Bài làm kiểm tra môn An Toàn và bảo mật thông tin

Thương Mại điện tử (Trường Đại học Thương mại)

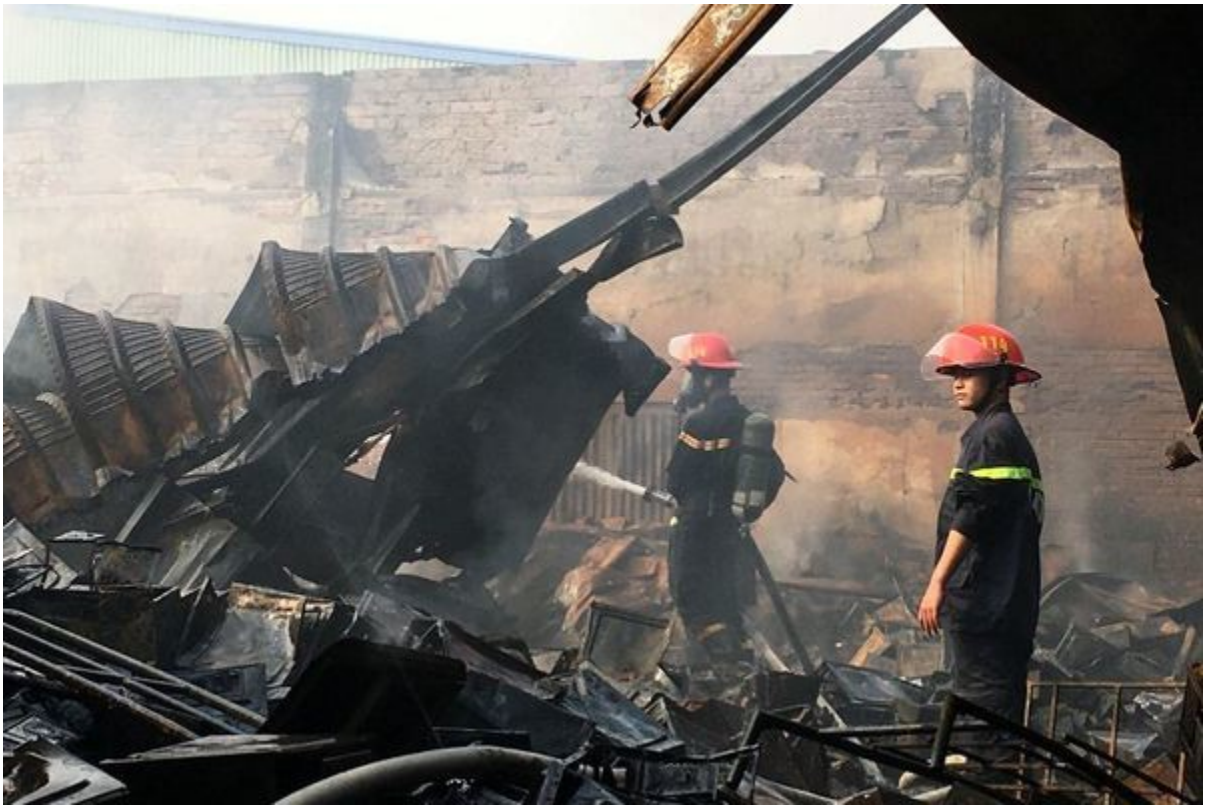
TRƯỜNG ĐẠI HỌC THƯƠNG MẠI HỌC KỲ II NĂM HỌC 2021 – 2022 *(Phần dành cho sinh viên/ học viên)*	
Bài thi học phần: An toàn và bảo mật thông tin **Mã số đề thi:** **Ngày thi:** 07/03/2022 **Số trang**: 11	**Số báo danh:** 06 **Lớp:** 2207eCIT0921 **Họ và tên:** Chu Quỳnh Chi
Điểm kết luận:	**GV chấm thi 1:** …….……..... **GV chấm thi 2:** …….…….....

