Nội dung trình bày

- Vấn đề về an toàn bảo mật hệ thống thông tin
- Phạm vi về an toàn bảo mật hệ thống thông tin
- Mục tiêu của an toàn bảo mật hệ thống thông tin
- Các nguồn nguy cơ và quy trình quản lý nguy cơ

Chương 1. Tổng quan

- Một số khái niệm
  - Khái niệm thông tin: Dữ liệu đưa lại tri thức.
    - Các loại hình khác nhau của dữ liệu: Lưu trữ trên máy tính, lưu trữ thiết bị lưu trữ điện tử, bản in, …
    - Đưa lại giá trị cho người khai thác
  - Hệ thống thông tin: Phần cứng phần mềm xử lý dữ liệu
    - Bao gồm phần cứng, phần mềm
    - Xử lý dữ liệu

Chương 1. Tổng quan

- Một số khái niệm
  - Bảo mật thông tin
    - Sự tự do trước tấn công
  - Đe dọa
    - Bất lợi có thể xảy ra với hệ thống
  - Nguy cơ
    - Những đe dọa, và đánh giá khả năng xảy ra với hệ thống

Chương 1. Tổng quan

- Phạm vi của vấn đề
  - Không giới hạn dữ liệu điện tử và các vấn đề liên quan đến máy tính
  - Không giới hạn vấn đề tấn công mạng máy tính mà tất cả các quy trình liên quan đến xử lý dữ liệu
  - Không giới hạn vấn đề liên quan đến tấn công mà liên quan đến vấn đề đảm bảo an toàn

Chương 1. Tổng quan

- Một số vấn đề về thực trạng ở Việt Nam
  - Bài: Tổng quan về an toàn an ninh thông tin, Lê Trung Nghĩa, văn phòng phối hợjp phát triển môi trường khoa học & công nghệ, bộ khoa hộc & công nghệ (Security-FOSS-th12-2012)
  - Bài: NGUY CƠ MẤT AN NINH, AN TOÀN THÔNG TIN, DỮ LIỆU VÀ MỘT SỐ GIẢI PHÁP KHẮC PHỤC, PGS.TS Phương Minh Nam

Chương 1. Tổng quan

- Một số vấn đề về thực trạng ở Việt Nam
  - Bài: Báo cáo an toàn thông tin phia nam năm 2012.
    - Microsoft số website bị tấn công tăng: 300 -> 2500
    - Số lượng máy tính nhiễm mã độc 18/1000 so với 7/1000 của thế giới
    - Ngoài mã độc, tấn công phần mềm xuất hiện quan ngại về sự không an toàn từ phần cứng

Chương 1. Tổng quan

- Một số vấn đề về thực trạng ở Việt Nam

Loại doanh nghiệp	**Tỉ lệ**
Tổ chức Hành chính sự nghiệp trực thuộc Trung Ương	1.8 %
Tổ chức Hành chính sự nghiệp trực thuộc địa phương	19.6 %
Doanh nghiệp Nhà nước	8%
Doanh nghiệp ngoài quốc doanh	34.7%
Doanh nghiệp nước ngoài, liên doanh, có vốn nước ngoài	28.9%
Tổ chức phi chính phủ	11.6%
Khác	13.3%

