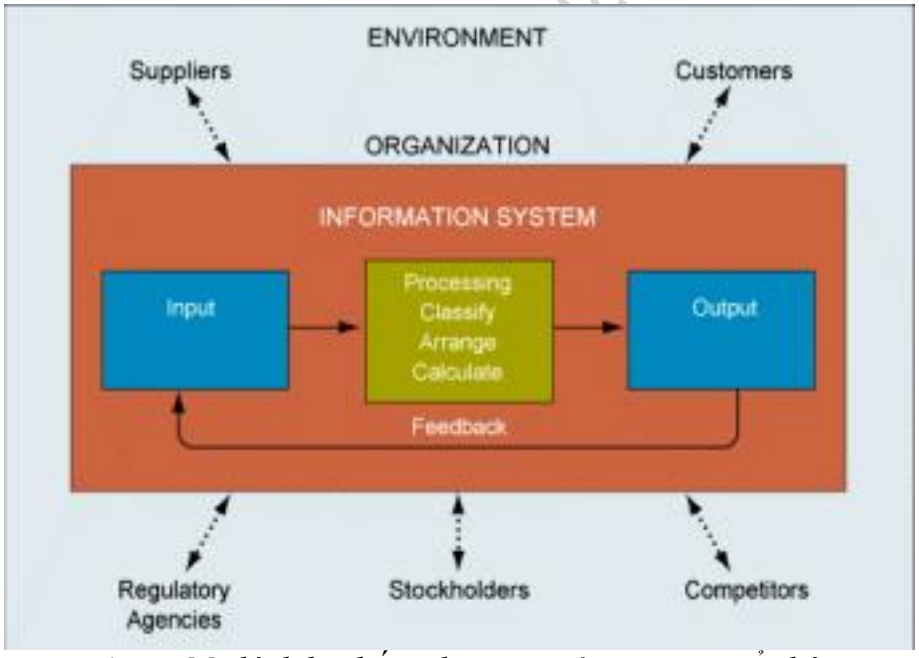
1. Khái quát về an toàn hệ thống thông tin

1.1 Các thành phần của hệ thống thông tin



Hình 1.9. Mô hình hệ thống thông tin của cơ quan, tổ chức

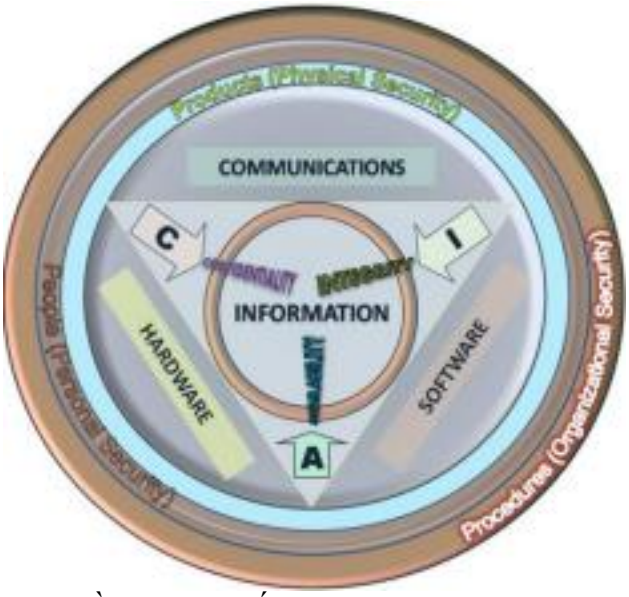
Hệ thống thông tin (Information system), theo cuốn sách Fundamentals of Information Systems Security [2] là một hệ thống tích hợp các thành phần nhằm phục vụ việc thu thập, lưu trữ, xử lý thông tin và chuyển giao thông tin, tri thức và các sản phẩm số. Trong nền kinh tế số, hệ thống thông tin đóng vai trò rất quan trọng trong hoạt động của các tổ chức, cơ quan và doanh nghiệp (gọi chung là tổ chức). Có thể nói, hầu hết các tổ chức đều sử dụng các hệ thống thông tin với các quy mô khác nhau để quản lý các hoạt động của mình. Hình 1.9 minh họa mô hình một hệ thống thông tin điển hình. Trong mô hình này, mỗi hệ thống thông tin gồm ba thành phần chính: (i) thành phần thu thập thông tin (Input), (ii) thành phần xử lý thông tin (Processing) và (iii) thành phần kết xuất thông tin (Output). Hệ thống thông tin được sử dụng để tương tác với khách hàng (Customers), với nhà cung cấp (Suppliers), với cơ quan chính quyền (Regulatory Agencies), với cổ đông và với đối thủ cạnh tranh (Competitors). Có thể nêu là một số hệ thống thông tin điển hình như các hệ lập kế hoạch nguồn lực doanh nghiệp, các máy tìm kiếm và các hệ thống thông tin địa lý.

