CHÍNH SÁCH AN TOÀN THÔNG TIN (INFORMATION SECURITY POLICY)

1

Nội dung

1. An toàn thông tin (Information Security)
2. Chính sách an toàn thông tin (Information Security Policy)
3. Tại sao nhân viên ngành CNTT nắm rõ về Chính sách an toàn thông tin tại nơi làm việc
4. Ví dụ về chính sách an toàn thông tin

2

1. An toàn thông tin (Information Security)

1. Thông tin là gì?
2. An toàn thông tin là gì?
3. Rủi ro, mối đe dọa, và lỗ hổng
4. Giải pháp để an toàn thông tin

3

1.1 Thông tin (Information) là gì

"Information is an asset which, like other important business assets, has value to an organization and consequently needs to be suitably protected"

(BS ISO 27002:2005)

4

1.1 Thông tin (Information) là gì

- Information có thể được
  - Tạo, lưu, xóa, xử lý, chuyển giao, sử dụng (cho đúng mục đích, sai mục đích), hư hỏng, mất, đánh cắp, in hoặc viết lên giấy, lưu trữ chuyển giao bằng cách đăng lên hoặc dùng các phương tiện điện tử, đưa vào các video, hiển thị/xuất bản,…
- '… whatever form the information takes, or means by which it is shared or stored, it should always be appropriately protected"

(BS ISO 27002:2005)

5

1.2 An toàn thông tin (Information Security) là gì

- Bảo vệ thông tin từ hàng loạt các mối đe dọa
- Đảm bảo tính liên tục kinh doanh
- Giảm thiểu tổn thất tài chính
- Tối ưu hóa lợi tức đầu tư
- Tăng cơ hội kinh doanh

6

1.2 An toàn thông tin (Information Security) là gì

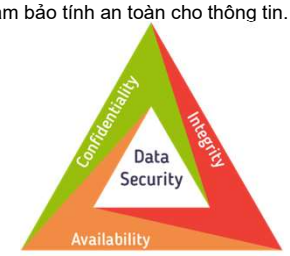
ISO 27002:2005 định nghĩa Information Security là phải duy trì:

- **Tính bí mật (Confidentiality)**: Thông tin chỉ được phép truy cập (đọc) bởi những đối tượng (người, chương trình máy tính,…) được cấp phép *(Ai có thể thấy được thông tin?)*
- **Tính toàn vẹn (Integrity)**: 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 *(Thông tin có đúng không?)*
- **Tính sẵn dùng (Availability)**: thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn *(thông tin sẵn sàng và dùng được không?)*

7

1.2 An toàn thông tin (Information Security) là gì

- Khi xây dựng hệ thống thông tin thì cần cân bằng 3 mục tiêu này để đảm bảo tính an toàn cho thông tin.



8

1.2 An toàn thông tin (Information Security) là gì

- Security bị vi phạm dẫn đến …
  - ❖ Uy tín bị mất
  - ❖ Tổn thất về tài chính
  - ❖ Mất mát tài sản trí tuệ
  - ❖ Vi phạm pháp luật dẫn đến hàng động pháp lý (luật CNTT)
  - ❖ Mất đi lòng tin cậy của khách hàng
  - ❖ Chi phí gián đoạn kinh doanh
  - ❖ ….

9

1.2 An toàn thông tin (Information Security) là gì

- Information Security là "Organizational Problem" hơn là "IT Problem"
- Hơn 70% các mối đe dọa là nội bộ (internal)
- Hơn 60% các thủ phạm là kẻ lừa đảo lần đầu tiên (First Time fraudsters)
- Mối nguy hiểm lớn nhất: con người
- Tài sản lớn nhất: con người
- Kỹ thuật "Social Engineering" là mối đe dọa chính

10

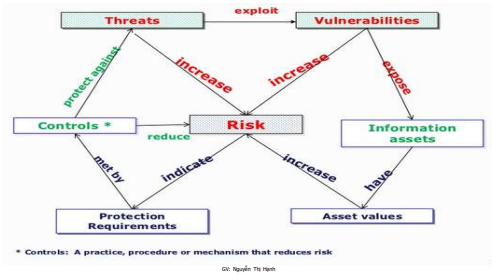
1.3 Lỗ hổng, mối đe dọa, rủi ro

- **Vulnerability (lỗ 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 hổng trong tài sản và gây ra nguy hại hoặc mất mát đến tài sản.

11

1.3 Lỗ hổng, mối đe dọa, rủi ro

- Mối quan hệ giữa lỗ hổng, mối đe dọa, rủi ro



12

1.3 Vulnerability, Threat, Risk

Thread (mối đe dọa) xuất phát từ đâu?

