ĐẢM BẢO AN TOÀN THÔNG TIN TRONG THƯ VIỆN ĐIỆN TỬ

ThS Nguyễn Văn Hiệp
Trường Đại học KHXH&NV Tp. Hồ Chí Minh

Sự phát triển của công nghệ thông tin và truyền thông đã và đang tác động sâu sắc đến kinh tế, chính trị và đời sống xã hội. Ngày càng nhiều tổ chức, đơn vị, doanh nghiệp hoạt động lệ thuộc gần như hoàn toàn vào hệ thống mạng máy tính, máy tính và cơ sở dữ liệu. Nói cách khác, khi hệ thống thông tin (HTTT) hoặc cơ sở dữ liệu gặp sự cố thì hoạt động của các đơn vị này bị ảnh hưởng nghiêm trọng, thậm chí có thể bị tê liệt hoàn toàn.

Vấn đề đảm bảo an toàn thông tin (ATTT) ngày càng nhận được nhiều sự quan tâm. Giờ đây ATTT được xếp ngang hàng với những vấn đề thiết thực trong cuộc sống như: an toàn thực phẩm, an toàn y tế, an toàn lao động... và được Đảng và Nhà nước ta đặc biệt quan tâm. Đã có rất nhiều văn bản của chính phủ được đưa ra yêu cầu các cơ quan, tổ chức, doanh nghiệp thực hiện các biện pháp đảm bảo ATTT trong hoạt động của đơn vị mình [4, 5, 6, 7].

Tuy nhiên, xây dựng một hệ thống đảm bảo ATTT toàn diện, hiệu quả không phải là một công việc dễ dàng, đặc biệt đối với các cơ quan thông tin-thư viện, nơi ATTT còn là một khái niệm khá mới, đội ngũ cán bộ còn yếu về công nghệ thông tin và vấn đề ATTT thường được mặc định chỉ dành cho bộ phận công nghệ thông tin.

1. Khái niệm về An toàn thông tin

"*An toàn thông tin: bao gồm các hoạt động quản lý, nghiệp vụ và kỹ thuật đối với hệ thống thông tin nhằm bảo vệ, khôi phục các hệ thống, các dịch vụ và nội dung thông tin đối với nguy cơ tự nhiên hoặc do con người gây ra. Việc bảo vệ thông tin, tài sản và con người trong hệ thống thông tin nhằm bảo đảm cho các hệ thống thực hiện đúng chức năng, phục vụ đúng đối tượng một cách sẵn sàng, chính xác và tin cậy. ATTT bao hàm các nội dung bảo vệ và bảo mật thông tin, an toàn dữ liệu, an toàn máy tính và an toàn mạng"* [4].

Theo ISO 17799/27001 [10], *ATTT là khả năng bảo vệ đối với môi trường thông tin kinh tế- xã hội, đảm bảo cho việc hình thành, sử dụng và phát triển vì lợi ích của mọi công dân, mọi tổ chức và của quốc gia. Thông qua các chính sách về ATTT, lãnh đạo thể hiện ý chí và năng lực của mình trong việc quản lý hệ thống thông tin. ATTT được xây dựng trên nền tảng một hệ thống các chính sách, quy tắc, quy trình và các giải pháp kỹ thuật nhằm mục đích đảm bảo an toàn tài nguyên thông tin mà tổ chức đó sở hữu cũng như các tài nguyên thông tin của các đối tác, các khách hàng trong một môi trường thông tin toàn cầu.*

Tựu chung lại, ATTT là sự duy trì tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin, trong đó:

***Tính bí mật**:* thông tin chỉ được khai thác bởi những đối tượng (người, chương trình máy tính…) được cấp phép.

Tính toàn vẹn: thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được cấp phép và phải đảm bảo thông tin vẫn còn chính xác khi được lưu trữ và truyền đi.

***Tính sẵn sàng**:* thông tin có thể được truy xuất bởi những người được phép vào bất cứ khi nào họ muốn.

Trong hoạt động thư viện, ATTT "là việc đảm bảo phần cứng, các dịch vụ, các chương trình và thông tin luôn ở trạng thái sẵn sàng cho người sử dụng" [12]. Nói cách khác, đảm bảo ATTT trong thư viện là việc bảo vệ thông tin và HTTT khỏi các truy cập, chỉnh sửa hoặc sử dụng thông tin trái phép. Việc đảm bảo

ATTT trong thư viện cũng phải duy trì được tính bí mật, tính toàn vẹn và tính sẵn sàng, cụ thể như sau:

Tính bí mật: chỉ những người dùng được cấp quyền mới được phép truy cập vào các cơ sở dữ liệu, nguồn tài liệu điện tử và các tài nguyên khác của thư viện. Thư viện không được phép tiết lộ thông tin của người sử dụng như thông tin cá nhân của người sử dụng, thông tin về lịch sử mượn - trả…

Tính toàn vẹn: đảm bảo sự chính xác, không thay đổi của thông tin gốc, ví dụ như các thông tin thư mục trong các cơ sở dữ liệu, thông tin được đăng tải trên website của thư viện…