Trong lớp các hệ thống thông tin, hệ thống thông tin dựa trên máy tính (Computer based information system), hay sử dụng công nghệ máy tính để thực thi các nhiệm vụ là lớp hệ thống thông tin được sử dụng rộng rãi nhất. Hệ thống thông tin dựa trên máy tính thường gồm các thành phần: phần cứng (Hardware) để thu thập, lưu trữ, xử lý và biểu diễn dữ liệu; phần mềm (Software) chạy trên phần cứng để xử lý dữ liệu; cơ sở dữ liệu (Databases) để lưu trữ dữ liệu; mạng (Networks) là hệ thống truyền dẫn thông tin/dữ liệu; và các thủ tục (Procedures) là tập hợp các lệnh kết hợp các bộ phận nêu trên để xử lý dữ liệu, đưa ra kết quả

mong muốn.

1.2 An toàn hệ thống thông tin là gì?

An toàn hệ thống thông tin (Information systems security) là việc đảm bảo các thuộc tính an ninh, an toàn của hệ thống thông tin, bao gồm tính *bí mật* (confidentiality), tính *toàn vẹn* (integrity) và tính *sẵn dùng* (availability). Hình 1.10 minh họa các thành phần của Hệ thống thông tin dựa trên máy tính và An toàn hệ thống thông tin.



Hình 1.10. Các thành phần của hệ thống thông tin và an toàn hệ thống thông tin

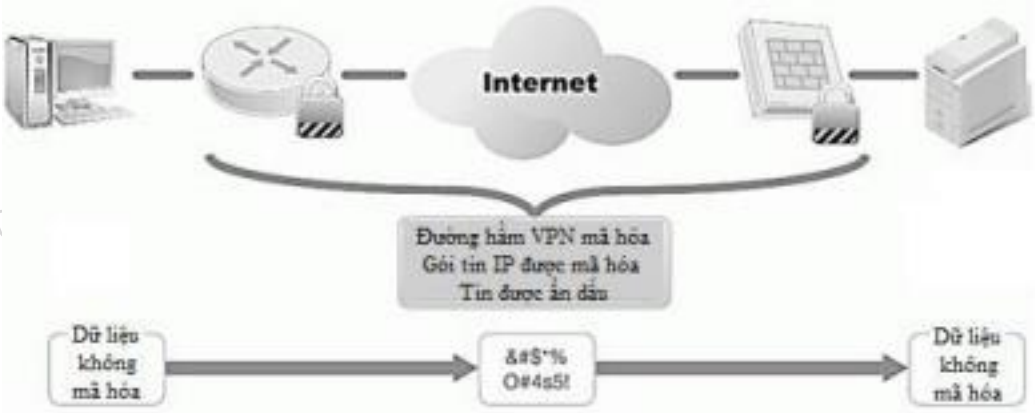
2. Các yêu cầu đảm bảo an toàn hệ thống thông tin

Như đã trình bày trong Mục 1.1.1**Error! Reference source not found.**, việc đảm bảo an toàn thông tin, hoặc hệ thống thông tin là việc đảm bảo ba thuộc tính của thông tin, hoặc hệ thống, bao gồm tính *Bí mật* (Confidentiality), tính *Toàn vẹn* (Integrity) và tính *Sẵn dùng* (Availability). Đây cũng là ba yêu cầu đảm bảo an toàn thông tin và hệ thống thông tin.

