AN TOÀN THÔNG TIN

I. MỞ ĐẦU

Ngày nay với sự phát triển bùng nổ của công nghệ thông tin, hầu hết các thông tin của các tổ chức, cá nhân đều được lưu trữ trên hệ thống máy tính. Cùng với sự phát triển của tổ chức là những đòi hỏi ngày càng cao của môi trường hoạt động cần phải chia sẻ thông tin của mình cho nhiều đối tượng khác nhau qua mạng. Việc mất mát, rò rỉ thông tin có thể ảnh hưởng nghiêm trọng đến tài nguyên thông tin, tài chính, danh tiếng của tổ chức, cá nhân.

Các phương thức tấn công thông qua mạng ngày càng tinh vi, phức tạp có thể dẫn đến mất mát thông tin, thậm chí có thể làm sụp đổ hoàn toàn hệ thống thông tin của tổ chức. Vì vậy an toàn thông tin là nhiệm vụ quan trọng, nặng nề và khó đoán trước đối với các hệ thống thông tin.

II. NỘI DUNG

1. Tổng quan về an toàn thông tin

a. Khái niệm an toàn thông tin

An toàn thông tin là các hoạt động bảo vệ tài sản thông tin và là một lĩnh vực rộng lớn. Nó bao gồm cả những sản phẩm và những quy trình nhằm ngăn chặn truy cập trái phép, hiệu chỉnh, xóa thông tin,...

An toàn thông tin liên quan đến hai khía cạnh đó là an toàn về mặt vật lý và an toàn về mặt kỹ thuật.

- Mục tiêu cơ bản của an toàn thông tin

    + Đảm bảo tính bảo mật

+ Đảm bảo tính toàn vẹn

+ Đảm bảo tính xác thực

+ Đảm bảo tính sẵn sàng

b. Sự cần thiết của an toàn thông tin

Hệ thống thông tin là thành phần thiết yếu trong mọi cơ quan, tổ chức và đem lại khả năng xử lý thông tin, là tài sản quan trọng nhưng hệ thống thông tin cũng chứa rất nhiều điểm yếu và rủi do. Do máy tính được phát triển với tốc độ rất nhanh để đáp ứng nhiều yêu cầu của người dùng, các phiên bản được phát hành liên tục với các tính năng mới được thêm vào ngày càng nhiều, điều này làm cho các phần mềm không được kiểm tra kỹ trước khi phát hành và bên trong chúng chứa rất nhiều lỗ hổng có thể dễ dàng bị lợi dụng. Thêm vào đó là việc phát triển của hệ thống mạng, cũng như sự phân tán của hệ thống thông tin, làm cho người dùng truy cập thông tin dễ dàng hơn và tin tặc cũng có nhiều mục tiêu tấn công dễ dàng hơn.

c. Mục đích của an toàn thông tin

*** Bảo vệ tài nguyên của hệ thống**

Các hệ thống máy tính lưu giữ rất nhiều thông tin và tài nguyên cần được bảo vệ. Trong một tổ chức, những thông tin và tài nguyên này có thể là dữ liệu kế toán, thông tin nguồn nhân lực, thông tin quản lý, bán hàng, nghiên cứu, sáng chế, phân phối, thông tin về tổ chức và thông tin về các hệ thống nghiên cứu. Đối với rất nhiều tổ chức, toàn bộ dữ liệu quan trọng của họ thường được lưu trong một cơ sở dữ liệu và được quản lý và sử dụng bởi các chương trình phần mềm.

Các tấn công vào hệ thống có thể xuất phát từ những đối thủ của tổ chức hoặc cá nhân do đó, các phương pháp để bảo đảm an toàn cho những thông tin này có thể rất phức tạp và nhạy cảm. Các tấn công có thể xuất phát từ nhiều nguồn khác nhau, cả từ

bên trong và bên ngoài tổ chức. Hậu quả mà những tấn công thành công để lại sẽ rất nghiêm trọng.

*** Bảo đảm tính riêng tư**

Các hệ thống máy tính lưu giữ rất nhiều thông tin cá nhân cần được giữ bí mật. Những thông tin này bao gồm: Số thẻ bảo hiểm xã hội, số thẻ ngân hàng, số thẻ tín dụng, thông tin về gia đình,…

Tính riêng tư là yêu cầu rất quan trọng mà các ngân hàng, các công ty tín dụng, các công ty đầu tư và các hãng khác cần phải đảm bảo để gửi đi các tài liệu thông tin chi tiết về cách họ sử dụng và chia sẻ thông tin về khách hàng. Các hãng này có những quy định bắt buộc để bảo đảm những thông tin cá nhân được bí mật và bắt buộc phải thực hiện những quy định đó để bảo đảm tính riêng tư. Hậu quả nghiêm trọng sẽ xảy ra nếu một kẻ giả mạo truy nhập được những thông tin cá nhân.

2. Các nguy cơ mất an toàn thông tin

*** Nguy cơ mất an toàn thông tin về khía cạnh vật lý**

Nguy cơ mất an toàn thông tin về khía cạnh vật lý là nguy cơ do mất điện, nhiệt độ, độ ẩm không đảm bảo, hỏa hoạn, thiên tai, thiết bị phần cứng bị hư hỏng, các phần tử phá hoại như nhân viên xấu bên trong và kẻ trộm bên ngoài.

*** Nguy cơ bị mất, hỏng, sửa đổi nội dung thông tin:**

Người dùng có thể vô tình để lộ mật khẩu hoặc không thao tác đúng quy trình tạo cơ hội cho kẻ xấu lợi dụng để lấy cắp hoặc làm hỏng thông tin.

Kẻ xấu có thể sử dụng công cụ hoặc kỹ thuật của mình để thay đổi nội dung thông tin (các file) nhằm sai lệnh thông tin của chủ sở hữu hợp pháp.

