Yêu cầu:

1. **Hãy nhận dạng và giải thích được ít nhất 3 mối đe dọa ảnh hưởng đến an toàn đến dịch vụ/hệ thống/dữ liệu của công ty/doanh nghiệp được mô tả trong tình huống.**
   (tình huống cô sẽ cho tương tự như các tình huống minh họa ở dưới, các câu hỏi tương tự như các câu hỏi minh họa)

1. Tấn công mạng: Đây là một trong những mối đe dọa nghiêm trọng nhất đối với an ninh mạng của một công ty hay doanh nghiệp. Tấn công mạng có thể làm gián đoạn hoạt động của hệ thống, đánh cắp dữ liệu quan trọng, hoặc thậm chí làm thay đổi hoặc phá hủy dữ liệu.
2. Virus và phần mềm độc hại: Virus và phần mềm độc hại có thể được sử dụng để truy cập trái phép vào hệ thống của một công ty hay doanh nghiệp. Chúng có thể lây nhiễm qua email, trang web độc hại, hoặc từ các thiết bị lưu trữ bên ngoài.
3. Lỗi phần mềm: Lỗi phần mềm có thể cho phép kẻ tấn công truy cập vào hệ thống hay dữ liệu của một công ty hay doanh nghiệp. Các lỗ hổng bảo mật này có thể được khai thác để truy cập thông tin quan trọng hoặc để tấn công hệ thống.
4. Lỗi con người: Những sai sót như mật khẩu yếu, sử dụng mật khẩu giống nhau cho nhiều tài khoản, hay để lại thông tin đăng nhập trên các thiết bị công cộng có thể làm cho hệ thống của một công ty hay doanh nghiệp trở nên dễ bị tấn công.
5. Sự cố thiên tai: Sự cố thiên tai như chập điện hay ngập lụt có thể gây ra hư hỏng vật chất, làm gián đoạn hoạt động của hệ thống, hoặc làm mất dữ liệu.
6. Tình trạng nhân viên không an toàn: Tình trạng nhân viên không an toàn có thể làm cho dữ liệu quan trọng của một công ty hay doanh nghiệp bị rò rỉ, hoặc cho phép tấn công viên có thể truy cập trái phép vào hệ thống.

Để bảo vệ an toàn dữ liệu và hệ thống của một công ty hay doanh nghiệp, cần có các giải pháp bảo mật như mật khẩu mạnh, phần mềm bảo mật, đào tạo nhân viên về an ninh mạng

Lưu ý: Sinh viên được tham khảo tài liệu của chính mình

TiKi.vn là top 3 trong danh sách các sàn giao dịch thương mại điện tử của Việt Nam. Tiki sở hữu hơn 800.000 khách hàng và cung cấp đến 120.000 sản phẩm thuộc 10 ngành hàng khác nhau như: Sách, làm đẹp – sức khỏe, nhà cửa – đời sống, điện thoại – Máy tính bảng, ... với mức doanh số tăng trưởng gấp ba lần mỗi năm. Dịch vụ vận chuyển trong 24h giúp khách hàng trải nghiệm mua sắm trực tuyến một cách tiện lợi vừa tiết kiệm được thời gian, công sức mà vẫn bảo đảm được các quyền lợi về bảo hành hay đổi/trả dễ dàng trong vòng 30 ngày. Web Tiki.vn được thiết lập để phục vụ toàn bộ quy trình của hoạt động mua bán hàng hóa hay cung ứng dịch vụ. Bao gồm từ trưng bày, giới thiệu hàng hóa, dịch vụ đến giao kết hợp đồng, cung ứng dịch vụ, quản lý thông tin khách hàng, thanh toán và dịch vụ sau bán hàng, quảng cáo và 1 số dịch vụ liên quan đến online marketing.

