Chương 1

TỔNG QUAN VỀ AN TOÀN THÔNG TIN

Giáo viên: ThS.Lê Quốc Anh

Nội dung

1. Giới thiệu chung
2. Các khái niệm cơ bản
3. Các nguyên tắc nền tảng của An toàn thông tin
4. Tầm quan trọng an toàn thông tin đối với xã hội/ doanh nghiệp/ cá nhân
5. Các phương pháp đảm bảo an toàn thông tin
6. Các thành phần cần bảo vệ trong một HTTT
7. Câu hỏi và bài tập

1. Giới thiệu chung

- Công nghệ thông tin và truyền thông có sự phát triển vượt bậc trong khoảng hai thập kỷ qua, với hội tụ nhiều loại công nghệ tiên tiến, mở ra một kỷ nguyên mới của nhân loại → **Kỷ nguyên số**.
- Xã hội loài người ngày càng phụ thuộc nhiều vào CNTT&TT trong các ngành từ sản xuất công nghiệp, nông nghiệp đến y tế giáo dục, văn hóa, giải trí … CNTT&TT đang có mặt trong mọi đời sống xã hội
- CNTT&TT đang làm biến đổi mọi mặt xã hội từ công việc đến đời sống

Slide: 3

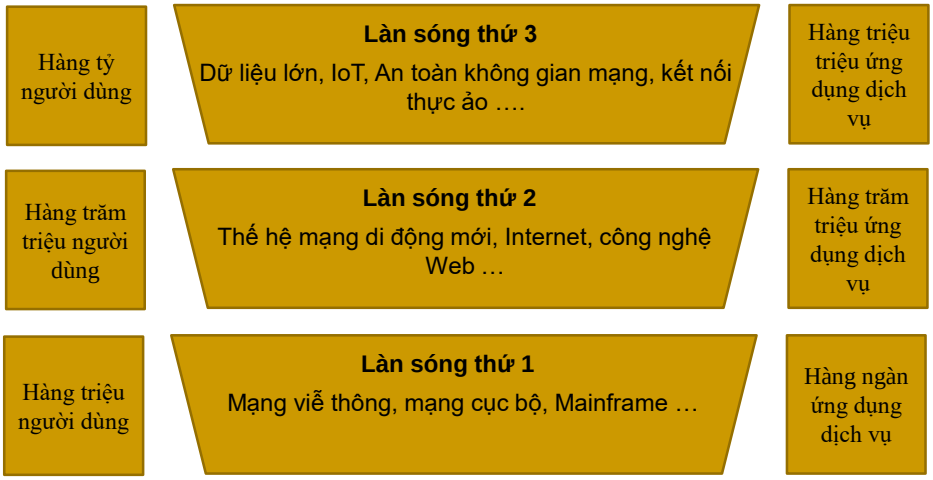
1. Giới thiệu chung

- Xu thế phát triển CNTT&TT theo dự đoán của các nhà khoa học gồm những đặc trưng cơ bản:
  - **Công nghệ di động:** Thiết bị di động và ứng dụng di động gia tăng về số lượng và chủng loại, thế hệ mạng thông tin di động sẽ chiếm ưu thế trong những năm tới
  - **Điện toán đám mây:** Công nghệ đám mây có thay đổi cơ bản về kiến trúc, dịch vụ, hoạt động kinh doanh
  - **Dữ liệu lớn:** Dữ liệu có xu thế bùng nổ, đặt ra những vấn đề về phân tích dữ liệu lớn và ứng dụng trí tuệ nhân tạo
  - **Công nghệ xã hội:** Phát triển và ứng dụng đa phương tiện trong mọi lĩnh vực xã hội. Thực tế ảo (VR) tạo ra thay đổi trong cuộc sống
  - **Internet kết nối vạn vật (IoT):** Kết nối mọi thứ vào Internet
  - **An toàn không gian mạng:** Công nghệ, kỹ thuật tấn công song song với sự phát triển CNTT&TT → nhu cầu mua sản phẩm bảo vệ gia tăng

Slide: 4

1. Giới thiệu chung

- Các làn sóng phát triển CNTT&TT



Slide: 5

1. Giới thiệu chung

- Số lượng cư dân mạng tăng một cách nhanh chóng, năm 2005 tầm 1 tỷ, 2015 có trên 3 tỷ.

- An toàn không gian mạng là một vấn đề gắn liền với CNTT&TT. Tốc độ và phạm vi kết nối mạng ngày càng tăng và mở rộng, số lượng người dùng ngày càng tăng nhanh → nguy cơ mất An toàn thông tin càng tăng và nghiêm trọng hơn.

