GIỮA KÌ – NHẬP MÔN AN TOÀN THÔNG TIN – LO4

LO4 - Giải thích được các khái niệm cơ bản về An toàn thông tin, hệ mã hóa

MỤC LỤC

1. An toàn thông tin là gì?

An toàn thông tin (Information Security)

+ Là tập các quy trình và công cụ được thiết kế và triển khai để bảo vệ các thông tin nhạy cảm của doanh nghiệp từ sự truy cập, hiệu chỉnh, phá hủy không hợp pháp

+ An toàn thông tin mạng (information security), an toàn máy tính (computer security), đảm bảo thông tin (information assurance) được sử dụng hoán đổi cho nhau.

Tại sao một doanh nghiệp cần phải có các biện pháp khác nhau để đảm bảo tính an toàn thông tin của doanh nghiệp?

+ Thông tin là một tài sản, giống như các tài sản quan trọng khác của doanh nghiệp, có giá trị đối với tổ chức và cần được bảo vệ một cách phù hợp.

+ Nếu thông tin của tổ chức lọt vào tay những những người không có thẩm quyền hoặc không hợp pháp thì dẫn đến những hậu quả rất rất nghiêm trọng

+ Vì thế, bảo vệ thông tin trở thành một yêu cầu không thể thiếu trong mọi hoạt động nói chung và hoạt động điện tử nói riêng. An toàn thông tin trong thời đại số là quan trọng hơn bao giờ hết.

2. Hệ thống thông tin là gì?

- Hệ thống thông tin là một hệ thống bao gồm các yếu tố có quan hệ với nhau cùng làm nhiệm vụ thu thập, xử lý, lưu trữ và phân phối thông tin và dữ liệu và cung cấp một cơ chế phản hồi để đạt được một mục tiêu định trước

-Là hệ thống mà mối liên hệ giữa các thành phần của nó cũng như mối liên hệ giữa nó với các hệ thống thông tin khác. Là sự trao đổi thông tin. Mục tiêu của hệ thống thông tin là cung cấp thông tin phục vụ cho con người trong một tổ chức nào đó

Hãy cho ví dụ một hệ thống thông tin mà bạn biết.

Ví dụ: Máy tính là một hệ thống thông tin. Một máy tính là công cụ để xử lý thông tin. Khinhoạt động, các thành phần của máy tính trao đổi thông tin với nhau. Máy chấm công là một hệ thống thông tin

Đưa ra dữ liệu/thông tin/chức năng nào cần đảm bảo an toàn, nêu lý do

Ví dụ 2 : Hệ thống AAA trong bảo mật sử dùng tên đăng nhập và mật khẩu là cơ chế truyền thống và vẫn còn được sử dụng rộng rải hiện nay. Chiến lược bảo mât hê thống AAA (Điều khiển truy xuất-Access control, Xác thực-Authentication, Kiểm tra-Auditing) được xem là bước tiếp cận cơ bản và là chiến lược nền tảng để thực thi các chính sách bảo mật trên một hệthống được mô tả theo mô hình CIA (Tính bí mật-Confidentiality, Tính toàn vẹn-

Intergrity, Tính khả dụng- Availability). Thiết lập các cơ chế điều khiển truy xuất cho từng đối tượng (Access control) Xác thực các đối tượng trước khi cho phép thao tác trên hệ thống (Authentication) Lí do: nhằm đảm bảo có thể nhận dạg đúng người dùn, đúng họ và tên nhân viên đúng phòng ban

3. Tam giác CIA là gì?

An toàn máy tính xét trên tính bí mật, tính toàn vẹn, tính sẵn sàng. Ba tính đó còn gọi là tam giác C-I-A (confidentiality, integrity,availability). Đảm bảo an toàn hệ thống thông tin là đảm bảo an toàn của hệ thống thông tin (phần cứng, phần mềm, dữ liệu) trước các mối đe dọa (sự truy cập, sửa đổi, phá hoại dữ liệu bất hợp pháp) bằng các biện pháp kỹ thuật lẫn phi kỹ thuật (mã hóa, kiểm soát truy cập, chính sách …). Một hệ thống thông tin được xem là an toàn khi đảm bảo ít nhất ba mục tiêu cơ bản: tính bí mật, tính toàn vẹn, tính sẵn sàng. Ngoài ra còn có các mục tiêu khác như: tính không thể chối cãi, tính xác thực.

- **C – Confidentiality – Tính bảo mật**: Đảm bảo tính bí mật của thông tin, tức là thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính) được cấp phép.Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ tiếp cận trực tiếptới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin từ xa qua môi trường mạng.
- **I – Integrity – Tính toàn vẹn**: Đảm bảo tính toàn vẹn thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được cho phép và phải đảm bảo băng thông vẫn còn chính xác khi được lưu trữ hay truyền đi. Về điểm này, nhiều người thườnghay nghĩ tính toàn vẹn đơn giản chỉ là đảm bảo thông tin không bị thay đổi là chưa đầy đủ.
- **A – Availability – Tính sẵn sàng**: Đảm bảo độ sẵn sàng của thông tin, tức là thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn. Ví dụ, nếumột server chỉ bị nhưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng nó là 99,999%

Mối tương quan của CIA:

C, I, A phải luôn gắn chặt với nhau, là tiền đề để bảo đảm cho một hệ thống thông tin được ăn toàn và tránh được các rủi ro. C, I, A được tạo thành các góc của hình tam giác cho thấy sự quan trọng của chúng là như nhau, chỉ khi cả 3 tính trên cùng tồn tại thì mới bảo đảm tamgiác hình thành và sự an toàn của thông tin mới được bảo vệ. Khi có C tồn tại, thông tin mới được giữ bí mật, I tồn tại thông tin toàn vẹn và A tồn tại thì thông tin mới luôn sẵn sàng để phục vụ cho những việc cần thiết

4. Vulnerability (lổ hổng) - Threat (mối nguy/mối đe dọa) - Risk (rủi ro) là gì?

+ Vulnerability (lổ hổng): một điểm yếu trong tổ chức, hệ thống IT, hoặc mạng mà có thể được khám phá bởi mối đe dọa.

+ Threat (mối nguy/mối đe dọa): một cái gì đó mà có thể gây thiệt hại đến tổ chức, hệ thống IT hoặc hệ thống mạng.

+ Risk (rủi ro): một khả năng mà một mối đe dọa khai thác lỗ hỏng trong tài sản và gây ra nguy hại hoặc mất mát đến tài sản

Nêu mối tương quan giữa 3 yếu tố đó

Threat Agent thông qua ==> Threat, để khai thác ==> Vulnerability, dẫn đến ==> Risk, gây ra tổn thất cho ==> Asset, sinh ra ==> Exposure, chúng ta có thể ngăn chặn giảm thiểu bằng ==> Safeguard, tác động trực tiếp đến ==> Threat Agent.

Mối tương quan: Ba yếu tố trên có mối quan hệ mật thiết với nhau có lỗ hổng sẽ dẫn đếncác mối đe dọa, nếu mối đe dọa gây ảnh hưởng hệ thống thông tin sẽ xảy ra các rủi ro. Cả ba yếu tố trên có sự gắn kết với nhau, yếu tố này sẽ gây ra yếu tố kia rồi cùng nhau tạo ra hậu quả đối với các cở sở dữ liệu và hệ thống thông tin

5. Tấn công (Attack) an toàn thông tin là gì?

- Hành động khai thác lỗ hổng (tức là một điểm yếu được xác định) trong hệ thống kiểm soát

- Thực hiện kẻ tấn công nhằm gây thiệt hại hoặc ăn cắp thông tin của tổ chức

Ai có thể trở thành kẻ tấn công (Attacker)?

