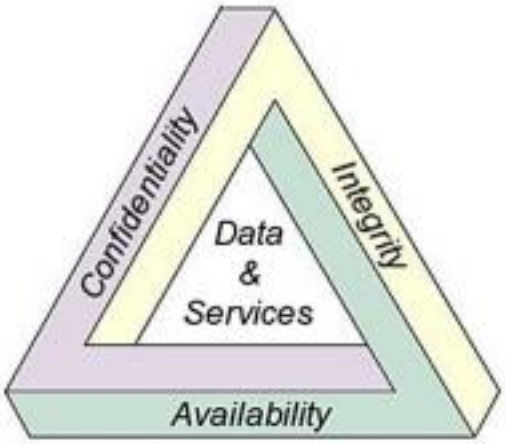
Chương 1 giới thiệu các khái niệm về an toàn thông tin, an toàn hệ thống thông tin và các yêu cầu đảm bảo an toàn thông tin và an toàn hệ thống thông tin. Chương này cũng đề cập các rủi ro và nguy cơ trong các vùng của hạ tầng công nghệ thông tin theo mức kết nối mạng. Phần cuối của chương giới thiệu mô hình tổng quát đảm an toàn hệ thống thông tin.

1. Khái quát về an toàn thông tin

1.1 An toàn thông tin là gì?

An toàn thông tin (Information security) là việc bảo vệ chống truy nhập, sử dụng, tiết lộ, sửa đổi, hoặc phá hủy thông tin một cách trái phép, theo trang Wikipedia (https://en.wikipedia.org/wiki/Information_security).

Theo cuốn Principles of Information Security, *An toàn thông tin* là việc bảo vệ các thuộc tính *bí mật* (confidentiality), tính *toàn vẹn* (integrity) và tính *sẵn dùng* (availability) của các tài sản thông tin trong quá trình chúng được lưu trữ, xử lý, hoặc truyền tải. Hình 1.1 minh họa ba thuộc tính cần bảo vệ nói trên của các tài sản thông tin, bao gồm dữ liệu (Data) và dịch vụ (Services).



Hình 1.1. Các thuộc tính cần bảo vệ của tài sản thông tin: Bí mật (Confidentiality), Toàn vẹn (Integrity) và Sẵn dùng (Availability)

An toàn thông tin gồm hai lĩnh vực chính là *An toàn công nghệ thông tin* (Information technology security, hay IT security) và *Đảm bảo thông tin* (Information assurance). An toàn công nghệ thông tin, hay còn gọi là *An toàn máy tính* (Computer security) là việc đảm bảo an toàn cho các hệ thống công nghệ thông tin, bao gồm các hệ thống máy tính và mạng, chống lại các cuộc tấn công phá hoại. Đảm bảo thông tin là việc đảm bảo thông tin không bị mất khi xảy ra các sự cố, như thiên tai, hỏng hóc, trộm cắp, phá hoại,…Đảm bảo thông tin thường được thực hiện sử dụng các kỹ thuật *sao lưu ngoại vi* (offsite backup), trong đó dữ liệu thông tin từ hệ thống gốc được sao lưu ra các thiết bị

lưu trữ vật lý đặt ở một vị trí khác.

Một số khái niệm khác trong an toàn thông tin:

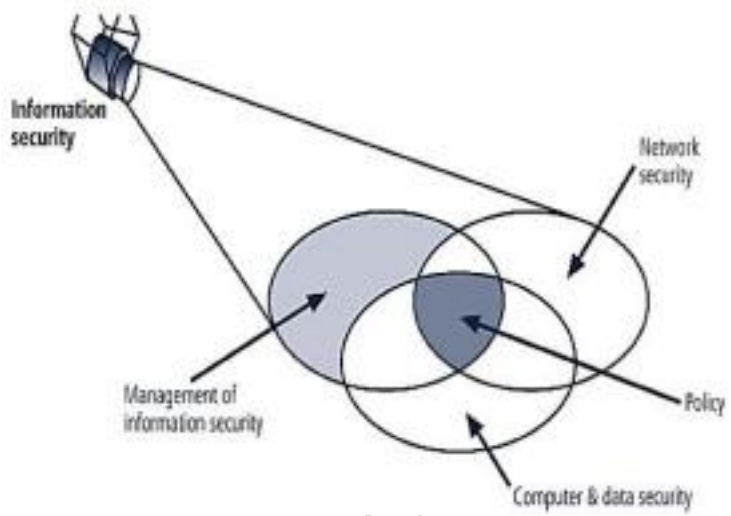
Truy nhập (Access) là việc một chủ thể, người dùng hoặc một đối tượng có khả năng sử dụng, xử lý, sửa đổi, hoặc gây ảnh hưởng đến một chủ thể, người dùng hoặc một đối tượng khác. Trong khi người dùng hợp pháp có quyền truy nhập hợp pháp đến một hệ thống thì tin tặc truy nhập bất hợp pháp đến hệ thống.