*** Nguy cơ bị tấn công bởi các phần mềm độc hại**

Các phần mềm độc hại tấn công bằng nhiều phương pháp khác nhau để xâm nhập vào hệ thống với các mục đích khác nhau như: virus, sâu máy tính (Worm), phần mềm gián điệp (Spyware),...

Virus: là một chương trình máy tính có thể tự sao chép chính nó lên những đĩa, file khác mà người sữ dụng không hay biết. Thông thường virus máy tính mang tính chất phá hoại, nó sẽ gây ra lỗi thi hành, lệch lạc hay hủy dữ liệu. Chúng có các tính chất: Kích thước nhỏ, có tính lây lan từ chương trình sang chương trình khác, từ đĩa này sang đĩa khác và do đó lây từ máy này sang máy khác, tính phá hoại thông thường chúng sẽ tiêu diệt và phá hủy các chương trình và dữ liệu (tuy nhiên cũng có một số virus không gây hại như chương trình được tạo ra chỉ với mục đích trêu đùa).

Worm: Loại virus lây từ máy tính này sang máy tính khác qua mạng, khác với loại virus truyền thống trợớc đây chỉ lây trong nội bộ một máy tính và nó chỉ lây sang máy khác khi ai đó đem chương trình nhiễm virus sang máy này.

Trojan, Spyware, Adware: Là những phần mềm được gọi là phần mềm gián điệp, chúng không lây lan như virus. Thường bằng cách nào đó (lừa đảo người sử dụng thông qua một trang web, hoặc một người cố tình gửi nó cho người khác) cài đặt và nằm vùng tại máy của nạn nhân, từ đó chúng gửi các thông tin lấy được ra bên ngoài hoặc hiện lên các quảng cáo ngoài ý muốn của nạn nhân.

*** Nguy cơ xâm nhập từ lỗ hổng bảo mật**

Lỗ hổng bảo mật thường là do lỗi lập trình, lỗi hoặc sự cố phần mềm, nằm trong một hoặc nhiều thành phần tạo nên hệ điều hành hoặc trong chương trình cài đặt trên máy tính.

Hiện, nay các lỗ hổng bảo mật được phát hiện ngày càng nhiều trong các hệ điều hành, các web server hay các phần mềm khác, ... Và các hãng sản xuất luôn cập nhật

các lỗ hổng và đưa ra các phiên bản mới sau khi đã vá lại các lỗ hổng của các phiên bản trước.

*** Nguy cơ xâm nhập do bị tấn công bằng cách phá mật khẩu**

Quá trình truy cập vào một hệ điều hành có thể được bảo vệ bằng một khoản mục người dùng và một mật khẩu. Đôi khi người dùng khoản mục lại làm mất đi mục đích bảo vệ của nó bằng cách chia sẻ mật khẩu với những người khác, ghi mật khẩu ra và để nó công khai hoặc để ở một nơi nào đó cho dễ tìm trong khu vực làm việc của mình.

Những kẻ tấn công có rất nhiều cách khác phức tạp hơn để tìm mật khẩu truy nhập. Những kẻ tấn công có trình độ đều biết rằng luôn có những khoản mục người dùng quản trị chính.

Kẻ tấn công sử dụng một phần mềm dò thử các mật khẩu khác nhau có thể. Phần mềm này sẽ tạo ra các mật khẩu bằng cách kết hợp các tên, các từ trong từ điển và các số. Ta có thể dễ dàng tìm kiếm một số ví dụ về các chương trình đoán mật khẩu trên mạng Internet như: Xavior, Authforce và Hypnopaedia. Các chương trình dạng này làm việc tương đối nhanh và luôn có trong tay những kẻ tấn công.

*** Nguy cơ mất an toàn thông tin do sử dụng e-mail**

Tấn công có chủ đích bằng thư điện tử là tấn công bằng email giả mạo giống như email được gửi từ người quen, có thể gắn tập tin đính kèm nhằm làm cho thiết bị bị nhiễm virus. Cách thức tấn công này thường nhằm vào một cá nhân hay một tổ chức cụ thể. Thư điện tử đính kèm tập tin chứa virus được gửi từ kẻ mạo danh là một đồng nghiệp hoặc một đối tác nào đó. Người dùng bị tấn công bằng thư điên tử có thể bị đánh cắp mật khẩu hoặc bị lây nhiễm virus.

Rất nhiều người sử dụng e-mail nhận ra rằng họ có thể là nạn nhân của một tấn công e-mail. Một tấn công e-mail có vẻ như xuất phát từ một nguồn thân thiện, hoặc

thậm chí là tin cậy như: một công ty quen, một người thân trong gia đình hay một đồng nghiệp. Người gửi chỉ đơn giản giả địa chỉ nguồn hay sử dụng một khoản mục e-mail mới để gửi e-mail phá hoại đến người nhận. Đôi khi một e-mail được gửi đi với một tiêu đề hấp dẫn như "Congratulation you've just won free software. Những e-mail phá hoại có thể mang một tệp đính kèm chứa một virus, một sâu mạng, phần mềm gián điệp hay một trojan horse. Một tệp đính kèm dạng văn bản word hoặc dạng bảng tính có thể chứa một macro (một chương trình hoặc một tập các chỉ thị) chứa mã độc. Ngoài ra, e-mail cũng có thể chứa một liên kết tới một web site giả.

*** Nguy cơ mất an toàn thông tin trong quá trình truyền tin**

Trong quá trình lưu thông và giao dịch thông tin trên mạng internet nguy cơ mất an toàn thông tin trong quá trình truyền tin là rất cao do kẻ xấu chặn đường truyền và thay đổi hoặc phá hỏng nội dung thông tin rồi gửi tiếp tục đến người nhận.