-Ai có thể trở thành kẻ tấn công: Những người có kiến thức cực kỳ chuyên sâu về an ninh mạng, khao học máy tính, khoa học mật mã, cơ sở dữ liệu,.. . Có thểlà người tốt hoặc người xấu, do đó Hacker được chia làm nhiều nhóm sau:

+ Hacker mũ trắng có mục đích tốt. Khi họ xâm nhập thành công vào hệ thống của một tổ chức, họ thường cố gắng liên hệ với tổ chức để thông báo về sự không an toàn của hệ thống bởi họ tìm ra được các lỗ hổng và các nguy cơ bị tấn công. Hacker mũ trắng là hacker có đạo đức

+ Hacker mũ đen thường truy cập trái phép vào các hệ thống như website, mạng nội bộ, các thiết bị, ứng dụng.. để có thể làm bất kỳ những gì họ muốn. Hacker mũ đen luôn làm những việc bất hợp phát với mục đích xấu như nghe lén, ăn trộm đánh cắp thông tin dữ liệu; tống tiền; gây hại cho các ngân hàng, doanh nghiệp, nhà nước

-Ngoài ra còn có hacker mũ xám, hacker mũ đỏ, tân binh,..

6. Mã độc (Malware) là gì?

Malware (hay phần mềm độc hại) là thuật ngữ mô tả các chương trình hoặc mã độc có khả năng cản trở hoạt động bình thường của hệ thống bằng cách xâm nhập, kiểm soát, làm hỏng hoặc vô hiệu hóa hệ thống mạng, máy tính, máy tính bảng và thiết bị di động,…

VD: Mã hóa thông tin cá nhân cảu người dùng *Các loại malware: Có nhiều loại phần mềm độc hại khác nhau chứa các đặc điểm và đặc tính riêng.

Nêu các loại mã độc?

+ Vi-rút là loại phần mềm độc hại phổ biến nhất và được xác định là một chương trình độc hại có thể tự thực thi và lây lan bằng cách lây nhiễm các chương trình hoặc tệp khác.

+ Worm là một loại phần mềm độc hại có thể tự tái tạo mà không cần chương trình chủ; sâu thường lây lan mà không có bất kỳ sự tương tác của con người hoặc chỉ thị từ các tác giả phần mềm độc hại.

+ Trojan là một chương trình độc hại được thiết kế như một chương trình hợp pháp; được kích hoạt sau khi cài đặt, Trojans có thể thực thi các chức năng độc hại của chúng.

+ Spyware là một loại phần mềm độc hại được thiết kế để thu thập thông tin và dữ liệu về người dùng và quan sát hoạt động của họ mà họ không hề biết

Cho ví dụ về một tình huống bị tấn Công

Ví dụ như Ransomware được thiết kế để lây nhiễm vào hệ thống của người dùng và mã hóa dữ liệu. Các tội phạm mạng sau đó yêu cầu một khoản tiền chuộc từ nạn nhân để đổi lấy việc giải mã dữ liệu của hệ thống. Rootkit là một loại phần mềm độc hại được thiết kế để có quyền truy cập cấp quản trị viên vào hệ thống của nạn nhân. Sau khi cài đặt, chương trình cung cấp cho hacker có thể root hoặc đặc quyền truy cập vào hệ thống. Virus backdoor hoặc Trojan truy cập từ xa (RAT) là một chương trình độc hại bí mật tạo ra một backdoor vào một hệ thống bị nhiễm cho phép các tác nhân đe dọa truy cập từ xa mà không cần cảnh báo người dùng hoặc các chương trình bảo mật của hệ thống

7. Tấn công mật khẩu là gì?

Có 3 dạng tấn công Password phổ biến:

- Brute Force Attack (tấn công dò mật khẩu)

- Dictionary Attack (tấn công từ điển)

- Key Logger Attack (tấn công Key Logger)

Cho ví dụ về một tình huống bị tấn công.

Brute Force Attack (tấn công dò mật khẩu): Kẻ tấn công sử dụng một công cụ mạnh mẽ, có khả năng thử nhiều username và password cùng lúc (từ dễ đến khó) cho tới khi đăng nhập thành công.

VD: đặt mật khẩu đơn giản như 123456, password123, daylamatkhau,… rất dễ bị tấn công brute force.

Dictionary Attack (tấn công từ điển): Là một biến thể của Brute Force Attack, Tuy nhiên kẻ tấn công nhắm vào các từ có nghĩa thay vì thử tất cả mọi khả năng. Nhiều người dùng có xu hướng đặt mật khẩu là những từ đơn giản và có ngữ nghĩa.

VD: motconvit, iloveyou,… Đây là lý do khiến Dictionary Attack có tỉ lệ thành công cao hơn.

Key Logger Attack (tấn công Key Logger): Kẻ tấn công lưu lại lịch sử các phím mà nạn nhân gõ, bao gồm cả ID, password hay nhiều nội dung khác. Kẻ tấn công cần phải sử dụng một phần mềm độc hại (malware) đính kèm vào máy tính (hoặc điện thoại) nạn nhân, phần mềm đó sẽ ghi lại tất cả những ký tự mà nạn nhân nhập vào máy tính và gửi về cho kẻ tấn công. Phần mềm này được gọi là Key Logger. Nguy hiểm hơn 2 cách tấn công trên, do việc đặt mật khẩu phức tạp không giúp ích gì trong trường hợp này.

3 tấn công trên chỉ là các dạng tấn công mật khẩu trực tiếp. Ngoài ra, kẻ tấn công có thể tấn công gián tiếp thông qua việc:

+ Lừa đảo người dùng tự cung cấp mật khẩu (Tấn công giả mạo Phishing);

+ Tiêm nhiễm Malware

+ Tấn công vào cơ sở dữ liệu – kho lưu trữ mật khẩu người dùng của các dịch vụ…

Cách phòng chống tấn công mật khẩu?

- **Đặt mật khẩu phức tạp**

  + Tuy đơn giản nhưng biện pháp này giúp người dùng phòng tránh được hầu hết các cuộc tấn công dò mật khẩu thông thường.

  + Một mật khẩu mạnh thường bao gồm: chữ IN HOA, chữ thường, số, ký tự đặc biệt (ví dụ @$* %&#)

- **Bật xác thực 2 bước:**

  + Hầu hết dịch vụ cho phép người dùng bật xác thực 2 bước khi đăng nhập trên thiết bị mới. Điều này khiến hacker có hack được mật khẩu cũng không thể đăng nhập được.

  + Hiện tại Facebook, Gmail, các ngân hàng, ví điện tử… đều có tính năng này.

- **Quản lý mật khẩu tập trung:**

+ Việc lưu tất cả mật khẩu trên một thiết bị là con dao hai lưỡi. Người dùng cân nhắc khi thực hiện.

- **thay đổi mật khẩu định kì:**

  + Gây khó khăn cho quá trình hack mật khẩu của tin tặc.

- Thận trọng khi duyệt web:

+ Tin tặc có thể hack mật khẩu của bạn bằng cách tạo ra một đường link giả mạo. Link giả thường gần giống trang web chính vì thế, luôn thận trọng với các đường link trước khi đưa thông tin cá nhân

- **Cẩn trọng khi mở email, tải file:**

+ Tuyệt đối không mở file lạ, và luôn kiểm tra địa chỉ email người gửi xem có chính xác không.