Tài sản (Asset) là tài nguyên của các tổ chức, cá nhân được bảo vệ. Tài sản có thể là tài sản lô gíc, như một trang web, thông tin, hoặc dữ liệu. Tài sản có thể là tài sản vật lý, như hệ thống máy tính, thiết bị mạng, hoặc các tài sản khác.

Tấn công (Attack) là hành động có chủ ý hoặc không có chủ ý có khả năng gây hại, hoặc làm thỏa hiệp các thông tin, hệ thống và các tài sản được bảo vệ. Tấn công có thể chủ động hoặc thụ động, trực tiếp hoặc gián tiếp.

1.2 Các thành phần của an toàn thông tin

An toàn thông tin có thể được chia thành ba thành phần chính: *an toàn máy tính và dữ liệu* (Computer & data security), *an ninh mạng* (Network security) và *quản lý an toàn thông tin* (Management of information security). Ba thành phần của an toàn thông tin có quan hệ mật thiết và giao thoa với nhau, trong đó phần chung của cả ba thành phần trên là *chính sách an toàn thông tin* (Policy) như minh họa trên Hình 1.2.



Hình 1.2. Các thành phần chính của An toàn thông tin

1.2.1 An toàn máy tính và dữ liệu

An toàn máy tính và dữ liệu là việc đảm bảo an toàn cho hệ thống phần cứng, phần mềm và dữ liệu trên máy tính; đảm bảo cho máy tính có thể vận hành an toàn, đáp ứng các yêu cầu của người sử dụng. An toàn máy tính và dữ liệu bao gồm các nội dung:

- Đảm bảo an toàn hệ điều hành, ứng dụng, dịch vụ;
- Vấn đề điều khiển truy nhập;
- Vấn đề mã hóa và bảo mật dữ liệu;
- Vấn đề phòng chống phần mềm độc hại;
- Việc sao lưu tạo dự phòng dữ liệu, đảm bảo dữ liệu lưu trong máy tính không bị mất mát khi xảy ra sự cố.

Hình 1.3. Đảm bảo an toàn máy tính và dữ liệu

1.2.2 An ninh mạng

An ninh mạng là việc đảm bảo an toàn cho hệ thống mạng và các thông tin truyền tải trên mạng, chống lại các tấn công, xâm nhập trái phép. Các kỹ thuật và công cụ thường được sử dụng trong an ninh mạng bao gồm:

- Các tường lửa, proxy cho lọc gói tin và điều khiển truy nhập;
- Mạng riêng ảo và các kỹ thuật bảo mật thông tin truyền như SSL/TLS, PGP;
- Các kỹ thuật và hệ thống phát hiện, ngăn chặn tấn công, xâm nhập;
- Vấn đề giám sát mạng.

Hình 1.4. Đảm bảo an toàn cho hệ thống mạng và thông tin truyền trên

mạng

1.2.3 Quản lý an toàn thông tin

Quản lý an toàn thông tin là việc quản lý và giám sát việc thực thi các biện pháp đảm bảo an toàn thông tin, giúp nâng cao hiệu quả của chúng. Một trong các nội dung cốt lõi của quản lý an toàn thông tin là việc quản lý các rủi ro (Risk management), trong đó việc nhận dạng và đánh giá rủi ro (Risk assessment) đóng vai trò then chốt. Các nội dung khác của quản lý an toàn thông tin, bao gồm các chuẩn an toàn thông tin, chính sách an toàn thông tin và vấn đề đào tạo, nâng cao ý thức an toàn thông tin của người dùng.