Câu 1:

Một thông điệp truyền trên một kênh truyền tin nào đó có thể gặp những nguy cơ mất an toàn khi các lỗ hổng của hệ thống bị tấn công từ bên trong hoặc bên ngoài. Hệ thống thông tin có thể gặp những dạng nguy cơ khác nhau và được chia ra theo nhiều cách. Trong đó, có thể chia những dạng nguy cơ này thành hai nhóm:

1. Nhóm nguy cơ ngẫu nhiên: bao gồm các hiểm dọa do thiên nhiên; là hiểm họa chung đối với tất cả các hoạt động của con người trên phạm vi toàn thế giới, được đề cập đến nhiều và có tính thông dụng. Ví dụ: Lũ lụt, dịch bệnh, hỏa hoạn

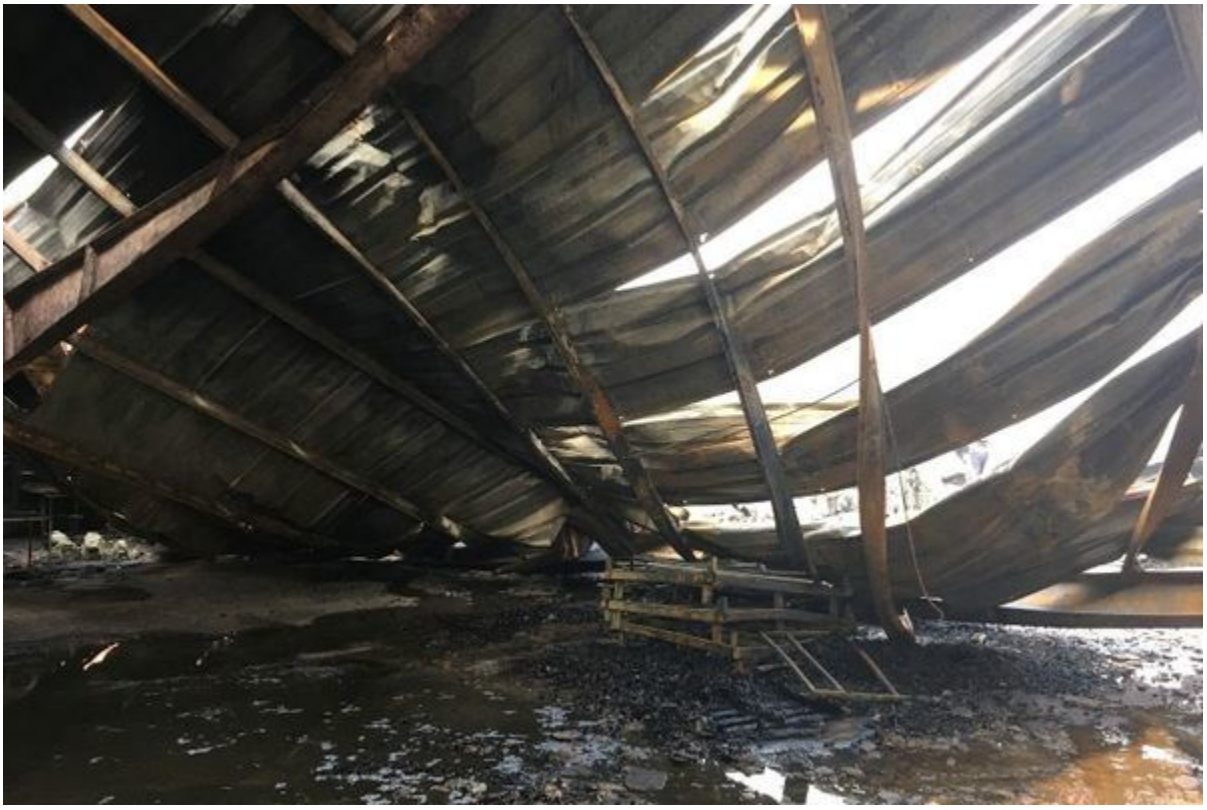
   Cháy lớn 2 công ty sát nhau ở Hải Dương, 10 tỷ thiết bị máy tính thành tro.
   Vụ hỏa hoạn từ 1 nhà kho chứa máy tính đã lan tiếp sang nhà máy hạt nhựa khiến 1.500m2 nhà xưởng đổ sập, gây thiệt hại lớn. Khoảng 4h30 sáng ngày 23/02/2020, vụ hỏa hoạn lớn xảy ra tại 2 công ty sát nhau làm 1.500m2 nhà xưởng bị đổ sập. Vụ cháy gây thiệt hại tài sản trên 10 tỷ đồng.
   Công an TP Hải Dương cho hay, ngọn lửa bùng phát tại khu nhà công ty CP XNK Coolerplus sau đó lan sang nhà xưởng của công ty CP nhựa thông minh Việt Nam. 2 công ty này nằm sát nhau và cùng có địa chỉ tại khu công nghiệp Cẩm Thượng (phường Việt Hòa, TP Hải Dương, tỉnh Hải Dương).
   Bên trong các nhà kho trước khi xảy ra hỏa hoạn chứa hàng nghìn máy tính và các linh kiện liên quan đến máy tính và thiết bị điện tử khác. Tuy nhiên vụ cháy chỉ được báo cho cơ quan chức năng khi được công nhân của công ty gần đó phát hiện.