+ VD: tên người gửi là Ngọc Luân JSC nhưng địa chỉ email là ngoclunajsc thì chắc chắn có dấu hiệu lừa đảo

8. Tấn công backdoor là gì?

Backdoor (cửa hậu)

+ Backdoor trong phần mềm hay hệ thống máy tính thường là một cổng không được thông báo rộng rãi.

+ Cho phép người quản trị xâm nhập hệ thống để tìm nguyên nhân gây lỗi hoặc bảo dưỡng (do nhà phát triển tạo ra).

+ Hacker và gián điệp dùng backdoor để truy cập bất hợp pháp vào hệ thống (cài đặt thông qua một số mã độc).

Cho ví dụ về một tình huống bị tấn công.

Ví dụ: Một ví dụ khác về cửa hậu dẫn chúng ta đến Sony, thật đáng ngạc nhiên. Bạn thấy đấy, công ty Nhật Bản vào năm 2005 đã vận chuyển hàng triệu đĩa CD nhạc cho khách hàng trên khắp thế giới, nhưng có một vấn đề lớn với những sản phẩm này. Công ty đã chọn cài đặt bộ rootkit trên mỗi đĩa CD, có nghĩa là, bất cứ khi nào đĩa CD được đặt vào máy tính, rootkit sau đó sẽ tự cài đặt vào hệ điều hành. Khi điều đó được thực hiện, rootkit sẽ theo dõi thói quen nghe của người dùng và gửi dữ liệu trở lại máy chủ Sony.

Cách phòng chống?

+ Tuân thủ đúng các phương pháp bảo mật

+ Chỉ cài đặt các phần mềm tin cậy và đảm bảo đã bật tường lửa (firewall) trên thiết bị (firewall có thể ngăn chặn các cuộc tấn công backdoor, hạn chế lưu lượng truyền qua các cổng mở)

+ Theo dõi lưu lượng mạng để phát hiện và kiểm tra xem có sự hiện diện của backdoor hay không

9. Tấn công từ chối dịch vụ (DoS, DDoS) là gì?

- ***Denial-of-service (DoS)***

+ Là hình thức tấn công khá phổ biến hiện nay, nó khiến cho máy tính mục tiêu không thể xử lý kịp các tác vụ và dẫn đến quá tải.

+ Các cuộc tấn công DOS này thường nhắm vào các máy chủ ảo (VPS) hay Web Server của các doanh nghiệp lớn như ngân hàng, chính phủ hay là các trang thương mại điện tử … hoặc hacker cũng có thể tấn công để "bỏ ghét".

+ Tấn công DOS thường chỉ được tấn công từ một địa điểm duy nhất, tức là nó sẽ xuất phát tại một điểm và chỉ có một dải IP thôi. Bạn có thể phát hiện và ngăn chặn được.

+ Là một dạng tấn công nhằm gây cạn kiện tài nguyên hệ thống máy chủ và làm ngập lưu lượng băng thông Internet, khiến truy cập từ người dùng tới máy chủ bị ngắt quãng, truy cập chập chờn, thậm chí không thể truy cập được internet, làm tê liệt hệ thống hoặc thậm chí là cả một hệ thống mạng nội bộ.

+ Tấn công DDOS mạnh hơn DOS rất nhiều, điểm mạnh của hình thức này đó là nó được phân tán từ nhiều dải IP khác nhau, chính vì thế người bị tấn công sẽ rất khó phát hiện để ngăn chặn được.

+ Hacker không chỉ sử dụng máy tính của họ để thực hiện một cuộc tấn công vào một trang web hay một hệ thống mạng nào đó, mà họ còn lợi dùng hàng triệu máy tính khác để thực hiện việc này.

Cho ví dụ về một trường hợp bị tấn công.

Tại gmail, kẻ tấn công sẽ gửi hàng loạt yêu cầu với số lượng cực lớn (vượt quá khả năng xử lý tới hệ thống nạn nhân), khiến cho hệ thống gmail quá tải, phải tạm dừng hoạt động do không thể gửi cũng như nhận thêm mail nào.

Cách phòng chống?

-Tăng cường khả năng xử lý của hệ thống:

+ Tối ưu hóa các thuật toán xử lý, mã nguồn của máy chủ web

+ Nâng cấp hệ thống máy chủ

+ Nâng cấp đường truyền và các thiết bị liên quan,

+ Cài đặt đầy đủ các bản vá cho hệ điều hành và các phần mềm khác để phòng ngừa khả năng bị lỗi tràn bộ đệm, cướp quyền điều khiển,v.v…

- Hạn chế số lượng kết nối tại thiết bị tường lửa tới mức an toàn hệ thống cho phép

- Sử dụng các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) để ngăn chặn các kết nối nhằm tấn công hệ thống.

- Phân tích luồng tin (traffic) để phát hiện các dấu hiệu tấn công và cài đặt các tường lửa cho phép lọc nội dung thông tin (tầng ứng dụng) ngăn chặn theo các dấu hiệu đã phát hiện.

Một số công cụ kỹ thuật phòng chống tấn công từ chối dịch vụ

Tùy khả năng đầu tư, các cổng/trang TTĐT có thể trang bị giải pháp hoặc sử dụng dịch vụ chống DoS/DDoS với các công cụ kỹ thuật sau:

- Sử dụng hệ thống thiết bị, phần mềm hoặc dịch vụ giám sát an toàn mạng (đặc biệt về lưu lượng) để phát hiện sớm các tấn công từ chối dịch vụ.

- Sử dụng thiết bị bảo vệ mạng có dịch vụ chống tấn công DDoS chuyên nghiệp kèm theo, ví dụ như: Arbor, Checkpoint, Imperva, Perimeter,…

10.Tấn công Social Engineering là gì?

- là kỹ thuật tác động đến con người, nhằm mục đích lấy được thông tin hoặc đạt được một mục đích mong muốn

- Dựa vào điểm yếu tâm lý, nhận thức sai lầm của con người về việc bảo mật thông tin, sử dụng sự ảnh hưởng và 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.

Cho ví dụ về một tình huống bị tấn công:

Nhận được cuộc gọi từ tổ chức uy tín như ngân hàng nói rằng mình trúng thưởng yêu cầu chia sẻ thông tin tài chính bí mật như: tên đăng nhập, mật khẩu giao dịch và những thông tin nhạy cảm khác.

Các hình thức tấn công Social Engineering phổ biến: Phishing, Watering Hole, Pretexting, Baiting và Quid Pro Quo

Cách phòng chống?

+ Không ở email từ người lạ

+ KHông nhấp vào các liên kết đáng ngờ trong email

+ Nếu nghi ngờ một trang web trong có vẻ hợp pháo, bạn hãy nhập địa chỉ trang web hợp pháp trên trình duyệt web tho cách thủ công

+ Kiểm tra xem các website có ùng các giao thức hỗ trợ bảo mật không

+ Nếu nhận một email không hợp pháp, hãy lấy các thông tin trong email đó để kiểm tra xem

có cuộc tấn công lừa đảo nào thực hiện bằng phương pháp tương tự không

+ Sử dụng phần mềm bảo mật chống phần mền đọc hại đáng tin cậy

11.Mật mã học là gì?

Mật mã học (Cryptography) là ngành khoa học nghiên cứu về việc đảm bảo an toàn thông tin. Mật mã học gắn liền với quá trình mã hóa nghĩa là chuyển đổi thông tin từ dạng "có thể hiểu được" thành dạng "không thể hiểu được" và ngược lại là quá trình giải mã. Cryptography giúp đảm bảo những tính chất sau cho thông tin:

+ Tính bí mật (confidentiality): thông tin chỉ được tiết lộ cho những ai được phép

+ Tính toàn vẹn (integrity): thông tin không thể bị thay đổi mà không bị phát hiện.