3. Các giải pháp bảo vệ an toàn thông tin

*** Bảo vệ thông tin về mặt vật lý**

Để bảo vệ an toàn thông tin của hệ thống cần có các thiết bị và biện pháp phòng chống các nguy cơ gây mất an toàn thông tin về khía cạnh vật lý như: Thiết bị lưu điện, lặp đặt hệ thống điều hòa nhiệt độ và độ ẩm. Luôn sẵn sàng các thiết bị chữa cháy nổ, không đặt các hóa chất gần thệ thống. Thường xuyên sao lưu dữ liệu. Sử dụng các chính sách vận hành hệ thống đúng quy trình, an toàn và bảo mật.

*** Bảo vệ với nguy cơ mất thông tin**

Cung cấp những hướng dẫn, những quy tắc, và những quy trình để thiết lập một môi trường thông tin an toàn. Các chính sách của hệ thống có tác dụng tốt nhất khi người dùng được tham gia vào xây dựng chúng, làm cho họ biết rõ được tầm quan trọng của an toàn. Đào tạo và cho người dùng tham gia vào uỷ ban chính sách an toàn

là 2 cách để bảo đảm rằng người dùng cảm thấy chính bản thân họ là những nhân tố trong việc xây dựng hệ thống an toàn mạnh. Một ưu điểm của việc gắn người dùng theo cách này là nếu người dùng hiểu được bản chất của các mối đe doạ về an toàn, họ sẽ không làm trái các nỗ lực bảo đảm an toàn. Một chính sách của một tổ chức có thể tập trung vào một số vấn đề sau:

- Đào tạo cho người dùng về các kỹ thuật an toàn.

- Đào tạo cho người dùng về các phần mềm phá hoại.

- Yêu cầu người dùng phải quét các thiết bị lưu trữ bằng các phần mềm quét virus trước khi sử dụng chúng.

- Thiết lập các chính sách quy định những phương tiện nào từ bên ngoài có thể mang được vào hệ thống và cách sử dụng chúng như thế nào.

- Thiết lập các chính sách để ngăn chặn người dùng tự cài đặt các phần mềm riêng của họ.

- Thiết lập các chính sách để giảm thiểu hoặc ngăn chặn người dùng tải về các tệp và yêu cầu người dùng phải quét virus đối với các tệp này.

- Tạo một vùng riêng để người dùng cách ly các tệp có nguồn gốc không rõ ràng để quét chúng trước khi sử dụng.

- Xây dựng chính sách giới hạn quyền để kiểm soát truy cập vào hệ thống

- Thường xuyên sao lưu tài nguyên thông tin quan trọng với hệ thống dự phòng. Sao lưu dự phòng hệ thống là việc quan trọng để bảo vệ hệ thống do lỗi đĩa, mất mát dữ liệu hay do phần mềm phá hoại. Nếu ta sao lưu dữ liệu mà sau đó hệ thống bị nhiễm một mã độc phá hoại các hay xoá các tệp, thì ta có thể khôi phục lại được các tệp đó hay toàn bộ hệ thống.

*** Bảo vệ với nguy cơ bị tấn công bởi các phần mềm độc hại**

"Phần mềm độc hại" là bất kỳ loại phần mềm nào được thiết kế để gây hại máy tính. Phần mềm độc hại có thể lấy cắp thông tin nhạy cảm từ máy tính, làm chậm máy tính hay thậm chí gửi email giả mạo từ tài khoản email của người dùng mà người dùng không biết. Dưới đây là một số loại phần mềm độc hại phổ biến mà bạn có thể đã nghe:

Vi rút: Một chương trình máy tính độc hại có thể tự sao chép và lây nhiễm máy tính.

Sâu máy tính: Một chương trình máy tính độc hại gửi bản sao của chính nó đến các máy tính khác thông qua mạng.

Phần mềm gián điệp: Phần mềm độc hại thu thập thông tin từ mọi người mà họ không biết.

Phần mềm quảng cáo: Phần mềm tự động phát, hiển thị hoặc tải xuống quảng cáo trên máy tính.

Ngựa Trojan: Một chương trình phá hoại giả vờ là một ứng dụng hữu ích nhưng gây hại máy tính hoặc đánh cắp thông tin của bạn sau khi được cài đặt.

Cách phần mềm độc hại phát tán:

Phần mềm độc hại có thể xâm nhập vào máy tính của bạn theo một số cách khác nhau. Dưới đây là một số ví dụ phổ biến:

- Tải xuống phần mềm miễn phí từ Internet bí mật chứa phần mềm độc hại

- Tải xuống phần mềm hợp pháp bí mật có kèm theo phần mềm độc hại

- Truy cập vào trang web bị nhiễm phần mềm độc hại

- Nhấp vào thông báo lỗi hoặc cửa sổ bật lên giả mạo bắt đầu tải xuống phần mềm độc hại

- Mở tệp đính kèm email chứa phần mềm độc hại

Có nhiều cách khác nhau để phần mềm độc hại phát tán, nhưng điều đó không có nghĩa là bạn không có cách để ngăn chặn phần mềm độc hại. Bây giờ bạn biết phần mềm độc hại là gì và phần mềm độc hại có thể làm gì, hãy đi sâu vào một số bước thực tế mà bạn có thể thực hiện để tự bảo vệ mình.

Cách ngăn chặn phần mềm độc hại:

Microsoft và các hãng khác thường phát hành các bản cập nhật cho hệ điều hành của họ và người dùng nên cài đặt các bản cập nhật này khi chúng có sẵn cho máy tính của mình. Những bản cập nhật này thường bao gồm các bản sửa lỗi có thể cải thiện tính bảo mật của hệ thống. Một số hệ điều hành cũng cung cấp bản cập nhật tự động để người dùng có thể tự động nhận được các bản cập nhật ngay sau khi chúng có sẵn.

