Hệ thống thông tin quản lí

Chương 6:Kiểm soát hệ thống thông tin

Chương6.
Kiểm soát hệ thống thông tin

Nội dung

- Hệ thống kiểm soát
- Phân loại rủi ro
- Bảo mật dữ liệu

Hệ thống kiểm soát

- Kiểm soát nội bộ trong HTTT
- Kiểm soát chung
- Kiểm soát ứng dụng

Kiểm soát nội bộ trong HTTT

- Các gian lận trong HTTT
  - Thay đổi dữ liệu nhập
  - Trojan Horse
  - Kỹ thuật Salami: gian lận số nhỏ
  - Kỹ thuật Superzapping: gian lận trong tình trạng kiểm soát yếu
  - Kỹ thuật Logic Bomb: phá hoại định kỳ hoặc phá hoại tại thời điểm thích hợp
  - Tìm kiếm trên các dấu vết khác
  - Giả danh hệ thống
  - Giả danh nhân viên
  - Tiếp cận nhân viên
  - Cài đặt thiết bị theo dõi
  - Cài đặt, giả mạo thiết bị nhập
  - Cài đặt, giả mạo, thay đổi thiết bị truyền tin

Kiểm soát chung

- Các hoạt động kiểm soát liên quan đến toàn bộ hệ thống xử lý và ảnh hưởng đến tất cả các hệ thống ứng dụng xử lý nghiệp vụ
- Nhằm đảm bảo toàn bộ hệ thống được vận hành ổn định và được quản trị tốt

Kiểm soát chung

1. Xác lập kế hoạch an ninh
2. Phân chia trách nhiệm
3. Kiểm soát dự án phát triển
4. Kiểm soát thâm nhập vật lý
5. Kiểm soát truy cập hệ thống
6. Kiểm soát lưu trữ dữ liệu
7. Kiểm soát truyền tải dữ liệu
8. Chuẩn hóa tài liệu hệ thống
9. Thời gian chết của hệ thống
10. Kiểm soát dấu vết
11. Kiểm soát phục hồi dữ liệu

1. Xác lập kế hoạch an ninh

- Kế hoạch an ninh
  - Ai cần thông tin? Khi nào? Ở đâu? Để làm gì? Vị trí nào trong hệ thống cung cấp thông tin? Mức độ cung cấp thông tin?
- Rủi ro mang tính hệ thống nhất là thiếu kế hoạch an ninh
- Kế hoạch an ninh phải được thường xuyên xem xét, đánh giá lại
- Các cấp lãnh đạo phải xác lập, giám sát, thúc ép toàn bộ nhân viên thực hiện kế hoạch an ninh

2. Phân chia trách nhiệm

- Hạn chế sự kiêm nhiệm của nhân viên
- Phân chia quyền lợi và trách nhiệm cụ thể
  - Chức năng phân tích hệ thống
  - Chức năng lập trình
  - Vận hành hệ thống
  - Người dùng hệ thống
  - Quản trị dữ liệu
  - Kiểm soát dữ liệu

3. Kiểm soát dự án phát triển

- Dự án phát triển hệ thống phải được kiểm soát để đảm bảo
  - Thời gian phát triển hợp lý
  - Giảm thiểu chi phí
  - Hệ thống hiệu quả
- Kiểm soát dự án bao gồm
  - Kế hoạch chiến lược
  - Kế hoạch phát triển dự án
  - Lịch trình xử lý dữ liệu
  - Quy định trách nhiệm
  - Đánh giá thực hiện dự án định kỳ
  - Đánh giá việc thực hiện chuyển đổi
  - Đo lường việc thực hiện hệ thống

4. Kiểm soát thâm nhập vật lý

- Kiểm soát hành vi sử dụng máy tính và các thiết bị trong hệ thống
  - Trang thiết bị phải đặt trong phòng có sự bảo vệ và chỉ có người có quyền mới được sử dụng
  - Cần các thiết bị giám sát, cảnh báo
  - Giới hạn truy xuất từ xa
  - Huấn luyện, cập nhật kiến thức vận hành, an ninh
  - Giám sát các hoạt động trên máy tính
  - Thuê chuyên giá đánh giá bảo mật
  - Mã hóa dữ liệu

5. Kiểm soát truy cập hệ thống

- Giới hạn đến từng nhóm, từng người dùng các quyền truy cập hệ thống, quyền truy cập dữ liệu, quyền sử dụng các chức năng của hệ thống
- Các quyền: sử dụng chức năng, đọc, ghi, thêm, xóa, sửa dữ liệu, quyền cấp quyền
- Biện pháp
  - Phân quyền và kiểm soát truy cập: mật khẩu, nhận dạng cá nhân, nhận dạng sinh học,…
  - Kiểm tra thủ tục kiểm soát: lưu dấu vết truy cập, kiểm tra tính tương thích chức năng

