Nhập môn An Toàn thông tin – Tiến độ giữa kỳ

Lưu ý:
(1) Sinh viên được tham khảo tài liệu, khuyến khích tự soạn trong tập vở.
(2) Thời gian: 60 phút
(3) Hình thức: Tự luận
(4) Các tình huống mang tính minh họa.

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.

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 thông tin 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.

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 giải thích sự ảnh hưởng của an toàn thông tin đối với cá nhân, tổ chức và xã hội.

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.

Ví dụ 1:

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

(1) Chỉ ra 3 mối đe dọa mà bạn A có thể gặp phải trong tình huống trên;
(2) Nêu ra được lý do tại sao có những mối đe dọa đó
(3) Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra
(4) Nêu một vài giải pháp khắc phục

Ví dụ 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:

(1) Chỉ ra 3 mối đe dọa mà bạn có thể gặp phải trong tình huống trên;
(2) Nêu ra được lý do tại sao có những mối đe dọa đó
(3) Phân tích hậu quả nếu các mối đe dọa đó thật sự xảy ra
(4) Nêu một vài 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)

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

Các khái niệm đã học.

Ví dụ:

1. An toàn thông tin là gì? Tại sao một doanh nghiệp cần phải có các biện pháp khác nhau để đảm bảo tính an toàn thông tin của doanh nghiệp?
2. Hệ thống thông tin là gì? Hãy cho ví dụ một hệ thống thông tin mà bạn biết. Đưa ra dữ liệu/thông tin/chức năng nào cần đảm bảo an toàn, nêu lý do
3. Tam giác CIA là gì? Nêu mối tương quan giữa C, I, A
4. Vulnerability (lổ hổng) - Threat (mối nguy/mối đe dọa) - Risk (rủi ro) là gì? Nêu mối tương quan giữa 3 yếu tố đó
5. Tấn công (Attack) an toàn thông tin là gì? Ai có thể trở thành kẻ tấn công (Attacker)?
6. Mã độc (Malware) là gì?. Nêu các loại mã độc? Cho ví dụ về một tình huống bị tấn công

7. Tấn công mật khẩu là gì? Cho ví dụ về một tình huống bị tấn công. Cách phòng chống tấn công mật khẩu?
8. Tấn công backdoor là gì? Cho ví dụ về một tình huống bị tấn công. Cách phòng chống?
9. Tấn công từ chối dịch vụ (DoS, DDoS) là gì? Cho ví dụ về một trường hợp bị tấn công. Cách phòng chống?
10. Tấn công Social Engineering là gì? Cho ví dụ về một tình huống bị tấn công. Cách phòng chống?
11. Mật mã học là gì? Nêu các chức năng của mật mã học? Nêu điểm khác biệt giữa mật mã đối xứng và bất đối xứng.
12. Mật mã bất đối xứng khắc phục những hạn chế gì của mật mã đối xứng?
13. Áp dụng mật mã Caesar để mã hóa bản rõ sau với khóa k = 4
    actions speak louder than words
14. Hãy mã hóa bằng phương pháp Playfair bản mã sau:
    Bản rõ: MATMAHOC
    Khóa: thework
15. So sánh và đánh giá về độ khó khi phá mã đối với các mật mã Ceasar, Monoalphabetic và Vigenère.

LO6- Giải thích một số vấn đề pháp lý liên quan đến an toàn HTTT

Đưa ra một tình huống mang tính thực tiễn liên quan đến việc vi phạm an toàn hệ thống thông tin. Yêu cầu sinh viên chỉ ra điểm vi phạm cụ thể điều khoản nào của luật nào, gợi ý để tránh vi phạm, nêu tình hình chung của tình huống vi phạm này. Ví dụ:

<u>Ví dụ 1:</u>

Để kiếm thêm thu nhập, bạn A đã tự tạo ra một website thương mại điện tử để bán thêm các quần áo, đồ dùng cá nhân, mỹ phẩm, thực phẩm chức năng, v.v. được chị của bạn A xách tay từ Nhật. Bạn A không đăng ký giấy phép kinh doanh cũng như đăng ký website với cơ quan có thẩm quyền. Ngoài ra, các hình ảnh quảng cáo các sản phẩm, bạn A vào các trang web khác lấy về và đăng tải lên trang thương mại điện tử của mình.

