tin
  - gửi tin nhắn
  - phê duyệt thông tin
  - nhận tin nhắn

# Nội dung

---

Nguyên tắc bảo mật



**Một số khái niệm**

NIST Cybersecurity Framework



# Lỗ hổng bảo mật - Vulnerability

---

Thiếu biện pháp đối phó hoặc một điểm yếu trong biện pháp đối phó được áp dụng.

- điểm yếu của phần mềm, phần cứng, quy trình hoặc con người có thể bị khai thác.

Có thể là

- dịch vụ chạy trên server, các ứng dụng hoặc hệ điều hành chưa được vá
- điểm truy cập không dây không hạn chế
- cổng mở trên tường lửa
- bảo mật vật lý lỏng lẻo
- quản lý mật khẩu không bắt buộc trên servers và workstations

# Mối đe dọa - Threat

---

Mối nguy hiểm tiềm ẩn liên quan đến việc khai thác lỗ hổng.

Ai đó/cái gì đó xác định một lỗ hổng cụ thể → sử dụng nó để chống lại công ty hoặc cá nhân.

Thực thể lợi dụng lỗ hổng được gọi là tác nhân đe dọa (Threat Agent)

Threat Agent có thể là

- Kẻ xâm nhập truy cập mạng bất hợp pháp
  - công trên tường lửa
  - quy trình truy cập dữ liệu theo cách vi phạm chính sách bảo mật
- Nhân viên phạm lỗi vô ý có thể làm lộ thông tin bí mật.

# Rủi ro - Risk

---

Khả năng Threat Agent khai thác lỗ hổng và tác động đến các nghiệp vụ tương ứng.

Nếu Firewall có nhiều ports được mở, thì nhiều khả năng xảy ra sự cố: kẻ tấn công xâm nhập trái phép vào mạng.

Nếu một người dùng không được đào tạo về processes và procedures, thì nhiều khả năng xảy ra sự cố về việc vô tình hoặc cố ý phá hủy dữ liệu.

Nếu một hệ thống phát hiện xâm nhập (IDS) không được triển khai trên mạng, thì khả năng xảy ra sự cố phát hiện chậm trễ các tấn công vào mạng.

Risk có mối quan hệ mật thiết với Vulnerability, Threat, Exposure

# Exposure

---

Mô tả tổn thất cho tổ chức.

Một Vulnerability có thể gây ra nhiều sự tổn thất.

- Nếu quản lý mật khẩu lỏng lẻo và không triển khai thực hiện quy định cho mật khẩu, tổ chức có thể bị tổn thất từ mối đe dọa capture mật khẩu người dùng hoặc sử dụng trái phép.
- Nếu tổ chức không thường xuyên kiểm tra hệ thống dây điện và không trang bị hệ thống phòng cháy chữa cháy, thì tổn thất có thể xảy ra do toàn bộ hệ thống bị tàn phá khi có sự cố hỏa hoạn.

