**ĐỀ CƯƠNG ĐẢM BẢO AN TOÀN THÔNG TIN**

**PHẦN I:**

**Câu hỏi 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**

Khác nhau

Mức 1: dùng để tạo nên tầm nhìn chung và định hướng

+ Chủ đề : vấn đề mà chính sách đề cập đến, phạm vi chính sách quan tâm

+ Giới hạn : giới hạn người có ảnh hưởng bởi chính sách và đối tượng có điều chỉnh của chính sách.

+ Trách nhiệm: trách nhiệm cá nhân

+ Sự tuân thủ hoặc những kết quả xấu : hình thức xử phạt khi không tuân thủ

Mức 2: đề cập đến các mục tiêu riêng biệt và quan tâm

+ Chủ đề : tập chung đến vấn đề liên quan và quan tâm hiện tại

+ Thay đổi theo thời gian , sự thay đổi công nghệ và các nhân tố khác

Mức 3: tập chung trên các quyết định được áp dụng bởi người để điều khiển các úng dụng riêng biệt

+ Chính sách mức 3 là chính sách ở mức ứng dụng. chính sách này không có mô hình chặt chẽ như mức 1, 2.

+ Ở chính sách này phải hiểu được nhiệm vụ mục tiêu toàn cục của công ty, hiểu được nhiệm vụ chương trình của hệ thống. thiết lập các yêu cầu hổ trợ hai mục tiêu.

Ví dụ về chính sách mức 1 : giới hạn người có ảnh hưởng bởi chính sách và đối tượng có điều chỉnh của chính sách. Hầu hết các công ty đều cung cấp nhiều đặc quyền cho người dùng hơn so với cần thiết. Giám sát truy cập dữ liệu cực kỳ quan trọng của người dùng và theo dõi truy cập không xác định với dữ liệu ở mức nguy hiểm cao là những bước không thể thiếu.

Tạo quy định truy cập nhằm giới hạn đặc quyền mạng của người dùng một cách chặt chẽ. Chỉ cho phép truy cập lớp dữ liệu tương ứng cần thiết cho công việc của từng kiểu người dùng, đồng thời thiết lập các điều khiển nhằm bắt buộc nhân viên trong công ty phải tuân thủ quy định nội bộ đã xây dựng. Ví dụ, đưa ra cảnh báo khi ai đó vốn bình thường chỉ làm việc với 10 tập tài liệu mỗi ngày, đột nhiên bắt đầu truy cập số với lượng lớn hơn. Việc đưa ra quyết định điều khiển truy cập cho thành viên nội bộ và người ngoài là khá đơn giản mà hiệu quả.

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

Mục tiêu của an toàn bảo mật hệ thống thông tin:

\* 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 như tiếp cận trực tiếp tới thiết bị lưu trữ thông tin đó…) và logic (ví dụ, truy cập thông tin đó từ xa qua môi trường mạng…) hoặc mã hóa thông tin trước khi truyền nó đi qua 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 phương thức (như SSL/TSL…) và thuật toán (như AES, DES…) mạnh.

\* Tính toàn vẹn

- Đảm bảo tính toàn vẹn của thông tin, tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi (về điểm này, nhiều người thường hay nghĩ tính “integrity” đơn giản chỉ là đảm bảo thông tin không bị thay đổi (modify) là chưa chuẩn xác).

- Ngoài ra, một 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.

- Sau đây là một số trường hợp tính “integrity” của thông tin bị phá vỡ:

• Thay đổi giao diện trang chủ của một website (hay còn gọi là deface website).

• Chặn đứng và thay đổi gói tin được gửi qua mạng.

• Chỉnh sửa trái phép các file được lưu trữ trên máy tính.

• Do có sự cố trên đường truyền mà tín hiệu bị nhiễu hoặc suy hao dẫn đến thông tin bị sai lệch.

\* 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, nếu một server chỉ bị ngưng hoạt động hay ngừng cung cấp dịch vụ trong vòng 5 phút trên một năm thì độ sẵn sàng của nó là 99,999%.

- Ví dụ dưới đây cho thấy hacker có thể cản trở tính sẵn sàng của hệ thống như thế nào:

• 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…

Như vậy, vấn đề bảo mật thông tin không chỉ đơn thuần là việc chống lại các cuộc tấn công từ hacker, ngăn chặn malware để đảm bảo thông tin không bị phá hủy hoặc bị tiết lộ ra ngoài… Hiểu rõ 3 mục tiêu của bảo mật ở trên là bước căn bản đầu tiên trong quá trình xây dựng một hệ thống thông tin an toàn nhất có thể. Ba mục tiêu này còn được gọi là tam giác bảo mật C-I-A

Ví dụ việc đảm bảo các mục tiêu đảm bảo an toàn thông tin

Tính bảo mật \*

Các hệ thống thông tin đều được bảo mật. Bất kì người nào muốn xem hoặc tác động lên thông tin đều phải qua một bước là đăng nhập tài khoản cá nhân đề phân quyền hạn người dung, mức độ tác động đến thông tin. Chẳng hạn trên trang web [www.mta.edu.vn](http://www.mta.edu.vn) -> sinhvien -> đăng nhập. Sinh viên chỉ được quyền xem kết quả học tập và đăng kí tín chỉ, không có quyền thay đổi điểm và quá trình học tập. Nó nói lên tính cẩn mật của thông tin.