Slide: 6

Nguy cơ mất an toàn thông tin

Loại nguy cơ	Ví dụ điển hình
Lỗi người dùng hoặc lỗi hệ thống	Sự cố, lỗi khai thác của kỹ thuật viên; lỗi kỹ thuật của hệ thống. Hành vi đó có thể do vô tình (do thiếu hiểu biết, thiếu cẩn thận) hoặc cố ý (cố tình lọt thông tin, không áp dụng các biện pháp bảo vệ…) của người dung hợp pháp.
Vi phạm sở hữu trí tuệ	Gián điệp, bẻ khóa bản quyền số. Sở hữu trí tuệ có thể bảo gồm: bí mật thương mại, bản quyền thương hiệu, phát minh sáng chế. Gián điệp bẻ khóa bản quyền phần mềm đang là mối quan tâm. Theo hiệp hội phần mềm thương mại năm 2006 có ít nhất là 1/3 tổng số phần mềm bị bi phạm quyền sở hữu
Nguy cơ phần mềm	Virut, mã độc, sâu, từ chối dịch vụ
Lỗi phần mềm	Lỗi mã lệnh, lỗ hổng chưa biết
Nguy cơ phá hoại	Phá hủy hệ thống hoặc xóa thông tin

Slide: 7

2. Các khái niệm cơ bản

- **Không gian mạng (Cyber space):** được hiểu là một không gian ảo có tính động, kết hợp các thành phần điện tử và phổ điện tử nhằm mục đích tạo lập, lưu trữ, xử lý, sửa đổi, trao đổi, chia sẻ, sử dụng thông tin và tài nguyên vật lý.
- Không gian mạng bao gồm
  - Tài nguyên vật lý
  - Các hệ thống máy tính và phần mềm
  - Mạng lưới kết nối
  - Các thiết bị truy nhập đầu cuối
  - Dữ liệu và ứng dụng

Slide: 8

Không gian mạng

Slide: 9

Không gian mạng

- Không gian mạng (Cyber space) có thể được định nghĩa như sau:
  - Là các hệ thống thông tin (gồm phần cứng, phần mềm, cơ sở dữ liệu, quy trình thủ tục và nhân sự vận hành) có kết nối với nhau thành mạng (qua môi trường hữu tuyền và vô tuyến)
  - Nhằm mục đích chia sẻ thông tin (tín hiệu, số liệu, văn bản, âm thanh, hình ảnh, video …) và các tài nguyên (hạ tầng kỹ thuật, phần mềm, dữ liệu, ứng dụng);
  - Thông qua các hoạt động (Tạo lập, thu thập, lưu trữ, xử lý, phâ phối, truyền gửi và nhận);
  - Phục vụ cho nhu cầu đa dạng trong đời sống xã hội

Slide: 10

Dữ liệu (Data) và thông tin (Information)

Dữ liệu

Baker, Kenneth D.	324917628
Doyle, Joan E.	476193248
Finkle, Clive R.	548429344
Lewis, John C.	551742186
McFerran, Debra R.	409723145

Thông tin

Class Roster

Course: MGT 500 Business Policy Semester: Spring 2010

Section: 2

Name	ID	Major	GPA
Baker, Kenneth D.	324917628	MGT	2.9
Doyle, Joan E.	476193248	MKT	3.4
Finkle, Clive R.	548429344	PRM	2.8
Lewis, John C.	551742186	MGT	3.7
McFerran, Debra R.	409723145	IS	2.9
Sisneros, Michael	392416582	ACCT	3.3

Slide: 11

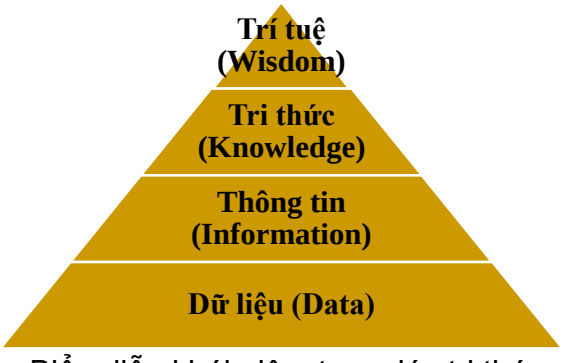
Dữ liệu (Data) và thông tin (Information)

- Dữ liệu (Data): Các giá trị đại lượng vật lý, ký tự, ký hiệu, âm thanh, hình ảnh được biểu thị dưới dạng thuận tiện cho việc truyền tải, xử lý.
- Thông tin (information): Thông tin là dữ liệu tổ chức xử lý, biểu diễn, kết hợp, chuyển đổi thành dạng có nghĩa theo ngữ cảnh cụ thể.
- Dữ liệu là nguyên liệu thô của thông tin, là tổ chức thấp hơn của thông tin. Thông tin là dữ liệu chuyển tải sang dạng có nghĩa cho người nhận

Slide: 12

Dữ liệu (Data) và thông tin (Information)

- Tri thức (Knowledge): là thông tin thu nhận được, hiểu được, diễn giải và suy luận được.
- Trí tuệ (Wisdom): là sự tích hợp có chọn lọc của tri thức hiểu được, cảm nhận được