- Nhân viên
- Các bộ phận bên ngoài
- Sự thiếu nhận thức về các vấn đề an toàn
- Sự phát triển việc kết nối mạng và các máy tính phân tán
- Sự phát triển trong mức độ phức tạp và hiệu suất của các công cụ tấng công và virus
- Thảm họa tự nhiên như cháy, lũ lụt, động đất,…

13

1.3 Vulnerability, Threat, Risk

No	Categories of Threat	Example
1	Human Errors or failures	Accidents, Employee mistakes
2	Compromise to Intellectual Property	Piracy, Copyright infringements
3	Deliberate Acts or espionage or trespass	Unauthorized Access and/or data collection
4	Deliberate Acts of Information extortion	Blackmail of information exposure / disclosure
5	Deliberate Acts of sabotage / vandalism	Destruction of systems / information
6	Deliberate Acts of theft	Illegal confiscation of equipment or information
7	Deliberate software attacks	Viruses, worms, macros Denial of service
8	Deviations in quality of service from service provider	Power and WAN issues
9	Forces of nature	Fire, flood, earthquake, lightening
10	Technical hardware failures or errors	Equipment failures / errors
11	Technical software failures or errors	Bugs, code problems, unknown loopholes
12	Technological Obsolesce	Antiquated or outdated technologies

14

1.3 Vulnerability, Threat, Risk

15

1.4 Các giải pháp để an toàn thông tin

16

1.4 Giải pháp để An toàn thông tin

17

2. Information Security Policy (IPS)

2.1 Chính sách an toàn thông tin là gì?
2.2 Mục tiêu của ISP
2.3 Phạm vi của ISP
2.4 Tầm quan trọng ISP
2.5 Ai là người dùng ISP
2.6 Các bước triển khai ISP
2.7 Xác định được vấn đề cần ISP
2.8 Nội dung có trong tài liệu ISP

18

2.1 Chính sách an toàn thông tin (ISP) là gì

- **Information Security Policy (ISP)**

ISP là một tập các quy tắc, hướng dẫn mà tổ chức đưa ra nhằm đảm bảo tính an toàn hệ thống thông tin và miễn nhiễm chống lại tấng công nguy hiểm.

19

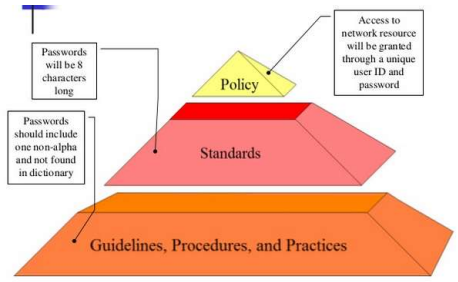
2.1 Information Security Policy là gì?

- ISP cung cấp ***một môi trường để quản lý thông tin một cách an toàn trong toàn tổ chức.***
- ISP được viết cho ***tất cả các cấp nhân viên khác nhau.***
- ISP gồm ***các quy tắc chung về tất cả các chủ đề có liên quan đến an ninh thông tin và sử dụng máy tính hoặc các quy tắc riêng biệt về các chủ đề khác nhau***
- Ví dụ: quy tắc dùng e-mail, quyền hạn truy xuất dữ liệu, quy trình backup dữ liệu,....

20

2.1 Information Security Policy là gì?

-



21

2.2 Mục đích của ISP

Các tổ chức đưa ra các ISP bởi nhiều lý do khác nhau:

- Thiết lập một cách tiếp cận chung đối với an ninh thông tin.
- Phát hiện và ngăn chặn sự thoả hiệp của an ninh thông tin như lạm dụng dữ liệu, mạng, hệ thống máy tính và các ứng dụng.
- Để bảo vệ danh tiếng của công ty đối với trách nhiệm đạo đức và pháp lý của công ty.
- Thực hiện các quyền của khách hàng; Cung cấp cơ chế hiệu quả để đáp ứng các khiếu nại và thắc mắc liên quan đến sự không tuân thủ chính sách thực tế hoặc không nhận thức được là một cách để đạt được mục tiêu này.

22

2.3 Phạm vi của ISP

- ISP thường nhắm vào tất cả:
  - **Các dữ liệu**
  - **Chương trình**
  - **Hệ thống**
  - **Phương tiện**
  - **Cấu trúc hạ tầng cơ sở**
  - **Các người dùng, các bên tham gia thứ 3,**
  - **Các nhóm bên ngoài (third parties) tổ chức**
  - **Không có trường hợp ngoại lệ**.
- ISP được dùng để hỗ trợ ***việc bảo vệ, điều khiển và quản lý*** các tài sản thông tin của tổ chức.

23

2.3 Phạm vi của ISP

- ISP được yêu cầu là bao hàm tất cả các thông tin bên trong tổ chức mà có thể bao gồm dữ liệu và thông tin như sau:
  - Lưu trữ trong các CSDL, trong máy tính ở các đĩa cứng cố định
  - Truyền qua mạng nội bộ và công cộng
  - In hoặc viết tay trên giấy, bảng trắng ...
  - Gửi qua fax, telex hoặc các phương tiện truyền thông khác
  - Lưu trữ trên phương tiện di động như CD-ROM, đĩa cứng, băng và các phương tiện tương tự khác
  - Tổ chức trên phim, các trang trình chiếu, máy chiếu, sử dụng phương tiện nghe nhìn và âm thanh
  - Phát biểu trong các cuộc gọi điện thoại và các cuộc họp được chuyển tải bằng bất kỳ phương pháp nào khác