- Luôn cập nhật máy tính và phần mềm đang dùng: Người dùng Windows có thể cài đặt bản cập nhật bằng cách sử dụng tính năng được gọi là "Cập nhật Windows", trong khi người dùng các sản phẩm khác có thể cài đặt bản cập nhật bằng cách sử dụng tính năng được gọi là "Cập nhật phần mềm". Nếu người dùng không quen với các tính năng này thì nên tìm kiếm trang web Microsoft và trang các hãng tương ứng để biết thêm thông tin về cách cài đặt bản cập nhật hệ thống trên máy tính của mình.

Ngoài hệ điều hành của máy tính, phần mềm máy tính cũng phải được cập nhật với phiên bản mới nhất. Phiên bản mới hơn thường chứa bản sửa lỗi bảo mật hơn để ngăn chặn phần mềm độc hại tấn công.

- Sử dụng tài khoản không phải là quản trị bất cứ khi nào có thể: Hầu hết các hệ điều hành đều cho phép người dùng tạo nhiều tài khoản người dùng trên máy tính để những người dùng khác nhau có thể có các cài đặt khác nhau. Người dùng có thể thiết lập những tài khoản này để có các cài đặt bảo mật khác nhau.

Ví dụ: tài khoản "quản trị" (hoặc "quản trị viên") thường có khả năng cài đặt phần mềm mới, trong khi tài khoản "có giới hạn" hoặc "chuẩn" thường không có khả năng làm như vậy. Khi duyệt web hàng ngày, bạn có thể không cần phải cài đặt phần mềm mới, vì vậy chúng tôi khuyên bạn nên sử dụng tài khoản người dùng "có giới hạn" hoặc "chuẩn" bất cứ khi nào có thể. Làm điều này có thể giúp ngăn chặn phần mềm độc hại cài đặt trên máy tính của bạn và thực hiện các thay đổi trên toàn bộ hệ thống.

- Hãy cân nhắc mỗi khi nhấp vào liên kết hoặc tải bất cứ thứ gì về máy: Trong thế giới thực, hầu hết mọi người đều có thể hơi nghi ngờ khi bước vào tòa nhà có vẻ khả nghi với bảng hiệu trưng bày "Máy tính miễn phí!" có đèn nhấp nháy. Trên web, bạn cũng nên áp dụng mức độ thận trọng tương tự khi truy cập vào trang web không quen thuộc tuyên bố cung cấp những thứ miễn phí.

Tải xuống là một trong những cách chính khiến mọi người bị nhiễm phần mềm độc hại, vì vậy, hãy nhớ suy nghĩ thật kỹ về nội dung bạn tải xuống và nơi bạn tải xuống.

- Hãy thận trọng khi mở tệp đính kèm hoặc hình ảnh trong email: Người dùng nên thận trọng nếu một người nào đó gửi cho mình email đáng ngờ có chứa tệp đính kèm hoặc hình ảnh. Đôi khi, những email đó có thể chỉ là spam, nhưng đôi khi, những email đó có thể bí mật chứa phần mềm độc hại gây hại.

- Sử dụng phần mềm diệt virus: Nếu bạn cần phải tải xuống mục gì đó, bạn nên sử dụng chương trình diệt vi rút để quét phần mềm độc hại cho bản tải xuống đó trước khi mở. Phần mềm diệt vi rút cũng cho phép quét phần mềm độc hại trên toàn bộ máy tính của người dùng. Nên thường xuyên quét máy tính của mình để sớm phát hiện phần mềm độc hại và ngăn chặn phần mềm độc hại đó phát tán.

Sử dụng các công cụ quét phần mềm phá hoại là một cách hiệu quả để bảo vệ hệ điều hành. Mặc dù chúng có thể quét hệ thống để phát hiện virus, sâu mạng và trojan horse, nhưng chúng thường được gọi là công cụ quét virus.

Khi mua một phần mềm quét virus, ta cần chú ý đến một số tính năng sau đây:

- Quét bộ nhớ và diệt virus.

- Quét bộ nhớ một cách liên tục.

- Quét ổ đĩa và diệt virus.

- Quét tất cả các định dạng tệp, kể cả tệp nén.

- Tự động chạy theo một thời gian biểu do người sử dụng đặt.

- Có tuỳ chọn chạy nhân công.

- Phát hiện cả phần mềm phá hoại đã công bố hoặc phần mềm phá hoại mới (chưa được biết đến).

- Quét các tệp tải về từ trên mạng hoặc từ internet.

- Sử dụng một vùng được bảo vệ hoặc được cách ly để chứa các tệp tải về để tự động quét chúng ở một nơi an toàn trước khi sử dụng chúng.

Về các phần mềm phá hoại chưa được biết đến, các công cụ quét có thể được tạo ra để quét và ghi nhớ cấu trúc của các tệp, đặc biệt là các tệp thực thi. Khi chúng phát hiện một số lượng bất thường, như kích cỡ của tệp lớn đột đột hoặc một thuộc tính của tệp bị thay đổi, thì công cụ quét sẽ được cảnh báo có thể đó là một phần mềm phá hoại chưa được biết đến. Trong trường hợp này, công cụ quét có thể thông báo cho người dùng và chỉ ra một số cách để giải quyết chúng.

*** Bảo vệ với dạng tấn công lỗ hổng bảo mật**

Một số hệ điều hành mới thường có những lỗ hổng bảo mật truy nhập internet hoặc các lỗi làm cho hệ thống bị các xung đột không mong muốn, làm cho các lệnh không hoạt động bình thường và nhiều vấn đề khác.