+ Tính xác thực (authentication): người gửi (hoặc người nhận) có thể chứng minh đúng họ.

+ Tính chống chối bỏ (non-repudiation): người gửi hoặc nhận sau này không thể chối bỏ việc đã gửi hoặc nhận thông tin

Nêu các chức năng của mật mã học?

Bảo mật thông tin: Mật mã học giúp bảo vệ thông tin quan trọng khỏi sự truy cập trái phép bằng cách chuyển đổi dữ liệu thành dạng mà chỉ có người được ủy quyền có thể đọc được thông qua việc sử dụng các thuật toán mã hóa.

Mã hóa: Mã hóa là quá trình chuyển đổi dữ liệu ban đầu thành dữ liệu không thể đọc được mà chỉ có người có khóa giải mã mới có thể đọc được. Mã hóa được sử dụng để bảo vệ dữliệu trên mạng, trong cơ sở dữ liệu, hoặc trên các thiết bị lưu trữ.

Giải mã: Giải mã là quá trình chuyển đổi dữ liệu đã được mã hóa trở lại thành dạng ban đầu bằng cách sử dụng khóa giải mã tương ứng. Điều này cho phép người nhận hoặc người được ủy quyền có thể đọc thông tin.

Xác thực: Mật mã học cũng được sử dụng để xác thực danh tính và nguồn gốc của dữ liệu và người gửi. Các kỹ thuật chữ ký số được sử dụng để đảm bảo tính toàn vẹn của dữ liệu và xácđịnh xem dữ liệu có được gửi từ nguồn tin cậy hay không.

Quản lý khóa: Mật mã học cũng liên quan đến quản lý khóa, bao gồm tạo, phân phối và quản lý các khóa mã hóa và giải mã. Việc quản lý khóa hiệu quả là một phần quan trọng của bảo mật thông tin

Bảo vệ quyền riêng tư: Mật mã học đóng vai trò quan trọng trong việc bảo vệ quyền riêng tư của cá nhân và doanh nghiệp bằng cách mã hóa dữ liệu cá nhân và dữ liệu nhạy cảm.

Tóm lại, chức năng cơ bản của mật mã học là bảo vệ thông tin, bảo mật dữ liệu, xác thực

nguồn gốc của dữ liệu và người gửi, và bảo vệ quyền riêng tư thông qua việc sử dụng các kỹ

thuật mã hóa và quản lý khóa

Nêu điểm khác biệt giữa mật mã đối xứng và bất đối xứng

+ Mã hóa đối xứng là một kỹ thuật đã được giới thiệu từ lâu, trong khi mã hóa bất đối xứng là kỹ thuật mới hơn.

+ Mã hóa bất đối xứng mất nhiều thời gian hơn để thực hiện do logic phức tạp liên quan. Vì lý do này, mã hóa đối xứng vẫn được ưu tiên sử dụng khi truyền dữ liệu hàng loạt.

+ Mã hóa bất đối xứng an toàn hơn vì nó sử dụng các key khác nhau cho quá trình mã hóa và giải mã.

+ Mã hóa đối xứng:

- Khóa: Mã hóa đối xứng sử dụng cùng một khóa để thực hiện cả quá trình mã hóa và giải mã. Khóa này cần được chia sẻ giữa người gửi và người nhận, điều này đòi hỏi quản lý khóa an toàn và hiệu quả.

- Tính đối xứng: Quá trình mã hóa và giải mã đều sử dụng cùng một khóa, tạo ra tính đối xứng trong cách thực hiện. Điều này có nghĩa là nếu ai đó biết khóa mã hóa, họ cũng có khả năng giải mã dữ liệu.

- Tốc độ: Mã hóa đối xứng thường nhanh hơn mã hóa bất đối xứng vì chỉ cần thực hiện một loạt các phép biến đổi đơn giản.

+ Mã hóa bất đối xứng:

- Khóa: Mã hóa bất đối xứng sử dụng một cặp khóa, gồm khóa công khai và khóa riêng tư. Khóa công khai được chia sẻ công khai và dùng để mã hóa dữ liệu, trong khi khóa riêng tư được giữ bí mật và dùng để giải mã dữ liệu. Không cần chia sẻ khóa riêng tư.

- Tính bất đối xứng: Khóa công khai và khóa riêng tư đóng vai trò không đối xứng, điều này có nghĩa là dữ liệu mã hóa bằng khóa công khai chỉ có thể được giải mã bằng khóa riêng tư, và ngược lại.

- Độ bảo mật: Mã hóa bất đối xứng thường đảm bảo độ bảo mật cao hơn do không cần chia sẻ khóa riêng tư. Người gửi chỉ cần biết khóa công khai của người nhận để mã hóa dữ liệu, và người nhận giữ khóa riêng tư để giải mã.

Tóm lại: Sự khác biệt cơ bản giữa mã hóa đối xứng và mã hóa bất đối xứng là trong việc sử dụng khóa và cách thức thực hiện quá trình mã hóa và giải mã. Mã hóa đối xứng sử dụng cùng một khóa cho cả hai quá trình, trong khi mã hóa bất đối xứng sử dụng cặp khóa khác nhau cho việc mã hóa và giải mã. Mã hóa bất đối xứng thường đảm bảo tính bảo mật cao hơn, trong khi mã hóa đối xứng thường nhanh hơn trong việc thực hiện quá trình mã hóa và giải mã.

12.Mật mã bất đối xứng khắc phục những hạn chế gì của mật mã đối xứng?

Khóa chia sẻ an toàn: Trong mật mã đối xứng, cần chia sẻ khóa giữa các bên trao đổi thông tin, đòi hỏi một kênh an toàn để chia sẻ khóa. Mật mã bất đối xứng sử dụng cặp khóa (public key và private key) để giải quyết vấn đề này. Khóa công khai được công khai rộng rãi, nhưng khóa riêng tư được bảo mật hoàn toàn.

Hiệu suất thời gian: Mặc dù mật mã bất đối xứng thường mất nhiều thời gian hơn so với mật mã đối xứng, nhưng hiệu suất này đã được cải thiện qua các thuật toán như RSA và ECC.

Khả năng chống lại tấn công brute force: Mật mã bất đối xứng có khả năng chống lại tấn công brute force tốt hơn. Với khóa đối xứng, việc thử tất cả các khóa có thể dễ dàng thực hiện nếu khóa bị rò rỉ, trong khi đối với mật mã bất đối xứng, việc này trở nên khó khăn đáng kể do phải thử từng cặp khóa.

Chữ ký số: Mật mã bất đối xứng cho phép tạo chữ ký số, giúp xác minh danh tính và tính toàn vẹn của thông tin, cung cấp một cơ chế quan trọng để xác thực dữ liệu và người gửi.