**Câu hỏi 3:** **ý nghĩa của phân lớp tài sản ? Ví dụ minh họa phân lớp tài sản thông tin.**

Trả lời: ý nghĩa của phân lớp tài sản:

\* đảm bảo các tài sản được phân lớp theo đúng giá trị

\* cơ sở cho các chính sách đảm bảo trên các phân lớp

- tiến trình quyết định công việc

\* trách nhiệm và thực thi trách nhiệm quản lí tài sản của người quản lí

\* vấn đề liên quan

+ nhiệm vụ quan trọng ,hành động nhạy cảm

+ nơi nào là nhiệm vụ quan trọng và thông tin nhạy cảm được lưu trữ

+ nơi mà những thông tin nhạy cảm này được xử lý

+ người nào là cần thiết truy xuất thông tin này

\* tiến hành tại mỗi đơn vị, nơi quản lí thông tin

\* đưa raphaan lớp riêng đặc thù

\* không nên tạo quá nhiều phân lớp

\* một số vấn đè liên quan :

+luật bản quyền

+luật sang chế

+luật thương hiệu

\*Một số thành phần trong phân lớp tài sản

Người sở hữu

1. Xác định phân lớp tài sản thông tin trong đơn vị mình
2. Xác định và thực hiện các bảo vệ tích ứng để đảm bảo tính mật,tính toàn vẹn,tính khả dụng của tài nguyên thông tin
3. Quản lí việc bảo vệ an toàn để đảm bảo sự tuân thủ và thông báo trạng thái không tuân thủ
4. Xác thực việc truy xuất ai có công việc liên quan
5. Loại bỏ quyền truy xuất với những người không còn có công việc liên quan

\*Một số thành phần trong phân lớp tài sản

Người bảo vệ

+ không có quyền ,thay đổi ,cho phép sử dụng thông tin nếu không có sự cấp phép người chủ sở hữu

+ trông coi ,thực hiện việc bảo vệ cần thiết theo yêu cầu

Người sử dụng

+ người được cấp quyền truy xuất

+ thực hiện đúng theo quyền cho phép

+ chỉ được cấp quyền theo nguyên tắc tối thiểu

+ Tuân thủ những điều khiển mà người sở hữu quy định

\*\* Ví dụ về phân lớp thông tin

* Top secret – tối mật:
* Confidential – mật:
* Restricted – giới hạn:
* Internal Use – sử dụng nội bộ :
* Public – công khai:
* Company Confidential Red – thông tin mật màu đỏ:
* Company Confidential Yellow – thông tin mật màu vàng
* Company Confidential Green – thông tin mật màu xanh:
* Company Public – thông tin công khai:

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

a, Ý nghĩa điều khiển truy xuất:

* Giải quyết các vấn đề liên quan tới con người.
* Cơ sở để xem xét giải quyết các anhhf động của con người để đánh giá.
* Kết hợp với các giải pháp để quản lý hệ thống.
* Nền tảng cho việc hát triển và triển khai chương trình an toàn và bảo mật an toàn thông tin.

b, Các vấn đề trong quản lý truy xuất người dùng:

* Cơ chế quản lý:
* Quản lý truy xuất theo chính sách

+ Quản lý theo mô hình dán nhãn

+ Các bảo vệ theo nhóm đã phân

* Quản lý tùy biến

+ Tuân theo mô hình dữ liệu miêu tả

+ hạn chế mô hình cấp điều khiển tùy biến.

* Quy trình quản lý:

1, Cấp phép tài khoản

* Kiểm tra người dùng đăng kí tài khoản
* Cung cấp truy vấn đầu tiên với hệ thống

2, Quản lý quyền ưu tiên truy xuất

* Đảm bảo kiểm tra các ưu tiên theo thời gian với ngườ dùng
* Đảm bảo sự tồn tài người dùng với thực tế
* Có cơ chế loại bỏ quyền nhanh chóng với các cá nhân

3, Quản lý xác thực tài khoản

* Mật khẩu thay đổi theo tiêu chuẩn công nghiệp, 30 ngày
* Thời gian thay đổi mật khẩu thể hiện sự cần thiết bảo mật của thông tin trong hệ thống
* Mật khẩu phải được lựa chọn tốt: ít nhất có 8 kí tự, không sử dụng các kí tự trong từ điển, và có ký tự đặc biệt
* Hỗ trợ đăng nhập một lần (single – sign - on).
* Cơ chế xác thực

+ những vấn đề người đó có

* Thẻ thông minh
* Thẻ từ
* Thẻ phần cứng
* Thẻ phần mềm

+ Người dùng là ai

* Vân tay
* Sơ đồ võng mạc
* Hình học tay
* Vân gan bàn tay
* Cơ chế xác thực

+ Người dùng biết:

* Mật khẩu
* Số pin (số xác định nhười dùng)
* Mệnh đề phát biểu
* Thông báo chính xác nhưng giới hạn và quyền , nghĩa vụ tham gia hệ thống
* Kiểm soát thao tác
* Kiểm soát thông tin người dùng

**Câu hỏi 5: Ý nghĩa bảo mật vật lý**

Ý nghĩa của bảo mật vật lý là :

Sử dụng các phương pháp bảo mật vật lí trước các đe dọa vật lí vào hệ thống

* Hệ thống canh phòng
* Hệ thống quan sát
* Hệ thống báo cháy
* Hệ thống báo đột nhập
* Hệ thống hủy tài liệu

Chính sách bảo mật vật lí :

Chính sách trách nhiệm của người quản lí cung cấp an toàn và bảo mật vật lí làm việc cho mọi nhân viên.