Hiện nay nhiều kẻ xấu hay lợi dụng những lỗ hổng bảo mật để tấn công vào các hệ thống để phá hoại hoặc lấy cắp thông tin vì vậy người dùng nên thường xuyên cài đặt các bản cập nhật (updates) bảo vệ hệ thống của mình. Việc cài đặt các bản cập nhật và các bản vá lỗi (patches) là cách rất hiệu quả để chống lại các tấn công trên một hệ điều hành.

Người dùng có thể tải các phiên bản vá lỗi mới nhất cho các hệ điều hành và phần mềm Microsoft khác nhau từ địa chỉ www.microsoft.com/downloads.

*** Bảo vệ thông tin trước nguy cơ tấn công bằng cách phá mật khẩu**

- Sử dụng phương thức chứng thực tên truy cập và mật khẩu là phương pháp được dùng phổ biến đối với các hệ thống vì vậy xây dựng một chính sách sử dụng mật tốt sẽ đạt hiệu quả cao như: Tạo một quy tắc đặt mật khẩu riêng cho mình, không nên dùng lại mật khẩu đã sử dụng, tránh những mật khẩu dễ đoán như ngày sinh, tên người thân,… thường xuyên thay đổi mật khẩu đăng nhập hệ thống để tránh trường hợp người dùng vô tình làm lộ mật khẩu hoặc kẻ xấu cố tình lấy cắp mật khẩu.

- Sử dụng các ký tự mật khẩu có tính an toàn cao như: Sử dụng mật khẩu có độ dài đủ lớn (8 ký tự trở lên) và trong đó có sử dụng các ký tự chữ in, chữ thường, ký tự đặc biệt, ký tự số,… Ví dụ: Lee_Thuyr;DT612

*** Bảo vệ thông tin do nguy cơ do sử dụng e-mail**

Trong thời gian gần đây virus hoành hành và tấn công vào các Email đã trở thành vấn đề nhức nhối đối với người sử dụng và các tổ chức gây các tổn thất nặng nề.

Để đảm bảo an toàn cho Email cần có ý thức bảo vệ được máy tính bằng việc tuân thủ các điều sau:

- Không mở bất kỳ tập tin đính kèm được gửi từ một địa chỉ e-mail mà không biết rõ hoặc không tin tưởng.

- Không mở bất kỳ e-mail nào mà mình cảm thấy nghi ngờ, thậm chí cả khi e-mail này được gửi từ bạn bè hoặc đối tác bởi hầu hết virus được lan truyền qua đường e-mail và chúng sử dụng các địa chỉ trong sổ địa chỉ (Address Book) trong máy nạn nhân để tự phát tán. Do vậy, nếu không chắc chắn về một e-mail nào thì hãy tìm cách xác nhận lại từ phía người gửi.

- Không mở những tập tin đính kèm theo các e-mail có tiêu đề hấp dẫn, nhạy cảm.

- Nên xóa các e-mail không rõ hoặc không mong muốn và không forward (chuyển tiếp) chúng cho bất kỳ ai hoặc reply (hồi âm) lại cho người gửi. Những e-mail này thường là thư rác (spam).

- Không sao chép vào đĩa cứng bất kỳ tập tin nào mà bạn không biết rõ hoặc không tin tưởng về nguồn gốc xuất phát của nó.

- Hãy thận trọng khi tải các tập tin từ Internet về đĩa cứng của máy tính. Dùng một chương trình diệt virus được cập nhật thường xuyên để kiểm tra những tập tin này. Nếu nghi ngờ về một tập tin chương trình hoặc một e-mail thì đừng bao giờ mở nó ra hoặc tải về máy tính của mình. Cách tốt nhất trong trường hợp này là xóa chúng hoặc không tải về máy tính của mình.

- Dùng một chương trình diệt virus tin cậy và được cập nhật thường xuyên như Norton Anti Virus, McAffee, Trend Micro, BKAV, D32... Sử dụng những chương trình diệt virus có thể chạy thường trú trong bộ nhớ để chúng thường xuyên giám sát các hoạt động trên máy tính và ở chức năng quét e-mail.

*** Bảo vệ do mất an toàn thông tin trong quá trình lưu thông và truyền tin**

Để bảo vệ thông tin trong quá trình lưu thông và truyền tin trên mạng thường dùng các kỹ thuật an toàn thông tin như: mã hóa, giấu tin, thủy vân số, chữ ký số,..

*** Bảo vệ hệ thống bằng tường lửa (firewall)**

Tường lửa có thể là hệ thống phần cứng, phần mềm hoặc kết hợp cả hai. Nếu là phần cứng thì sử dụng bộ bộ định tuyến (router). Bộ định tuyến có các tính năng bảo mật cao cấp, trong đó có khả năng kiểm soát địa chỉ IP (IP Address ố là sơ đồ địa chỉ hoá để định nghĩa các trạm (host) trong liên mạng). Quy trình kiểm soát cho phép định ra những địa chỉ IP có thể kết nối với mạng của tổ chức, cá nhân và ngược lại. Tính chất chung của các tường lửa là phân biệt địa chỉ IP hay từ chối việc truy nhập không hợp pháp căn cứ trên địa chỉ nguồn.

Chức năng chính của Firewall là kiểm soát luồng thông tin từ giữa Intranet và Internet. Thiết lập cơ chế điều khiển dòng thông tin giữa mạng bên trong (Intranet) và mạng Internet. Cụ thể là:

Cho phép hoặc cấm những dịch vụ truy nhập ra ngoài (từ Intranet ra Internet).

Cho phép hoặc cấm những dịch vụ phép truy nhập vào trong (từ Internet vào Intranet).

Theo dõi luồng dữ liệu mạng giữa Internet và Intranet.