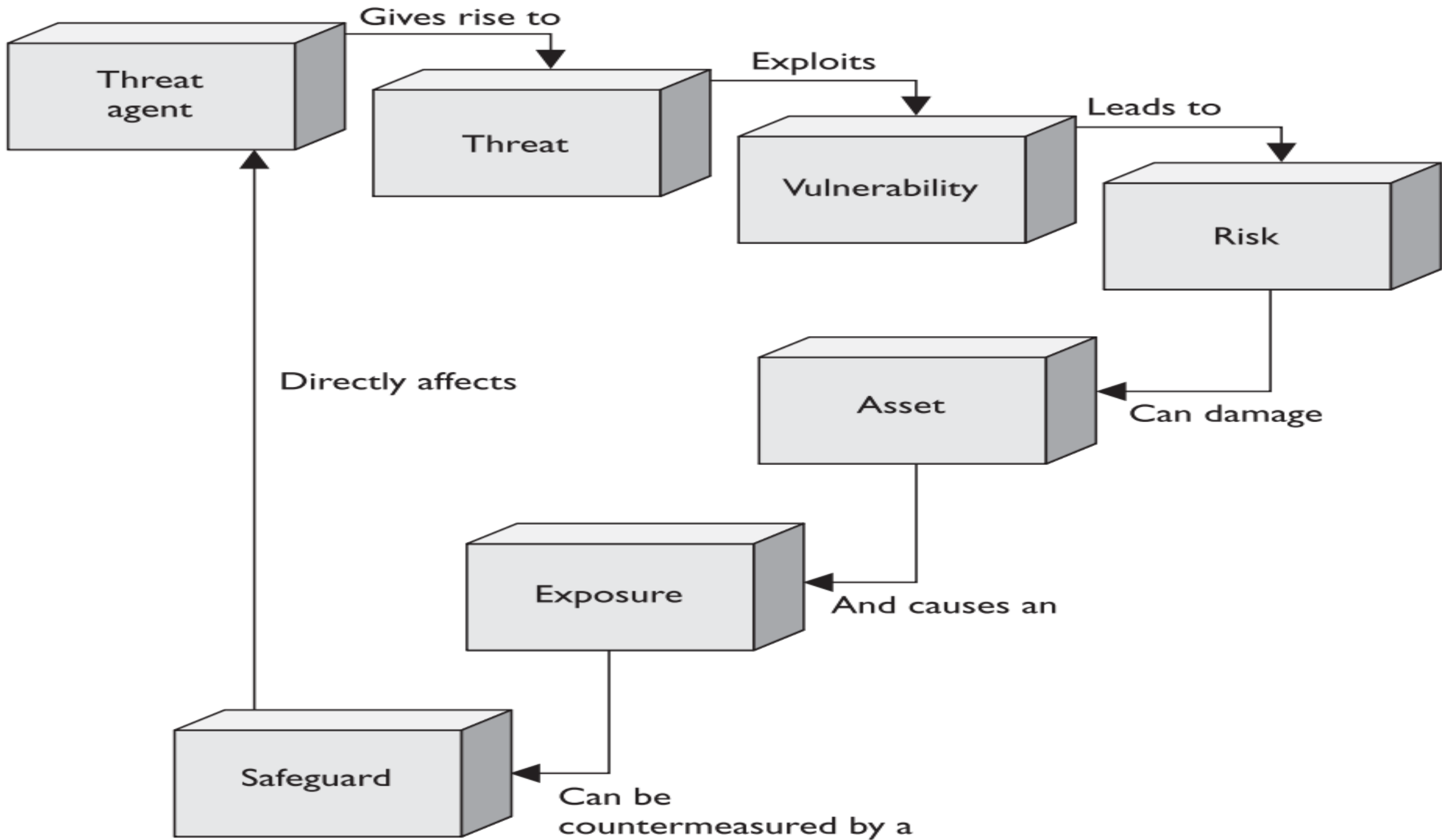
# Biện pháp kiểm soát/biện pháp đối phó - Control/Countermeasure

---

Được đưa ra để giảm thiểu rủi ro tiềm ẩn.

Biện pháp đối phó có thể là

- cấu hình phần mềm
- thiết bị phần cứng
- quy trình loại bỏ lỗ hổng bảo mật
- làm giảm khả năng Threat Agent có thể khai thác lỗ hổng.



# Nội dung

---

Nguyên tắc bảo mật

Một số khái niệm

★ **NIST Cybersecurity Framework**

# NIST Cybersecurity Framework

---

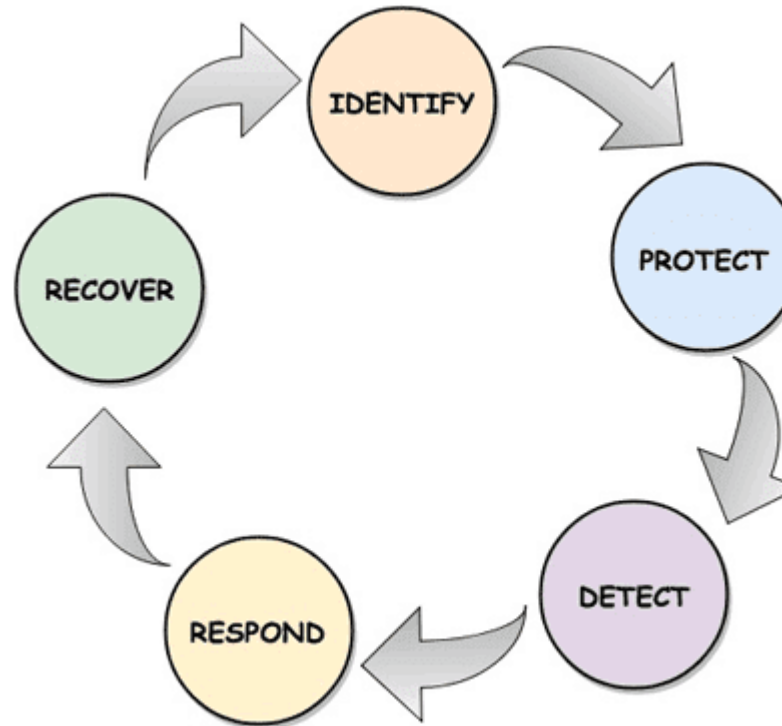
Xác định

Bảo vệ/Ngăn chặn

Phát hiện

Ứng phó

Phục hồi





# Xác định

---

Lập danh sách tất cả tài sản

- thiết bị
- phần mềm
- dữ liệu
- ...