2.1 Bí mật

Tính bí mật đảm bảo rằng chỉ người dùng có thẩm quyền mới được truy nhập thông tin, hệ thống. Các thông tin bí mật có thể bao gồm: (i) dữ liệu riêng của cá nhân, (ii) các thông tin thuộc quyền sở hữu trí tuệ của các doanh nghiệp hay các cơ quan, tổ chức và (iii) các thông tin có liên quan đến an ninh của các quốc gia và các chính phủ. Hình 1.11
minh họa một văn bản được đóng dấu *Confidential* (Mật), theo đó chỉ những người có thẩm quyền (có thể không gồm người soạn thảo văn bản) mới được đọc và phổ biến văn bản.

Hình 1.11. Một văn bản được đóng dấu Confidential (Mật)



Hình 1.12. Đảm bảo tính bí mật bằng đường hầm VPN, hoặc mã hóa

Thông tin bí mật lưu trữ hoặc trong quá trình truyền tải cần được bảo vệ bằng các biện pháp phù hợp, tránh bị lộ lọt hoặc bị đánh cắp. Các biện pháp có thể sử dụng để đảm bảo tính bí mật của thông tin như bảo vệ vật lý, hoặc sử dụng mật mã (cryptography). Hình 1.12 minh họa việc đảm bảo tính bí mật bằng cách sử dụng đường hầm VPN, hoặc mã hóa để truyền tải thông tin.

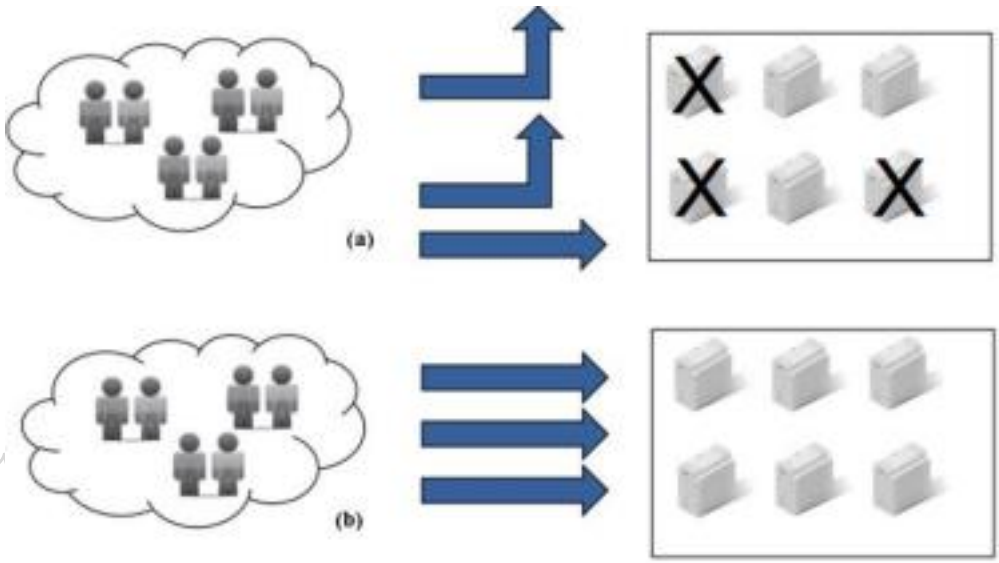
2.2 Toàn vẹn

Tính toàn vẹn đảm bảo rằng thông tin và dữ liệu chỉ có thể được sửa đổi bởi những người dùng có thẩm quyền. Tính toàn vẹn liên quan đến tính hợp lệ (validity) và chính xác (accuracy) của dữ liệu. Trong nhiều tổ chức, thông tin và dữ liệu có giá trị rất lớn, như bản quyền phần mềm, bản quyền âm nhạc, bản quyền phát minh, sáng chế. Mọi thay đổi không có thẩm quyền có thể ảnh hưởng rất nhiều đến giá trị của thông tin. Thông tin hoặc dữ liệu là toàn vẹn nếu nó thỏa mãn ba điều kiện: (i) không bị thay đổi, (ii) hợp lệ và (iii) chính xác.

