Đề cương chi tiết
Bộ môn: An toàn thông tin
Phần I: 10 câu
By Phan Kid

Mục lục

Lưu ý trước khi đọc

- Đây là những câu trả lời t tự soạn thảo dựa trên bài giảng của thầy và tìm hiểu trên mạng.
- Những chỗ nào chữ màu nâu là những phần thuộc về cá nhân t, mang tính chất kết hợp trên mạng và tổng hợp kiến thức bản thân nên độ tin cậy có thể không cao. Các bạn đọc những phần này tham khảo để tự tìm ra cho mình một cách trả lời khác chính xác và hợp lý hơn.
- Một số chỗ một vài từ ngữ được **bôi đen**, nó có ý nghĩa đánh dấu sự khác biệt, trong những câu hỏi so sánh.
- Các câu trả lời này nếu có vấn đề, sai sót, thiếu sót gì, xin vui lòng liên hệ qua FB hoặc qua sđt **0167 5894 643** , để t kịp thời chỉnh sửa, xin cảm ơn.
- Chân thành cảm ơn mọi ý kiến đóng góp của các bạn ☺

Chúc các bạn ôn bài tốt !

Câu 1: Khác nhau giữa các nhóm chính sách: mức 1, mức 2, mức 3. Đưa ra một chính sách mức 1 an toàn bảo mật hệ thống thông tin theo một mô hình công ty.

- Định nghĩa: Chính sách là phát biểu mức cao của niềm tin, mục tiêu, đối tượng của công ty và nghĩa chung cho mục tiêu cần đạt được trong một lĩnh vực.
- ***Chính sách chia làm 3 nhóm: Chung (mức 1), Hướng đến chủ đề (mức 2), Hướng ứng dụng (mức 3)***

Mức 1	Mức 2	Mức 3
- Dùng để tạo nên **tầm nhìn chung** và **định hướng** .	- Đề cập đến các mục tiêu **riêng biệt** quan tâm	- Tập trung trên các quyết định được áp dụng bởi **người quản lý** để điều khiển các **ứng dụng riêng biệt**.

- ***VD chính sách mức 1 an toàn bảo mật hệ thống thông tin theo một mô hình công ty:***

Chính sách về quyền riêng tư: Nhân viên công ty có quyền bảo mật thông tin riêng tư, cá nhân, người quản lý thông tin sẽ không được tùy tiện tiết lộ thông tin của nhân viên hay tiết lộ tài khoản quản lý thông tin nhân viên của bản thân. Mỗi nhân viên khi truy cập hệ thống sẽ được giới hạn một phạm vi thông tin nào đó mà không được cung cấp đầy đủ hoàn toàn những thông tin nằm trong phần bảo mật (đã được điều chỉnh bởi người quản lý cấp cao hoặc người có thẩm quyền, trách nhiệm)

Vấn đề mà chính sách này đề cập đến là phạm vi chính sách quan tâm: "Quyền riêng tư của nhân viên"

Giới hạn người có ảnh hưởng bởi chính sách là nhân viên công ty

Giới hạn đối tượng điều chỉnh của chính sách là những người quản lý cấp cao của công ty.

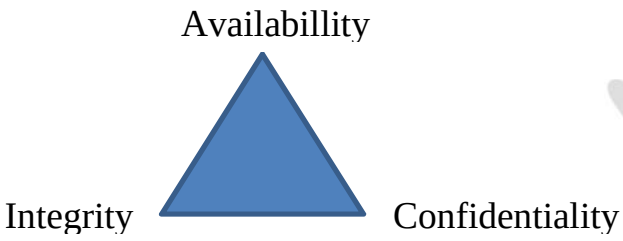
Trách nhiệm của các cá nhân là không cố tình tìm cách truy cập thông tin bất hợp pháp hay phá hoại các thông tin riêng tư

Và áp dụng các hình thức xử phạt hợp lý với những trường hợp vi phạm.

Câu 2: Mục tiêu của an toàn bảo mật thông tin. Đưa ra các ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin.