Xác định các mối đe dọa có thể xảy ra với mỗi tài sản

Đánh giá mức độ ưu tiên của tài sản và các mối đe dọa

Tài sản	Độ ưu tiên
TS1	1
TS2	1
TS3	2
TS4	3
...	

# Xác định các mối đe dọa

---

Các mối đe dọa được chia làm 4 loại:

- Xem thông tin một cách bất hợp pháp
- Chỉnh sửa thông tin một cách bất hợp pháp
- Từ chối dịch vụ
- Từ chối hành vi

# Các mối đe dọa thường gặp

---

Lỗi và thiếu sót của người dùng (Errors and Omissions)

Gian lận và đánh cắp thông tin (Fraud and Theft)

Malicious Hackers

Malware

Tấn công từ chối dịch vụ (Denial-of-Service Attacks – DoS/DDoS)

Tấn công XSS

Tấn công SQL Injection

Social Engineering

# Lỗi và thiếu sót của người dùng

---

Mối đe dọa của hệ thống thông tin xuất phát từ những lỗi bảo mật, lỗi thao tác của những người dùng trong hệ thống.

Là mối đe dọa hàng đầu đối với một hệ thống thông tin

Giải pháp:

- Huấn luyện người dùng thực hiện đúng các thao tác, hạn chế sai sót
- Nguyên tắc: quyền tối thiểu (least privilege)
- Thường xuyên back-up hệ thống

# Gian lận và đánh cắp thông tin

---

Mối đe dọa này do những kẻ tấn công từ bên trong hệ thống (inner attackers), gồm những người dùng giả mạo hoặc những người dùng có ý đồ xấu.

Giải pháp:

- Định ra những chính sách bảo mật tốt: có chứng cứ xác định được kẻ tấn công từ bên trong

# Malicious Hackers

---

Kẻ tấn công nguy hiểm xâm nhập vào hệ thống để tìm kiếm thông tin, phá hủy dữ liệu, phá hủy hệ thống.

5 bước để tấn công vào một hệ thống:

- Thăm dò (Reconnaissance)
- Quét lỗ hổng để tấn công (Scanning)
- Cố gắng lấy quyền truy cập (Gaining access)
- Duy trì kết nối (Maintaining access)
- Xóa dấu vết (Cover his track)

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- Trojan horses
- Ransomware
- Spyware
- Botnet
- Adware



# Viruses

---

Là chương trình được thiết kế để thực hiện tối thiểu hai việc

- tự xen vào hoạt động hiện hành của máy tính để thực hiện tự nhân bản và những công việc theo chủ ý của người lập trình
- tự sao chép chính nó (nhân bản) lây nhiễm vào những tập tin (file) hay các vùng xác định (boot, FAT sector) ở các thiết bị lưu trữ như đĩa cứng, đĩa mềm, thiết bị nhớ flash (phổ biến là USB),... thậm chí cả EPROM chính của máy

# Các loại virus

---

System/Boot Sector Virus

Direct Action Virus

Resident Virus

Multipartite Virus

Polymorphic Virus

Overwrite Virus

Cavity/Space-filler Virus

File infectors

Macro Virus

Rootkit virus

# Virus

---

Cách virus che dấu để tránh các chương trình antivirus:

- Mã hóa chính nó
- Thay đổi thư mục với các byte virus bổ sung
- Sử dụng thuật toán ẩn để chuyển hướng dữ liệu

# Phần mềm độc hại - Malware

---

- Viruses
- **Worms**
- Trojan horses
- Ransomware
- Spyware
- Botnet
- Adware

# Phần mềm độc hại - Malware

---

- Viruses
- **Worms**
- Trojan horses
- Ransomware
- Spyware
- Botnet
- Adware

# Worm

---

Sâu máy tính là một loại phần mềm độc hại lây lan các bản sao của nó từ máy tính này sang máy tính khác.

Sâu có thể tự nhân bản mà không cần bất kỳ sự tương tác nào của con người

Nó không cần phải gắn vào một chương trình phần mềm để gây hại.