Chương 1. Tổng quan

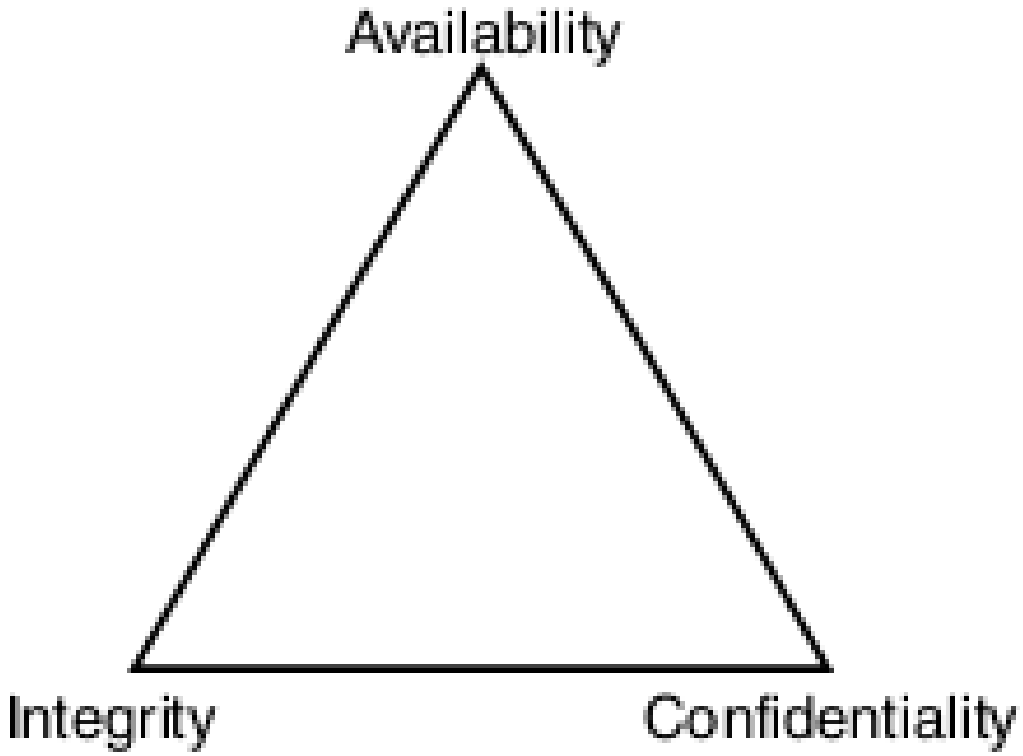
- Một số vấn đề về thực trạng ở Việt Nam
  - Một số kết luận của bài báo cáo thấy sự quan tâm đã tăng lên nhưng vẫn chưa đáp ứng được vấn đề
  - Nhiều người còn nhầm lẫn chỉ dừng lại ở vấn đề máy tính, mạng

Chương 1. Tổng quan

- Mục tiêu: Bảo vệ tài nguyên của tổ chức, đảm bảo thực hiện tốt nhất nhiệm vụ. Dựa trên thành phần:
  - Phục vụ nhiệm vụ của tổ chức
  - Dựa trên trách nhiệm trung thành và tận tụy
  - Dựa trên yếu tố hiệu quả: triển khai dựa trên đánh giá đúng
  - Dựa trên trách nhiệm và đánh giá: ai vai trò, trách nhiệm
  - Dựa trên trách nhiệm người sở hữu, quản lý
  - Toàn diện, tích hợp các công đoạn
  - Đánh giá, thay đổi phù hợp

Chương 1. Tổng quan

- Ba mục tiêu chính bảo vệ tài sản



Chương 1. Tổng quan

- Tính toàn vẹn
  - Cung cấp đúng thông tin
  - Cung cấp chính xác thông tin
- Tính cẩn mật
  - Thông tin chỉ được truy cập người được phép
- Tính sẵn sàng
  - Đáp ứng khi có yêu cầu
  - Vấn đề: thảm họa, tấn công từ bên ngoài

Chương 1. Tổng quan

- Các nguồn tấn công hệ thống thông tin
  - Nguồn tấn công hệ thống
    - Nhân viên tham gia hệ thống
    - Tấn công từ bên ngoài
  - Điều tra: Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare
    - 80% tội phạm tiềm tàng từ nhân viên
    - Còn lại là: các đối thủ, nhân sự hợp đồng, nhóm lợi ích cộng đồng, nhà cung cấp, và chính phủ các quốc gia khác

Chương 1. Tổng quan

- Các loại lỗi
  - Bỏ quên và lỗi - 65%
  - Nhân viên bất lương chiếm 13%
  - Những nhân viên chán việc 10%
  - Những mất mát bởi thiết bị vật lý hoặc cơ sở hạ tầng – 8%
  - Vấn đề cuối cùng là các hacker, cracker 5-8%

Chương 1. Tổng quan

- Các loại hình tấn công
  - Tấn công kỹ thuật
  - Tấn công xã hội
  - Kết hợp các loại hình tấn công trên

Chương 1. Tổng quan

- Giải pháp
  - Không thể chỉ dừng lại giải pháp về kỹ thuật: khóa, các phần mềm, …
  - Cần có chương trình về an toàn bảo mật hệ thống thông tin
    - Phân tích đánh giá
    - Thiết lập chính sách, quy định, chỉ dẫn
    - Truyền thông, tuyên truyền
    - Đánh giá, tuân thủ, phát triển