13.Áp dụng mật mã Caesar để mã hóa bản rõ sau với khóa k = 4

actions speak louder than words

Gốc	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
K=4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D

Bản rõ	A	C	T	I	O	N	S	S	P	E	A	K	L	O	U	D	E	R	T	H	A	N	W	O	R	D	S
Bản mã	E	G	X	N	S	R	W	W	T	I	E	O	P	S	Y	H	I	V	X	L	E	R	A	U	V	H	W

14.Hãy mã hóa bằng phương pháp Playfair bản mã sau:

Bản rõ: MATMAHOC Khóa: thework

Lập bản 5 x 5 và phủ khóa vào các ô theo thứ tự và sắp xếp các chữ cái còn thiếu vào sau

Gốc	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Bản rõ M: MATMAHOC

Bản rõ M: MA TM AH OC

Bản mã C: PR RU KE CL

T	H	E	W	O
R	K	A	B	C
D	F	G	I/J	L
M	N	P	Q	S
U	V	X	Y	Z

15. So sánh và đánh giá về độ khó khi phá mã đối với các mật mã Ceasar, Monoalphabetic và Vigenère

	Ceasar	Monoalphabetic	Vigenere
Độ khó	Mật mã Caesar dễ bị phá mã bằng cách thử tất cả các khả năng dịch chuyển. Với bảng chữ cái tiếng Anh, chỉ có 25 khả năng (vì không cần thử dịch chuyển 26 bước). Mật mã Caesar không đủ an toàn để bảo vệ thông tin quan trọng.	Mật mã monoalphabetic khó hơn mật mã Caesar vì không có quy tắc dịch chuyển cố định. Tuy nhiên, nó vẫn có thể bị phá mã bằng cách phân tích tần suất xuất hiện của các ký tự và so sánh với tần suất xuất hiện trong ngôn ngữ gốc. Không an toàn: Mật mãmonoalphabetic cũng không đủ an toàn để bảo vệ thông tin quan trọng	Phức tạp hơn để phá mã so với Caesar và Monoalphabetic, đặc biệt khi sử dụng từ khóa dài và không dễ dàng đoán được. Đòi hỏi phải xác định đúng độ dài của từ khóa trước khi thực hiện phân tích. Có thể sử dụng các kỹ thuật như chỉ số trùng lặp, phân tích tần số của các phần của văn bản để giảm thiểu không gian khóa có thể.

16. "Theo dõi sự tuân thủ (Monitor for Compliance)" là một trong 10 bước triển khai ISP. Bạn hãy phân tích để thấy được tại sao cần có "theo dõi sự tuân thủ" trong khi triển khai ISP của một doanh nghiệp.

Theo dõi sự tuân thủ là gì?

-Là quá trình đảm bảo công ty và các nhân viên của doanh nghiệp tuân thủ các chính sách an toàn thông tin mà doanh nghiệp đã triển khai

Tại sao phải theo dõi sự tuân thủ

- Ở cấp độ cơ bản, theo dõi sự tuân thủ đảm bảo rằng các hoạt động an toàn thông tin của doanh nghiệp đang diễn ra và hoạt động như bình thường theo các chính sách doanh nghiệp triển khai. Rộng hơn, nó có thể xác định bất kỳ lĩnh vực nào không tuân thủ thì sẽ có biện pháp khắc phục
- Việc "theo dõi sự tuân thủ" có thể giúp tổ chức chứng minh rằng các quy trình đúng là chuẩn mực và họ thường mạnh mẽ trong việc thực thi chúng ', do đó giúp giảm thiểu tác động tiêu cực nếu bất kỳ sự không tuân thủ nào

Nếu không có bước "theo dõi sự tuân thủ" thì hậu quả như thế nào?

- Thì doanh nghiệp sẽ không biết được các nhân viên của mình có tuân thủ các chính sách mà doanh nghiệp đề ra hay không và từ đó nếu không tuân thủ các chính sách thì việc đảm bảo an toàn thông tin cho doanh nghiệp sẽ bị ảnh hưởng có thể kể đến như các dữ liệu, trang web của doanh nghiệp

12.“Hiệu chỉnh chính sách (Modify Policy)” là một trong 10 bước triển khai ISP.

Bạn hãy phân tích để thấy được tại sao cần có “hiệu chỉnh chính sách” trong khi triển khai ISP của một doanh nghiệp.

-Hiệu chỉnh chính sách (Modify Policy) là chỉnh sửa những vấn đề có sai sót trong chính sách an toàn thông tin mà doanh nghiệp định triển khai nhằm giúpnhững chính sách hoàn thiện hơn, đạt được độ chính xác cao.

-Việc “ hiệu chỉnh chính sách” là một trong 10 bước triển khai ISP là rất quan trọng vì khi doanh nghiệp tiến hành triển khai ISP sẽ gặp ít hoặc nhiều các vấn đề sinh ra trong các chính sách đề ra vì thế phải có bước hiệu chỉnh chính sách để có thể sửa lại các sai sót tồn đọng trong chính sách an toàn thông tin của doanh nghiệp.

- Nếu bước “hiệu chỉnh chính sách” không có hoặc không được triển khai sẽ làm các vấn đề sai sót sẽ luôn nằm trong chính sách an toàn thông tin của doanh nghiệp từ đó việc thực hiện các chính sách đó sẽ gặp các vấn đề và kéo theo nhiều hệ lụy cho doanh nghiệp.

13.”Đánh giá tính hiệu quả (Evaluate Effectiveness)” là một trong 10 bước triển khai ISP. Bạn hãy phân tích để thấy được tại sao cần có “Đánh giá tính hiệu quả” trong khi triển khai ISP của một doanh nghiệp.

- Đánh giá tính hiệu quả (Evaluate Effectiveness) là quá trình xem xét hiệu quả và khả năng giải quyết được các mỗi đe dọa về an toàn thông tin khi thực hiện của chính sách an toàn thông tin dựa trên các chính sách mà doanh nghiệp đã triển khai

- Bước đánh giá tính hiệu quả của chính sách là 1 trong các bước rất quan trọng trong việc triển khai chính sách an toàn thông tin nhằm giúp doanh nghiệp thấy được sự hiệu quả và có thể giải quyết được những vấn đề về an toàn thông tin mà doanh nghiệp đang gặp phải.

- Nếu tính hiệu quả trong việc triển khai chính sách không được thực hiện thì doanh nghiệp không thể biết được các chính sách đã đề ra thực hiện có khả năng giải quyết được các mối đe dọa không và từ đó các thông tin dữ liệu của doanh nghiệp có thể bị đe dọa

14.”Nhận thức và tập huấn (Awareness & Training)” là một trong 10 bước triển khai ISP.

Bạn hãy phân tích để thấy được tại sao cần có “Nhận thức và tập huấn” trong khi triển khai ISP của một doanh nghiệp.

- Nhận thức và tập huấn trong các bước triển khai IPS là doanh nghiệp sẽ tiến hành tuyên truyền, củng cố và nâng cao nhận thức về an toàn thông tin hiện nay và sẽ doanh nghiệp sẽ tiến hành các hoạt động tập huấn giả lập các tình huống mất an toàn thông tin trong doanh nghiệp.
- Bước “nhận thức và tập huấn” sẽ giúp cho doanh nghiệp nói chung và các cá nhân trong doanh nghiệp nói riêng sẽ có các kiến thức về đảm bảo an toàn thông tin trong hiện nay

và sẽ có kinh nghiệm để xử lý một cách nhanh chóng và hiệu quả khi gặp các vấn đề về an toàn thông tin

- Nếu bước "nhận thức và tập huấn" không được triển khai thì doanh nghiệp và các cá nhân sẽ không có các kiến thức hay các kinh nghiệm để xử lý các tình huống nguy cấp từ đó làm cho các thông tin của doanh nghiệp sẽ bị đe dọa nghiêm trọng

II. LO1- Nhận dạng được các mối đe dọa ảnh hưởng đến ATTT của một tổ chức/cá nhân

Tình huống 1:

Bạn là một nhân viên thu ngân phí bảo hiểm của công ty bảo hiểm ANZ. Bạn được cấp một máy tính có kết nối internet và phần mềm để thực hiện công việc hàng ngày của mình. Do ít khách hàng nên bạn cũng khá nhàn rỗi. Những lúc nhàn rỗi, bạn hay dùng máy tính làm việc lên internet để tải game, nhạc, phim về để giải trí. Các trang web bạn vào hầu như là các trang web không an toàn. Bạn hãy:

Bài làm

(1) Chỉ ra 2 mối đe dọa mà bạn có thể gặp phải trong tình huống trên;

- Lỗ hỏng
- Hành động vô ý thức
- Mã độc xâm nhập

(2) Nêu ra được lý do tại sao có những mối đe dọa đó

- Lỗ hỏng: Hệ thống bảo mật của tổ chức không đảm bảo an toàn khi truy cập vào các trang web, điều này tạo cơ hội cho tin tặc khai thác những điểm yếu của hệ thống an ninh hiện tại và dễ dàng xâm nhập trong môi trường của họ

- Hành động vô ý thức: nhân viên truy cập vào các trang mạng để giải trí nhưng vô tình lại không biết bản thân mình đã vào các web không an toàn, có thể khiến cho hệ thống máy tính gặp rủi ro vì phần mềm độc hại hoặc hành vi lừa đảo chẳng hạn như tiết lộ mật khẩu hoặc thông tin cá nhân, thường là thông qua một trang web giả mạo.

- Mã độc: Các trang web có chứa các phần mềm độc hại do các tay tin tặc hay các kẻ phá hoại tạo ra nhằm gây hại cho các máy tính thông qua các cuộc tấn công của Virus,… mà không có sự đồng thuận của người dùng

(3) Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra

- Các virus, mã độc xâm nhập vào máy tính làm nhiễu thông tin, làm mất dữ liệu => không báo cáo được.

- Hệ thống không hoạt động bình thường, bị nhiễm độc -> Công việc bị đình đốn => Ảnh hưởng đến công ty.

- Mất uy tín của công ty, mất niềm tin của khách hang -> Ảnh hưởng đến doanh thu, phòng quản lí sẽ kỹ luật nhắc nhở, bản thân người nhân viên sẽ có nguy cơ bị mất việc

(4)Giải pháp:

Công ty nên áp dụng nguyên tắc: "quyền tối thiểu" đối với nhân viên để không thể truy cập vào những phần mềm khác ngoài những phần mềm của công ty. Huấn luyện nhân viên thực hiện đúng các thao tác, hạn chế sai sót Thường xuyên backup hệ thống

Tình huống 2:

Bạn là trưởng phòng kinh doanh của một công ty lớn. Bạn thường xuyên phân công công việc, theo dõi công việc các nhân viên thuộc cấp dưới của mình qua hệ thống website của doanh nghiệp. Đồng thời thường xuyên giao dịch hợp đồng với khách hàng qua email, cũng như báo cáo kết quả công việc cho sếp. Đợt vừa rồi bạn có một chuyến công tác 1 tuần ở các một số tỉnh. Thật là không may mắn, máy laptop làm việc của bạn bị hư đột xuất và không có nơi nào sữa chữa liền được. Để giải quyết các công việc hàng ngày, bạn phải dùng máy tính công cộng tại các khách sạn mà bạn lưu trú tại nơi công tác.

Bạn hãy:

Bài làm

(1) Chỉ ra 2 mối đe dọa có thể gặp phải trong tình huống trên.

- Hành động vô ý

- Mã độc.

(2) Lý do tại sao có những mối đe dọa đó:

- Hành động vô ý: Khi gặp sự cố ngoài ý muốn, trưởng phòng muốn giải quyết công việc nên phải sử dụng máy tính công công nhưng không biết rằng máy tính liệu có cài đặt các phần mềm ộc hại chẳng hạn Key logger, Phishing…) hay không? Hoặc Internet công cộng có an toàn khi truy cập ? v.v…

- Mã độc: có thể chứa có virus, mã độc dạng E-mail, … tạo cơ hội cho kẻ xâm nhập đánh cắp tài khoản Username và password. Ngoài ra, các tài khoản liên kết E-mail có thể bị đánh cắp…

(3) Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra.

- Máy tính công cộng không an toàn, được nhiều người sử dụng, có thể bị cài đặt các phần mềm độc hại có chứa virus nên khi truy cập vào rất dễ bị mất dữ liệu => Mất thông tin của khách hàng, những hợp đồng quan trọng thậm chí những báo cáo công việc cho sếp cũng bị ảnh hưởng.

- Mất niềm tin của đối tác kinh doanh => ảnh hưởng đến uy tín của công ty.

- Sự phân công công việc cho nhân viên cấp dưới sẽ trì trễ hoặc có thể bị hoãn

Tình huống 3

Công ty cổ phần Chứng khoán FPT (tên viết tắt: FPTS) là thành viên của tập đoàn FPT, được cấp phép thành lập và hoạt động theo giấy phép của ủy ban chứng khoán nhà nước cấp ngày13/07/2007. Ngành nghề kinh doanh chính: Môi giới chứng khoán; hoạt động tự doanh chứng khoán; tư vấn đầu tư chứng khoán; bảo lãnh phát hành chứng khoán; lưu ký và quản lý cổ đông...

Giải :

1. 3 mối đe dọa

- Tấn công giả mạo, lừa đảo qua tin nhắn

- Mã độc

- Lấy trộm và đánh cắp dữ liệu

2. Lý do có những mối đe dọa đó:

- Thiếu ý thức trong việc bảo mật cho đội ngũ làm việc, người dùng bị đánh lừa bởi một website giả mạo gần như giống hệt với website thật.

- Có thể do thiếu cẩn trọng tạo điều kiện cho tội phạm mạng có cơ hội tấn công. Có thể là do nhân viên sơ ý nhấp vào email giả mạo và vô tình phát tán mã độc khắp hệ thống mạng.

- Lợi dụng vị trí trong tổ chức để thực hiện hành vi phá hoại hoặc bị hack vào hệ thống hoặc sử dụng thiết bị công cộng.

3. Phân tích hậu quả

- Đánh lừa người dùng, khai thác sự bất tiện của công nghệ bảo mật web. Lấy được các thông tin quan trọng, mật khẩu và các chi tiết thẻ tín dụng bằng cách giả dạng thành 1 chủ thể tin cậy trong giao dịch điện tử. Các giao dịch thường dùng để đánh lừa những người dùng ít đa nghi. Thường được thực hiện qua thư điện tử hoặc tin nhắn nhanh, yêu cầu người dùng nhập thông tin vào website giả mạo.

- Gây thiệt hại lớn cho cả máy chủ và người dùng, mức độ phụ thuộc vào mục đích của hacker. Nếu nhắm vào máy chủ, chúng có thể làm tê liệt website hoặc triển khai những nội dung sai lệch. Khách hàng cũng sẽ gặp vấn đề khi truy cập website.

- Gây ra những tổn thất tài chính nghiêm trọng, nguy cơ bị tống tiền, lừa đảo, chiếm đoạt tài sản, bôi nhọ và xâm phạm danh dự, nhân phẩm.

4. Biện pháp phòng ngừa

- Cần tập trung cảnh giác trước các phương thức tấn công kỹ thuật, cảnh giác với những email lạ, địa chỉ email không rõ ràng.

+ Không tải tập tin và những đường dẫn đáng ngờ

+ Đào tạo nhân viên những dấu hiệu nhận biết website/ email giả mạo

- Sử dụng các công cụ diệt virus để xóa hết thư rác và mã độc trên website.