2.3 Sẵn dùng

Tính sẵn dùng, hoặc khả dụng đảm bảo rằng thông tin, hoặc hệ thống có thể truy nhập bởi người dùng hợp pháp bất cứ khi nào họ có yêu cầu. Tính sẵn dùng có thể được đo bằng các yếu tố:

- Thời gian cung cấp dịch vụ (Uptime);
- Thời gian ngừng cung cấp dịch vụ (Downtime);
- Tỷ lệ phục vụ: A = (Uptime) / (Uptime + Downtime);
- Thời gian trung bình giữa các sự cố;
- Thời gian trung bình ngừng để sửa chữa;
- Thời gian khôi phục sau sự cố.



Hình 1.13. Minh họa tính sẵn dùng: (a) không đảm bảo và (b) đảm bảo tính sẵn dùng

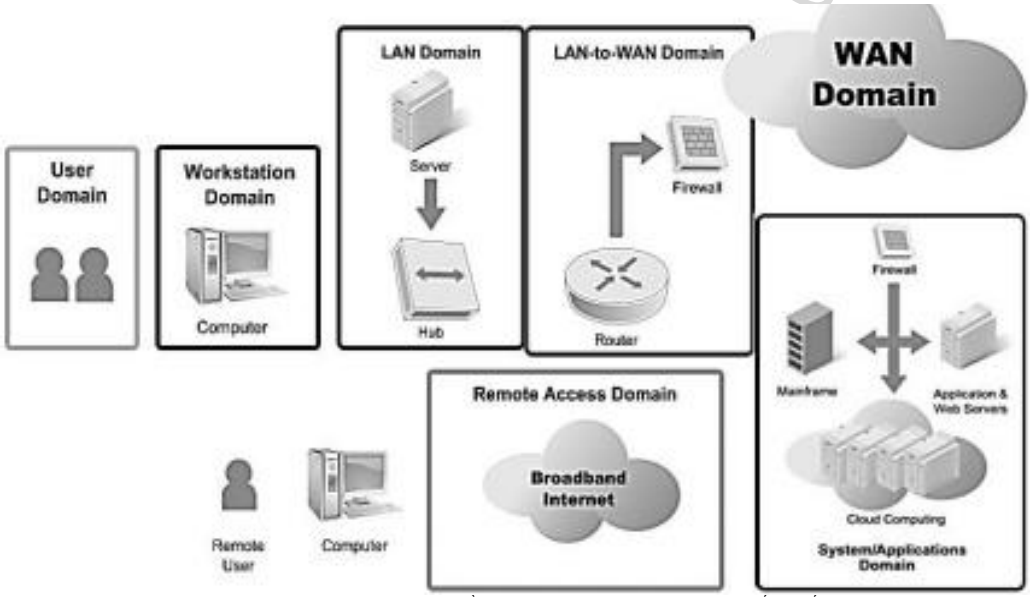
Hình 1.13 minh họa tính sẵn dùng: trường hợp (a) hệ thống không đảm bảo tính sẵn dùng khi có một số thành phần gặp sự cố thì không có khả năng phục vụ tất cả các yêu cầu của người dùng và (b) hệ thống đảm bảo tính sẵn dùng khi các thành phần của nó hoạt động bình thường.

2.4 Bảy vùng trong hạ tầng CNTT và các mối đe dọa

2.4.1 Bảy vùng trong cơ sở hạ tầng CNTT

Hạ tầng công nghệ thông tin (IT Infrastructure) của các cơ quan, tổ chức, doanh nghiệp có thể có quy mô lớn hay nhỏ khác nhau, nhưng thường gồm bảy vùng theo mức kết nối mạng như minh họa trên Hình 1.14.

Các vùng cụ thể gồm: vùng người dùng (User domain), vùng máy trạm (Workstation domain), vùng mạng LAN (LAN domain), vùng LAN-to-WAN (LAN-to-WAN domain), vùng mạng WAN (WAN domain), vùng truy nhập từ xa (Remote Access domain) và vùng hệ thống/ứng dụng (Systems/Applications domain). Do mỗi vùng kể trên có đặc điểm khác nhau nên chúng có các mối đe dọa và nguy cơ mất an toàn thông tin khác nhau.