Hình 1.5. Chu trình quản lý an toàn thông tin

Việc thực thi quản lý an toàn thông tin cần được thực hiện theo chu trình lặp lại, từ khâu lập kế hoạch (Plan), thực thi kế hoạch (Implement), giám sát kết quả thực hiện (Monitor) và thực hiện các kiểm soát (Control) như minh họa trên Hình 1.5, do các điều kiện bên trong và bên ngoài thay đổi theo thời gian.

1.2.4 Chính sách an toàn thông tin

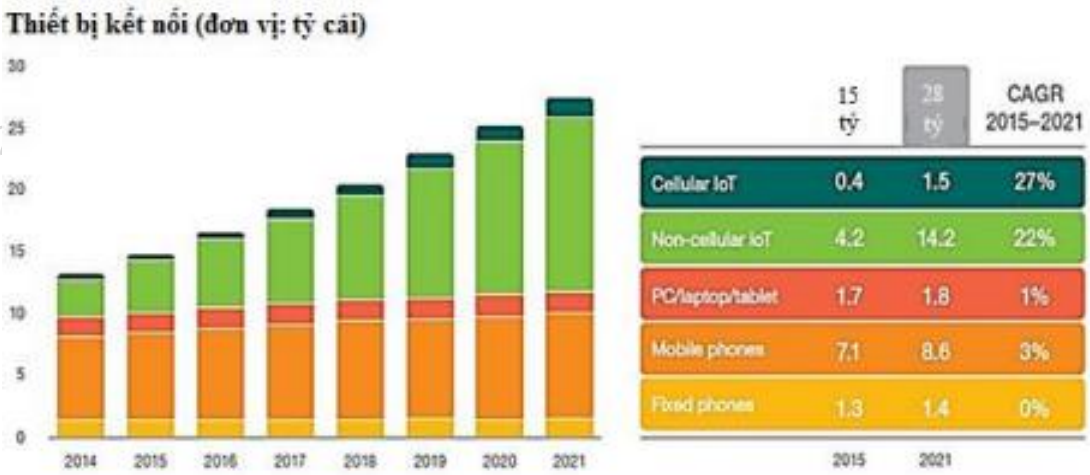
Hình 1.6. Chính sách an toàn thông tin

Chính sách an toàn thông tin (Information security policy) là các nội quy, quy định của cơ quan, tổ chức, nhằm đảm bảo các biện pháp đảm bảo an toàn thông tin được thực thi và tuân thủ. Chính sách an toàn thông tin, như minh họa trên Hình 1.6 gồm 3 thành phần:

- Chính sách an toàn ở mức vật lý (Physical security policy);
- Chính sách an toàn ở mức tổ chức (Organizational security policy); - Chính sách an toàn ở mức logic (Logical security policy).

Một ví dụ về chính sách an toàn thông tin: để tăng cường an toàn cho hệ thống công nghệ thông tin, một tổ chức có thể áp dụng chính sách xác thực 'mạnh' sử dụng các đặc điểm sinh trắc (Biometrics), như xác thực sử dụng vân tay thay cho mật khẩu truyền thống cho hệ thống cửa ra vào trung tâm dữ liệu, hoặc đăng nhập vào hệ thống máy tính.