+ Thay đổi tất cả mật khẩu

+ Liên hệ với nhà cung cấp dịch vụ lưu trữ web

+ Cập nhật hoặc cài đặt bản sao lưu trên website

- Hạn chế sử dụng thiết bị công cộng, không nhấn vào đường link lạ, hạn chế sử dụng wifi công cộng để đăng nhập vào các tài khoản cá nhân. Hạn chế cho người khác sử dụng thiết bị cá nhân

LO1- Giải thích được sự ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội

Đưa ra một hệ thống thông tin, yêu cầu sinh viên giải thích sự cần thiết của an toàn thông tin đối với hệ thống đó, từ đó nêu ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội.

Ví dụ 1:

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.

Hãy trình bày ít nhất 3 tính cần thiết của an toàn thông tin đối với website của trung tâm. Từ đó giải thích sự ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội.

Các tính cần thiết của an toàn thông tin đối với website của trung tâm tin học là những yếu tố quan trọng giúp bảo vệ thông tin cá nhân của sinh viên, đảm bảo tính toàn vẹn và bảo mật của dữ liệu học phí và kết quả thi, và duy trì uy tín của trung tâm. Dưới đây là ba tính cần thiết của an toàn thông tin cùng với sự ảnh hưởng của chúng đối với cá nhân, tổ chức và xã hội:

1. **Bảo vệ thông tin cá nhân của sinh viên**:
    - **Tính cần thiết**: Đảm bảo rằng thông tin cá nhân của sinh viên như họ tên, số điện thoại, địa chỉ email và thông tin thanh toán được bảo vệ và không bị rò rỉ.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Sinh viên cảm thấy an tâm hơn khi biết thông tin cá nhân của họ được bảo vệ, giúp tăng cường sự tin tưởng và sự hài lòng với dịch vụ.
        - **Tổ chức**: Duy trì uy tín và danh tiếng của trung tâm tin học, tạo điều kiện thuận lợi cho sự phát triển kinh doanh và thu hút sinh viên mới.
        - **Xã hội**: Đảm bảo tính riêng tư và bảo vệ quyền lợi của sinh viên trên internet, góp phần vào việc xây dựng một môi trường trực tuyến an toàn và đáng tin cậy.
2. **Bảo vệ dữ liệu học phí và kết quả thi**:
    - **Tính cần thiết**: Triển khai các biện pháp bảo mật như mã hóa dữ liệu và cơ chế kiểm soát truy cập để bảo vệ thông tin về học phí và kết quả thi khỏi các cuộc tấn công mạng.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Sinh viên cảm thấy an tâm hơn khi biết dữ liệu về học phí và kết quả thi của họ được bảo vệ khỏi sự xâm phạm và sửa đổi trái phép.
        - **Tổ chức**: Bảo vệ uy tín và độ tin cậy của trung tâm tin học, giúp duy trì sự hài lòng của sinh viên và thu hút sinh viên mới.
        - **Xã hội**: Đảm bảo tính toàn vẹn và minh bạch của hệ thống giáo dục, góp phần vào việc xây dựng một xã hội công bằng và phát triển bền vững.
3. **Bảo vệ thông tin thanh toán trực tuyến**:
    - **Tính cần thiết**: Đảm bảo rằng thông tin về thẻ ngân hàng và giao dịch thanh toán trực tuyến được mã hóa và bảo vệ an toàn.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Tăng cường sự tin tưởng và an tâm khi thực hiện giao dịch thanh toán trực tuyến, giảm nguy cơ mất mát tiền bạc và thông tin cá nhân.
        - **Tổ chức**: Xây dựng uy tín và độ tin cậy với sinh viên, tạo điều kiện thuận lợi cho việc phát triển kinh doanh trực tuyến và mở rộng thị trường.
        - **Xã hội**: Thúc đẩy việc sử dụng thanh toán trực tuyến, tạo điều kiện thuận lợi cho thương mại điện tử phát triển và góp phần vào việc phát triển kinh tế số.

Ví dụ 2:

Nhà ăn của trường Đại học Công nghiệp Tp. HCM có một Website ĐẶT THỰC ĐƠN CÁC MÓN ĂN TRỰC TUYẾN (http://www.cantin_iuh.edu.vn) nhằm giúp cho các nhân viên, giáo viên và sinh viên (gọi chung là khách hàng) của trường có thể tìm và đặt thực đơn các món ăn cho bữa ăn sáng/trưa/tối thông qua website và thức ăn sẽ được giao tới tận phòng/khoa của khách hàng mà khách hàng yêu cầu. Website có hiển thị danh mục và giá cả của các món ăn để khách hàng tham khảo. Để có thể đặt các món ăn, khách hàng phải đăng ký làm thành viên của Website. Để đăng ký thành viên thì khách hàng phải cung cấp thôngtin cá nhân như họ tên, số điện thoại, địa chỉ email, mã số giáo viên/mã sinh viên để hệ thống lưu trữ và quản lý. Khi đặt món khách hàng có thể thanh toán đơn đặt hàng trực tuyến hoặc trả tiền mặt ngay khi nhận các món ăn. Khi thanh toán thực đơn trực tuyến khách hàng phải cung cấp thông tin về thẻ ngân hàng thanh toán. Hãy trình bày ít nhất 3 tính cần thiết của an toàn thông tin đối với website nhà ăn. Từ đó giải thích sự ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội.

Các tính cần thiết của an toàn thông tin đối với website nhà ăn là những yếu tố quan trọng để đảm bảo bảo vệ thông tin cá nhân của khách hàng, ngăn chặn các cuộc tấn công mạng và duy trì uy tín của doanh nghiệp. Dưới đây là ba tính cần thiết của an toàn thông tin cùng với sự ảnh hưởng của chúng đối với cá nhân, tổ chức và xã hội:

1. **Bảo vệ thông tin cá nhân của khách hàng**:
    - **Tính cần thiết**: Đảm bảo rằng thông tin cá nhân như họ tên, số điện thoại, địa chỉ email và thông tin thanh toán được bảo vệ và không bị rò rỉ.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Người dùng cảm thấy an tâm hơn khi biết thông tin cá nhân của họ được bảo vệ, giúp tăng cường sự tin tưởng và sự hài lòng với dịch vụ.
        - **Tổ chức**: Duy trì uy tín và danh tiếng của nhà ăn, tạo điều kiện thuận lợi cho sự phát triển kinh doanh trong tương lai.
        - **Xã hội**: Đảm bảo tính riêng tư và bảo vệ quyền lợi của người dùng trên internet, góp phần vào việc xây dựng một môi trường trực tuyến an toàn và đáng tin cậy.
2. **Ngăn chặn các cuộc tấn công mạng**:
    - **Tính cần thiết**: Triển khai các biện pháp bảo mật như tường lửa, phần mềm diệt virus và mã hóa dữ liệu để ngăn chặn các cuộc tấn công từ bên ngoài.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Người dùng cảm thấy an tâm hơn khi biết thông tin cá nhân của họ được bảo vệ khỏi các cuộc tấn công mạng, giảm nguy cơ mất mát thông tin và tiền bạc.

- **Tổ chức**: Bảo vệ hệ thống thông tin của nhà ăn khỏi các mối đe dọa mạng, giúp duy trì sự ổn định của dịch vụ và tránh mất mát về kinh phí và uy tín.
- **Xã hội**: Góp phần vào việc tạo ra một môi trường trực tuyến an toàn hơn cho tất cả người dùng, ngăn chặn tội phạm mạng và bảo vệ hệ thống thông tin quan trọng.