- ***Mục tiêu của an toàn bảo mật thông tin: Bảo vệ tài nguyên của tổ chức, đảm bảo thực hiện tốt nhất nhiệm vụ.***

  3 mục tiêu chính



Availabillity: Tính sẵn sàng

Đáp ứng khi có yêu cầu, tuy nhiên thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn => thảm họa tấn công từ bên ngoài.

Integrity: Tính toàn vẹn

Cung cấp đúng thông tin, cung cấp thông tin chính xác.

Confidentiality: Tính cẩn mật (tin cậy)

Đảm bảo tính bí mật của thông tin. Thông tin chỉ được truy cập bởi người được phép.

- ***Đưa ra các ví dụ việc đảm bảo các mục tiêu của an toàn và bảo mật thông tin:***

  + **Availabillity**: Máy của hacker sẽ gửi hàng loạt các gói tin có các MAC nguồn giả tạo đến switch làm bộ nhớ lưu trữ MAC address table của switch nhanh chóng bị đầy khiến switch không thể hoạt động bình thường được nữa. Đây cũng thuộc hình thức tấn công từ chối dịch vụ (DoS). Để tăng khả năng chống trọi với các cuộc tấn công cũng như duy trì độ sẵn sàng của hệ thống ta có thể áp dụng một số kỹ thuật như: Load Balancing, Clustering, Redudancy, Failover…

  + **Integrity:** Giải pháp "data integrity" có thể bao gồm thêm việc xác thực nguồn gốc của thông tin này (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy và ta gọi đó là tính "authenticity" của thông tin.

  + **Confidentiality:** Tính bí mật của thông tin có thể đạt được bằng cách giới hạn truy cập về cả mặt vật lý, ví dụ như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó hoặc logic, ví dụ như truy cập thông tin đó từ xa qua môi trường mạng. Sau đây là một số cách thức như vậy:

    - Khóa kín và niêm phong thiết bị.
    - Yêu cầu đối tượng cung cấp credential, ví dụ, cặp username + password hay đặc điểm về sinh trắc để xác thực.
    - Sử dụng firewall hoặc ACL trên router để ngăn chặn truy cập trái phép.
    - Mã hóa thông tin sử dụng các giao thức và thuật toán mạnh như SSL/TLS, AES, v.v..

Câu 3: Ý nghĩa phân lớp tài sản. Ví dụ minh họa phân lớp tài sản thông tin.

- ***Ý nghĩa:***

  + Đảm bảo cho các tài sản được phân lớp đúng theo giá trị
  + Cơ sở cho các chính sách đảm bảo trên các phân lớp
  + Đảm bảo trách nhiệm, và thực thi trách nhiệm quản lý tài sản của người quản lý
  + Đưa ra phân lớp riêng theo đặc thù

- ***Ví dụ minh họa phân lớp tài sản thông tin:***

  + Bí mật:
    - Hồ sơ bảo hiểm y tế (kể cả hồ sơ y tế, kê đơn và tâm lý)
    - Kế hoạch hoạt động cụ thể, kế hoạch tiếp thị
    - Doanh thu, chi phí, lợi nhuận hoặc các kết quả tài chính khác không được công khai
    - Hồ sơ cán bộ, thông tin khách hàng
    - Chiến lược kinh doanh
    - Những thay đổi lớn trong cơ cấu quản lý công ty
    - Những thông tin đòi hỏi kỹ năng hoặc đào tạo đặc biệt
  + Nội bộ:
    - Thông tin hoạt động kinh doanh/báo cáo
    - Danh sách điện thoại công ty
    - Chính sách, tiêu chuẩn, thủ tục
    - Thông báo nội bộ
  + Công khai:
    - Báo cáo thường niên
    - Bản tinh dịch vụ công cộng, tài liệu quảng cáo tiếp thị

Câu 4: Ý nghĩa điều khiển truy xuất, các vấn đề trong quản lý truy xuất người dùng.