Nhà xưởng đổ sập

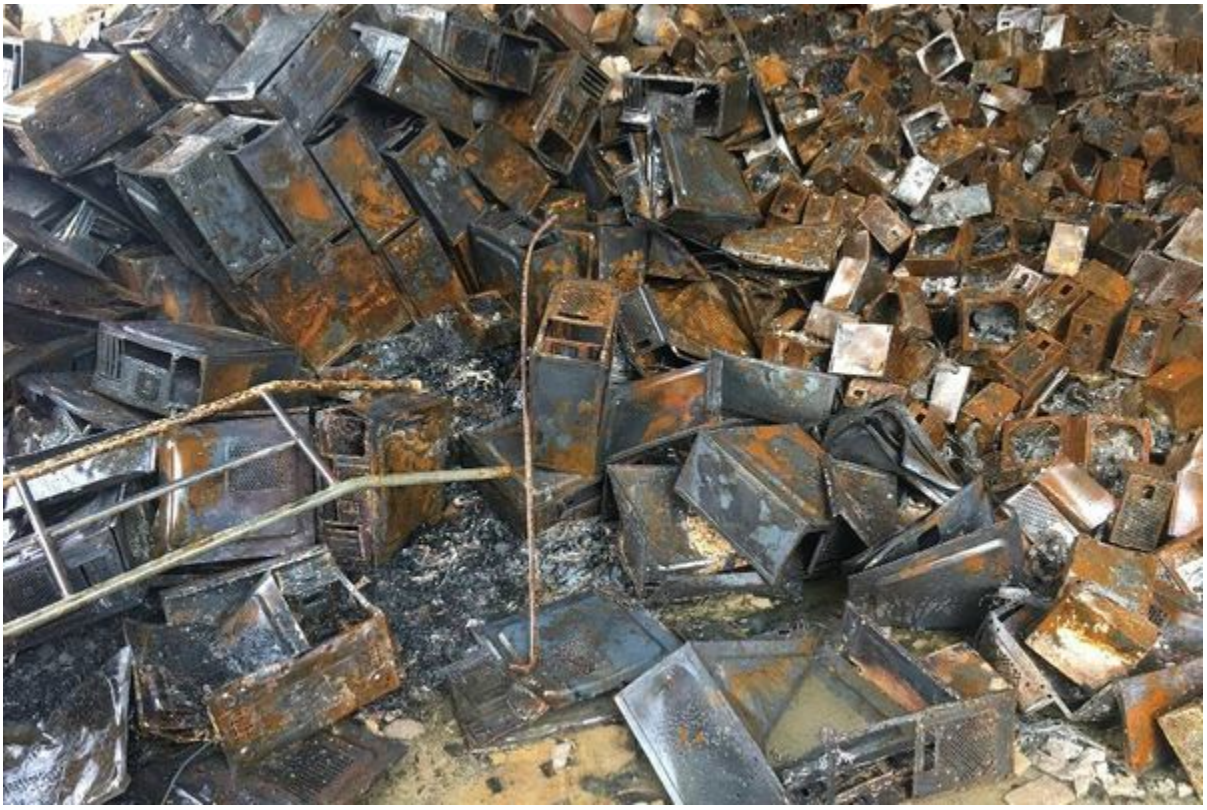
Rất may vụ cháy không gây thiệt hại về người nhưng ước tính ban đầu thiệt hại về tài sản trên 10 tỷ đồng.

Nhận được tin báo, Phòng Cảnh sát PCCC&CNCH Công an tỉnh Hải Dương phối hợp với Công an TP Hải Dương điều động lực lượng cán bộ chiến sĩ cùng 4 xe chữa cháy tiếp cận hiện trường để dập lửa.