Biểu diễn khái niệm tam giác tri thức

Slide: 13

Hệ thống thông tin

- ***Hệ thống thông tin (Information Systems)***
  - Là một hệ thống gồm con người, dữ liệu và những hoạt động xử lý dữ liệu và thông tin trong một tổ chức.
- **Tài sản của hệ thống thông tin bao gồm:**
  - ✓ Phần cứng
  - ✓ Phần mềm
  - ✓ Dữ liệu
  - ✓ Truyền thông giữa các máy tính của hệ thống
  - ✓ Môi trường làm việc
  - ✓ Con người

Slide: 14

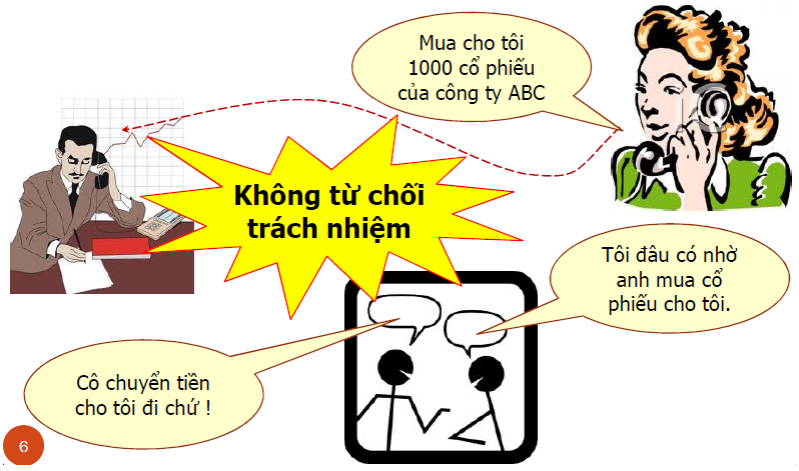
An Toàn thông tin là gì? (Information Security)

Slide: 15

An Toàn thông tin là gì? (Information Security)

Slide: 16

An Toàn thông tin là gì? (Information Security)



Slide: 17

An Toàn thông tin là gì? (Information Security)

- An toàn thông tin bao hàm một lĩnh vực rộng lớn các hoạt động trong một tổ chức. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin và dữ liệu.

- Mục đích là đảm bảo một môi trường thông tin tin cậy, an toàn và trong sạch cho mọi thành viên và tổ chức trong xã hội.

Slide: 18

An Toàn thông tin là gì? (Information Security)

- Hai nguyên tắc của an toàn bảo mật thông tin:
  - Việc thẩm định về bảo mật phải đủ khó và cần tính tới tất cả các tình huống và khả năng tấn công có thể được thực hiện.
  - Tài sản phải được bảo vệ cho tới khi hết gía trị sử dụng hoặc hết ý nghĩa bí mật.
- **An toàn thông tin (information Security):** là đảm bảo cho tính bí mật (Confidence), tính toàn vẹn (Intergrity), tính khả dụng (Availability), tính xác thực (Authenticity), tính chống chối bỏ (Non-repudiation) của thông tin và hệ thống thông tin; chống bị truy nhập sử dụng sửa đổi trái phép; chống tiết lộ, cản trở, phá hoại. An toàn không gian mạng (Cyber Security) là an toàn thông tin trong không gian mạng

Slide: 19

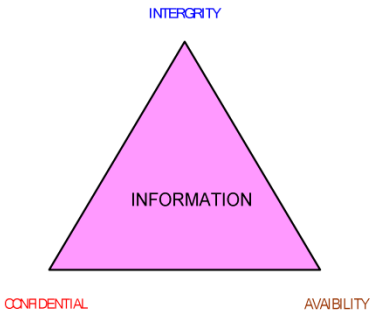
Đảm bảo an toàn thông tin là gì?

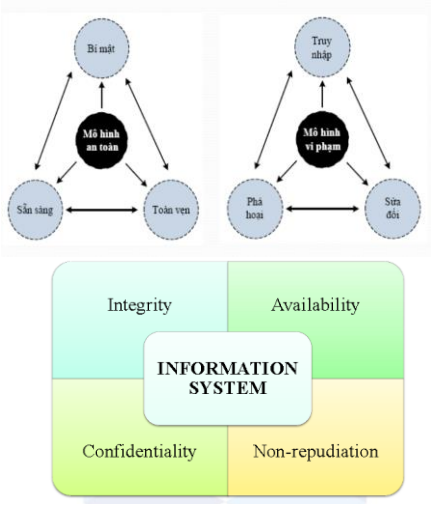
- **Đảm bảo ATTT** là đảm bảo an toàn kỹ thuật cho hoạt động của các cơ sở HTTT, trong đó bao gồm đảm bảo an toàn cho cả phần cứng và phần mềm hoạt động theo các tiêu chuẩn kỹ thuật do nhà nước ban hành; ngăn ngừa khả năng lợi dụng mạng và các cơ sở HTTT để thực hiện các hành vi trái phép; đảm bảo các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng.