Tiêu chuẩn:

Các văn phòng công ty sẽ được bảo vệ bằng truy xuất không được phép

Khu vực quan trọng chứa thông tin , thiết bị.Hệ thống thiết bị là quan trọng với bảo mật công ty sẽ được xác định thông qua thiết bị phân tích tác động của công việc và sẽ đc bảo vệ tránh lỗi nguồn

Trách nhiệm :

Người quản lí cao cấp và nhân viên văn phòng công ty yêu cầu duy trì tài liệu toàn vẹn để thiết kế điều khiển nội bộ bảo đảm an toàn tài sản chống lại sự phá hủy bất hợp pháp.

Các tài sản của công ty bao gồm

* Của cải vật lí : máy móc,thiết bị …
* Của cải trí tuệ : các phát minh , bí mật thương mại ,…
* Các chú ý thương mại : tài sản khác …

Trách nhiệm của hệ thống quản lí nhân viên quan tâm thực hiện đúng chỉ dẫn về bảo mật và các vấn đề lien quan

Tuân thủ:

người quản lí có trách nhiệm tổ chức khóa định kì là để tuân thủ các chính sách ,chỉ dẫn ,thực hiện ,tiêu chuẩn

Các nhân viên không tuân thủ với chính sách sẽ bị coi là vi phạm và bị xử phạt tương ứng.

**Câu hỏi 6: Ý nghĩa của phân tích nguy cơ**

Ý nghĩa của phân tích nguy cơ :

Quản lý nguy cơ là tiến trình cho phép người quản lí doanh nghiệp cân bằng giữa thực thi ,chi phí của bảo vệ và kết quả giành được không những

Phân tích nguy cơ giúp công ty chủ động hơn trong việc điều khiển những vấn đề lien quan đến vận mệnh của công ty đó

Tiến trình phân tích nguy cơ được thực hiện với các điều kiện bảo vệ khác sẽ được thực hiện

Công ty sẽ phải tuân thủ và yêu cầu kiểm tra những điều kiện sau khi phân tích nguy cơ.

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

**Khái niệm kế hoạch công việc liên tục:**

Kế hoạch liên tục kinh doanh (Business Continuity Plan) là một bản kế hoạch hậu cần thực tiễn được xây dựng, triển khai nhằm giúp các doanh nghiệp có thể phục hồi hoạt động sau khi bị gián đoạn một phần hoặc toàn bộ hoạt động sau khi một tai họa bất ngờ ập đến.

**Ý Nghĩa:**

Nếu được xây dựng hiệu quả, bản kế hoạch này sẽ giúp các công ty có thể :  
- Hạn chế được tối đa các hậu quả mà tai họa mang đến cho công ty cũng như cho khách hàng.  
- Khả năng trở lại hoạt động trong thời gian sớm nhất có thể nếu gặp rủi ro dừng hoạt động.  
- Trấn an và đáp ứng được yêu cầu về thông tin của khách hàng cũng như các đối tác.

**Sự liên quan của quá trình phân tích tác động công việc với các bước khác:**

**-** Quá trình phân tích tác động công việc. Trong giai đoạn này, từ việc đánh giá, xem xét tất cả tài sản quan trọng và các quy trình then chốt của doanh nghiệp mình, nhà quản trị phải xác định được những nguy cơ, tai họa có thể xảy đến với doanh nghiệp cũng như mức độ hậu quả mà nó mang đến. Sau đó, họ có thể hoạch định trước một số kịch bản thảm họa chính sẽ xảy ra và có kế hoạch ứng phó. Khi đề ra các giải pháp ứng phó như vậy phải tính đến vấn đề chi phí để thực hiện chúng, như vậy mới xác định được rõ quy mô của kế hoạch phù hợp với nhu cầu cũng như nguồn lực của công ty. Kế hoạch sau khi được xây dựng hoàn chỉnh thì phải được phổ biến, tuyên truyền cho toàn thể nhân viên để nâng cao nhận thức cảnh giác, và quan trọng là cần thường xuyên thực hiện việc bảo trì, tiến hành diễn tập, test kiểm tra khả năng hoạt động của những giải pháp dự phòng đó. Cuối cùng là đánh giá, kiểm soát định kì nhằm phát hiện thêm những rủi ro mới để chỉnh sửa, cập nhật bản kế hoạch BCP của doanh nghiệp mình.

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

Chính sách:

An ninh thông tin là một vấn đề kinh doanh , không chỉ là một vấn đề công nghệ . Lý do các tổ chức muốn bảo vệ thông tin do mục đích kinh doanh. Kiến thức của công ty và dữ liệu được cho là tài sản quan trọng nhất của bất kỳ tổ chức nào. Tổng công ty phải đảm bảo bí mật , toàn vẹn và sẵn sàng của dữ liệu của họ . Ba mục tiêu của chính sách là trả lời câu hỏi : "Ai thấy dữ liệu ", " Có dữ liệu bị hỏng ? " và "Tôi có thể truy cập vào máy chủ hoặc dữ liệu khi tôi cần nó? "

Tiêu chuẩn:

* Việc áp dụng một tiêu chuẩn hệ thống quản lý an toàn thông tin sẽ giúp các tổ chức/doanh nghiệp ngăn ngừa, hạn chế các tổn thất trong sản xuất, kinh doanh liên quan tới việc hư hỏng, mất mát các thông tin, dữ liệu quan trọng.
* Chứng tỏ sự cam kết đảm bảo sự an toàn về thông tin ở mọi mức độ thống nhất hành động của nhân viên và người quản lý trong việc bảo đảm an toàn thông tin.
* Đảm bảo tính sẵn sàng và tin cậy của phần cứng và các cơ sở dữ liệu.
* Bảo mật thông tin, tạo niềm tin cho đối tác, khách hàng.
* Nâng cao nhận thức và trách nhiệm của nhân viên về an ninh thông tin.