# Một số loại worm

---

Internet Worms

Email Worms

Instant Messaging Worms

File-Sharing Worms

IRC Worms

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- **Trojan horses**
- Ransomware
- Spyware
- Botnet
- Adware



# Trojan horses

---

Một loại phần mềm độc hại được ngụy trang dưới dạng phần mềm hợp pháp, chạy ẩn trên hệ thống bị nhiễm

Tội phạm mạng lừa người dùng tải Trojan lên máy tính của họ với nhiều mục đích khác nhau:

- sửa đổi dữ liệu
- sao chép dữ liệu
- xóa dữ liệu
- chặn dữ liệu
- ...

# Một số loại trojan horses

---

Trojan-Banker

Trojan-DDoS

Trojan-Downloader

Trojan-IM

Backdoor Trojan

Trojan-SMS

....

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- Trojan horses
- **Ransomware**
- Spyware
- Botnet
- Adware

# Ransomware

---

một loại phần mềm độc hại mà tội phạm mạng sử dụng để đòi tiền chuộc.

chặn quyền truy cập vào hệ thống hoặc mã hóa dữ liệu trên hệ thống  
có thể lây lan sang máy tính thông qua

- file đính kèm hoặc link trong email lừa đảo
- các trang web bị nhiễm virus
- download
- USB driver bị nhiễm.

# Một số loại ransomware

---

## Crypto ransomware

- mã hóa các file có giá trị trên máy tính để người dùng không thể truy cập chúng.

## Locker ransomware

- khóa không cho nạn nhân truy cập vào thiết bị của họ,

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- Trojan horses
- Ransomware
- **Spyware**
- Botnet
- Adware

# Spyware

---

phần mềm được thiết kế để thu thập dữ liệu của người dùng và chuyển tiếp dữ liệu đó cho bên thứ ba mà người dùng không đồng ý hoặc không biết

- phần mềm gián điệp có thể nắm bắt thông tin thẻ tín dụng của người dùng.

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- Trojan horses
- Ransomware
- Spyware
- **Botnet**
- Adware



# Botnet

---

Là sự kết hợp của hai từ, “robot” và “network”

Là một mạng các máy tính bị xâm nhập được giám sát bởi một kênh chỉ huy và kiểm soát (C&C)

Máy tính bị nhiễm

- Bot được gọi là Zombie
- Bị chỉ huy và kiểm soát bởi Botmaster
- Được sử dụng để
  - khởi động các cuộc tấn công DDoS
  - Lan truyền malware, spam hoặc nội dung độc hại
  - thu thập thông tin đăng nhập
  - thực hiện các tác vụ đòi hỏi nhiều CPU,...

# Phần mềm độc hại - Malware

---

- Viruses
- Worms
- Trojan horses
- Ransomware
- Spyware
- Botnet
- **Adware**

# Adware

---

là phần mềm không mong muốn

được thiết kế để hiển thị quảng cáo trên màn hình thiết bị của người dùng, điều hướng các yêu cầu tới website quảng cáo và thu thập các kiểu marketing data khác nhau

# Tấn công từ chối dịch vụ

---

Là kiểu tấn công ngăn không cho những người dùng khác truy cập vào hệ thống

Làm cho hệ thống bị quá tải và không thể hoạt động

DoS: tấn công “one-to-one”

DDoS(distributed denial of service)

Sử dụng các Zombie host

Tấn công “many-to-one”

# Tấn công XSS

---

Cross-Site Scripting là lỗ hổng bảo mật cho phép những kẻ tấn công đưa mã độc vào một trang web hợp pháp.

Các tập lệnh này có được quyền của các tập lệnh được tạo bởi trang web mục tiêu và do đó có thể ảnh hưởng đến tính bảo mật và tính toàn vẹn của việc truyền dữ liệu giữa trang web và khách hàng.

Các trang web dễ bị tấn công nếu chúng hiển thị dữ liệu do người dùng cung cấp từ các request hoặc form mà không làm sạch dữ liệu trước khi thực thi.

# Tấn công SQL Injection

---

Khai thác lỗ hổng bảo mật SQL injection

Có thể thực hiện khi website có lỗ hổng bảo mật có thể gây ra SQL injection

Kẻ tấn công có thể gửi một yêu cầu với các tham số để thực hiện cuộc tấn công SQL injection → cho phép xâm nhập cơ sở dữ liệu, thông tin đăng nhập của người dùng và trong một số cấu hình nhất định, truy cập vào hệ điều hành.