Tình huống 2:

Trung tâm tin học của khoa công nghệ thông tin có nhiệm vụ đào tạo các khóa học ngắn hạn về CNTT cho các sinh viên của trường. Hiện nay trung tâm có một website http://www.ttth_iuh.edu.vn để sinh viên xem, đăng ký và thanh toán học phí các khóa học qua website. Sau khi thi xong sinh viên cũng có thể xem kết quả của các khóa học qua website này. Khi đăng ký học các khóa học sinh viên phải cung cấp đầy đủ thông tin cá nhân để trung tâm lưu trữ quản lý. Khi thanh toán học phí trực tuyến sinh viên phải cung cấp thông tin về thẻ ngân hàng thanh toán. Thông tin các khóa học cũng được website cung cấp cho sinh viên tham khảo và chọn lựa. Giáo viên sau khi giảng dạy thì nhập các kết quả thi của sinh viên thông qua website.

Hướng dẫn:

Bạn nên liệt kê và giải thích từng mối đe dọa;

Các mối đe dọa có thể là: Mất tính bảo mật (Rò rỉ) thông tin dữ liệu; Mất tính toàn vẹn (bị thêm bớt xóa sửa 1 cách bất hợp pháp) của dữ liệu; Mất tính sẵn dùng của hệ thống (hệ thống hoạt động không bình thường hoặc dữ liệu không truy xuất được); Mất tính xác thực (không xác thực được nguồn gốc) của dữ liệu,….

Mỗi mối đe dọa: phải chỉ rõ thông tin dữ liệu/chức năng nào của hệ thống có thể gặp phải mối đe dọa đó, nêu gặp phải mối đe đọa đó thì phải phân tích hậu quả của nó

Vì dụ

- Mối đe dọa 1: <Tên mối đe dọa XXXXXXXXX>
  < (1) Thông tin dữ liệu/chức năng nào trong tình huống có thể gặp phải mối đe dọa và nêu lý do tại sao>; (2) Giải thích/phân tích thấy được hậu quả nếu xảy ra mối đe dọa đó: doanh nghiệp thì sao? Khách hàng?>
- Mối đe dọa 2: <Tên mối đe dọa XXXXXXXXX>
  < (1) Thông tin dữ liệu/chức năng nào trong tình huống có thể gặp phải mối đe dọa và nêu lý do tại sao>; (2) Giải thích/phân tích thấy được hậu quả nếu xảy ra mối đe dọa đó: doanh nghiệp thì sao? Khách hàng?>
- Mối đe dọa 3: <Tên mối đe dọa XXXXXXXXX>
  < (1) Thông tin dữ liệu/chức năng nào trong tình huống có thể gặp phải mối đe dọa và nêu lý do tại sao>; (2) Giải thích/phân tích thấy được hậu quả nếu xảy ra mối đe dọa đó: doanh nghiệp thì sao? Khách hàng?>

MỤC LỤC

1. liệt kê và giải thích từng mối đe dọa

Mối đe dọa 1: Rò rỉ thông tin dữ liệu(tính bảo mật)

Thông tin cá nhân và thanh toán của sinh viên, thông tin kết quả thi của sinh viên và các thông tin liên quan đến khóa học trong hệ thống đều có thể bị rò rỉ nếu không có các biện pháp bảo mật đúng đắn. Nguyên nhân có thể do hacker tấn công vào hệ thống hoặc nhân viên trung tâm tin học không tuân thủ các quy định bảo mật.

+Đối với khách hàng: Nếu thông tin cá nhân của sinh viên bị lộ như số điện thoại, mssv, họ tên , cccd sẽ làm cho kẻ xấu có thể gọi điện các cuộc gọi gây làm phiền đến mình

+Đối với doanh nghiệp : Hậu quả nếu thông tin bị rò rỉ có thể làm mất lòng tin của sinh viên và làm giảm uy tín của trung tâm tin học. Nếu thông tin thanh toán bị rò rỉ, thì có thể dẫn đến việc mất tiền của sinh viên. Nếu thông tin cá nhân bị rò rỉ, có thể dẫn đến việc lừa đảo hoặc đánh cắp danh tính của sinh viên.

Mối đe dọa 2: Mất tính toàn vẹn dữ liệu

(1) Dữ liệu trong hệ thống có thể bị mất tính toàn vẹn nếu bị thêm, bớt, xóa hoặc sửa đổi không đúng quy định hoặc bị tấn công từ phía bên ngoài.