Slide: 20

3. Các nguyên tắc nền tảng của An toàn thông tin

- Các tính chất cần thiết để một hệ thống đảm bảo an toàn thông tin

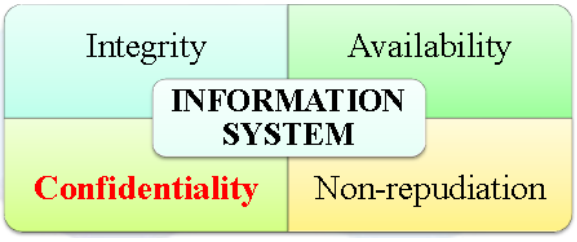




Slide: 21

3. Các nguyên tắc nền tảng của An toàn thông tin

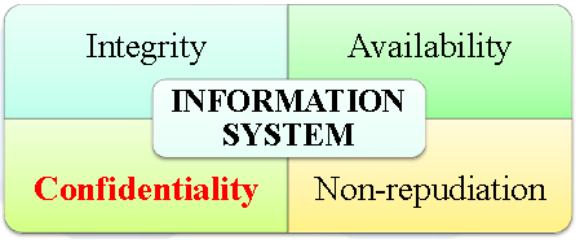
- ***Tính bí mật (Confidentiality)***: bảo vệ dữ liệu không bị lộ ra ngoài một cách trái phép.
  - Ví dụ: Trong hệ thống quản lý sinh viên, một sinh viên được phép xem thông tin kết quả học tập của mình nhưng không được phép xem kết quả học tập của sinh viên khác.



Slide: 22

3. Các nguyên tắc nền tảng của An toàn thông tin

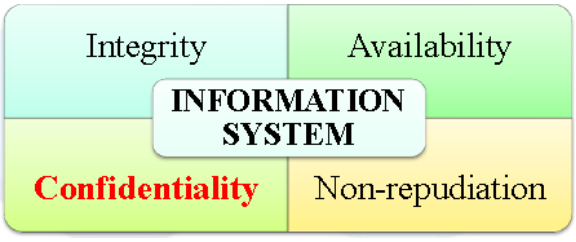
- ***Tính toàn vẹn (Integrity)***: Chỉ những người dùng được ủy quyền mới được phép chỉnh sửa dữ liệu.
  - Ví dụ: Trong hệ thống quản lý sinh viên, không cho phép sinh viên được phép tự thay đổi thông tin kết quả học tập của mình.



Slide: 23

3. Các nguyên tắc nền tảng của An toàn thông tin

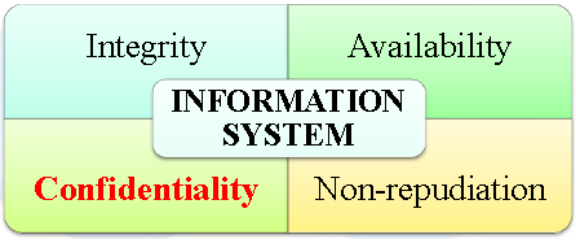
- ***Tính sẵn sàng (Availability)***: Đảm bảo dữ liệu luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền yêu cầu.
  - Ví dụ: Trong hệ thống quản lý sinh viên, cần đảm bảo rằng sinh viên có thể truy vấn thông tin kết quả học tập của mình bất cứ lúc nào.



Slide: 24

3. Các nguyên tắc nền tảng của An toàn thông tin

- ***Tính chống thoái thác (Non-repudiation)***: Khả năng ngăn chặn việc từ chối một hành vi đã làm.
  - Ví dụ: Trong hệ thống quản lý sinh viên, có khả năng cung cấp bằng chứng để chứng minh một hành vi sinh viên đã làm, như đăng ký học phần, hủy học phần.



Slide: 25

Các nguy cơ mất ATTT

- ***Cơ sở hạ tầng mạng***: Cơ sở hạ tầng không đồng bộ, không đảm bảo yêu cầu thông tin được truyền trong hệ thống an toàn và thông suốt.

- ***Thông tin*****:** Dữ liệu chưa được mô hình hóa và chuẩn hóa theo tiêu chuẩn về mặt tổ chức và mặt kỹ thuật. Yếu tố pháp lý chưa được chú trọng trong truyền đưa các dữ liệu trên mạng, nghĩa là các dữ liệu được truyền đi trên mạng phải đảm bảo tính hợp pháp về mặt tổ chức và mặt kỹ thuật.