Tính sẵn sàng: các nguồn tin của thư viện phải luôn trong trạng thái sẵn sàng cho người sử dụng truy cập bất cứ thời gian nào, ví dụ: hệ thống OPAC, website thư viện, các cơ sở dữ liệu điện tử…

2. Thư viện điện tử và các điểm yếu an toàn thông tin

2.1. Khái niệm thư viện điện tử

Thư viện điện tử (TVĐT) là một khái niệm chưa được định nghĩa thống nhất và còn nhiều tranh luận. Theo Hiệp hội Thư viện Viện nghiên cứu (Association of Research Library), các thuật ngữ như: "Thư viện điện tử - E - Library", "Thư viện số - Digital Library", "Thư viện ảo - Virtual Library", " Thư viện tin học hoá", "Thư viện đa phương tiện",… được sử dụng cùng một nội dung, ý nghĩa. Tuy nhiên, ngày nay thuật ngữ "thư viện số" được cộng đồng thư viện thế giới sử dụng nhiều và phổ biến. Còn ở Việt Nam, thuật ngữ "Thư viện điện tử" lại được sử dụng phổ biến hơn. Theo Philip Baker: "*TVĐT là thư viện lưu trữ và phục vụ cả ấn phẩm lẫn tư liệu điện tử (tư liệu số hóa)" [14]*. Theo Liên đoàn Thư viện số - 1993: "*Các thư viện số là các tổ chức cung cấp các nguồn lực, cung cấp khả năng truy cập tới các nguồn tri thức, phiên dịch, phân phối, bảo đảm tính toàn vẹn và lâu dài của các bộ sưu tập số để cho một cộng đồng hoặc một tập hợp cộng đồng người dùng tin xác định luôn có thể sử dụng một cách nhanh chóng, kịp thời và kinh tế*" [15].

Tóm lại, TVĐT thực chất là một hệ thống thông tin hoàn chỉnh, được hiểu là nơi lưu trữ nguồn thông tin số hóa, đặc biệt là thông tin toàn văn, đồng thời sử dụng các phương tiện điện tử trong thu thập, lưu trữ, xử lý, tìm kiếm và phổ biến thông tin. Cũng chính vì lẽ đó, vấn đề ATTT trong các TVĐT là một trong các yếu tố sống còn của một HTTT thư viện. Yêu cầu đặt ra là phải làm sao để có thể đáp ứng mọi dịch vụ của một thư viện, đồng thời phải luôn đảm bảo hệ thống được vận hành một cách an toàn.

2.2. Các yêu cầu về ATTT trong TVĐT

Mục tiêu của các cuộc tấn công vào HTTT trong đó có TVĐT là nhằm phá vỡ cấu trúc ATTT dựa trên ba tính chất là " tính bí mật", " tính toàn vẹn" và "tính sẵn sàng". Chính vì vậy, các yêu cầu về ATTT cũng xoay quanh việc xây dựng các giải pháp nhằm chống trả các hành vi làm vô hiệu một hoặc cả ba tính chất trên. Cần nhấn mạnh rằng, mặc dù ba tính chất trên có tính độc lập, song trong thực tế chúng có ảnh hưởng lẫn nhau. Khi một tính chất bị xâm hại, cấu trúc ATTT sẽ bị phá vỡ và sẽ tác động đến các tính chất còn lại. Vì vậy, để đảm bảo ATTT cần có một giải pháp toàn diện, đồng bộ.

Vì những lý do trên, *yêu cầu đầu tiên* về ATTT cho hệ thống TVĐT là *"Tính nhất quán, đồng bộ trong việc quản lý ATTT"*. Yêu cầu trên chỉ có thể được thực hiện khi xây dựng được một bộ chính sách về ATTT dựa trên một tiêu chuẩn nào đó, ví dụ như ISO17799 / ISO 27001. Hiện nay nhiều cơ quan, tổ chức đang đi theo hướng này.

Yêu cầu thứ hai là tính liên tục: HTTT TVĐT hoạt động liên tục, vì vậy các quy trình về ATTT phải được vận hành liên tục 24/7.