Chương 1. Tổng quan

- Nguy cơ: là khả năng bất lợi có thể xảy ra
- Quá trình quản lý nguy cơ
  - Xác định nguy cơ
  - Ước định khả năng xảy ra
  - đưa ra những bước để giảm nguy cơ đến mức cho phép được

Chương 1. Tổng quan

- Thực hiện quản lý nguy cơ
  - 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)

Chương 1. Tổng quan

- Đề xuất các điều khiển
  - Ưu tiên cho vấn đề sản xuất
  - Quan tâm đến chi phí: ban đầu, duy trì
  - Tính phù hợp với các mô hình: công ty nhiều chi nhánh, quốc gia
  - Có thể chấp nhận tồn tại nguy cơ, trong trường hợp đã được xem xét kỹ
    - Mô hình của nguy cơ có thể khác nguy cơ trước
    - Nguy cơ là kỹ thuật và khó có thể nắm bắt được
    - Mô trường hiện tại có thể làm khó xác định được nguy cơ

Chương trình bảo vệ thông tin điển hình

- Các lĩnh vực quan tâm
  - Điều khiển Firewall (Firewall control)
  - Phân tích nguy cơ (Risk analysis)
  - Phân tích sự tác động công việc (Business Impact Analysis - BIA)
  - Đội phản ứng virus và điều khiển virus (Virus control and virus response team)
  - Đội phản ứng khẩn cấp máy tính (Computer Emergency Response Team - CERT)

Chương trình bảo vệ thông tin điên hình

- Điều tra tội phạm máy tính (Computer crime investigation)
- Quản lý các bản ghi (Records management)
- Mã hoá (Encryption)
- Các chính sách về internet, thư điện tử (E-mail, voice-mail, Internet, video-mail policy)
- Chương trình bảo vệ thông tin trong công ty mở rộng (Enterprisewide information protection program)

Chương trình bảo vệ thông tin điên hình

- Điều tra tội phạm máy tính (Computer crime investigation)
- Quản lý các bản ghi (Records management)
- Mã hoá (Encryption)
- Các chính sách về internet, thư điện tử (E-mail, voice-mail, Internet, video-mail policy)
- Chương trình bảo vệ thông tin trong công ty mở rộng (Enterprisewide information protection program)

Chương trình bảo vệ thông tin điên hình

- Điều khiển gián điệp công nghiệp (Industrial espionage controls)
- Chấp nhận không công khai thông tin trong hợp đồng nhân sự (Contract personnel nondisclosure agreements)
- Phát hành pháp luật, qui định (Legal issues)
- Quản lý internet (Internet monitoring)
- Kế hoạch thảm hoạ (Disaster planning)
- Kế hoạch công việc liên tục (Business continuity planning)

Chương trình bảo vệ thông tin điên hình

- Chữ ký điện tử (Digital signature)
- Bảo mật đăng nhập đơn (Secure single sign-on)
- Phân loại thông tin (Information classification)
- Mạng nội bộ (Local area networks)
- Điều khiển modem (Modem control)
- Truy xuất từ xa (Remote access)
- Chương trình quan tâm đến bảo mật (Security awareness programs)

Nội dung trình bày

- Có sự phát triển theo các năm
- An toàn bảo mật hệ thống thông tin là tổng thể cho hệ thống
- Mục tiêu nhiệm vụ công việc. 3 mục tiêu theo sơ đồ
- Các nguồn nguy cơ và quy trình quản lý nguy cơ

Bài tập

- Khảo sát một hệ thống thông tin có thể tiếp cận được (thư viện, ql điểm,…)
  - Những quy định (chính sách, thủ tục, chỉ dẫn) liên quan đến vấn đề an toàn bảo mật thông tin
  - Các giải pháp kỹ thuật đã được áp dụng bảo vệ hệ thống
  - Phân tích các loại tài sản cần được bảo vệ
  - Những yếu tố liên quan đến 3 mục tiêu cần bảo vệ của hệ thống là gì?

Tham khảo

- Báo cáo 1 (http://www.mediafire.com/view/?8g6hugr1wbkxnzn)
- Báo cáo 2 (http://www.mediafire.com/view/?oih5nn4ovnzj8vp)
- Báo cáo 3 (http://www.mediafire.com/view/?9dw7pt9klc897y3)