- ***Ý nghĩa:***

  + Đảm bảo việc truy xuất đến tài nguyên của hệ thống
  + Đảm bảo quá trình triển khai cho hệ thống của các chính sách ở trên
  + Sử dụng các cơ chế về mặt kỹ thuật, con người để đảm bảo các cơ chế đã được mô tả
  + Đưa ra nhân tố chính trong thực thi các chính sách đã mô tả

- ***Các vấn đề trong quản lý truy xuất người dùng:***

  + Đảm bảo tính đồng nhất hệ thống
    - Triển khai hệ thống phần mềm, hệ điều hành đồng nhất tránh dị biệt
    - Kiểm soát được các ứng dụng cài đặt và sử dụng
  + Quy trình thay đổi truy xuất với hệ thống
    - Nếu có sự thay đổi của hệ thống thì cần phải được thay đổi và kiểm nghiệm
    - Kiểm tra sự thay đổi này và yêu cầu điều khiển thay đổi
    - Thử nghiệm phần mềm được thiết kế
    - Lặp lại đến khi chất lượng chấp nhận được
    - Thực hiện, mã, hệ thống, cá nhân thay đổi được thực hiện
    - Cập nhật thông tin phiên bản. Sau khi các thay đổi được thực hiện, các văn bản phải được thay đổi
    - Báo cáo thay đổi đối với người quản lý.
  + Các vấn đề về điều khiển
    - Thực hiện điều khiển trên hệ điều hành
    - Thực hiện điều khiển trên hệ thống mạng
    - Thực hiện điều khiển trên hệ thống phần mềm
    - Thực hiện điều khiển trên hệ thống vật lý
  + Các nghiệp vụ chú ý
    - Ghi nhật ký
    - Phát hiện xâm nhập

Câu 5: Ý nghĩa bảo mật vật lý, ví dụ chính sách bảo mật vật lý

- ***Ý nghĩa:***

  + Bảo vệ hệ thống trước đe dọa vật lý

  + Phòng ngừa để bảo vệ việc truy xuất thiết bị toàn bộ tổ chức

  + Đảm bảo không có sự hư hỏng và thay đổi các thiết bị mà thông tin được lưu trữ

  + Việc xây dựng bảo vệ vật lý cho trung tâm dữ liệu phải tương ứng với giá trị dư liệu được lưu trữ trong đó.

- ***Ví dụ chính sách bảo mật vật lý***

  + Các máy chủ, các thiết bị truyền thông: Router, moderm, firewall phải được đặt trong phòng máy riêng được bảo vệ tốt kể cả yêu cầu về nhiệt độ, độ ẩm theo đúng khuyến cáo của sản phẩm

  + Đảm bảo nguồn điện luôn được cung cấp

  + Hệ thống UPS cung cấp nguồn khi mất điện lưới trong thời gian ngắn và làm nhiệm vụ chuyển tiếp sang hệ thống máy phát điện dự phòng

  + Giám sát môi trường theo các chỉ số nhiệt độ, độ ẩm, bụi và những mối đe dọa môi trường vật lý khác

  + Lựa chọn cấp nguồn qua Ethernet giảm việc phải đi cáp tới các thiết bị chuyên dụng

  + Các dạng cảnh báo khác nhau cho phép gửi thông báo qua quản trị SNMP, các hệ thống mail, máy chủ web, điện thoại,…

  + Kiểm soát vào ra phòng máy chủ, kiểm soát truy cập hệ thống bằng công nghệ thông minh như camera giám sát, camera hồng ngoại, cảm biến,.v…

  + Chỉ có những người thuộc nhóm quản trị hệ thống hoặc người trực ca mới được phép vào và thao tác trên các máy chủ trong phòng máy. Các cá nhân khác chỉ được vào phòng máy khi được cho phép bởi người quản trị hệ thống hoặc người trực phòng máy.

Câu 6: Ý nghĩa của phân tích nguy cơ, tiến trình phân tích quản lý nguy cơ

- Khái niệm Nguy cơ: là khả năng bất lợi có thể xảy ra cho hệ thống
- ***Ý nghĩa:***

  + Phân tích được các nguy cơ, mức độ ưu tiên của các nguy cơ, từ đó đánh giá, đưa ra các xử lý tương ứng.