Kiểm soát địa chỉ truy nhập, cấm địa chỉ truy nhập.

Kiểm soát người sử dụng và việc truy nhập của ngời sử dụng.

Kiểm soát nội dung thông tin thông tin lu chuyển trên mạng.

Các thành phần Firewall chuẩn bao gồm một hay nhiều các thành phần sau đây:

Bộ lọc packet (packet-filtering router)

Cổng ứng dụng (application-level gateway hay proxy server)

Cổng mạch (circuite level gateway)

Bộ lọc paket (Paket filtering router).

4. Một số kỹ thuật an toàn và bảo mật thông tin

* Mã hóa thông tin

Trong khoa học mật mã là việc sử dụng các kỹ thuật thích hợp để biến đổi một bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau giữa người gửi và người nhận mà người ngoài cuộc có thể có được sự hiện hữu của dãy mã ngẫu nhiên đó nhưng khó có thể chuyển thành bản thông điệp ban đầu nếu không có "khóa" để giải mã của thông điệp.

Mã hóa và giải mã gồm:

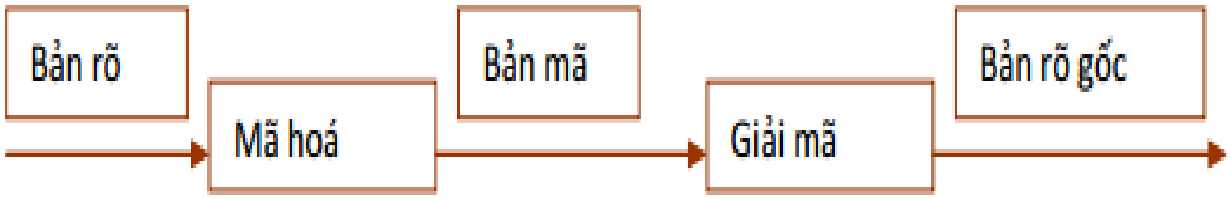
- Bản rõ (plaintext or cleartext): Chứa các xâu ký tự gốc, thông tin trong bản rõ là thông tin cần mã hoá để giữ bí mật.

- Bản mã (ciphertext): Chứa các ký tự sau khi đã được mã hoá, mà nội dung của nó được giữ bí mật.

- Mật mã học (Crytography) Là nghệ thuật và khoa học để giữ thông tin được an toàn.

- Sự mã hoá (Encryption): Quá trình che dấu thông tin bằng phương pháp nào đó để làm ẩn nội dung bên trong gọi là sự mã hoá.

- Sự giải mã (Decryption): Quá trình biến đổi trả lại bản mã bản thành bản rõ gọi là giải mã.

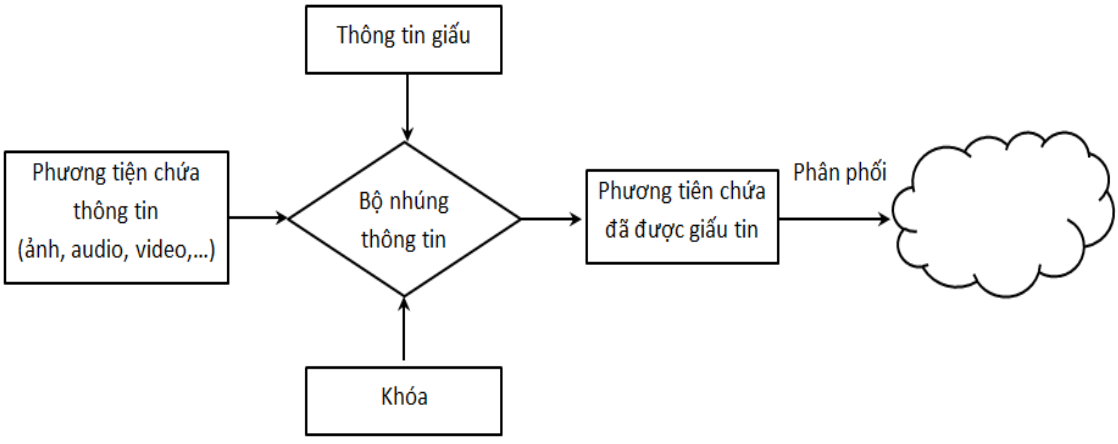


* Giấu tin

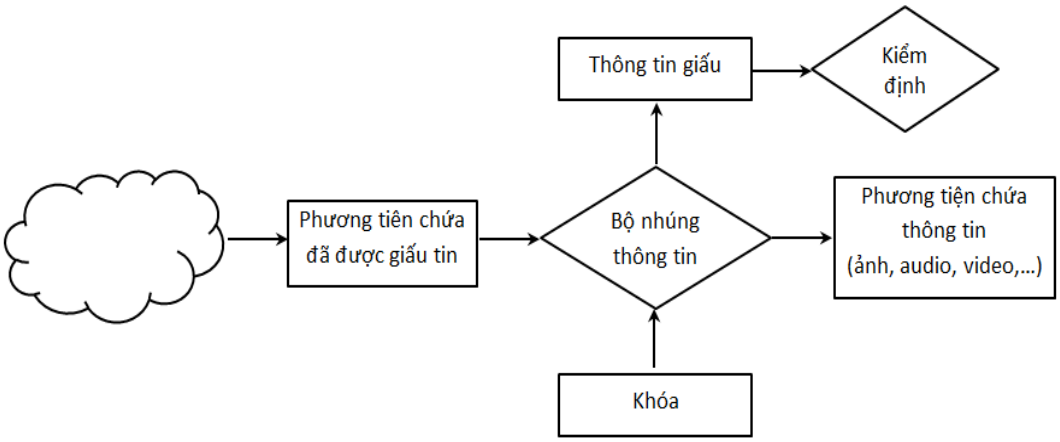
Giấu tin là kỹ thuật nhúng một lượng thông tin số (ảnh, audio, video) vào trong một đối tượng dữ liệu số khác. Một trong những yêu cầu cơ bản của giấu tin là đảm bảo tính chất ẩn của thông tin được giấu, đồng thời không làm ảnh hưởng đến chất lượng của dữ liệu gốc. Mục đích của giấu tin là làm cho thông tin đã giấu không thể nghe thấy hoặc nhìn thấy được, người ngoài cuộc không thể nhận thấy được sự tồn tại của thông tin đã giấu.