**Chỉ dẫn:**

* Nó là cần thiết như các nguyên tắc cơ bản việc xây dựng các chính sách cơ bản nên biện pháp đối phó để đảm bảo an ninh thông tin của hệ thống thông tin của các bộ và cơ quan.
* Chỉ dẫn các công việc cần làm khi có sự cố xảy ra.

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

**-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 quy định chủ đề (phạm vi mà chính sách quan tâm), giới hạn người chịu ảnh hưởng của chính sách và các đối tượng điều chỉnh của chính sách. Chính sách quy định trách nhiệm của từng cá nhân, tập thể,….và hình thức xử phạt nếu vi phạm chính sách.

Một số chính sách tiêu biểu:

+ Phân lớp tài sản

+ Quản lý tài liệu

+ Điều khiển truy xuất

+ Bảo mật vật lý

+ Công việc liên tục

Ví dụ:

Chính sách quản lý tài liệu thực hiện trên các giai đoạn lưu trữ, xử lý, hủy tài liệu. Đồng thời phân rõ **trách nhiệm** của các nhóm:

+ Chủ sở hữu: gán mức bảo vệ, xem xét lại phân lớp theo thời gian, thông tin yêu cầu bảo vệ và truy xuất cho người bảo vệ và người sử dụng, cung cấp sự truy xuất với các tài liệu công việc, đánh giá nguy cơ mất mát thông tin….

+ Người bảo vệ: cung cấp bảo vệ thích ứng cho công cụ xử lý, lưu trữ thông tin, lưu bản sao và hồi phục, đưa ra môi trường xử lý an toàn có sự bảo vệ haonf toàn về tính toàn vẹn, bảo mật khả dụng của thông tin…..

+ Người sử dụng: sử dụng thông tin chỉ cho mục đích của nó, duy trì tính toàn vẹn, bảo mật, khả dụng của dữ liệu…..

**-Tiêu chuẩn:** Là yêu cầu bắt buộc để hỗ trợ các chính sách riêng lẻ. Các chuẩn chung và cụ thể để áp dụng cho từng đối tượng. Đó là những yêu cầu mà hệ thống cần đáp ứng (phải đạt được) để đảm bảo an toàn, bảo mật.

Ví dụ:

+ Về cung cấp thông tin (tài liệu up lên trang web hệ thống phải đảm bảo được kiểm duyệt, thông tin chính xác, cung cấp thông tin mới, ghi rõ nguồn sao lưu ở đâu, …..)

+ Tài liệu phải tuân theo các tiêu chuẩn về font form …..

Tiêu chuẩn TCVN 27001

Tiêu chuẩn này hướng tới việc áp dụng rộng rãi cho nhiều loại hình tổ chức khác nhau (ví dụ : tổ chức thương mại, cơ quan nhà nước, các tổ chức phi lợi nhuận v.v… ). Nội dung tiêu chuẩn chỉ rõ yêu cầu cho từng quá trình: thiết lập; triển khai; điều hành; giám sát; soát xét; bảo trì và nâng cấp một hệ thống ISMS để đảm bảo an toàn thông tin trước những tất cả các rủi ro có thể xảy ra với tổ chức. Tiêu chuẩn này cũng chỉ rõ các yêu cầu khi triển khai các biện pháp bảo vệ an toàn đã được chọn lọc phù hợp với nhu cầu của tổ chức hoặc một bộ phận của tổ chức.

Hệ thống ISMS được thiết kế các biện pháp đảm bảo an toàn thông tin phù hợp và đầy đủ để bảo vệ các tài sản thông tin và đem lại sự tin tưởng của các bên liên quan như đối tác, khách hàng v.v…

**-Chỉ dẫn:** là sự cần thiết, từng bước, hành động chi tiết hóa, yêu cầu phải thực hiện để hoàn thành một công việc.

Chỉ dẫn về quy trình làm việc, quy trình hoạt động, các bước tiến hành để không sai sót, sai lệch thông tin và đảm bảo tính chính xác. Nhằm đảm bảo tính toàn vẹn, bảo mật, khả dụng của thông tin.

Ví dụ: sinh viên đăng ký tín chỉ học thì phải thực hiện theo các bước như thế nào đó (đăng nhập -> Đăng kí tín chỉ -> Đăng ký môn học -> rà soát lại -> thêm sửa xóa tín chỉ đăng ký nhầm hay thiếu, …..)

**Câu hỏi 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, c ũng là công vi ệc 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

PHẦN II:

**Câu hỏi 11: Tấn công DoS, DDoS nguyên lý và khả năng phòng chống?**

**Cách phòng chống:**

+ Tăng cường “phần cứng” cũng là giải pháp tốt, nhưng thường xuyên theo dõi để phát hiện và ngăn chặn kịp thời cái gói tin IP từ các nguồn không tin cậy là hữu hiệu nhất.