  + Không có mục đích loại bỏ tất cả các nguy cơ mà nhằm mục đích giảm nguy cơ đến mức tối thiểu có thể được.
- ***Tiến trình phân tích, quản lý nguy cơ***

  + Phân tích:
    - Xác định nguy cơ
    - Ước định khả năng xảy ra
    - Đưa ra những bước để giảm nguy cơ đến mức cho phép được

  + Quản lý:
    - Xác định tài sản cần được xem xét
    - Xác định các đe dọa xảy ra
    - Sắp xếp các đe dọa
    - Xác định các điều khiển, bảo vệ tương ứng

  Quá trình này được thực hiện lặp lại theo thời gian (tài sản, đe dọa, ưu tiên, giải pháp đã bị thay đổi)

Câu 7: Ý nghĩa kế hoạch công việc liên tục, sự liên quan của quá trình phân tích tác động công việc và các bước.

- ***Ý nghĩa:***

  + Đảm bảo công việc hoạt động trong các tình huống
  + Bao gồm cả kế hoạch phục hồi sự cố
  + Có tác dụng trong tình huống khẩn cấp
    - Khó kiểm tra
    - Khó thuyết phục người quản lý
    - Bảo hiểm chỉ giải quyết về mặt kinh tế
- ***Sự liên quan của quá trình phân tích tác động công việc: có nhiều yếu tố ảnh hưởng đến hoạt động***
    - Thảm họa tự nhiên: Lũ lụt, động đất, hỏa hoạn,v…
    - Tai nạn
    - Cạnh tranh, tấn công đối thủ
    - Năng lượng không được cung cấp
    - Các dịch vụ: kết nối, vận chuyển, bảo vệ không hoạt động
    - Thảm họa về môi trường
    - Tấn công của hacker
- ***Các bước tiến hành:***

  + Xác định các tài nguyên
  + Xác định các đe dọa
  + Xác định các nguy cơ
  + Xác định ảnh hưởng đến hệ thống
  + Xác định các dịch vụ và hệ thống cần được khôi phục ngay
  + Xác định tài nguyên để hồi phục hệ thống

Câu 8: Nêu lý do vì sao phải thiết lập chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin trong doanh nghiệp.

- Các vấn đề của an toàn và bảo mật xảy ra trong suốt quá trình hình thành, phát triển, tồn tại của hệ thống. Trong chuỗi mắt xích bảo vệ, sức mạnh chuỗi bảo vệ chính là điểm yếu nhất của nó.
- Bảo vệ dữ liệu: hiện nay các biện pháp tấn công ngày càng tinh vi, sự đe dọa tới độ an toàn thông tin có thể đến từ nhiều nơi theo nghiều cách, vì thế chúng ta nên đưa ra các chính sách và chỉ dẫn đề phòng cần thiết.
- Bảo vệ các tài nguyên sử dụng trên mạng: Sau khi làm chủ được hệ thống bên trong, kẻ tấn công có thể sự dụng các máy này để phục vụ cho mục đích của mình như dò mật khẩu người sử dụng, sử dụng liên kết mạng sẵn có để tiếp tục tấn công hệ thống khác.
- Bảo vệ danh tiếng doanh nghiệp, cơ quan: Trong trường hợp người quản trị hệ thống chỉ được biến đến sau khi chính hệ thống của mình được dùng làm bàn đạp để tấn công các hệ thống khác, thì sẽ để lại tổn thất về uy tín và hậu quả lâu dài.
- Chính sách, tiêu chuẩn, chỉ dẫn về an toàn và đảm bảo thông tin sẽ hướng dẫn giải quyết các vấn đề liên quan đến con người:
  + Cơ sở để xem xét các hành động của con người để đánh giá
  + Kết hợp với các giải pháp kỹ thuật quản lý toàn bộ hệ thống
  + Nền tảng cho việc triển khai chương trình an toàn vào bảo mật hệ thống thông tin.

    ⇨ Nhìn chung cuối cùng là tránh tổn thất cho các doanh nghiệp về mặt dữ liệu, tài nguyên, danh tiếng, uy tín,..v..v..