Slide: 26

Các nguy cơ mất ATTT

- ***Công nghệ***: Chưa chuẩn hóa cho các loại công nghệ, mô hình kiến trúc tham chiếu nhằm đảm bảo cho tính tương hợp, tính sử dụng lại được, tính mở, an ninh, mở rộng theo phạm vi, tính riêng tư vào trong HTTT.
- ***Con người*****:** Sự hiểu biết của những người trực tiếp quản lý, vận hành các HTTT, xây dựng và phát triển hệ thống phần mềm, hệ thống thông tin còn chưa đồng đều và chưa theo quy chuẩn của các cơ quan tổ chức đó.

Slide: 27

Các nguy cơ mất ATTT

Quy trình, quản lý:

- Chưa chuẩn hóa qui trình nghiệp vụ trong vận hành HTTT.
- Chưa chuẩn hóa các thủ tục hành chính, các qui định pháp lý trong việc đảm bảo ATTT.
- Tổ chức quản lý thay đổi hệ thống, ứng dụng chưa đúng cách, chưa chuẩn hóa và có chế tài mang tính bắt buộc thực hiện.
- Như vậy để đảm bảo ATTT thì các cơ quan tổ chức phải làm tốt và hạn chế tối đa 5 yếu tố trên.

Slide: 28

5.Các phương pháp đảm bảo an toàn thông tin

Mô hình các biện pháp đảm bảo ATTT

Slide: 29

5. Các phương pháp đảm bảo an toàn thông tin

- **Các biện pháp công nghệ (Technology):** Bao hàm tất cả các biện pháp phần cứng, các phần mềm, phần sụn cũng như các kỹ thuật công nghệ liên quan được áp dụng nhằm đảm các yêu cầu an toàn của thông tin trong các trạng thái của nó.

Slide: 30

5. Các phương pháp đảm bảo an toàn thông tin

- **Các biện pháp về chính sách và tổ chức (Policy & Practices):** Đưa ra các chính sách, quy định, phương thức thực thi.
- Thực tế cho thấy, ATTT không chỉ đơn thuần là vấn đề thuộc phạm trù công nghệ, kỹ thuật. Hệ thống chính sách và kiến trúc tổ chức đóng một vai trò hữu hiệu trong việc đảm bảo an toàn thông tin.

Slide: 31

5. Các phương pháp đảm bảo an toàn thông tin

Các biện pháp về đào tạo, tập huấn, nâng cao nhận thức (Education, training & Awarenness):

- Các biện pháp công nghệ hay các biện pháp về tổ chức thích hợp phải dựa trên các biện pháp đào tạo, tập huấn và tăng cường nhận thức để có thể triển khai đảm bảo an toàn thông tin từ nhiều hướng khác nhau.
- Các nhà nghiên cứu và các kỹ sư cũng cần phải hiểu rõ các nguyên lý an toàn hệ thống thông tin, thì mới mong các sản phẩm và hệ thống do họ làm ra đáp ứng được các nhu cầu về an toàn thông tin của cuộc sống hiện tại đặt ra.

Slide: 32

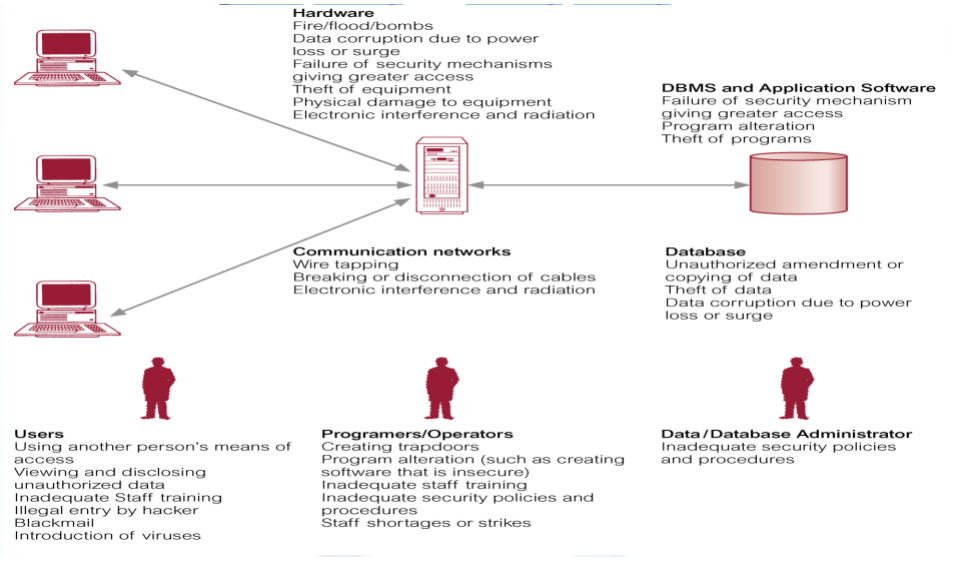
5. Các phương pháp đảm bảo an toàn thông tin

Biện pháp hợp tác quốc tế

- Hợp tác với các quốc gia có kinh nghiệm, kế thừa những thành tựu khoa học của các quốc gia đi trước trong vấn đề đảm bảo ATTT.
- Xây dựng các quy chế phối hợp với các cơ quan tổ chức quốc tế trong ứng phó các sự cố về ATTT.

