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 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.

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
  - cổng 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.

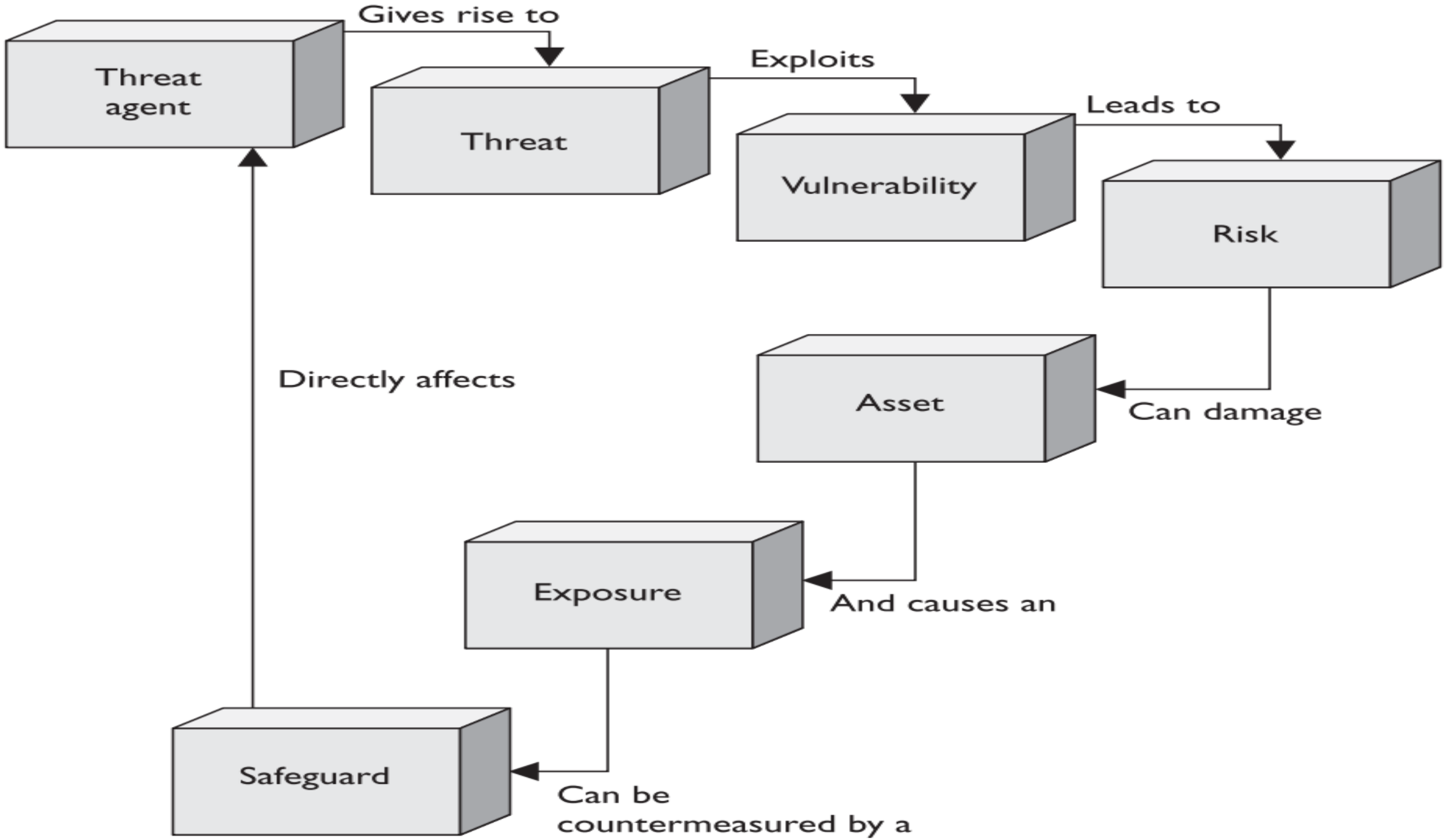
- Nếu quản lý mật khẩu lỏng lẻo và không triển khai thực hiện quy định cho mật khẩu, tổ chức có thể bị tổn thất từ mối đe dọa capture mật khẩu người dùng hoặc sử dụng trái phép.
- Nếu tổ chức không thường xuyên kiểm tra hệ thống dây điện và không trang bị hệ thống phòng cháy chữa cháy, thì tổn thất có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