Hình 1.14. Bảy vùng trong hạ tầng CNTT theo mức kết nối mạng

2.4.2 Các mối đe dọa

Vùng người dùng

Có thể nói vùng người dùng là vùng có nhiều mối đe dọa và nguy cơ nhất do người dùng có bản chất khó đoán định và khó kiểm soát hành vi. Các vấn đề thường gặp như thiếu ý thức, coi nhẹ vấn đề an ninh an toàn, vi phạm các chính sách an ninh an toàn; đưa CD/DVD/USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép; phá hoại dữ liệu, ứng dụng và hệ thống; các nhân viên bất mãn có thể tấn công hệ thống từ
bên trong, hoặc nhân viên có thể tống tiền hoặc chiếm đoạt thông tin nhạy cảm, thông tin quan trọng.

Vùng máy trạm

Vùng máy trạm cũng có nhiều mối đe dọa và nguy cơ do vùng máy trạm tiếp xúc trực tiếp với vùng người dùng. Các nguy cơ thường gặp gồm: truy nhập trái phép vào máy trạm, hệ thống, ứng dụng và dữ liệu; các lỗ hổng an ninh trong hệ điều hành, trong các phần mềm ứng dụng máy trạm; các hiểm họa từ vi rút, mã độc và các phần mềm độc hại. Ngoài ra, vùng máy trạm cũng chịu các nguy cơ do hành vi bị cấm từ người dùng, như đưa CD/DVD/USB với các file cá nhân vào hệ thống; tải ảnh, âm nhạc, video trái phép.

Vùng mạng LAN

Các nguy cơ có thể có đối với vùng mạng LAN bao gồm: truy nhập trái phép vào mạng LAN vật lý, truy nhập trái phép vào hệ thống, ứng dụng và dữ liệu; các lỗ hổng an ninh trong hệ điều hành và các phần mềm ứng dụng máy chủ; nguy cơ từ người dùng giả mạo trong mạng WLAN; tính bí mật dữ liệu trong mạng WLAN có thể bị đe dọa do sóng mang thông tin của WLAN truyền trong không gian có thể bị nghe trộm. Ngoài ra, các hướng dẫn và cấu hình chuẩn cho máy chủ LAN nếu không được tuân thủ nghiêm ngặt sẽ
dẫn đến những lỗ hổng an ninh mà tin tặc có thể khai thác.

Vùng mạng LAN-to-WAN

Vùng mạng LAN-to-WAN là vùng chuyển tiếp từ mạng nội bộ ra mạng diện rộng, nên nguy cơ lớn nhất là tin tặc từ mạng WAN có thể thăm dò và rà quét trái phép các cổng dịch vụ, nguy cơ truy nhập trái phép. Ngoài ra, một nguy cơ khác cần phải xem xét là lỗ hổng an ninh trong các bộ định tuyến, tường lửa và các thiết bị mạng khác.

Vùng mạng WAN

Vùng mạng WAN, hay mạng Internet là vùng mạng mở, trong đó hầu hết dữ liệu được truyền dưới dạng rõ, nên các nguy cơ lớn nhất là dễ bị nghe trộm và dễ bị tấn công phá hoại, tấn công từ chối dịch vụ (DoS) và từ chối dịch vụ phân tán (DDoS). Kẻ tấn công có thể tự do, dễ dàng gửi email có đính kèm vi rút, sâu và các phần mềm độc hại.

Vùng truy nhập từ xa

Trong vùng truy nhập từ xa, các nguy cơ điển hình bao gồm: tấn công kiểu vét cạn vào tên người dùng và mật khẩu, tấn công vào hệ thống đăng nhập và điều khiển truy nhập; truy nhập trái phép vào hệ thống CNTT, ứng dụng và dữ liệu; các thông tin bí mật có thể bị đánh cắp từ xa; và vấn đề rò rỉ dữ liệu do vi phạm các tiêu chuẩn phân loại dữ
liệu.