Kỹ thuật giấu tin gồm 2 phần là thuật toán giấu tin và thuật toán tách thông tin đã giấu trong ra khỏi phương tiện mang tin đã giấu.

Giấu tin khác với mật mã ở chỗ trong khi kỹ thuật giấu tin mật là tìm cách ẩn giấu thông điệp vào một phương tiện số như hình ảnh, audio, video mà người ngoài cuộc khó có thể phát hiện được sự hiện hữu của thông điệp trong phương tiện số đó mặc dù người ngoài cuộc có thể có nó trong tay. Còn trong khoa học mật mã người ta tìm cách để biến đổi bản thông điệp có ý nghĩa thành một dãy mã ngẫu nhiên để liên lạc với nhau trên mạng công cộng mà người ngoài cuộc có thể có được sự hiện hữu của dãy mã ngẫu nhiên đó nhưng khó có thể chuyển thành bản thông điệp ban đầu nếu không có "khóa" để giải mã của thông điệp.



Quá trình giấu tin



Quá trình tách (lấy ra) thông tin đã giấu

*** Thủy vân số**

Thủy vân số là kỹ thuật nhúng thông tin vào dữ liệu (dữ liệu có thể là văn bản, hình ảnh, audio, video hay cơ sở dữ liệu,...) trước khi phân phối dữ liệu trên môi trường trao đổi thông tin nhằm xác định thông tin về chủ sở hữu hoặc nhận biết sự tấn công trái phép từ bên ngoài đối với dữ liệu đã được thủy vân. Thông tin giấu trong dữ liệu được gọi là thủy vân (watermark).

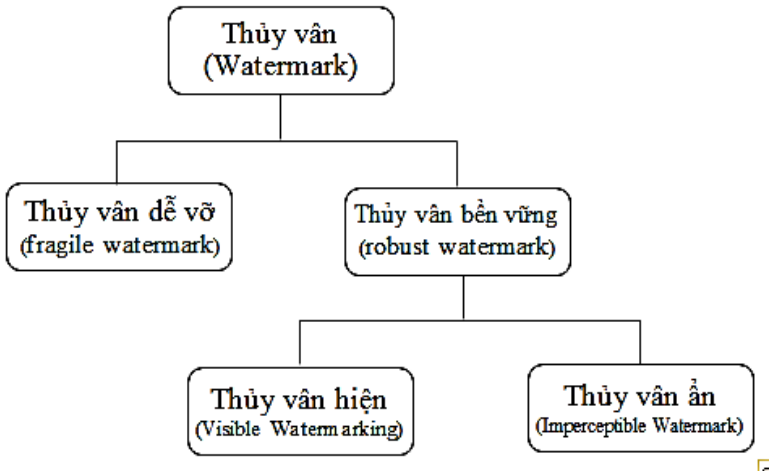
Thủy vân bền vững là kỹ thuật nhúng thủy vân vào dữ liệu sao cho khi phân phối dữ liệu trong môi trường mở thủy vân này luôn tồn tại bền vững với dữ liệu gốc và không dễ bị phá hủy trước những biến đổi, tấn công dữ liệu. Kỹ thuật này thường được sử dụng trong các ứng dụng bảo vệ bản quyền, chứng minh quyền sở hữu. Trong những ứng dụng này, thủy vân đóng vai trò là thông tin sở hữu của người chủ hợp pháp. Thủy vân được nhúng trong sản phẩm như một hình thức dán tem bản quyền. Trong trường hợp này thủy vân phải tồn tại bền vững với sản phẩm nhằm chống lại việc tẩy xóa, làm giả hay biến đổi phá hủy thủy vân. Một yêu cầu đối với thủy vân bền vững là nếu muốn loại bỏ thủy vân thì chỉ có một cách đó là phá hủy sản phẩm.

Trong thủy vân bền vững được chia làm hai loại là thủy vân ẩn và thủy vân hiện.

Thủy vân ẩn: Là thủy vân mà mắt thường không thể nhìn thấy thủy vân, chỉ chủ sở hữu sản phẩm mới có khả năng nhìn thấy được sau khi giải mã khóa. Trong bảo vệ bản quyền, thủy vân ẩn mang tính bất ngờ hơn trong việc phát hiện sản phẩm bị đánh cắp. Người chủ sở hữu sẽ chỉ ra bằng chứng là thủy vân đã được nhúng trong sản phẩm.

Thủy vân hiện: Là loại thủy vân được hiện ngay trên sản phẩm và người dùng có thể nhìn thấy được giống như các biểu tượng logo trên các sản phẩm, trên các kênh truyền hình mà ta thường thấy. Các thủy vân hiện trên sản phẩm thường dưới dạng chìm, mờ hoặc trong suốt để không gây ảnh hưởng đến chất lượng sản phẩm gốc. Đối với thủy vân hiện, thông tin bản quyền hiển thị ngay trên sản phẩm.