+ Thiết lập mật khẩu mạnh để bảo vệ các thiết bị mạng và các nguồn tài nguyên quan trọng khác

+ Thiết lập các mức xác thực đối với người sử dụng cũng như các nguồn tin trên mạng. Đặc biệt, nên thiết lập chế độ xác thực khi cập nhật các thông tin định tuyến giữa các router.

+ Xây dựng hệ thống lọc thông tin trên router, firewall… và hệ thống bảo vệ chống lại SYN flood.

+ Xây dựng hệ thống định mức, giới hạn cho người sử dụng, nhằm mục đích ngăn ngừa trường hợp người sử dụng ác ý muốn lợi dụng các tài nguyên trên server để tấn công chính server hoặc mạng và server khác.

+ Liên tục cập nhật, nghiên cứu, kiểm tra để phát hiện các lỗ hổng bảo mật và có biện pháp khắc phục kịp thời.

+ Sử dụng các biện pháp kiểm tra hoạt động của hệ thống một cách liên tục để phát hiện ngay những hành động bất bình thường.

Xây dựng và triển khai hệ thống dự phòng.

***Câu hỏi 4:*** Phân tích sự khác biệt mã hóa cổ điển và mã công khai, khả năng kết hợp giữa hai loại khóa trong truyền tin?

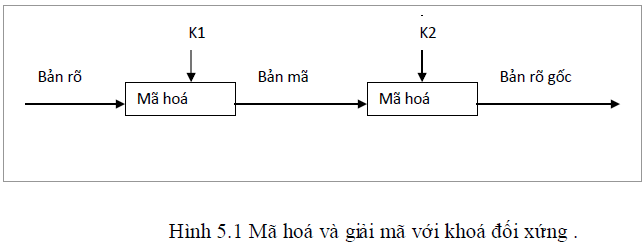
Bài Làm:

Sự khác biệt giữa mà hóa cổ điển và mã hóa công khai là:

**Các hệ mật mã đối xứng và công khai**

*1. Hệ mật mã đối xứng*

Thuật toán đối xứng hay còn gọi thuật toán mã hoá cổ điển là thuật toán mà tại đó khoá mã hoá có thể tính toán ra được từ khoá giải mã. Trong rất nhiều trường hợp, khoá mã hoá và khoá giải mã là giống nhau. Thuật toán này còn có nhiều tên gọi khác như thuật toán khoá bí mật, thuật toán khoá đơn giản, thuật toán một khoá. Thuật toán này yêu cầu người gửi và người nhận phải thoả thuận một khoá trước khi thông báo được gửi đi, và khoá này phải được cất giữ bí mật. Độ an toàn của thuật toán này vẫn phụ thuộc và khoá, nếu để lộ ra khoá này nghĩa là bất kỳ người nào cũng có thể mã hoá và giải mã thông báo trong hệ thống mã hoá. Sự mã hoá và giải mã của thuật toán đối xứng biểu thị bởi :

EK( P ) = C DK( C ) = P

Trong hình vẽ trên thì :

K1có thể trùng K2, hoặc

K1 có thể tính toán từ K2, hoặc K2 có thể tính toán từ K1.

***Một số nhược điểm của hệ mã hoá cổ điển***

Các phương mã hoá cổ điển đòi hỏi người mã hoá và người giải mã phải cùng chung một khoá. Khi đó khoá phải được giữ bí mật tuyệt đối, do vậy ta dễ dàng xác định một khoá nếu biết khoá kia.

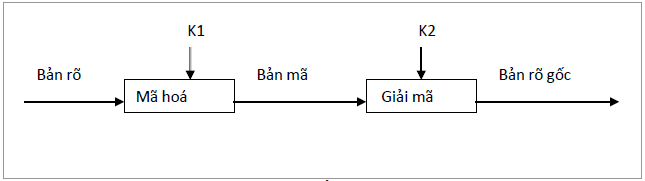
Hệ mã hoá đối xứng không bảo vệ được sự an toàn nếu có xác suất cao khoá người gửi bị lộ. Trong hệ khoá phải được gửi đi trên kênh an toàn nếu kẻ địch tấn công trên kênh này có thể phát hiện ra khoá.

Vấn đề quản lý và phân phối khoá là khó khăn và phức tạp khi sử dụng hệ mã hoá cổ điển. Người gửi và người nhận luôn luôn thông nhất với nhau về vấn đề khoá. Việc thay đổi khoá là rất khó và dễ bị lộ.

Khuynh hướng cung cấp khoá dài mà nó phải được thay đổi thường xuyên cho mọi người trong khi vẫn duy trì cả tính an toàn lẫn hiệu quả chi phí sẽ cản trở rất nhiều tới việc phát triển hệ mật mã cổ điển.

*2.Hệ mật mã công khai*

Vào những năm 1970 Diffie và Hellman đã phát minh ra một hệ mã hoá mới được gọi là **hệ mã hoá công khai** hay **hệ mã hoá phi đối xứng** Thuật toán mã hoá công khai là khác biệt so với thuật toán đối xứng. Chúng được thiết kế sao cho **khoá** sử dụng vào việc mã hoá là khác so với **khoá**



giải mã. Hơn nữa khoá giải mã không thể tính toán được từ khoá mã hoá. Chúng được gọi với tên hệ thống mã hoá công khai bởi vì khoá để mã hoá có thể công khai, một người bất kỳ có thể sử dụng khoá công khai để mã hoá thông báo, nhưng chỉ một vài người có đúng khoá giải mã thì mới có khả năng giải mã. Trong nhiều hệ thống, khoá mã hoá gọi là khoá công khai (public key), khoá giải mã thường được gọi là khoá riêng (private key).