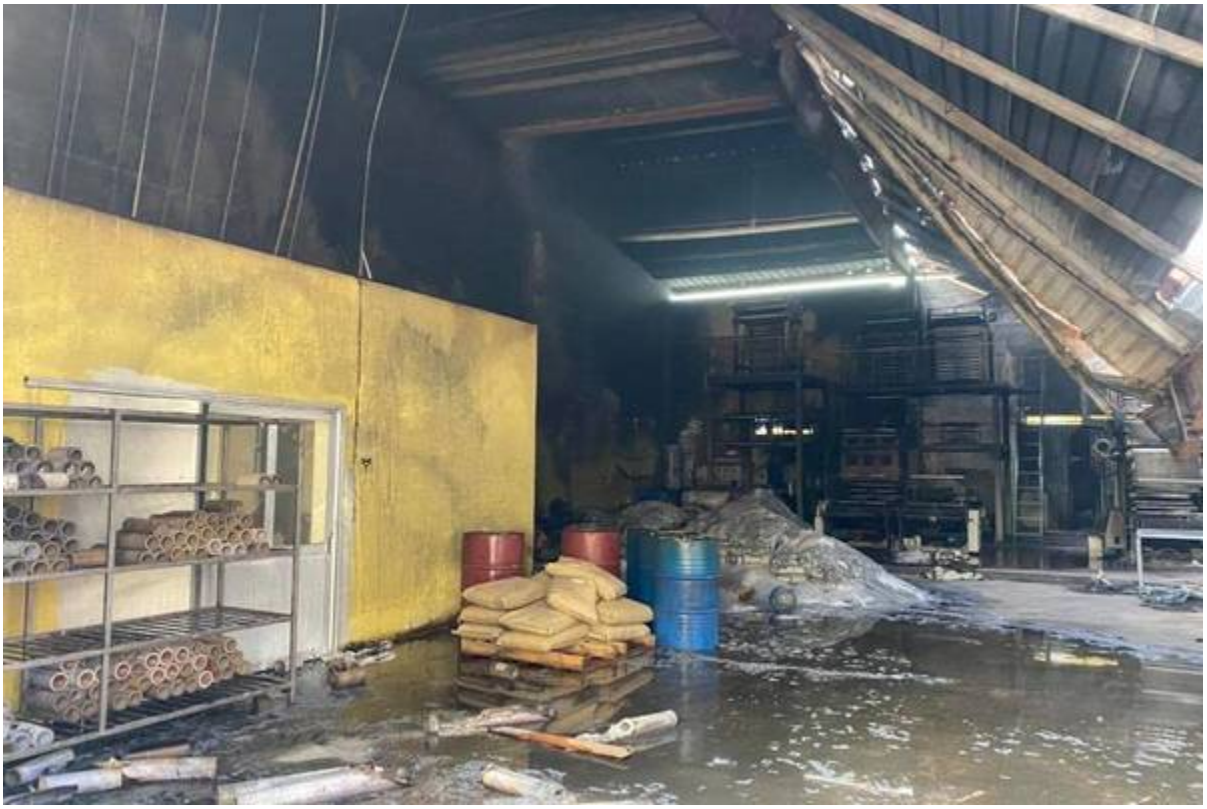


2 công ty liên tiếp nhau nên công tác chữa cháy gặp khó khăn

Đến 6h30, lực lượng chức năng đã khống chế và dập tắt vụ cháy và kịp thời ngăn chặn không để cháy lan sang hơn 3.000m2 nhà xưởng khác. Tuy nhiên, sau 2 tiếng nỗ lực dập lửa, 1.500m2 nhà xưởng của 2 công ty bị đổ sập.



Cháy 2 công ty sát nhau ở Hải Dương hơn 10 tỷ thiết bị máy tính thành than



Hơn 10 tỷ đồng đã bị thiêu thành than

Nguồn: (Báo Vietnamnet.vn.) https://vietnamnet.vn/vn/thoi-su/chay-lon-2-cong-ty-sat-nhau-o-hai-duong-10-ty-thiet-bi-may-tinh-thanh-tro-618697.html.

Biện pháp phòng tránh những nguy cơ trên:

a. Sao lưu dữ liệu dự phòng thường xuyên.
   Với giải pháp này chỉ có phương án sao lưu dữ liệu dự phòng ra băng từ (tape) hoặc các thiết bị khác. Dữ liệu được sao lưu hằng ngày và các băng từ được chuyển đến một nơi khác (offsite) để cất giữ. nên khi cần khôi phục các băng từ được mang trở lại để khôi phục lại phần dữ liệu bị sự cố.
b. Giải pháp xây dựng trung tâm dữ liệu dự phòng và sao lưu dữ liệu theo chu kỳ.
   Sao lưu dự phòng dữ liệu kết hợp với một trung tâm dự phòng nhưng ở mức chỉ an toàn cho dữ liệu. Một khi có sự cố tại trung tâm chính, toàn bộ dữ liệu của doanh nghiệp vẫn an toàn nhưng cần có thời gian nhất định để khôi phục cho hệ thống hoạt động lại. Tuy nhiên do dữ liệu chỉ được sao lưu theo chu kỳ nên có thể sẽ có sự mất mát nhỏ dữ liệu của những giao dịch nằm trong khoảng giữa chu kỳ sao lưu. Ưu điểm của giải pháp là chi phí thấp và hầu như đảm bảo dữ liệu không bị mất mát khi có thảm hoạ xảy ra.
c. Giải pháp xây dựng trung tâm dữ liệu dự phòng và sao lưu dữ liệu trực tuyến (online)
   Với giải pháp này chúng ta đảm bảo dữ liệu không bị mất mát và khắc phục được các nhược điểm của giải pháp trên nhờ sao lưu dữ liệu liên tục và tự động thông qua đường truyền nhưng chi phí đầu tư cao hơn. Tuy chưa đảm bảo an toàn cho tất cả dữ liệu vì sao lưu trực tuyến nhưng hệ thống vẫn cần một khoảng thời gian ngắn để thực thi, nhưng giải pháp này đã có thể đảm bảo gần như 99,99% dữ liệu của doanh nghiệp được sao lưu an toàn.