Đối với doanh nghiệp: Hậu quả của việc mất tính toàn vẹn dữ liệu có thể làm ảnh hưởng đến chất lượng và độ chính xác của dữ liệu, ảnh hưởng đến quá trình học tập và dạy học, làm giảm uy tín của trung tâm tin học và có thể gây ra thiệt hại cho sinh viên.

Đối với cá nhân: việc thêm, bớt , sửa xóa kết quả gây mất sự công bằng cho sinh viên

Mối đe dọa 3: Mất tính sẵn dùng của hệ thống

Thông tin dữ liệu/chức năng liên quan đến việc truy cập website, đăng ký khóa học, thanh toán học phí, xem kết quả thi có thể gặp phải mối đe dọa này. Nguyên nhân có thể là do lỗi kỹ thuật, tấn công mạng, sự cố hệ thống, hoặc sự cố về cơ sở dữ liệu.

Đối với doanh nghiệp : Nếu hệ thống bị mất tính sẵn dùng, các chức năng của trung tâm sẽ không thể hoạt động bình thường, dẫn đến sự cố về truy cập, đăng ký, thanh toán học phí, xem kết quả thi. Điều này có thể gây ảnh hưởng đến chất lượng dịch vụ của trung tâm, gây thất vọng cho khách hàng, ảnh hưởng đến uy tín của trung tâm.

Đối với cá nhân: khiến sinh viên không thể đăng kí và thanh toán khóa học

Mối đe dọa 4 Mất tính xác thực (không xác thực được nguồn gốc) của dữ liệu:

Chức năng quản lý thông tin khách hàng hoặc giao dịch của hệ thống có thể gặp phải mối đe dọa này khi dữ liệu không được xác thực đúng nguồn gốc.

Đối với doanh nghiệp: có thể gặp phải rủi ro về an ninh thông tin và bị mất danh tính khách hàng, dẫn đến thiệt hại về uy tín và danh tiếng

2. Cho 2 số p và q, thực hiện phát sinh khóa công khai (PU) và khóa riêng phần (PR). Thực hiện mã hóa và giải mã thông điệp m
Ví dụ: p=23, q=19, m=8; p=17, q=19, m=8
p=29, q=13, m=8 p=31, q=37, m=8

Chọn 2 số nguyên tố p và q khác nhau, tính n = p*q

Tính hàm số Euler của n: φ(n) = (p-1)*(q-1)

Chọn số nguyên e sao cho 1 < e < φ(n) và e là số nguyên tố cùng nhau với φ(n). e được sử dụng làm phần tử công khai của khóa.

Tính số nguyên d sao cho d = e^-1 mod φ(n) và d < mod φ(n) . d được sử dụng làm phần tử riêng phần của khóa.

Khóa công khai (PU) là cặp giá trị (e, n), khóa riêng phần (PR) là cặp giá trị (d, n).

Hủy bỏ các giá trị bí mật p và q

Bài mẫu : p=23, q=19, m=8;

B1: chọn 2 số nguyên tố p=23, q=19

B2: n=p*q=23*19= 437

B3: tính φ(n) = (p-1)*(q-1)=22*18=396

B4: Chọn e: với gcd(e, φ(n))=1, chọn e=17

B5: xác định d: d = e^-1 mod φ(n) và d < mod φ(n)=396

*(Mặc định ban đầu t1=0,t2=1, t=t1-g*t2)*

q	R1	R2	R	T1	T2	T
23	396	17	5	0	1	-23
3	17	5	2	1	-23	70
2	5	2	1	-23	70	-163
2	2	1	0	70	-163	396

	1	0		-163	396	

D= -163 hoặc 233

Chọn d=233 vì d*e=233*17=3961=10*396+1

B6: Công bố KU={e,n}={17,437}

B7: Công bố KR={d,n}={233,437}

Hủy bỏ các giá trị bí mật p=23,q=19

Mã hóa bằng KU={e,n}={17,437}, m=8

C=m^e mod n=8^17 mod 437=335

Đổi e=17 ra dạng binary: 10001

B[i]	P=p^2	P=p mod 437	P*x	P=p(mod 437)
1	1	1	1*8=8	8
0	8^2	64	-	64
0	64^2	163	-	163
0	163^2	349	-	349
1	349^2	315	315*8=2520	335