Trong hình vẽ trên thì : K1 không thể trùng K2, hoặc K2 không thể tính toán từ K1. Đặc trưng nổi bật của hệ mã hoá công khai là cả khoá công khai(public key) và bản tin mã hoá (ciphertext) đều có thể gửi đi trên một kênh thông tin không an toàn. ***Diffie và Hellman đã xác đinh rõ các điều kiện của một hệ mã hoá công khai như sau :***

1. Việc tính toán ra cặp khoá công khai KB và bí mật kB dựa trên cơ sở các điều kiện ban đầu phải được thực hiện một cách dễ dàng, nghĩa là thực hiện trong thời gian đa thức.

2. Người gửi A có được khoá công khai của người nhận B và có bản tin P cần gửi đi thì có thể dễ dàng tạo ra được bản mã C.

C = EKB (P) = EB (P) Công việc này cũng trong thời gian đa thức.

3. Người nhận B khi nhận được bản tin mã hóa C với khoá bí mật kB thì có thể giải mã bản tin trong thời gian đa thức.

P = DkB (C) = DB[EB(M)]

4. Nếu kẻ địch biết khoá công khai KB cố gắng tính toán khoá bí mật thì khi đó chúng phải đương đầu với trường hợp nan giải, trường hợp này đòi hỏi nhiều yêu cầu không khả thi về thời gian.

5. Nếu kẻ địch biết được cặp (KB,C) và cố gắng tính toán ra bản rõ P thì giải quyết bài toán khó với số phép thử là vô cùng lớn, do đó không khả thi.

**Khả năng kết hợp giữa hai loại khóa trong truyền tin:**

Không phải tất cả các [thuật toán](http://vi.wikipedia.org/wiki/Thu%E1%BA%ADt_to%C3%A1n) [mật mã hóa khóa bất đối xứng](http://vi.wikipedia.org/wiki/M%E1%BA%ADt_m%C3%A3_h%C3%B3a_kh%C3%B3a_b%E1%BA%A5t_%C4%91%E1%BB%91i_x%E1%BB%A9ng) đều hoạt động giống nhau nhưng phần lớn đều gồm 2 [khóa](http://vi.wikipedia.org/wiki/Kh%C3%B3a_(m%E1%BA%ADt_m%C3%A3)) có quan hệ [toán học](http://vi.wikipedia.org/wiki/To%C3%A1n_h%E1%BB%8Dc) với nhau: một cho [mã hóa](http://vi.wikipedia.org/wiki/M%C3%A3_h%C3%B3a) và một để [giải mã](http://vi.wikipedia.org/w/index.php?title=Gi%E1%BA%A3i_m%C3%A3&action=edit&redlink=1). Để thuật toán đảm bảo an toàn thì không thể tìm được khóa giải mã nếu chỉ biết khóa đã dùng mã hóa. Điều này còn được gọi là mã hóa công khai vì khóa dùng để mã hóa có thể công bố công khai mà không ảnh hưởng đến bí mật của văn bản mã hóa. Trong ví dụ ở trên, khóa công khai có thể là những hướng dẫn đủ để tạo ra khóa với tính chất là một khi đã khóa thì không thể mở được nếu chỉ biết những hướng dẫn đã cho. Các thông tin để mở khóa thì chỉ có người sở hữu mới biết.

**Câu hỏi 5: Giới thiệu về mã hóa ECC nguyên lý và ứng dụng.**

Việc sử dụng ECC mang lại những hiệu quả sau: tăng tốc độ, yêu cầu khả năng tính toán thấp hơn, tiết kiệm dải thông đường truyền, tăng hiệu quả lưu trữ, giảm độ dài các chứng nhận...Các ưu điểm trên của hệ mật ECC có thể phát huy hiệu quả trong các ứng dụng mà đường truyền, khả năng tính toán, tốc độ và lưu trữ bị hạn chế. Và các ứng dụng đó được thể hiện rất hiệu quả trong thương mại điện tử, web servers…

### Câu 9: Nguyên lý, khả năng, phương thức phòng chống với các phương thức tấn công mạng máy tính: Hijacking attack, Replay attack, Man-in-the-middle attack

A, Hijacking attack:

* Nghe lén thông tin liên lạc
* Đợi kết thúc quá trình xác thực
* Gửi tín hiệu yêu cầu kết thúc
* Tiếp tục liên kết với máy còn lại

Giải pháp:

* Tiến hành mã hóa phiên
* Xác thực phiên theo thời gian

B,Replay attack:

Một cuộc tấn công phát lại là một hình thức tấn công mạng, trong đó một truyền dữ liệu hợp lệ là độc hại hoặc gian lận lặp đi lặp lại hoặc trì hoãn. Này được thực hiện bằng cách người khởi tạo hay của một kẻ thù người chặn các dữ liệu và truyền lại nó, có thể là một phần của một cuộc tấn công giả trang bởi gói thay thế IP (chẳng hạn như tấn công mật mã dòng).