2. Nguy cơ có chủ đích gồm ba nhóm: Mối đe dọa từ các thiết bị phần cứng, mối đe dọa từ các phần mềm và mối đe dọa từ con người. Ví dụ: Virus thư điện tử, thiết bị (có kết nối thông qua bộ định tuyến Internet) bảo mật kém
   a. Mối đe dọa từ thiết bị phần cứng

Mối đe dọa từ các thiết bị phần cứng là mối đe dọa xuất hiện từ các thiết bị phần cứng hoặc các thiết bị vật lý trong hệ thống thông tin của tổ chức bao gồm:

- Các máy tính: Các máy chủ, các máy chủ lưu trữ trên mạng (NAS) và các máy chủ mạng vùng lưu trữ (SAN), máy tính để bàn, máy tính xách tay, máy tính bảng,...

- Các thiết bị truyền thông: Các bộ định tuyến (Routers), các bộ chuyển đổi (Switches), hệ thống tường lửa phần cứng (Firewalls), các mô đem, các bộ phân nhánh nội bộ (Private Branch Exchanges (PBXs), hệ thống máy fax, v.v...

- Các thiết bị công nghệ: Bộ hỗ trợ nguồn điện, các bộ hỗ trợ chống sốc (UPSs), các thiết bị điều hòa nguồn, điều hòa không khí,...

- Các thiết bị lưu trữ: Các hệ thống lưu trữ, các thiết bị lưu trữ như bộ nhớ trong, bộ nhớ ngoài, bộ nhớ dự phòng, các loại đĩa,...

- Các thiết bị nội thất, các hệ thống đánh giá,...

- Các loại thẻ thanh toán, các loại cổ phiếu, thẻ ghi nợ, dữ liệu cá nhân lưu trữ trên giấy, điện thoại cá nhân,...

Nhiều thiết bị trong số chúng có bảo mật kém, có thể tạo cơ hội cho kẻ tấn công lây nhiễm phần mềm độc hại, hoặc có thể theo dõi và kiểm soát chúng; Các thiết bị thường kết nối thông qua bộ định tuyến Internet, phần mềm độc hại từ thiết bị bị nhiễm có thể dễ dàng lây lan sang các thiết bị khác; Hoặc các thiết bị thường được thiết kế để hoạt động với các tài khoản trực tuyến; khi một thiết bị bị nhiễm cũng có thể cung cấp cho kẻ tấn công quyền truy cập vào các tài khoản đó...

Biện pháp đảm bảo an toàn:

1. Thường xuyên cập nhật các ứng dụng bảo mật
2. Chia nhỏ mạng nội bộ để dễ dàng quản lý
3. Tăng cường bảo mật thiết bị IoT (Internet-of-Things)

b. Mối đe dọa từ các phần mềm:

Đây là mục tiêu chung của các kẻ tấn công, bởi các lỗ hổng, các bug và các vấn đề của phần mềm cho phép kẻ tấn công có thể truy cập từ xa vào máy tính hoặc các thiết bị phần cứng, có thể tác động đến hệ thống dữ liệu, các tài nguyên mạng nội bộ, các nguồn dữ liệu và cơ chế xử lý thông tin khác của tổ chức, doanh nghiệp. Những lỗ hổng bảo mật này cũng chính là nguyên nhân dẫn đến các vấn đề phát sinh khác ảnh hưởng đến sự an toàn của hệ thống thông tin trong quá trình hoạt động của tổ chức, doanh nghiệp, gây mất an toàn và bảo mật của thông tin; là nơi mà các phần mềm độc hại (malware) gây tác động phá hoại trực tiếp đến hệ thống thông tin của tổ chức, doanh nghiệp.