Threat agent
Gives rise to
Threat
Exploits
Vulnerability
Leads to
Risk
Asset
Can damage
Directly affects
Exposure
And causes an
Safeguard
Can be countermeasured by a

Nội dung

Nguyên tắc bảo mật

Một số khái niệm

NIST Cybersecurity Framework

NIST Cybersecurity Framework

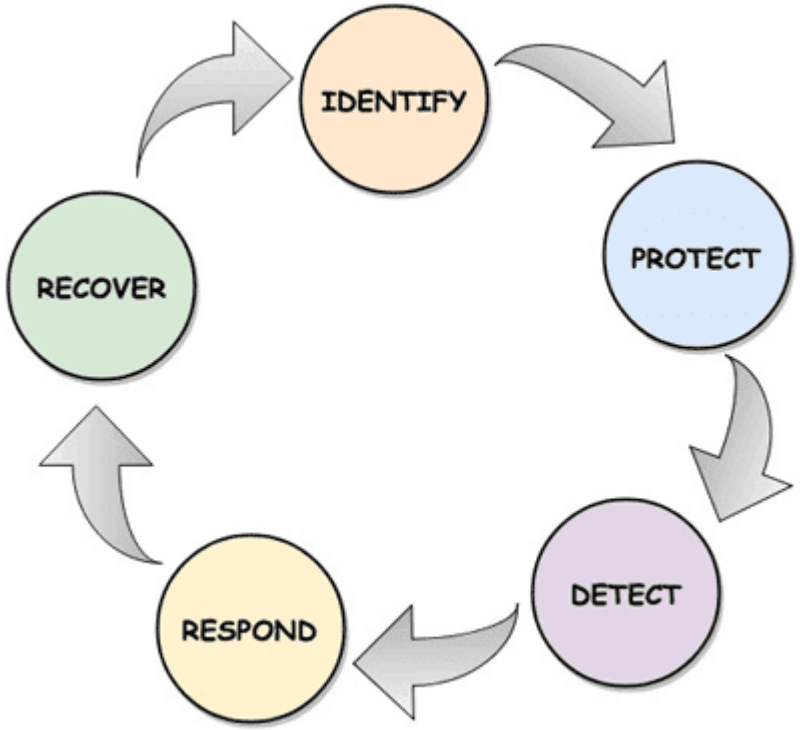
Xác định

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

Xác đinh các kiểu tấn công có thể thực hiện với mỗi tài sản

Một số kiểu tấn công:

- Tấn công có chủ đích (APT)
- Malware
- Từ chối dịch vụ (Denial-of-Service Attacks – DoS/DDoS)
- Man in the middle
- XSS
- SQL Injection
- Social Engineering

Tấn công có chủ đích (APT)

Kẻ tấn công xâm nhập vào hệ thống để tìm kiếm thông tin, thực hiện các hành vi bất hợp pháp

5 bước để tấn công vào một hệ thống:

- Thăm dò (Reconnaisance)
- 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

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 ransomeware

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

Từ chối dịch vụ (Dos/DDos)

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”

Man in the Middle (MITM)

Là một loại tấn công mạng mà hacker sẽ đứng giữa người dùng và ứng dụng. Kẻ tấn công chặn và kiểm soát toàn bộ quá trình giao tiếp giữa hai bên để người dùng tin rằng họ vẫn đang trực tiếp liên lạc với nhau.

Những kẻ tấn công sẽ nắm bắt hết mọi thông tin trao đổi kể cả những thông tin nhạy cảm như số tài khoản, số thẻ tín dụng…để đánh cắp danh tính, chuyển tiền hay gây ra các vụ lừa đảo.