Giải mã bằng KR={d,n}={233,437}

M'=c^d mod n=335^233 mod 437=8

Đổi d=233 ra binary=11101001

B[i]	P=p^2	P=p mod 437	P*x	P=p(mod 437)
1	1	1	1*335=335	335
1	335^2	353	353*335=118255	265
1	265^2	305	305*335=102175	354
0	354^2	334	-	334

1	334^2	121	121*335=40535	331
0	331^2	311	-	311
0	311^2	144	-	144
1	144^2	197	197*335	8

3. Giải thích được các khái niệm cơ bản về An toàn thông tin, hệ mã hóa

Tất cả các khái niệm có trong

Chương 1: Tổng quan về an toàn hệ thống thông tin

Chương 3a: Mối đe dọa

Chương 3: Hệ thống mật mã học

Phân biệt giữa tấn công từ chối dịch vụ (DoS) và tấn công từ chối dịch vụ phân tán (DDoS). Loại ngào nguy hiểm hơn? Tại sao?

DOS	DDOS
DoS là viết tắt của Denial of service.	DDoS là viết tắt của Distributed Denial of service.
Trong cuộc tấn công DoS, chỉ một hệ thống nhắm mục tiêu vào hệ thống nạn nhân.	Trong DDos, nhiều hệ thống tấn công hệ thống nạn nhân.
PC bị nhắm mục tiêu được load từ gói dữ liệu gửi từ một vị trí duy nhất.	PC bị nhắm mục tiêu được load từ gói dữ liệu gửi từ nhiều vị trí.
Tấn công DoS chậm hơn so với DDoS.	Tấn công DDoS nhanh hơn tấn công DoS.
Có thể bị chặn dễ dàng vì chỉ sử dụng một hệ thống.	Rất khó để ngăn chặn cuộc tấn công này vì nhiều thiết bị đang gửi gói tin và tấn công từ nhiều vị trí.
Trong cuộc tấn công DoS, chỉ một thiết bị duy nhất được sử dụng với các công cụ tấn công DoS.	Trong cuộc tấn công DDoS, nhiều bot được sử dụng để tấn công cùng một lúc.
Các cuộc tấn công DoS rất dễ theo dõi.	Các cuộc tấn công DDoS rất khó theo dõi.
Lưu lượng truy cập trong cuộc tấn công DoS ít hơn so với DDoS.	Các cuộc tấn công DDoS cho phép kẻ tấn công gửi một lượng lớn lưu lượng truy cập đến mạng nạn nhân.

Các loại tấn công DoS là: 1. Tấn công tràn bộ đệm 2. Tấn công Ping of Death hoặc ICMP flood 3. Tấn công Teardrop Attack	Các loại tấn công DDoS là: 1. Tấn công Volumetric (tấn công băng thông) 2. Tấn công Fragmentation Attack (phân mảnh dữ liệu) 3. Application Layer Attack (khai thác lỗ hổng trong các ứng dụng)

-Loại Nguy hiểm hơn là tấn công từ chối dịch vụ phân tán (DDoS).Tại vì đối với những vụ tấn công DDoS kỹ thuật cao có thể dẫn đến việc lấy trộm tiền bạc, dữ liệu khách hàng của công ty.

Trình bày các loại mã độc (malware). Sự khác biệt giữa worm và virus là gì? Trojan horse có chứa đựng virus hoặc worm không?

Virus	Sâu	Ngựa Trojan
Phụ thuộc vào việc phát tán các tệp bị nhiễm	Tự nhân bản, tự phát tán qua mạng kết nối	Ẩn dưới vỏ bọc chương tình tiện ích, chờ người dùng tải về
Có khả năng tự sao	Có khả năng tự sao nhanh chóng	Không có khả năng tự sao
Không bị điều khiển từ xa	Có thể bị người phát tán điều kiểm soát từ xa	Có thể bị người phát tán kiểm soát từ xa
Tốc độ lây lan vừa phải	Tốc độ lây lan khủng khiếp	Lây lan chậm
Chèn đoạn mã vào chương trình máy và sửa đổi dữ liệu	Tự nhân để làm quá tải hệ thống rồi treo máy	Chiếm quyền kiểm soát và đánh cắp thông tin

Tại sao tính đa hình của các mã độc lại gây ra mối quan tâm lớn hơn mã độc hại truyền thống? Nó ảnh hưởng đến việc phát hiện/nhận dạng mã độc như thế nào?