Slide: 33

6. Các thành phần cần bảo vệ trong hệ thống thông tin



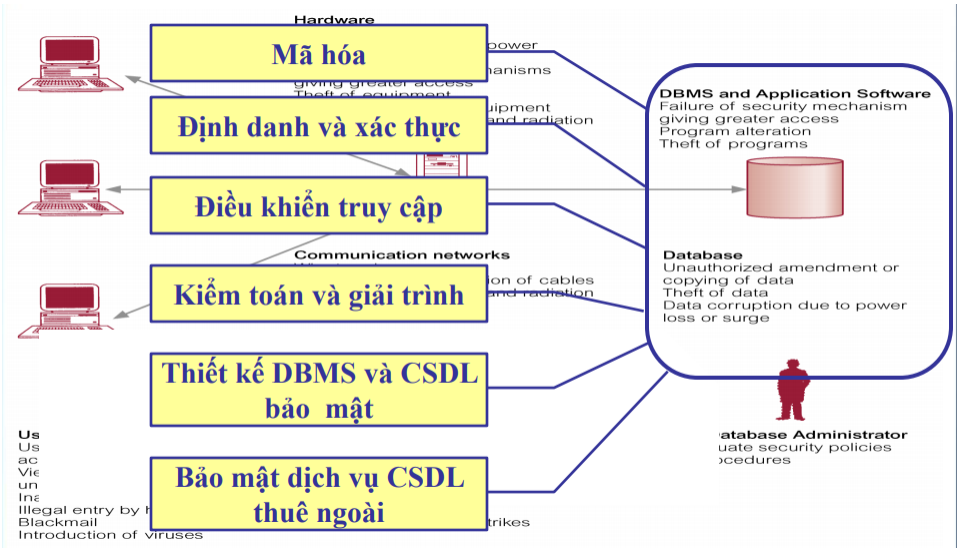
Slide: 34

Các thành phần cần bảo vệ trong hệ thống thông tin

- Phần cứng
- Mạng
- Cơ sở dữ liệu (CSDL)
- Hệ quản trị CSDL (database management system - DMBS), các ứng dụng
- Người dùng
- Người lập trình hệ thống
- Người quản trị CSDL