3. **Bảo vệ thông tin thanh toán trực tuyến**:
   - **Tính cần thiết**: Đảm bảo rằng thông tin về thẻ ngân hàng và giao dịch thanh toán trực tuyến được mã hóa và bảo vệ an toàn.
   - **Sự ảnh hưởng**:
     - **Cá nhân**: Tăng cường sự tin tưởng và an tâm khi thực hiện giao dịch thanh toán trực tuyến, giảm nguy cơ mất mát tiền bạc và thông tin cá nhân.
     - **Tổ chức**: Xây dựng uy tín và độ tin cậy với khách hàng, tạo điều kiện thuận lợi cho việc phát triển kinh doanh trực tuyến và mở rộng thị trường.
     - **Xã hội**: Thúc đẩy việc sử dụng thanh toán trực tuyến, tạo điều kiện thuận lợi cho thương mại điện tử phát triển và góp phần vào việc phát triển kinh tế số.

Ví dụ 3:

Đường sắt Việt Nam sử dụng website www.dsvn.vn để giúp hành khách đặt và mua vé trực tuyến. Thông qua website, các nhà ga quản lý được quá trình bán, mua vé của người dân cũng như thể hiện các tính ưu việt khác thông qua các nghiệp vụ điều hành. Website hiển thị các thông tin cần thiết mà khách hàng mong muốn: tuyến tàu, giá vé, thời gian chạy, thời gian đến, tình trạng số chỗ cho mỗi toa ... Để có thể đặt vé, hành khách truy cập vào website và tra cứu thông tin: chọn ngày đi, ga đi, ga đến, thời gian phù hợp, loại ghế ... cũng như bắt buộc phải cung cấp đúng thông tin cá nhân: họ tên người đi, thông tin giấy tờ tùy thân (số CMND hoặc thẻ căn cước, số hộ chiếu ...), năm sinh và một số thông tin bổ sung khác.

Khách hàng cũng có thể thanh toán trực tuyến hoặc thanh toán tại các địa điểm chỉ định(ngân hàng, nhà ga, đại lý, các điểm thu hộ ...). Quản lý ga/nhân viên tùy theo chức năng,nhiệm vụ được giao thực hiện các thao tác nghiệp vụ liên quan đến quy định đặt chỗ, bán vé,hủy vé, đổi ngày, cập nhật thông tin liên quan đến giá vé, giảm giá, các ưu đãi, khuyến cáo ...cũng thông qua cổng thông tin này.Hãy trình bày ít nhất 3 tính cần thiết của an toàn thông tin đối với website DSVN. Từ đó giảithích sự ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội.

Các tính cần thiết của an toàn thông tin đối với website DSVN (Đường sắt Việt Nam) là những yếu tố quan trọng giúp bảo vệ thông tin cá nhân của hành khách, đảm bảo tính toàn vẹn và bảo mật của dữ liệu vé tàu, và duy trì sự tin cậy của hệ thống vận tải đường sắt. Dưới đây là ba tính cần thiết của an toàn thông tin cùng với sự ảnh hưởng của chúng đối với cá nhân, tổ chức và xã hội:

1. **Bảo vệ thông tin cá nhân của hành khách**:
    - **Tính cần thiết**: Đảm bảo rằng thông tin cá nhân của hành khách như họ tên, số CMND hoặc thẻ căn cước, năm sinh và các thông tin khác được bảo vệ và không bị rò rỉ.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Hành khách cảm thấy an tâm hơn khi biết thông tin cá nhân của họ được bảo vệ, giúp tăng cường sự tin tưởng và sự hài lòng với dịch vụ.
        - **Tổ chức**: Duy trì uy tín và danh tiếng của DSVN, tạo điều kiện thuận lợi cho sự phát triển vận tải đường sắt và thu hút khách hàng mới.
        - **Xã hội**: Đảm bảo tính riêng tư và bảo vệ quyền lợi của hành khách trong việc sử dụng dịch vụ vận tải công cộng, góp phần vào việc xây dựng một môi trường trực tuyến an toàn và đáng tin cậy.
2. **Bảo vệ dữ liệu vé tàu và giao dịch thanh toán**:
    - **Tính cần thiết**: Triển khai các biện pháp bảo mật như mã hóa dữ liệu và cơ chế kiểm soát truy cập để bảo vệ thông tin về vé tàu và giao dịch thanh toán trực tuyến khỏi các cuộc tấn công mạng.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Hành khách cảm thấy an tâm khi biết dữ liệu về vé tàu và thanh toán của họ được bảo vệ khỏi sự xâm phạm và sửa đổi trái phép.
        - **Tổ chức**: Bảo vệ uy tín và độ tin cậy của DSVN, giúp duy trì sự hài lòng của hành khách và thu hút khách hàng mới.
        - **Xã hội**: Đảm bảo tính toàn vẹn và minh bạch của hệ thống vận tải đường sắt, góp phần vào việc xây dựng một xã hội công bằng và phát triển bền vững.
3. **Bảo vệ thông tin quản lý và hoạt động nghiệp vụ của DSVN**:
    - **Tính cần thiết**: Đảm bảo rằng thông tin quản lý về đặt chỗ, bán vé, cập nhật thông tin giá vé và các ưu đãi được bảo vệ khỏi sự xâm nhập và sửa đổi trái phép.
    - **Sự ảnh hưởng**:
        - **Cá nhân**: Hành khách cảm thấy an tâm khi biết hệ thống vận tải đường sắt hoạt động một cách an toàn và hiệu quả.
        - **Tổ chức**: Duy trì sự hoạt động ổn định và hiệu quả của DSVN, giúp nâng cao hiệu suất và lợi ích cho tổ chức.
        - **Xã hội**: Đảm bảo sự an toàn và tin cậy của hệ thống vận tải công cộng, góp phần vào việc cải thiện dịch vụ và giảm ùn tắc giao thông.

LO2- Nhận dạng được các mối đe dọa ảnh hưởng đến ATTT của một tổ chức / cá nhân

Đưa ra một tình huống mang tính thực tiễn của một hệ thống thông tin. Yêu cầu sinh viên chỉ ra các mối đe dọa, nêu ra được lý do, phân tích hậu quả và đưa ra các giải pháp khắc phục.

Một vài mối đe doạ đến an toàn thông tin:

- Một nhân viên dùng máy tính công cộng để đăng nhập và giải quyết công việc của công ty. (Hành động vô ý)
- Một nhân viên dùng máy tính đang làm việc ở công ty để tải game, tải nhạc, phim về máy để giải trí. Các trang web hầu như không rõ nguồn gốc. (Hành động vô ý)
- Một nhân viên tự ý cài đặt phần mềm vào máy tính của cơ quan mà không thông qua đơn vị có thẩm quyền. (Hành động vô ý hoặc cố ý)
- Một sinh viên CNTT thực hiện tấn công vào một trang web để thu thập, điều chỉnh, phá hoại thông tin, làm hư hại các chức năng của một hệ thống. (Hành động cố ý)
- Một nhân viên bị mua chuộc để cung cấp thông tin nhạy cảm của tổ chức. (Hành động cố ý)
- Một doanh nghiệp đặt trụ sở tại nơi thường xuyên xảy ra thiên tai, lũ lụt, mất điện. (Thiên tai)
- Một hệ thống mạng máy tính của công ty thường xuyên xảy ra lỗi phần cứng hoặc/và không cập nhật phần mềm hoặc sử dụng phần mềm không có bản quyền (Lỗi kỹ thuật)
- Một doanh nghiệp không đưa ra bất kỳ quy định nào về việc sử dụng hệ thống mạng máy tính trong tổ chức. (Lỗi quản lý)
- Một doanh nghiệp không xây dựng đội ngũ nhân viên bảo trì, quản trị hệ thống, không thường xuyên tập huấn để cập nhật công nghệ mới. (Lỗi quản lý)