5. Kiểm soát truy cập hệ thống

Ví dụ: ma trận kiểm tra tính tương thích chức năng

Người dùng		Chức năng			
Tên	Mật khẩu	Phiếu xuất kho	Hóa đơn GTGT	Bảng lương	Phân bổ TSCĐ
Trang	abc123	2	0	0	0
Bình	tuvucs	1	2	0	0
Tuấn	97821ab	0	0	2	0
Sinh	09871nnc	1	0	1	2
Hùng	a4786c	1	1	1	3

0: không có quyền 1: chỉ đọc
2: đọc, thêm mới, sửa 3: đọc, thêm mới, sửa, xóa

6. Kiểm soát lưu trữ dữ liệu

- Kiểm soát thiết bị lưu trữ
  - Đảm bảo an toàn vật lý cho thiết bị lưu trữ
  - Dán nhãn, đặt tên, phân loại, sắp xếp theo thời gian
  - Thay thế định kỳ và hủy thiết bị không sử dụng nữa
  - Bảo quản thiết bị ở nơi an toàn ngoài phạm vi tổ chức
- Kiểm soát sao lưu dự phòng

6. Kiểm soát lưu trữ dữ liệu

- Kiểm soát thiết bị lưu trữ
- Kiểm soát sao lưu dự phòng
  - Phương pháp sao lưu
  - Thời gian sao lưu
  - Quy trình sao lưu
  - Quy trình phục hồi
  - Trách nhiệm cá nhân người sao lưu/phục hồi

7. Kiểm soát truyền tải dữ liệu

- Thường xuyên giám sát mạng máy tính
- Tăng cường thủ tục bảo trì, sao lưu
- Mã hóa dữ liệu truyền
- Kiểm tra dữ liệu truyền chính xác
- Xác thực nơi gửi và nơi nhận

8. Chuẩn hóa tài liệu hệ thống

- Tài liệu quản trị
  - Thủ tục, quy định của quy trình xử lý
  - Thủ tục và quyền sử dụng hệ thống
  - Các tài liệu phát triển hệ thống
- Tài liệu ứng dụng
  - Mô tả ứng dụng
  - Cách nhập/xuất dữ liệu
  - Các lỗi hệ thống và hướng xử lý lỗi
- Tài liệu vận hành
  - Cấu hình phần cứng yêu cầu
  - Cách cấu hình phần mềm
  - Các nguy cơ gây lỗi hệ thống và cách khắc phục

9. Thời gian chết của hệ thống

- Bảo trì định kỳ trang thiết bị trong hệ thống
- Thay thế trang thiết bị hư hỏng hoặc sắp hết hạn sử dụng
- Sử dụng hệ thống điện ổn định
- Hạn chế mức thấp nhất thời gian hệ thống ngừng đột ngột hoặc ngừng hoàn toàn

10. Kiểm soát dấu vết

- Hệ thống phải hỗ trợ tạo ra các dấu vết nghiệp vụ
- Hạn chế việc chỉnh sửa dữ liệu
- Định kỳ khóa sổ dữ liệu và không được chỉnh sửa dữ liệu đã khóa sổ
- Tự động ghi nhận các hành vi truy cập hệ thống (logging)
- Dữ liệu logging phải có mức bảo mật cao nhất, người có quyền cao nhất cũng chỉ có quyền đọc, không có quyền thêm, sửa, xóa

11. Kiểm soát phục hồi dữ liệu

- Có kế hoạch phục hồi trong trường hợp hệ thống bị hư hại
- Kế hoạch vận hành tối thiểu
- Sao lưu dự phòng kể cả dữ liệu và chương trình
- Xác định trách nhiệm của nhóm phục hồi
- Mua bảo hiểm cho hệ thống
- Sử dụng dịch vụ sao lưu và phục hồi

Kiểm soát ứng dụng

- Kiểm soát liên quan đến hoạt động xử lý của một ứng dụng cụ thể
- 1. Kiểm soát nhập liệu
  - 1.1. Nguồn nhập liệu
  - 1.2. Quá trình nhập liệu
- 2. Kiểm soát quá trình xử lý dữ liệu
- 3. Kiểm soát thông tin đầu ra

Kiểm soát nguồn nhập liệu

- Đánh số và sắp xếp chứng từ gốc
- Sử dụng chứng từ luân chuyển
- Chứng từ/nghiệp vụ cần được phê duyệt
- Đánh dấu chứng từ đã nhập
- Kiểm tra tính hợp lệ của chứng từ trước khi nhập
- Dữ liệu nhập trực tiếp từ nghiệp vụ
- Tạo dữ liệu kiểm tra