# Social Engineering

---

Social engineering sử dụng sự ảnh hưởng và sự thuyết phục để đánh lừa người dùng nhằm khai thác các thông tin có lợi cho cuộc tấn công hoặc thuyết phục nạn nhân thực hiện một hành động nào đó

Kẻ tấn công có thể lợi dụng các đặc điểm sau của con người để tấn công:

Mong muốn trở nên hữu dụng

Tin người

Nỗi sợ gặp rắc rối

Đơn giản đến mức cầu thả

# Social engineering

---

Nhân viên gián điệp/giả mạo

Giả làm người cần được giúp đỡ

Giả làm người quan trọng

Giả làm người được ủy quyền

Giả làm nhân viên hỗ trợ kỹ thuật



# Social engineering

---

Phishing: lừa đảo qua thư điện tử

Vishing: lừa đảo qua điện thoại

Pop-up Windows

File đính kèm trong email

Các website giả mạo

Các phần mềm giả mạo

# NIST Cybersecurity Framework

---

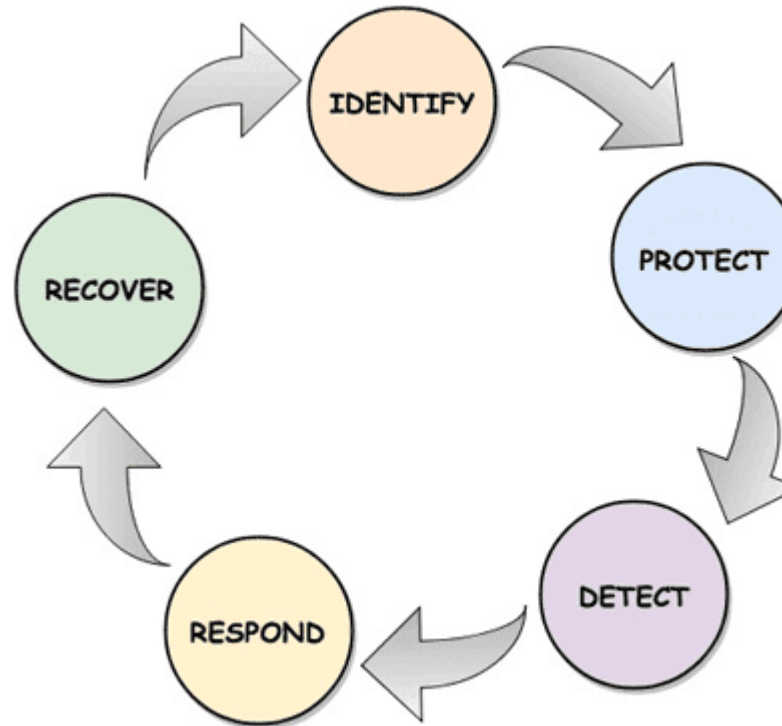
Xác định

Bảo vệ/Ngăn chặn

Phát hiện

Ứng phó

Phục hồi



# Bảo vệ/Ngăn chặn

---

kiểm soát truy cập của công ty, bảo mật dữ liệu và bảo trì,...

→ đảm bảo an ninh mạng trong và xung quanh môi trường kinh doanh.

# Phát hiện

---

Xác định bất kỳ vi phạm nào bằng cách

- Giám sát nhật ký
- Thực hiện các quy trình phát hiện xâm nhập ở cấp độ mạng và thiết bị
- ...

Thông tin bảo mật và quản lý sự kiện đều được bảo vệ theo thủ tục này.

# Ứng phó

---

Thực hiện sau khi phát hiện vi phạm

Các tổ chức cần có các quy trình ứng phó rủi ro: đào tạo nhân viên hiểu về các vi phạm, ứng phó khi rủi ro xảy ra, khắc phục lỗ hổng và tiến hành khôi phục.

→ Giảm thiểu hậu quả sau khi rủi ro xảy ra

# Phục hồi

---

Phục hồi các quy trình lập kế hoạch, hệ thống khắc phục thảm họa và kế hoạch dự phòng, ... sẽ được xử lý trong giai đoạn này

# Tình huống

---

Ban Giám đốc của một tổ chức dịch vụ tài chính quốc tế đang xem xét kế hoạch sáp nhập bí mật.

CIO nhận được một email đòi tiền chuộc từ một nguồn không xác định nói rằng họ biết về kế hoạch sáp nhập và có thông tin cá nhân của 150.000 khách hàng. Một mẫu chi tiết cá nhân của 500 khách hàng đã được đưa vào email đòi tiền chuộc làm "bằng chứng".

Tổ chức phải trả khoản tiền chuộc đáng kể bằng Bitcoin. Nếu không, kế hoạch sáp nhập sẽ bị công bố và thông tin khách hàng sẽ bị bán công khai trên mạng.