Các phần mềm độc hại ngày nay:

• Virus lây nhiễm: Là các chương trình lây nhiễm các chương trình khác bằng cách thêm vào đó một mã chương trình để có được quyền truy 101 cập vào một tập tin nhằm gây hại hay làm chúng bị nhiễm. Vì vậy, loại virus này còn gọi là virus lây nhiễm.

• Virus thư điện tử: Các loại virus thư điện tử hầu hết lây lan dựa vào các email độc hại mà người dùng bất cẩn nháy vào. Những loại virus này có thể làm ảnh hưởng đến khả năng bảo mật của máy tính hoặc đánh cắp dữ liệu, hoặc gián tiếp tác động lên máy chủ của thư điện tử.

• Virus macro: Hay còn gọi là virus tài liệu vì chúng lợi dụng các macro (các lệnh vĩ mô được nhúng trong phần mềm xử lý văn bản hoặc bảng tính để kích hoạt chạy tự động) để lây nhiễm vào máy tính của người dùng. Một virus macro có thể tự sao chép và lây lan từ tệp này sang tệp khác trong máy tính bị nhiễm. Do đó, nếu người dùng mở một tệp có chứa virus macro, nó sẽ tự sao chép vào các ứng dụng, lây lan sang các tệp tiếp theo và có thể lây lan sang các tệp dữ liệu khác trong mạng nội bộ hoặc mạng doanh nghiệp.

• Virus boot-sector: Đây là loại virus lây lan qua các thiết bị lưu trữ khi bị nhiễm như ổ đĩa cứng, ổ di động (USB) và các thiết bị lưu trữ khác. Gọi là virus boot-sector vì chúng hoạt động khi máy tính vừa khởi động, virus này sẽ thay thế chương trình boot-sector của máy tính bằng một chương trình khác. Vì

thế, khi máy tính khởi động xong thì chúng sẽ làm lây nhiễm trên các ổ đĩa và làm sai lạc thông tin các tập tin hoặc thay đổi nội dung các tập tin trong máy tính.

• Sâu máy tính (Worm): Sâu máy tính nằm trong danh sách các malware - mã độc hại. Mục đích của các loại sâu máy tính là chiếm dụng tài nguyên và có thể phát tán dữ liệu lên mạng. Sâu máy tính có khả năng tự di chuyển từ máy tính này đến các máy tính đang kết nối mạng để lây lan các đoạn mã độc hoặc chiếm dụng các tài nguyên khác.

c. Các mối đe dọa đối với thiết bị di động

• Bluejacking là việc gửi các tin nhắn không mong muốn hoặc không được yêu cầu cho người lạ thông qua công nghệ Bluetooth. Bluejacking là hành vi trộm cắp dữ liệu thực tế từ các thiết bị hỗ trợ cổng Bluetooth (bao gồm cả điện thoại di động và máy tính xách tay), các kiểu dữ liệu dễ bị đánh cắp như danh sách liên lạc, danh bạ, hình ảnh và một số kiểu dữ liệu khác.

• Virus di động: Thiết bị di động có thể bị nhiễm virus lây lan qua mạng điện thoại di động. Ngoài các phần mềm mã độc và các phần mềm độc hại gây ra cho các thiết bị di động, còn có một nhóm phần mềm liên quan đến trình duyệt Web khi hệ thống truy cập các ứng dụng thông qua mạng Internet hoặc hệ thống Client/Server đó là các Cookies.

• Cookie là một tệp văn bản nhỏ được lưu trên máy tính, giúp để người dùng không phải nhập lại địa chỉ trang web khi họ muốn truy cập lại trang web đã truy cập trước đó (chủ yếu được sử dụng làm phương tiện để quản lý phiên (session), cá nhân hóa và theo dõi khi truy cập các trang web). Cookie rất cần thiết cho việc lưu dấu vết cho các trang web, chẳng hạn như các cửa hàng mua sắm trên Internet vì những cookie này thường bị xóa sau khi người dùng rời khỏi trang web hoặc trong vài ngày sau đó người dùng không truy cập vào trang web đó. Tuy nhiên, bên cạnh các cookie có lợi cho người dùng thì một số cookie khác có thể gây tác động không tốt đối với người dùng, chẳng hạn có cookie tự tạo lại sau khi người dùng đã xóa chúng, có cookie có thể theo dõi thói quen kết nối trực tuyến của người dùng, hoặc có cookie có thể gây hại cho máy tính và các phiên truy cập của người dùng. Cookies session: Loại cookie này chỉ tồn tại trong suốt thời gian người dùng ở trên một trang web cụ thể và bị xóa khi đóng trình duyệt. Cookie phiên không thu thập bất kỳ thông tin nào về máy tính và cũng không chứa thông tin nhận dạng cá nhân nào có thể liên kết một phiên với một người dùng cụ thể. Cookie phiên có tính chất tạm thời, khi đóng trình duyệt, máy tính của bạn sẽ tự động xóa tất cả các cookie phiên. Cookie persistent: Loại cookie này còn được biết đến như là một 103 cookie theo dõi của Wap hoặc trong bộ nhớ cookie. Còn gọi là Cookie First-Party (cookie của bên thứ nhất) gần giống với bộ nhớ dài hạn của một trang web. Chúng giúp các trang web ghi nhớ thông tin và cài đặt của người dùng khi họ truy cập lại trong tương lai. Vì thế loại cookie này có thể được sử dụng để theo dõi người dùng. Không giống như cookie phiên, chúng ghi lại thông tin về thói quen duyệt web của người dùng trong toàn bộ thời gian chúng được kích hoạt.