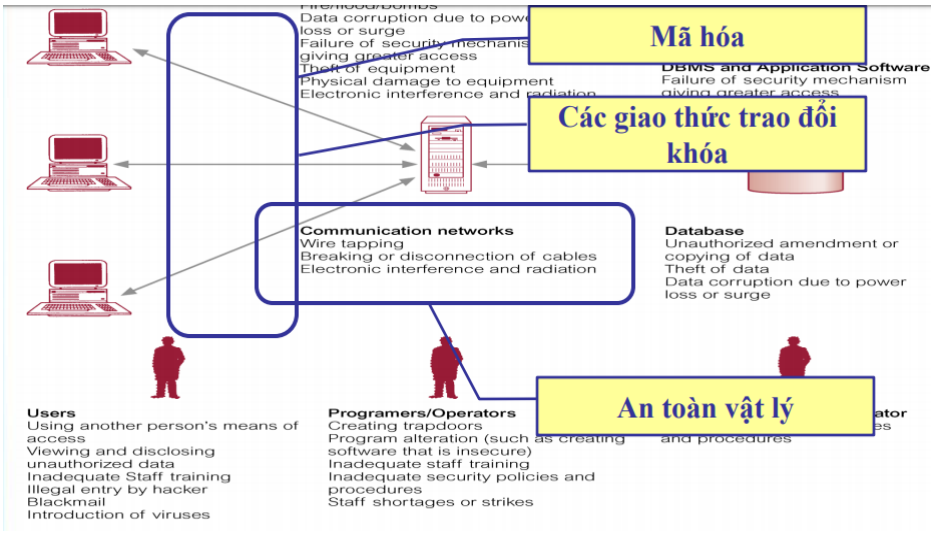
Slide: 35

Các phương pháp bảo vệ hệ thống thông tin



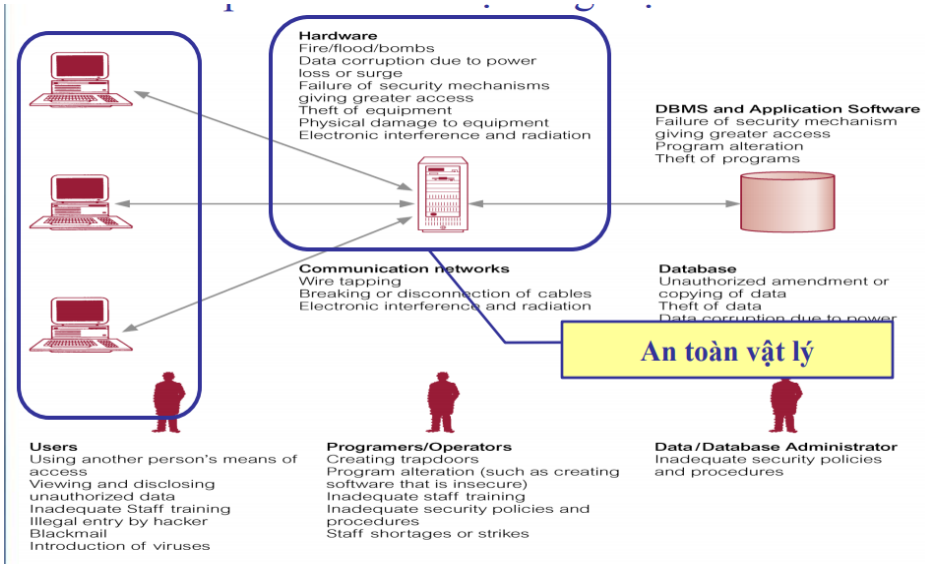
Slide: 36

Các phương pháp bảo vệ hệ thống thông tin



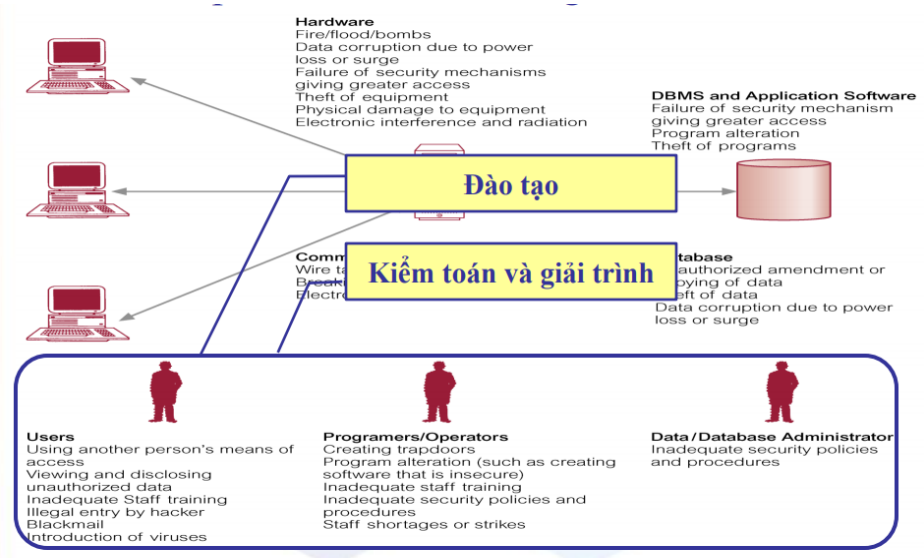
Slide: 37

Các phương pháp bảo vệ hệ thống thông tin



Slide: 38

Các phương pháp bảo vệ hệ thống thông tin



Slide: 39

4. Tầm quan trọng an toàn thông tin đối với xã hội/ doanh nghiệp/ cá nhân

- Quản lý và bảo mật thông tin nhân sự trong tổ chức cần được ưu tiên hàng đầu. Nguồn nhân lực chính là tài sản quý giá đối với mọi doanh nghiệp. Thông tin của nhân viên về chức vụ phòng ban, lương thưởng, nhiệm vụ đảm nhận,… có liên quan mật thiết đến các chiến lược của một doanh nghiệp.

- Do đó, việc để lọt những thông tin cá nhân của nhân viên và dữ liệu liên quan đến quản lý nhân sự cho đối tượng bên ngoài biết được sẽ là một bất lợi vô cùng lớn.

Slide: 40

Hậu quả khi thông tin của nhân viên bị tiết lộ ra bên ngoài

- Tin tặc có thể đem những thông tin như họ tên, địa chỉ nơi ở, email, số điện thoại… bán lại cho các doanh nghiệp khác sử dụng với mục đích tiếp thị.
- Cá nhân bị lộ thông tin có thể nhận hàng tá cuộc gọi, email, tin nhắn quảng cáo mỗi ngày, gây ra nhiều phiền nhiễu trong cuộc sống. Thậm chí, kẻ gian có thể lợi dụng những dữ liệu thu thập được để lừa đảo.
- Các thông tin liên quan đến tài khoản ngân hàng bị rò rỉ có thể gây thất thoát tài sản của cá nhân của nhân viên nếu không có biện pháp xử lý kịp thời. Bên cạnh đó, việc thông tin cá nhân bị tiết lộ cũng gây ra hoang mang, lo lắng khiến nhân viên mất niềm tin vào doanh nghiệp.