Vùng hệ thống và ứng dụng

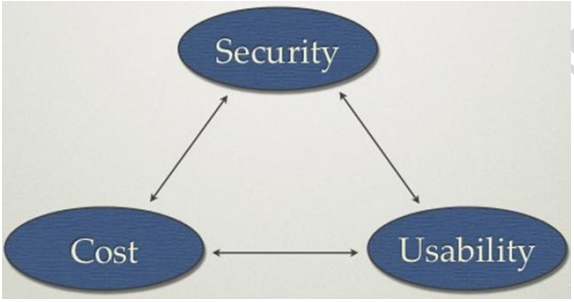
Trong vùng hệ thống và ứng dụng, các nguy cơ có thể bao gồm: truy nhập trái phép đến trung tâm dữ liệu, phòng máy hoặc tủ cáp; các khó khăn trong quản lý các máy chủ với yêu cầu tính sẵn dùng cao; các lỗ hổng trong quản lý các phần mềm ứng dụng của hệ điều hành máy chủ; các vấn đề an ninh trong các môi trường ảo của điện toán đám mây; và vấn đề hỏng hóc hoặc mất dữ liệu.

2.5 Mô hình tổng quát đảm bảo an toàn hệ thống thông tin

2.5.1 Giới thiệu mô hình Phòng vệ theo chiều sâu

Mô hình tổng quát đảm bảo an toàn hệ thống thông tin là *Phòng vệ theo chiều sâu* (Defence in Depth). Theo mô hình này, ta cần tạo ra nhiều lớp bảo vệ, kết hợp tính năng, tác dụng của mỗi lớp để đảm bảo an toàn tối đa cho thông tin, hệ thống và mạng. Một lớp, một công cụ phòng vệ riêng rẽ dù có hiện đại, nhưng vẫn không thể đảm bảo an toàn. Do vậy, việc tạo ra nhiều lớp bảo vệ có khả năng bổ sung cho nhau là cách làm hiệu quả. Một điểm khác cần lưu ý khi thiết kế và triển khai hệ thống đảm bảo an toàn thông tin là cần cân bằng giữa *tính hữu dụng* (Usability), *chi phí* (Cost) và *an toàn* (Security), như minh họa trên Hình 1.15. Hệ thống đảm bảo an toàn thông tin chỉ thực sự phù hợp và hiệu quả khi hệ thống được bảo vệ đạt mức an toàn phù hợp mà vẫn có khả năng cung cấp các tính năng hữu dụng cho người dùng, với chi phí cho đảm bảo an

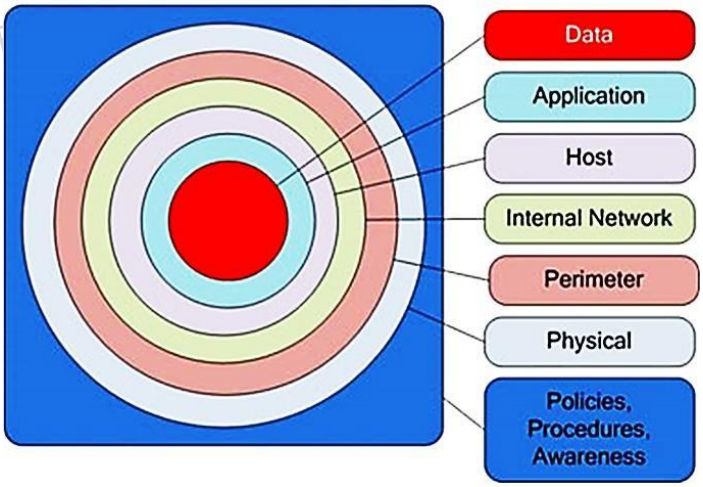
toàn phù hợp với tài sản được bảo vệ.



Hình 1.15. Các lớp bảo vệ cần cân bằng giữa Tính hữu dụng (Usability), Chi phí (Cost) và An toàn (Security)

2.5.2 Các lớp bảo vệ trong mô hình Phòng vệ theo chiều sâu

Hình 1.16 minh họa mô hình đảm bảo an toàn thông tin với bảy lớp bảo vệ, bao gồm lớp chính sách, thủ tục, ý thức (Policies, procedures, awareness); lớp vật lý (Physical); lớp ngoại vi (Perimeter); lớp mạng nội bộ (Internal network); lớp host (Host); lớp ứng dụng (Application) và lớp dữ liệu (Data). Trong mô hình này, để truy nhập được đến đối tượng đích là dữ liệu, tin tặc cần phải vượt qua cả 7 lớp bảo vệ.