* Sử dụng thông tin nghe lén

• Lưu trữ Lưu trữ

• Gửi lại thông tin đến máy cần để xác Gửi lại thông tin đến máy cần để xác thực

Giải pháp:

* Xác thực theo phiên(chỉ số phiên)
* Sử dụng phương thức xác thực lại theo thời gian(sau thời gian kết nối)

C, Man – in – the – middle:

* Nguyên lý, khả năng:
  + Tấn công khi làm cho hai bên kết nối hiểu nhầm người thứ 3 là đối tác của mình
  + Tấn công bằng bộ phát sóng giả mạo(AP)

• Sử dụng bộ phát có sóng mạnh hơn Sử dụng bộ phát có sóng mạnh hơn

• Máy kết nối nhầm, hoặc xác thực nhầm

* + Tấn công bằng làm giả tín hiệu ARP

• Gửi các thông điệp map giữa IP và MAC

* + Tấn công dựa vào DNS

• Dựa trên cơ chế gửi và nhận địa chỉ IP thông qua tên miền

• Gửi một địa chỉ IP khác với địa chỉ tên miền

* Phương thức phòng chống:

Bảo mật vật lý là phương thức tốt nhất để chống lại kiểu tấn công này

Ngoài ra, ta có thể ngăn chặn hình thức tấn công này bằng kĩ thuật mã hóa: mã hóa traffic trong môi trường hầm IPSec,hacker sẽ chỉ nhìn thấy những thông tin không có giá trị

**Câu 10: Tấn công SQL injection, tràn bộ đệm, chéo trang – cross**

**page attack? Giải pháp phòng chống?**

**Phòng chống SQL Injection**Các biện pháp phòng chống tấn công SQL Injection cho website phụ thuộc rất nhiều vào nền tảng (platform) xây dựng web. Ví dụ, website của bạn được xây dựng trên platform nào (Joomla, Wordpress hay DotNetNuke …) và sử dụng ngôn ngữ lập trình gì (ASP, PHP, .Net hay Java …). Website đó đang chạy trên Web Server (IIS, Apache…) nào, hệ quản trị CSDL của website là gì (Oracle, MySQL…)?   
Dưới đây là một số quy tắc chung trong việc phòng chống SQL Injection:   
1. Đối với website (dành cho lập trình viên): Cần kiểm tra tính đúng đắn của tất cả dữ liệu đầu vào. Dữ liệu đầu vào không chỉ là các tham số, mà bao gồm cả cookie, user agent, referer …   
Việc kiểm tra tính đúng đắn của dữ liệu có thể dựa trên các phương pháp sau:   
- Kiểm tra dựa vào kiểu dữ liệu (số, ngày tháng …)   
- Kiểm tra, giới hạn độ dài đầu vào   
- Loại bỏ các ký tự đặc biệt như: ‘ % ” ? # @ & …   
- Loại bỏ các từ đặc biệt: select, drop, delete, information\_schemal, insert, union, xp\_ …   
2. Đối với web server (dành cho quản trị mạng): Hầu hết các máy chủ web (web server) hiện nay đều có các module hỗ trợ việc phòng chống SQL Injection, ví dụ, Apache có modsecurity, IIS có URLScan. Bạn chỉ cần bật tính năng này và cấu hình cho phù hợp. Nếu website của bạn là dạng trang tin tức thì rất phù hợp để triển khai. Trong một số trường hợp khác, các module này có thể chặn nhầm, dẫn tới website hoạt động không chính xác.   
3. Đối với database server (dành cho quản trị mạng): Bạn cần thực hiện việc cấu hình phân quyền chặt chẽ đối với các tài khoản. Khi đó, dù tồn tại lỗi SQL Injection, thiệt hại cũng sẽ được hạn chế. Ngoài ra, bạn cần loại bỏ các bảng, thành phần và tài khoản không cần thiết trong hệ thống.   
4. Một số lời khuyên khác:   
- Bạn cần tắt tất cả các thông báo lỗi không cần thiết của web server. Hacker có thể lợi dụng chính các thông báo lỗi này để khai thác thông tin của hệ thống, phục vụ cho một cuộc tấn công SQL Injection.   
- Bạn cần bật các chế độ ghi log đầy đủ để phục vụ việc điều tra phát hiện cuộc tấn công và giải quyết sự cố.   
- Bạn cần thường xuyên theo dõi và cập nhật phiên bản cho platform của website (hệ điều hành, web server, database server…).

**Giải pháp phòng chống:**

Nhiều kỹ thuật đa dạng với nhiều ưu nhược điểm đã được sử dụng để phát hiện hoặc ngăn chặn hiện tượng tràn bộ đệm. Cách đáng tin cậy nhất để tránh hoặc ngăn chặn tràn bộ đệm là sử dụng bảo vệ tự động tại mức ngôn ngữ lập trình. Tuy nhiên, loại bảo vệ này không thể áp dụng cho [mã thừa kế](http://vi.wikipedia.org/w/index.php?title=M%C3%A3_th%E1%BB%ABa_k%E1%BA%BF&action=edit&redlink=1) (*legacy code*), và nhiều khi các ràng buộc kỹ thuật, kinh doanh hay văn hóa lại đòi hỏi sử dụng một ngôn ngữ không an toàn. Các mục sau đây mô tả các lựa chọn và cài đặt hiện có.