1.3 Sự cần thiết của an toàn thông tin

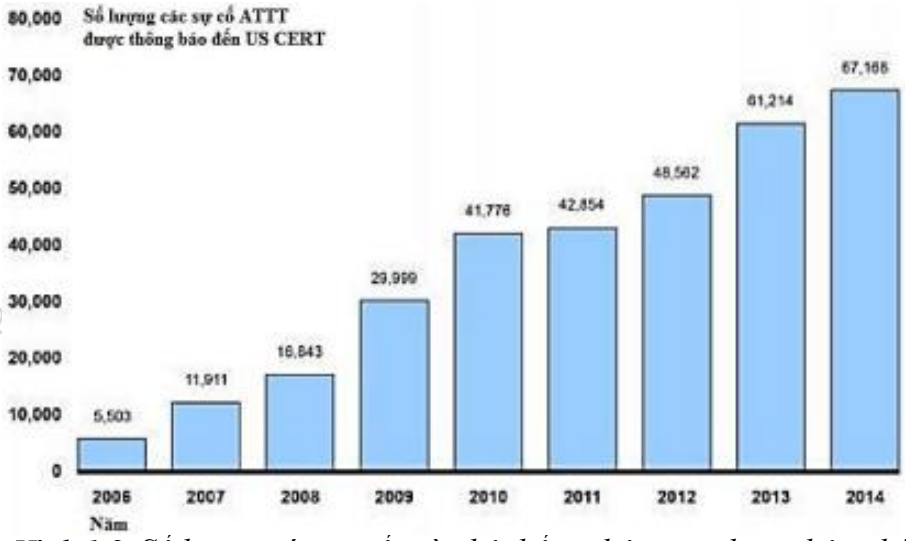


Hình 1.7. Số lượng các thiết bị kết nối vào Internet đến 2015 và dự báo đến 2021

Trong những năm gần đây, cùng với sự phát triển mạnh mẽ của các thiết bị di động, và đặc biệt là các thiết bị IoT (Internet of Things), số lượng người dùng mạng Internet và số lượng thiết bị kết nối vào mạng Internet tăng trưởng nhanh chóng. Theo thống kê và dự báo của Forbes [3] cho trên Hình 1.7, số lượng các thiết bị có kết nối Internet là khoảng 15 tỷ và dự báo sẽ tăng mạnh lên khoảng 28 tỷ thiết bị có kết nối vào năm 2021. Các thiết bị IoT kết nối thông minh là nền tảng cho phát triển nhiều ứng dụng quan trọng trong các lĩnh vực của đời sống xã hội, như thành phố thông minh, cộng đồng thông minh, ngôi nhà thông minh, ứng dụng giám sát và chăm sóc sức khỏe,…

Cùng với những lợi ích to lớn mà các thiết bị kết nối Internet mạng lại, các sự

cố mất an toàn thông tin đối với các hệ thống máy tính, điện thoại di động thông minh, các thiết bị IoT và người dùng cũng tăng vọt. Theo số liệu ghi nhận của Cơ quan Thống kê quốc gia Hoa Kỳ cho trên Hình 1.8, số lượng các sự cố mất an toàn hệ thống thông tin được thông báo đến Cơ quan ứng cứu khẩn cấp máy tính (US-CERT) trong giai đoạn 2006 – 2014 tăng rất mạnh, từ 5.503 vụ vào năm 2006 lên đến 67.168 vụ vào năm 2014. Ở Việt Nam, trong báo cáo "*Tổng kết an ninh mạng năm 2015 và dự báo xu hướng 2016*" [5], Tập đoàn Bkav cho biết 8.700 tỷ đồng là tổng thiệt hại ước tính do vi rút máy tính gây ra đối với người dùng Việt Nam trong năm 2015. Con số này vẫn ở mức cao và tiếp tục tăng so với 8.500 tỷ đồng của năm 2014. Dự báo trong năm 2016 và các năm tiếp theo, số lượng sự cố và thiệt hại do mất an toàn thông tin gây ra còn có thể lớn hơn nữa, do số lượng thiết bị kết nối tăng trưởng nhanh chóng và nguy cơ từ sự phát triển mạnh của các phần mềm độc hại và các kỹ thuật tấn công, phá hoại tinh vi.



Hình 1.8. Số lượng các sự cố toàn hệ thống thông tin được thông báo đến Cơ quan ứng cứu khẩn cấp máy tính (US-CERT) trong giai đoạn 2006 – 2014

Như vậy, việc đảm bảo an toàn cho thông tin, máy tính, hệ thống mạng và các thiết bị kết nối khác, chống lại các truy nhập trái phép và các cuộc tấn công phá hoại là rất cần thiết không chỉ đối với các cá nhân, cơ quan, tổ chức, doanh nghiệp mà còn đối với an ninh quốc gia. Hơn nữa, việc xây dựng các giải pháp an toàn thông tin chỉ thực sự hiệu quả khi được thực hiện bài bản, đồng bộ, đảm bảo cân bằng giữa tính an toàn, tính hữu dụng của hệ thống và chi phí đầu tư cho các biện pháp đảm bảo an toàn.