24

2.4 Tầm quan trọng của ISP

- Giảm thiểu nguy cơ rò rỉ dữ liệu hoặc mất mát
- Bảo vệ tổ chức khỏi những người dùng nội bộ và bên ngoài "độc hại"
- Thiết lập các hướng dẫn, thực tiễn tốt nhất về sử dụng và đảm bảo tuân thủ đúng.
- Thông báo nội bộ và bên ngoài thông tin đó là tài sản, tài sản riêng của tổ chức, và được bảo vệ khỏi bị truy cập trái phép, sửa đổi, tiết lộ và hủy hoại.
- Đẩy mạnh lập trường chủ động cho tổ chức khi có vấn đề pháp lý phát sinh
- Cung cấp hướng nâng cấp các tiêu chuẩn an ninh trong và ngoài tổ chức

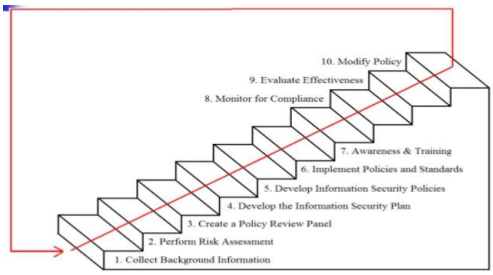
25

2.5 Ai là người dùng ISP

- Người quản lý – tất cả các cấp độ
- Nhân viên kỹ thuật – người quản trị hệ thống, …
- Người dùng cuối – tất cả các người dùng dịch vụ của hệ thống

26

2.6 Các bước triển khai ISP



27

2.6 Các bước triển khai ISP

-

28

2.7 Xác định vấn đề cần Policy

- Các nguồn tài nguyên và thông tin cần truy suất có thẩm quyền
- Không tiết lộ hoặc không được phép tiết lộ thông tin
- Quy trình cần tuân theo
- Lỗi và lỗi người dùng

29

Quan tâm đến an toàn dữ liệu

- **Xử lý dữ liệu:**
  - Chính sách: Cách dữ liệu được xử lý như thế nào và cách duy trì tính bí mật và toàn vẹn của dữ liệu.
  - Sự tồn tại của dữ liệu bên thứ ba
  - Dữ liệu cá nhân
  - Dữ liệu nhân sự
  - Bảo vệ sự riêng tư
  - Chi phí giấy phép phần mềm

30

Quan tâm đến an toàn dữ liệu

- **Sao lưu (Backups)**
  - Dữ liệu nào cần sao lưu
  - Tần suất sao lưu
  - Kiểm soát các quy trình sao lưu
  - Lưu trữ dữ liệu tại chỗ hoặc ngoài nơi lưu trữ dữ liệu

31

Quan tâm đến an toàn dữ liệu

- **Tiêu hủy dữ liệu**
  - Xem xét các ổ cứng cũ
  - Dumpster diving: kỹ thuật được dùng để lấy ra thông tin từ các dữ liệu đã bị xóa
- **Các quyền và chính sách về sở hữu trí tuệ**
  - Ai là chủ quyền đối với các tài sản trí tuệ
  - Ghi nhãn để thực thi quyền sở hữu trí tuệ

32

2.8 Nội dung của một tài liệu Policy

- Giới thiệu
- Mục đích
- Phạm vi
- Chính sách
- Vài trò và trách nhiệm
- Vi phạm và xử lý
- Lịch sửa đổi và cập nhật
- Thông tin liên hệ
- Định nghĩa/thuật ngữ

33

3. Tại sao nhân viên ngành CNTT nắm rõ về Information Security Policy tại nơi làm việc

34

4. Ví dụ về chính sách an toàn thông tin

-

35

4. Ví dụ về chính sách an toàn thông tin

-

36

4. Ví dụ về chính sách an toàn thông tin

-

37

4. Ví dụ về chính sách an toàn thông tin

-

38

4. Ví dụ về chính sách an toàn thông tin

39

4. Ví dụ về chính sách an toàn thông tin

-

40

4. Ví dụ về chính sách an toàn thông tin

-

41

4. Ví dụ về chính sách an toàn thông tin

-

42

4. Ví dụ về chính sách an toàn thông tin

- https://www.sans.org/security-resources/policies/

43

Câu hỏi & Bài tập

1. Chính sách an toàn thông tin (ISP) của một doanh nghiệp là gì? Trình bày và giải thích được ít nhất 3 lý do tại sao một doanh nghiệp cần có một ISP?
2. Là kỹ sư CNTT, trình bày và giải thích ít nhất 3 lý do tại sao bạn cần nắm rõ những chính sách an toàn thông tin tại nơi bạn làm việc?
3. Hãy viết một chính sách an toàn thông tin dành cho các sinh viên có tham gia sử dụng các trang thiết bị, phần mềm ở phòng thực hành, chính sách cài đặt các phần mềm ứng dụng, phần phòng chống mã độc cho máy tính.

44

Câu hỏi & Bài tập

4. Hãy viết một chính sách sử dụng Wifi trong một phòng ban có khoảng 20 nhân viên
5. "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.
6. "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.

45