* Lựa chọn ngôn ngữ lập trình

### Sử dụng các thư viện an toàn

### Chống tràn bộ nhớ đệm trên stack

### Bảo vệ không gian thực thi

### Ngẫu nhiên hóa sơ đồ không gian địa chỉ

### Kiểm tra sâu đối với gói tin

### Chéo trang:

**Câu 13: Khả năng bảo vệ thống của trình quét virus và firewall.**

1. **Phần mềm diệt virus** là [phần mềm](http://vi.wikipedia.org/wiki/Ph%E1%BA%A7n_m%E1%BB%81m) có tính năng phát hiện, loại bỏ các [virus máy tính](http://vi.wikipedia.org/wiki/Virus_(m%C3%A1y_t%C3%ADnh)), khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

Để đạt được các mục tiêu tối thiểu trên và mở rộng tính năng, phần mềm diệt virus thường hoạt động trên các nguyên lí cơ bản nhất như sau:

* Kiểm tra (quét) các [tập tin](http://vi.wikipedia.org/wiki/T%E1%BA%ADp_tin) để phát hiện các virus đã biết trong cơ sở dữ liệu nhận dạng về virus của chúng.
* Phát hiện các hành động của các phần mềm giống như các hành động của virus hoặc các phần mềm độc hại.

2. Firewall   
Thuật ngữ Firewall có nguồn gốc từ một kỹ thuật thiết kế trong xây dựng để ngăn chặn, hạn chế hoả hoạn. Trong công nghệ mạng thông tin, Firewall là một kỹ thuật đ­ợc tích hợp vào hệ thống mạng để chống sự truy cập trái phép, nhằm bảo vệ các nguồn thông tin nội bộ và hạn chế sự xâm nhập không mong muốn vào hệ thống. Cũng có thể hiểu Firewall là một cơ chế (mechanism) để bảo vệ mạng tin t­ởng (Trusted network) khỏi các mạng không tin t­ởng (Untrusted network).  
Thông th­ờng Firewall đ­ợc đặt giữa mạng bên trong (Intranet) của một công ty, tổ chức, ngành hay một quốc gia, và Internet. Vai trò chính là bảo mật thông tin, ngăn chặn sự truy nhập không mong muốn từ bên ngoài (Internet) và cấm truy nhập từ bên trong (Intranet) tới một số địa chỉ nhất định trên Internet.  
**Chức năng chính**Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:  
- Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).   
- Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).   
- Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.   
- Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.   
- Kiểm soát ng­ời sử dụng và việc truy nhập của ng­ời sử dụng.   
- Kiểm soát nội dung thông tin thông tin l­u chuyển trên mạng.   
**Các thành phần:**  
Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:  
- Bộ lọc packet (packet-filtering router)   
- Cổng ứng dụng (application-level gateway hay proxy server)   
- Cổng mạch (circuite level gateway)   
- Bộ lọc paket (Paket filtering router)

**Câu hỏi 14: IPSec,VPN khả năng bảo vệ thông tin trên đường truyền.**

**1.khái niệm IPSec :**- IP Sercurity hay còn gọi là IPSec dựa trên nền tảng chuẩn được cung cấp một khoá   
cho phép bảo mật giữa hai thiết bị mạng ngang hàng.  
Hay nói cách khác nó là một tập hợp các chuẩn, các nguyên tắc đã được định nghĩa để   
kiểm tra, xác thực và mã hóa gói dữ liệu IP để cung cấp cho kênh truyền dẫn mạng bảo   
mật.  
**2. Vai trò của IPSec :**  
+ Cho phép xác thực hai chiều, trước và trong quá trình truyền tải dữ liệu.  
+ Mã hóa đường truyền giữa 2 máy tính khi được gửi qua một mạng.  
+ Bảo vệ gói dữ liệu IP và phòng ngự các cuộc tấn công mạng không bảo mật.  
+ IPSec bảo vệ các lưu lượng mạng bằng việc sử dụng mã hóa và đánh dấu dữ liệu.  
+ Một chính sách IPSec cho phép định nghĩa ra các loại lưu lượng mà IPSec sẽ kiểm   
tra và cách các lưu lượng đó sẽ được bảo mật và mã hóa như thế nào.  
**3. Những Tính Năng của IPSec (IPSec Security Protocol)**  
-Tính xác nhận và Tính nguyên vẹn dữ liệu (Authentication and data integrity).   
IPSec cung cấp một cơ chế mạnh mẽ để xác nhận tính chất xác thực của người gửi và   
kiểm chứng bất kỳ sự sửa đổi không được bảo vệ trước đó của nội dung gói dữ liệu bởi   
người nhận. Các giao thức IPSec đưa ra khả năng bảo vệ mạnh để chống lại các dạng tấn   
công giả mạo, đánh hơi và từ chối dịch vụ.  
-Sự cẩn mật (Confidentiality). Các giao thức IPSec mã hóa dữ liệu bằng cách sử dụng   
kỹ thuật mã hóa cao cấp, giúp ngăn cản người chưa chứng thực truy cập dữ liệu trên   
đường đi của nó. IPSec cũng dùng cơ chế tạo hầm để ẩn địa chỉ IP của nút nguồn (người   
gửi) và nút đích (người nhận) từ những kẻ nghe lén.   
- Quản lý khóa (Key management). IPSec dùng một giao thức thứ ba, Internet Key   
Exchange (IKE), để thỏa thuận các giao thức bảo mật và các thuật toán mã hóa trước và   
trong suốt phiên giao dịch. Một phần quan trọng nữa, IPSec phân phối và kiểm tra các   
khóa mã và cập nhật những khóa đó khi được yêu cầu.   
- Hai tính năng đầu tiên của bộ IPSec, authentication and data integrity, và   
confidentiality, được cung cấp bởi hai giao thức chính của trong bộ giao thức IPSec.   
Những giao thức này bao gồm Authentication Header (AH) và Encapsulating Security   
Payload (ESP).  
- Tính năng thứ ba, key management, nằm trong bộ giao thức khác, được bộ IPSec chấp 