Câu 9: Khác nhau giữa chính sách, tiêu chuẩn, chỉ dẫn. Đưa ra ví dụ minh chứng

Chính sách	Tiêu chuẩn	Chỉ dẫn
Một chính sách là phát biểu mức cao của **niềm tin**, **mục tiêu**, **đối tượng** của công ty và **nghĩa chung** cho mục tiêu cần đạt được trong **một lĩnh vực**.	Là yêu cầu **bắt buộc** để **hỗ trợ** các **chính sách riêng lẻ**	Chỉ dẫn là **sự cần thiết**, từng bước, hành động **chi tiết hóa**, yêu cầu phải thực hiện để hoàn thành **một công việc.**
VD: Chính sách bảo mật cá nhân. Tất cả mật khẩu nên được đặt theo đúng chỉ dẫn cách thức đặt mật khẩu an toàn. Các công việc khác nhau phải có những mật khẩu khác nhau. Chẳng hạn mật khẩu truy cập mạng và mật khẩu cho thư điện tử phải khác nhau.	VD: Mật khẩu truy cập ở mạng nội bộ phải được thay đổi ở lần truy nhập đầu tiên kể từ sau khi người quản trị tạo lập tài khoản truy nhập. Phải thay đổi định kỳ theo cảnh báo của hệ thống. Định kỳ thay đổi được quy định bởi người quản trị.	VD: Chỉ dẫn đặt mật khẩu an toàn: Chọn mật khẩu gồm cả chữ hoa, chữ thường (a-z, A-Z), chữ số, ký tự đặc biệt,v… Mật khẩu phải có độ dài tối thiểu 8 ký tự, mật khẩu không phải là 1 từ, không dựa trên thông tin cá nhân.

Câu 10: Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống ? Vòng đời của bảo mật thông tin.

- ***Sự tương ứng của phân tích nguy cơ và quá trình phát triển hệ thống:***

  + Phân tích nguy cơ chính thức cung cấp các tài liệu thẩm định hệ thống, cho phép doanh nghiệp kiểm soát vận mệnh của riêng mình.

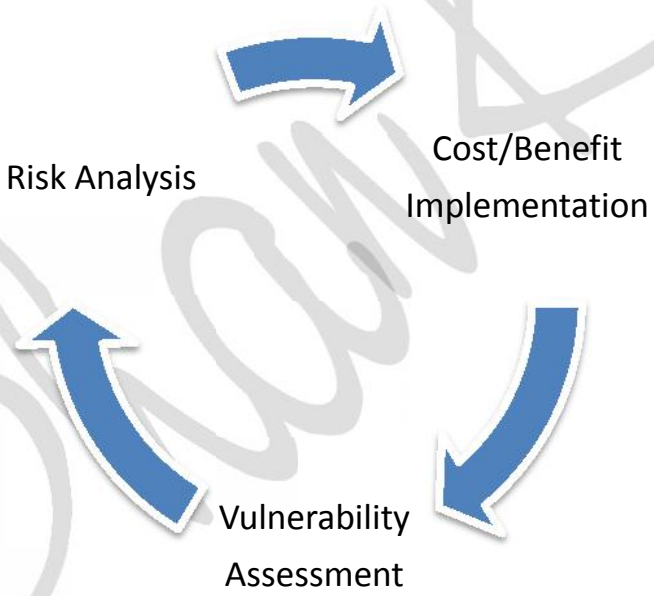
  + Không ai biết hệ thống rõ hơn những người phát triển và chạy chúng, vậy nên, để phân tích nguy cơ, cũng là công việc của chính những người phát triển hệ thống.

  + Phân tích nguy cơ có thể được sử dụng để xem xét lại bất cứ nhiệm vụ, dự án hoặc ý tưởng trong quá trình phát triển hệ thống.

  + Lợi ích lớn nhất của phân tích nguy cơ là xác định có hay không vấn đề để tiến hành tùy trình kế hoạch phát triển hệ thống

  + Quá trình phát triển hệ thống có xảy ra lỗ hổng hay lỗi gì hay không là do có được phân tích đầy đủ các nguy cơ hay không.

- ***Vòng đời của bảo mật thông tin***



Cost/Benefit Implementation: chi phí, lợi ích thực hiện
Vulnerability Assessment: đánh giá tổn thương, nguy hại
Risk Analysis: phân tích nguy cơ

+ Thông thường, kết quả phân tích nguy cơ sẽ được sử dụng trên 2 lần:

- Khi một quyết định cần phải được thực hiện
- Khi có phát sinh và cần phải kiểm tra quá trình ra quyết định