Slide: 41

Hậu quả khi thông tin của nhân viên bị tiết lộ ra bên ngoài

- Nếu thông tin của nhân viên rơi vào tay của đối thủ, doanh nghiệp sẽ đứng trước nguy cơ khủng hoảng nội bộ nghiêm trọng.
- Những thông tin quan trọng như chức vụ của nhân viên, các nhiệm vụ đã và đang đảm nhận và chế độ lương thưởng,… có thể bị các nhà tuyển dụng bên ngoài lợi dụng để chèo kéo nhân viên với vị trí tốt hơn, mức lương cao và phúc lợi tốt hơn.
- Doanh nghiệp có thể bị mất đi những nhân viên chủ lực, tài giỏi. Đánh mất nhân sự vào tay đối thủ sẽ gây ra sự xáo trộn trong bộ máy tổ chức, ảnh hưởng rất lớn đến các hoạt động và hiệu quả kinh doanh.
- Nếu đối thủ nắm trong tay những thông tin về sơ đồ tổ chức thì sẽ dễ dàng nắm được quy trình vận hành cũng như những ý định chiến lược của doanh nghiệp. Từ đó có những hành động gây bất lợi đến công ty.

Slide: 42

Một số lưu ý giúp doanh nghiệp bảo mật dữ liệu một cách hiệu quả

- Lên kế hoạch đồng bộ hóa và sao lưu dữ liệu một cách thường xuyên với nền tảng lưu trữ uy tín, nhất là sau khi có sự thay đổi và cập nhật mới nhân sự. Luôn có kịch bản ứng phó kịp thời khi sự cố xảy ra, tránh mất dữ liệu.
- Thiết lập một hệ thống mạng nội bộ an toàn bằng cách sử dụng chương trình, phần mềm hỗ trợ tính năng bảo mật cao. Nếu được, doanh nghiệp nên có chuyên viên có kiến thức về an ninh, bảo mật dữ liệu của doanh nghiệp chịu trách nhiệm về giám sát việc thực hiện các biện pháp an ninh, các quy trình đảm bảo an toàn dữ liệu.

Slide: 43

Một số lưu ý giúp doanh nghiệp bảo mật dữ liệu một cách hiệu quả

- Bảo mật hệ thống thiết bị làm việc bằng cách: Sử dụng phần mềm mã hóa dữ liệu; Cài đặt Phần mềm Anti-Virus có bản quyền và bật đầy đủ tính năng; Luôn cập nhật những phiên bản hệ điều hành mới nhất.
- Xây dựng chính sách bảo mật rõ ràng theo từng cấp bậc, chức vụ.
- Phân quyền truy cập vào hệ thống dữ liệu: Chỉ Ban lãnh đạo và phòng ban có liên quan mới xem và thao tác với các dữ liệu liên quan đến thông tin về nhân sự.
- Nâng cao nhận thức của nhân viên về bảo mật thông tin cá nhân cũng như của doanh nghiệp. Có những tài liệu hướng dẫn về kỹ thuật cũng như lưu ý, hỗ trợ nhân viên của mình trong việc bảo vệ thông dữ liệu.

Slide: 44

7. Câu hỏi và bài tập

- Câu 1: Trình bày các khái niệm về tính bí mật, tính sẵn sàng và tính an toàn trong ATTT?
- Câu 2: Trình bày một số kiểu tấn công mạng?
  - Tấn công quét mạng
  - Tấn công từ chối dịch vụ
  - Tấn công mã độc
  - Tấn công kỹ nghệ xã hội
- Câu 3: Trình bày và phân tích các giải pháp bảo đảm ATTT?
- Câu 4: Trình bày tổng quan về thực trạng ATTT trên thế giới và tại Việt Nam?

Slide: 45

7. Câu hỏi và bài tập

- 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.elearning.vinhuni.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 nêu và giải thích ít nhất 4 tính cần thiết của an toàn HTTT đối với website của trung tâm.

Slide: 46

7. Câu hỏi và bài tập

- Công ty VCCloud là một trong nhiều công ty viễn thông, cung cấp các dịch vụ CDN cho các cá nhân và doanh nghiệp tại Việt Nam. Dịch vụ CDN là mạng lưới gồm nhiều máy chủ lưu trữ đặt tại nhiều vị trí địa lý khác nhau, cùng làm việc chung để phân phối nội dung, truyền tải hình ảnh, CSS, Javascript, Video clip, Real-time media streaming, File download đến người dùng cuối. Cơ chế hoạt động của CDN giúp cho khách hàng truy cập nhanh vào dữ liệu máy chủ web gần họ nhất thay vì phải truy cập vào dữ liệu máy chủ web tại trung tâm dữ liệu.
- Hãy nêu và giải thích ít nhất 4 tính cần thiết của an toàn HTTT đối với công ty/doanh nghiệp được mô tả ở trên

Slide: 47

Xin chân thành cảm ơn!