Kiểm soát quá trình nhập liệu

- Kiểm tra tính tuần tự khi nhập liệu
- Kiểm tra miền giá trị của dữ liệu nhập
- Kiểm tra tính hợp lý
- Kiểm tra tính có thực
- Kiểm tra giới hạn
- Kiểm tra tính đầy đủ
- Kiểm tra nhập trùng
- Số kiểm soát
- Định dạng nhập dữ liệu
- Giá trị tự động
- Thông báo lỗi và hướng xử lý lỗi

Kiểm soát quá trình xử lý

- Kiểm tra ràng buộc toàn vẹn dữ liệu
- Kiểm tra dữ liệu hiện hành
- Kiểm soát trình tự xử lý
- Kiểm soát dữ liệu phù hợp
- Báo cáo yếu tố bất thường
- Đối chiếu với dữ liệu ngoài
- Lập trình các kiểm soát

Kiểm soát thông tin đầu ra

- Thông tin trên kết xuất phải đầy đủ và hình thức phải phù hợp
- Chuyển giao chính xác đến người cần sử dụng và có quyền sử dụng
- Người sử dụng có trách nhiệm kiểm tra lại tính chính xác, đầy đủ và trung thực của thông tin đã kết xuất
- Quy định việc hủy kết xuất khi không còn sử dụng nữa
- Tăng cường bảo mật mạng để bảo vệ thông tin truyền qua mạng

2. Phân loại rủi ro

2.1. Define viruses, worms, and Trojans.

2.2. Define adware, spyware, and grayware.

2.3. Spam

2.4. Explain TCP/IP attacks.

2.2.1. Viruses

- A virus is a program written with malicious intent and sent out by attackers
- A virus is attached to small pieces of computer code, software, or documents
- The virus executes when the software is run on a computer
- The virus is transferred to another computer through e-mail, file transfers, and instant messaging
- The virus hides by attaching itself to a file on the computer
- When the file is accessed, the virus executes and infects the computer
- Viruses may even alter or destroy information on a computer

2.2.2. Worm

- A worm is a self-replicating program that is harmful to networks
- A worm uses the network to duplicate its code to the hosts on a network
- Worm does not damage data or applications on the hosts it infects, it is harmful to networks because it consumes bandwidth

2.2.3. Trojan

- A Trojan is technically a worm. The Trojan does not need to be attached to other software. Instead, a Trojan threat is hidden in software that appears to do one thing, and yet behind the scenes it does another.
- Trojans are often disguised(cải trang) as useful software
- The Trojan program can reproduce like a virus and spread to other computers

2.2.4. Adware, spyware, and grayware

- Adware, spyware, and grayware are usually installed on a computer without the knowledge of the user.
  - **Adware** is a software program that displays advertising on your computer, is usually distributed with downloaded software.
  - **Grayware or malware** is a file or program other then a virus that is potentially harmful. Many grayware attacks are phishing(lừa đảo) attacks that try to persuade the reader to unknowingly provide attackers with access to personal information. As you fill out an online form, the data is sent to the attacker.
  - **Spyware**, a type of grayware, is similar to adware. the spyware monitors activity on the computer. The spyware then sends this information to the organization responsible for launching(thả, lao vào) the spyware

2.2.5.Spam

- Spam is unsolicited(không yêu cầu) e-mail.
- Spam is used as a method of advertising. However, spam can be used to send harmful links or deceptive(lừa đảo) content.
- Spam may include links to an infected website or an attachment that could infect a computer.

Bảo mật dữ liệu

- Virus protection software
  - Anti-virus software, is software designed specifically to detect, disable, and remove viruses, worms, and Trojans before they infect a computer.
  - Anti-virus software becomes outdated quickly, however, and it is the responsibility of the technician to apply the most recent updates, patches, and virus definitions as part of a regular maintenance schedule

Protect data

- **Password Protection**
- **Data Encryption (mã hóa)**
- **Port Protection**
- **Data Backups**
- **File System Security**

Password Protection

- Two levels of password protection are recommended:
  - BIOS – Prevents BIOS settings from being changed without the appropriate password
  - Login – Prevents unauthorized access to the network
    - Passwords should expire after a specific period of time.
    - Passwords should contain a mixture of letters and numbers so that they cannot easily be broken.

Data Encryption

- Encrypting data uses codes and ciphers.

- Traffic between resources and computers on the network can be protected from attackers monitoring or recording transactions by implementing encryption.

Port Protection

- Every communication using TCP/IP is associated with a port number. HTTPS, for instance, uses port 443 by default.
- A firewall is a way of protecting a computer from intrusion through the ports.
- The user can control the type of data sent to a computer by selecting which ports will be open and which will be secured.

Data Backups

- Data can be lost or damaged in circumstances such as theft, equipment failure, or a disaster such as a fire or flood.

- Backing up data is one of the most effective ways of protecting against data loss.

File System Security

- FAT 32
- NTFS