Man in the Middle (MITM)

Giả mạo IP

Giả mạo hệ thống tên miền (giả mạo DNS)

Giả mạo HTTPS

Đánh cắp lớp cổng bảo mật (SSL)

Đánh cắp email

Nghe trộm wifi

Đánh cắp session

Nhiễm độc bộ nhớ cache

...

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.

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 cẩu 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

Phising: 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

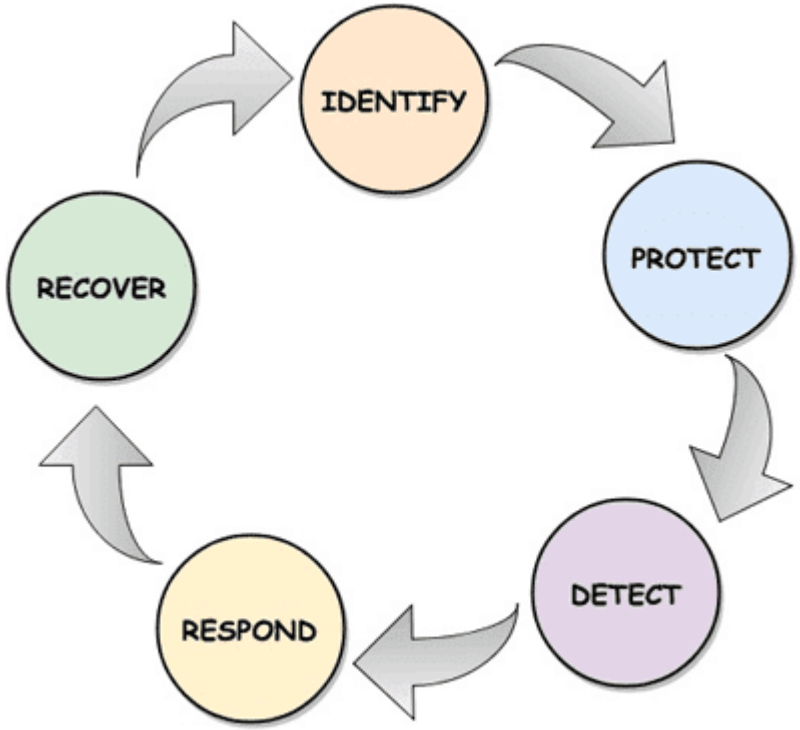
Xác định

Bảo vệ/Ngăn chặn

Phát hiện

Ứng phó

Phục hồi



Bảo vệ/Ngăn chặn

Hỗ trợ khả năng hạn chế hoặc ngăn chặn tác động của mối đe dọa an ninh mạng.

Bao gồm:

- Kiểm soát truy cập;
- Nhận thức và đào tạo;
- Bảo mật dữ liệu;
- Quy trình, thủ tục bảo vệ thông tin;
- Bảo trì
- Công nghệ/dịch vụ bảo mật

Phát hiện

Cho phép phát hiện kịp thời các sự cố an ninh mạng

Bao gồm:

- Phát hiện các thao tác bất thường
- Giám sát liên tục an ninh
- Quy trình phát hiện

Ứng phó

Thực hiện hành động thích hợp với sự cố an ninh mạng được phát hiện nhằm hỗ trợ khả năng ngăn chặn tác động của sự cố an ninh mạng, giảm thiểu thiệt hại

Bao gồm:

- Phân tích
- Giảm thiểu thiệt hại
- Lập kế hoạch ứng phó
- Truyền thông
- Cải tiến

Phục hồi

Các hoạt động thích hợp để khôi phục hoạt động kinh doanh hoặc dịch vụ nào bị thiệt hại do sự cố an ninh mạng, hỗ trợ phục hồi kịp thời các hoạt động bình thường để giảm tác động từ sự cố an ninh mạng.

Bao gồm:

- Lập kế hoạch phục hồi
- Truyền thông
- Cải tiến

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".

Tình huống

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.

Sau khi kiểm tra và xác định kẻ tấn công chỉ lấy được thông tin chi tiết của 500 khách hàng và một số file về kế hoạch sáp nhập