(1) Dựa vào các bộ luật bạn đã học, hãy chỉ ra bạn A đã vi phạm khoản nào của điều khoản nào trong bộ luật nào? Trình bày nội dung điều khoản luật đó
(2) Nếu bạn là bạn A thì bạn sẽ phải làm gì để không vi phạm các điều khoản luật mà vẫn đạt được mục tiêu đặt ra.
(3) Bạn hãy cho nhận xét về tình hình chung về việc vi phạm tương tự A ở Việt Nam, đề xuất một số giải pháp để giảm các hành vi vi phạm này.

<u>Ví dụ 2:</u>

Hơn 14.000 điện thoại ở Việt Nam đã bị một công ty tư nhân nghe lén. Các điện thoại này bị theo dõi tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh... Nghiêm trọng hơn, toàn bộ dữ liệu được gửi về máy chủ của công ty này. Kết quả thanh tra đã khiến người sử dụng điện thoại ở Việt Nam cảm thấy lo lắng.
Đoàn thanh tra liên ngành gồm thanh tra Sở Thông tin và Truyền thông Hà Nội, phòng Cảnh sát phòng chống tội phạm sử dụng công nghệ cao - PC50 của Công an Hà Nội đã thanh tra

tại công ty TNHH công nghệ Việt Hồng ở quận Thanh Xuân, Hà Nội và phát hiện công ty này kinh doanh phần mềm Ptracker.
Đây là phần mềm giúp người dùng có thể xem tin nhắn, danh bạ, ghi âm cuộc gọi, định vị điện thoại, quay phim, chụp ảnh, bật - tắt 3G/GPRS của điện thoại bị giám sát. Thậm chí người sử dụng còn có thể ra lệnh điều khiển từ xa điện thoại bị cài Ptracker bằng cách nhắn tin tới điện thoại này.

(1) Dựa vào các bộ luật bạn đã học, hãy chỉ ra công ty trên đã vi phạm khoản nào của điều khoản nào trong bộ luật nào? Trình bày nội dung điều khoản luật đó.
(2) Hãy bạn hiểu như thế nào về điều khoản luật này? Nếu bạn là chủ doanh nghiệp thì bạn sẽ giải quyết định gì về phần mềm này.
(3) Bạn hãy tìm hiểu và trình bày hiện nay có những phần mềm/trang mạng xã hội nào mà thông tin cá nhân người dùng có thể bị sử dụng bất hợp pháp?

<u>Một số tình huống vi phạm pháp luật:</u>

- Mở website thương mại điện tử nhưng không đăng ký website với cơ quan có thẩm quyền.
- Mở website và lấy hình ảnh, thông tin của trang web khác để đăng tải lên trang web của mình.
- Mở website thương mại điện tử nhưng không công bố địa chỉ, thông tin liên lạc của cơ sở kinh doanh.
- Một công ty kinh doanh sản phẩm phần mềm nghe lén, theo dõi tin nhắn, thu thập thông tin riêng tư của người dùng.
- Một sinh viên CNTT thực hiện tấn công vào một trang web để thu thập, sao chép thông tin nhạy cảm và đăng tải trên các diễn đàn để công bố chiến tích của mình.
- Một website thu thập thông tin cá nhân của người dùng và bán cho các bên quảng cáo, các trung tâm, cơ sở kinh doanh khác.
- Một người chụp ảnh người bệnh trong bệnh viện và đăng tải lên mạng xã hội.
- Một người livestream một bộ phim đang công chiếu lên mạng xã hội.