Mã độc đa phần đều có thể bị phát hiện và tiêu diệt bởi phần mềm phòng chống mã độc và các công cụ kiểm tra an toàn thông tin. Những loại mã độc đó được gọi là mã độc đơn hình. Để có thể vượt qua được các phần mềm phòng chống mã độc thì

mã độc trở nên càng ngày càng phức tạp, tinh vi hơn từ cách thức lây nhiễm, phương pháp ẩn mình và hành vi trên máy người dùng,… Những mã độc như vậy được gọi là mã độc đa hình.

Mã độc đa hình (polymorphic malware) có khả năng tự biến đổi bản thân thành nhiều dạng khác nhau.

Trong suốt qua trình tấn công, lây lan hay kết nối với máy chủ mã độc đơn hình chỉ sử dụng duy nhất một biến thể. Khác với mã độc đơn hình, mã độc đa hình bằng các kỹ thuật khác nhau như mã hóa, thay thế các lệnh, hoán vị lệnh, chèn các lệnh vô nghĩa,… để tạo ra các biến thể khác nhau sau mỗi lần lây nhiễm hay sau một khoảng thời gian nhất định. Sau khi sinh ra phiên bản mới, chúng còn có khả năng tự xóa phiên bản trước đó để tránh bị các chương trình phòng chống mã độc hay các chuyên gia phân tích phát hiện, làm tăng khả năng hay thời gian sống sót của chúng.

Do mã độc đa hình có thể liên tục biến đổi mã lệnh, nên khó có thể tìm được đoạn mã đặc trưng của nó, và do đó khó phát hiện bằng phương pháp so sánh mã truyền thống. Bất kể tồn tại ở dạng nào đều làm cho mã độc này trở nên nguy hiểm vì sự phức tạp và tốc độ của nó.

Các mối đe dọa:

- *Hành động vô ý (Inadvertent Acts)*

Là những hành đồng mà xảy bởi lỗi nào đó, người thực hiện không cố ý
- Kẻ tấn công không ác ý hoặc hiềm thù
- Các hành động lỗi của con người, sai lệch từ chất lượng vị vụ, truyền thông lỗi là ác hành động vô ý.
- Nhân viên oặc người dùng hệ thống là nối đe dọa nội bộ hệ thống

- *Hành động cố ý (Delierate Acts)*

- Là các hành động mà được thực hiện bởi người của tổ chứclà tổ hại đến thông tin

- Các kẻ tấn công có một ý định thâm độc và muốn ăn cấp hoặc phá hủy dữ liệu

- Bao gồm các hành động như gián điệp, hacking, Cracking

- *Thảm họa tự nhiên (Natural Disaster)*

- Sức mạnh của thiên nhiên là rất nguy hiểm bởi vì chúng là điều không ngờ và xuất hiện đôi khi không có cảnh báo

- Chúng phá vợ cuộc sống của con người nhưng cũng gây nguy hại dến thông tin mà được lưu vào trong máy tính

- Các mối đe dọa này có thể tránh nhưng chúng ta phải có những biện pháp phòng ngừa cần thiết

- *Lỗi về kỹ thuật (Technical Failures)*

- Lỗi về phần cứng: Nó xảy ra khi nhà sản xuất phân phối thiết bị có lỗi mà nhà sản xuất có thể biết hoặc không biết

- Lỗi phần mềm kỹ thuật: Những lỗi này có thể khiến hệ thống hoạt động theo cách không mong muốn hoặc bất ngờ. Một số trong số này là không thể phục hồi trong khi một số xảy ra định kỳ

- *Lỗi về quản lý (Management)*

- Quàn lý phải luôn luôn cập nhật về diễn biến và công nghệ hiện tại

- Kế hoạch phù hợp phải được thực hiện bởi nhà quản lý để bảo vệ tốt thông tin

- Các chuyên gia CNTT cũng phải giúp ban quản lý trong việc bảo vệ thông tin, bằng cách hỗ trợ an quản lý nâng cao công nghệ mới nhất