Thủy vân dễ vỡ là kỹ thuật nhúng thủy vân sao cho khi phân phối sản phẩm trong môi trường mở nếu có bất cứ sự biến đổi nào làm thay đổi sản phẩm gốc thì thủy vân đã được giấu trong đó sẽ không còn nguyên vẹn như trước khi giấu, tức là nó dễ bị biến đổi trước những tấn công dữ liệu. Kỹ thuật này thường được dùng trong các ứng dụng xác thực thông tin, đảm bảo sự toàn vẹn dữ liệu, chống xuyên tạc.



*** Chữ ký số**

Ngày nay, với sự phát triển bùng nổ của công nghệ thông tin nói chung và Internet nói riêng, công việc kinh doanh của các doanh nghiệp trở nên thuận lợi hơn,

tiết kiệm được rất nhiều thời gian cũng như các thủ tục hành chính. Tuy nhiên, Internet cũng mang lại nhiều rủi ro cho các tổ chức, cá nhân, mà một trong những vấn đề lớn nhất và vấn đề gian lận vì vậy chữ ký số đã được ra đời để đảm bảo sự an toàn trong việc giao dịch số.

Chữ ký điện số là thông tin đi kèm theo dữ liệu (văn bản, âm thanh,hình ảnh, video...) nhằm mục đích xác định người chủ của dữ liệu đó.

Chữ ký điện số là chuỗi thông tin cho phép xác định nguồn gốc, xuất xứ, thực thể đã tạo ra 1 thông điệp.

Chữ ký số khóa công khai là mô hình sử dụng các kỹ thuật mật mã để gắn với mỗi người sử dụng một cặp khóa công khai - bí mật, qua đó có thể ký các văn bản điện tử cũng như trao đổi các thông tin mật.

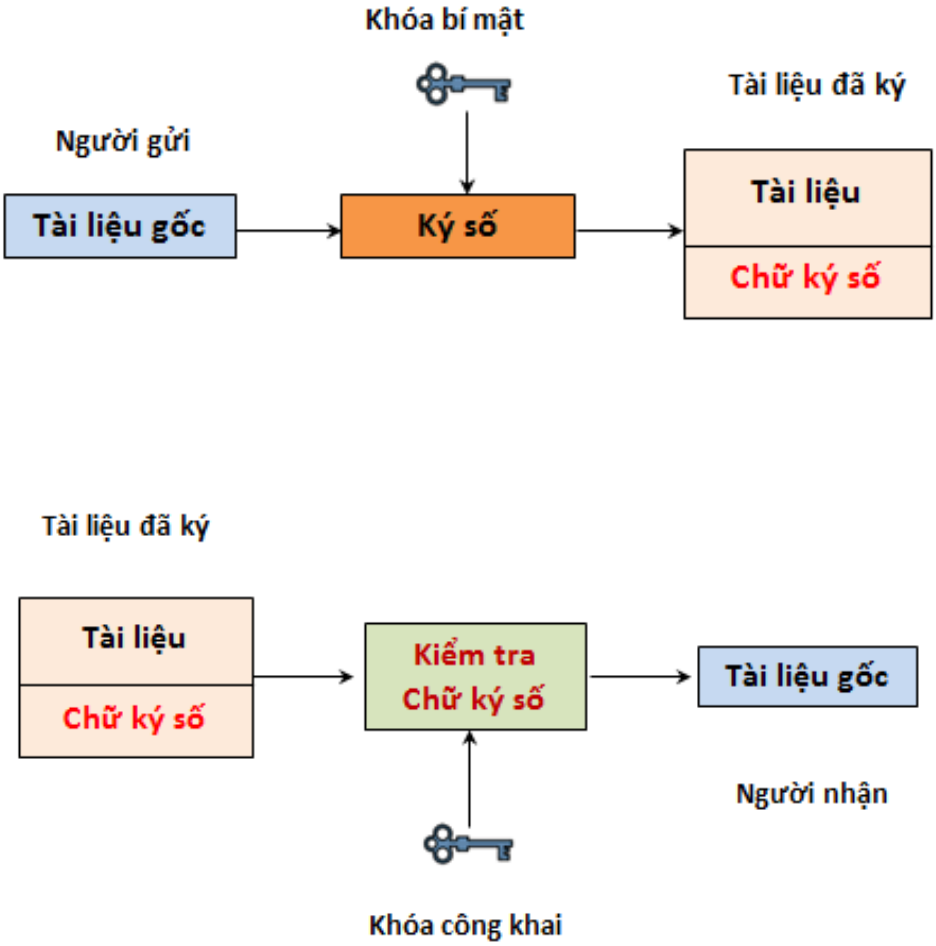
Khóa công khai thường được phân phối thông qua chứng thực khóa công khai.

Quá trình sử dụng chữ ký số bao gồm 2 phần: tạo chữ ký và kiểm tra chữ ký.

Mỗi người cần 1 cặp khóa gồm khóa công khai và khóa bí mật.

Khóa bí mật dùng để tạo chữ ký số (CKS) và khóa công khai dùng để thẩm định chữ ký số (xác thực)

Thẩm định chữ ký số: Quá trình thẩm định chữ ký số là quá trình xác thực được người gửi, chống chối bỏ, xác thực sự toàn vẹn của thông tin.



III. KẾT LUẬN

Công nghệ thông tin và truyền thông đóng vai trò ngày càng quan trọng trong cuộc sống hàng ngày của con người, làm biến đổi sâu sắc cách thức làm việc, giải trí, các nguyên tắc tiến hành kinh doanh…Vì vậy để đảm bảo an toàn thông tin cần phải tìm hiểu, nghiên cứu các nguy cơ mất an toàn thông tin như: nguy cơ về vật lý, về phầm mềm độc hại,…và sử dụng các biện pháp bảo vệ hệ thống thông tin một cách an toàn như: sử dụng các chính sách, các kỹ thuật an toàn thông tin và các phần mềm diệt virus.