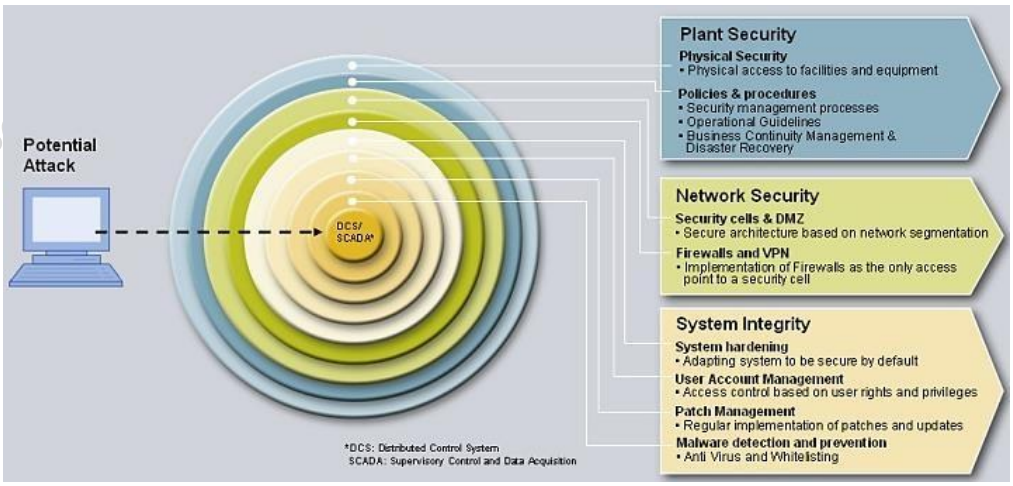


Hình 1.16. Mô hình đảm bảo an toàn thông tin với bảy lớp

Tương tự, Hình 1.17 minh họa mô hình phòng vệ gồm 3 lớp: lớp an ninh cơ quan/tổ chức, lớp an ninh mạng và lớp an ninh hệ thống. Mỗi lớp trên lại gồm một số lớp con như sau:

- Lớp an ninh cơ quan/tổ chức (Plant Security), gồm 2 lớp con:
  + Lớp bảo vệ vật lý (Physical Security) có nhiệm vụ kiểm soát các truy nhập vật lý đến các trang thiết bị hệ thống và mạng.
  + Lớp chính sách & thủ tục (Policies & procedures) bao gồm các quy trình quản lý ATTT, các hướng dẫn vận hành, quản lý hoạt động liên tục và phục hồi sau sự cố.

- Lớp an ninh mạng (Network Security), gồm 2 lớp con:
  + Lớp bảo vệ vùng hạn chế truy nhập (Security cells and DMZ) cung cấp các biện pháp bảo vệ cho từng phân đoạn mạng.
  + Lớp các tường lửa, mạng riêng ảo (Firewalls and VPN) được triển khai như điểm truy nhập duy nhất đến một phân đoạn mạng.
- Lớp an ninh hệ thống (System Integrity), gồm 4 lớp con:
  + Lớp tăng cường an ninh hệ thống (System hardening) đảm bảo việc cài đặt và cấu hình các thành phần trong hệ thống đảm bảo các yêu cầu an toàn. + Lớp quản trị tài khoản người dùng (User Account Management) thực hiện kiểm soát truy nhập dựa trên quyền truy nhập và các đặc quyền của người dùng. + Lớp quản lý các bản vá (Patch Management) có nhiệm vụ định kỳ cài đặt các bản vá an ninh và các bản cập nhật cho hệ thống.
  + Lớp phát hiện và ngăn chặn phần mềm độc hại (Malware detection and prevention) có nhiệm vụ bảo vệ hệ thống, chống vi rút và các phần mềm độc hại khác.



Hình 1.17. Mô hình đảm bảo an toàn thông tin với ba lớp chính