d. Mối đe dọa từ con người

Thường được chia ra thành hai nhóm là các mối đe dọa có chủ ý và các mối đe dọa ngẫu nhiên do con người gây ra:

• Các mối đe dọa ngẫu nhiên do con người gây ra như vô tình đánh mất các thiết bị phần cứng (điện thoại, máy tính xách tay...), vô tình tiết lộ thông tin, vô tình làm hỏng hóc dữ liệu, các lỗi và thiếu sót của người dùng...

• Các mối đe dọa có chủ ý do con người gây ra thường là vấn đề cố ý gian lận và đánh cắp thông tin (Fraud and Theft), cố ý lây lan mã độc và các chương trình độc hại, gây ra các cuộc tấn công như tấn công từ chối dịch vụ (Denial-of-Service Attacks) và cố ý sử dụng các kỹ thuật xã hội khác (Social Engineering) để tấn công vào hệ thống thông tin của tổ chức, doanh nghiệp, làm mất an toàn và bảo mật thông tin.

Ngoài ra, kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi mật khẩu, thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn được một cách hữu hiệu và chỉ có một cách tốt nhất là giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

Câu 2:

Một trong số những nguyên nhân lớn khiến các công ty Công nghệ tài chính (Fintech) và các thiết bị di động (moble devices) càng trở thành mục tiêu của các hacker là do sự phát triển mạnh mẽ của nó đã khiến các chính sách đi cùng để bảo vệ không theo kịp, và chưa chặt chẽ. Cùng với đó, sự thiếu thận trọng của đại đa số công ty, người sử dụng cũng trở thành nguyên nhân lớn cho các cuộc tấn coong cs chủ đích của hacker. Dưới đây là thực trạng sự phát triển của Công nghệ tài chính và các thiết bị di động trong khu vực ASEAN

Khu vực Đông Nam Á được đánh giá là nơi có hoạt động công nghệ tài chính (Fintech), hoạt động thương mại điện tử cũng như các hoạt động thanh toán trên điện thoại di động phát triển nhanh và năng động nhất thế giới. Sự phát triển của công nghệ thông tin trong kỷ nguyên số với nhiều sản phẩm, mô hình, dịch vụ tài chính mới, hiện đại, đặc biệt cùng với lợi thế dân số trẻ và sở thích sử dụng điện thoại thông minh cùng số giờ truy cập Internet cao nhất thế giới khiến khu vực này được dự đoán có nền kinh tế Internet năng động nhất toàn cầu.

Khi việc sử dụng điện thoại di động và Internet tăng lên thì người dùng và các tổ chức liên quan đến sản phẩm, dịch vụ cung cấp trực tuyến cũng phải đối mặt nhiều hơn với các nguy cơ bị tấn công mạng. Trong đó, tội phạm mạng trong lĩnh vực tài chính nổi lên như một thách thức với các cơ quan quản lý, các nhà hoạch định chính sách trong việc đảm bảo an ninh, an toàn các giao dịch tài chính, kiểm soát, phòng ngừa rủi ro và bảo vệ quyền lợi người tiêu dùng. Báo cáo bảo mật X-force 2020 do IBM thực hiện trên cơ sở phân tích và theo dõi hơn 150 tỷ sự kiện bảo mật hàng ngày tại hơn 130 quốc gia trên thế giới cho thấy lĩnh vực tài chính là mục tiêu xếp thứ hai của các nhóm tin tặc (hacker) sau ngành sản xuất và cung cấp năng lượng[1]. Tại Việt Nam, theo BKAV, Covid-19 đã làm gia tăng các cuộc tấn công mạng trong năm 2020 và xu hướng tấn công trong năm 2021 sẽ là các giao dịch trên điện thoại di động.

Mới đây, trong một nghiên cứu về an ninh mạng công bố vào đầu năm 2021, Paypal (*một công ty hoạt động trong lĩnh vực thương mại điện tử*) đã tiến hành khảo sát thực trạng về an toàn, an ninh mạng khu vực công nghệ tài chính tại ASEAN.

Kết quả khảo sát cho thấy, các nước khu vực ASEAN nơi có hệ sinh thái Fintech phát triển như Indonexia, Việt Nam, Singapore… cũng đã nhận thức được những thách thức về bảo đảm an ninh, an toàn mạng đối với khu vực Fintech bởi đây là nơi lưu giữ và xử lý khối lượng lớn thông tin người dùng, liên quan đến khối lượng lớn tài sản của người dân trong khi các quy định về an toàn, bảo mật công nghệ thông tin chưa nghiêm ngặt như đối với hệ thống ngân hàng. Để hệ sinh thái Fintech phát triển bền vững và an toàn, Chính phủ các quốc gia Đông Nam Á, tùy theo điều kiện từng nước, đã có những chính sách và quy định khá đồng bộ đối với khu vực này như xây dựng cơ chế quản lý thử nghiệm có kiểm soát (sandbox) cho hoạt động Fintech, quy định cơ chế đảm bảo an ninh, an toàn mạng, triển khai nhiều chương trình đầu tư, đào tạo, phát triển nguồn nhân lực công nghệ thông tin, ưu tiên ngân sách quốc gia cho các kế hoạch đảm bảo an ninh mạng, tổ chức truyền thông, giáo dục nâng cao kiến thức về tài chính và an ninh mạng,… Tuy nhiên, mức độ triển khai chính sách giữa các nước vẫn còn khoảng cách lớn đòi hỏi có sự phối hợp chặt chẽ và thống nhất hơn ở tầm khu vực.

Câu 3:

a. Các nguy cơ của người dùng trong tình huống là từ những phầm mềm độc hại được tải xuống và mã độc xâm nhập thông qua email. Trong đó có thể bao gồm:
    a. Virus lây nhiễm:
    b. Virus thư điện tử
    c. Sâu máy tính
b. Giải pháp nhằm đảm bảo an toàn cho người sử dụng:
    a. Luôn cập nhật máy tính và phần mềm của
    b. Sử dụng tài khoản không phải là quản trị viên bất cứ khi nào có thể
    c. Suy nghĩ kỹ trước khi nhấp vào các liên kết hoặc tải xuống bất cứ thứ gì
    d. Thận trọng khi mở tệp đính kèm hoặc hình ảnh trong email
    e. Không tin tưởng cửa sổ bật lên yêu cầu tải xuống phần mềm
    f. Hạn chế chia sẻ tệp
    g. Sử dụng phần mềm diệt vi rút

Câu 4:

a. Xác định và giải thích nguy cơ:
Trong tình huống trên, các trường đại học nổi tiếng đã bị các kẻ tấn công đánh cắp những thông tin nhạy cảm của các thành viên trong trường. Như vậy, các trường đại học đã có thể gặp phải những nguy cơ sau:
    1. Mối đe dọa từ các phần mềm: Điều này có thể bắt nguồn từ việc một vài thiết bọ trong hệ thống của trường đại học có bảo mật kém. Và khi kẻ tấn công đánh cắp được thông tin tại một vài thiết bị, chúng có thể mở rộng cuộc tấn công ra dựa vào những thông tin đã bị đánh cắp. Và các trường đại học có thể bị nhiễm các phần mềm sâu máy tính nhằm chiếm dụng các tài nguyên cad phát tán dữ liện lên mạnh
    2. Mối đe dọa đến từ con người.
    Ở đây, có thể một số các kẻ tấn công đã có được thông tin từ thành viên trong mạng nội bộ của các trường đại học do họ bất cẩn tiết lộ thông tin

Và mối đe dọa từ kẻ tấn công, Những đối tượng này có thể đã cố ý lây lan mã độc và các chương trình độc hại. Ngoài ra, kẻ tấn công có thể liên lạc với một người quản trị hệ thống, giả làm một người sử dụng để yêu cầu thay đổi quyền truy nhập của mình đối với hệ thống, hoặc thậm chí thay đổi một số cấu hình của hệ thống để thực hiện các phương pháp tấn công khác.

---Hết---