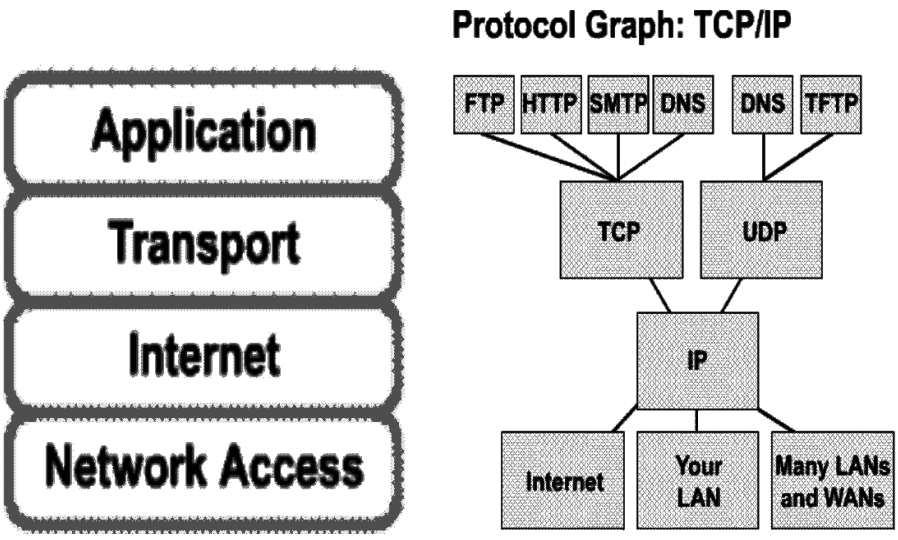
Tính liên tục đảm bảo cho HTTT được vận hành an toàn trong mọi tình huống, ngay cả những tình huống cực đoan như cháy nổ, khủng bố, thiên tai. Không nên hiểu ATTT chỉ là hành động nhất thời *"Thủng đâu vá đó"* mà đây là một quy trình liên tục: Lập kế hoạch (PLAN) →Xác định, phân tích, thiết kế (DO)→Kiểm tra ATTT (CHECK) → Duy trì ATTT (ACT).

Yêu cầu thứ ba về ATTT là tính phổ cập: Các quy tắc, quy trình về ATTT cần được quán triệt và liên tục được cập nhật trong phạm vi toàn thư viện nhằm nâng cao nhận thức cũng như trách nhiệm về ATTT của từng thành viên. ATTT không phải là chuyện riêng của lãnh đạo, nhà quản lý, cán bộ công nghệ thông tin mà là trách nhiệm của cộng đồng đối với nguồn tài nguyên thông tin của mình. Vì vậy ATTT thực sự được thực thi hiệu quả chỉ khi có sự chung tay góp sức của toàn thể người sử dụng trong HTTT của TVĐT.

2.3. Một số nguy cơ ATTT tác động lên TVĐT

Các nguy cơ từ cơ sở hạ tầng kỹ thuật: An toàn cơ sở hạ tầng kỹ thuật bao gồm nhiều yếu tố như: an toàn vật lý, an toàn phần cứng, an toàn phần mềm, an toàn hạ tầng mạng, an toàn hệ điều hành, an toàn ứng dụng web… Tuy nhiên, do nhận thức về ATTT chưa đầy đủ, kinh phí hoạt động eo hẹp, đặc biệt là kinh phí dành cho vấn đề đảm bảo ATTT, nên hiện nay đa phần các TVĐT chưa chú trọng đến việc đầu tư về cơ sở hạ tầng kỹ thuật. Đơn cử là việc rất nhiều thư viện sử dụng các phần mềm hệ điều hành không bản quyền, không quan tâm tới việc cập nhật các bản vá lỗi hệ điều hành, hệ thống không được trang bị các phương tiện ATTT và xây dựng các giải pháp ATTT như tường lửa, các hệ thống phát hiện xâm nhập trái phép (IDS, IPS…); Sử dụng các phần mềm quản trị thư viện tích hợp không được bảo hiểm về ATTT…

***Các nguy cơ trên giao thức TCP/IP*:** Hiện nay các TVĐT nói riêng và các hệ thống thông tin khác nói chung chủ yếu sử dụng giao thức TCP/IP. Đây là một giao thức dựa trên chuẩn ISO, cho phép sự tương giao (interoperability) giữa các hệ máy (platform) đa dạng được cung cấp bởi các nhà sản xuất khác nhau. Mô hình TCP/IP (Hình 1) dựa trên nền tảng cấu trúc OSI 7 lớp. Đây là một giao thức đơn giản, dễ sử dụng và phổ cập. Tuy nhiên, do cấu trúc và một số đặc tính truyền giao dữ liệu, giao thức này còn mang trong mình rất nhiều điểm yếu.



Hình 1. *Mô hình TCP/IP*

Một số nguy cơ TCP/IP có thể bị tấn công như:

• *TCP/IP Attacks*: Loại tấn công này xảy ra trên lớp IP hay "host-to-host". Một số Router/Firewall có thể ngăn chặn một số giao thức khó kiểm soát trên Internet, tuy nhiên vẫn có một số giao thức không an toàn mà hacker có thể lợi dụng như SMTP & ICMP, TCP, UDP và IP.

• *Các hình thức tấn công TCP/IP gặp phải như*:

- Port Scans (Quét các cổng).

- TCP SYN or TCP ACK Flood Attack (tấn công tràn bộ đệm).

- TCP Sequence Number Attack.

- TCP/IP Hijacking (Giả mạo TCP/IP).

- Network Sniffers: Bắt giữ và hiển thị các thông báo trên mạng.

- Tấn công từ chối dịch vụ (Denial Of Service attacks- DOS/DDOS): Loại tấn công khai thác các điểm yếu trên các dịch vụ TCP và UDP nhằm vô hiệu các dịch vụ của thư viện. Bản chất thực sự của DOS/DDOS là kẻ tấn công sẽ chiếm dụng một lượng lớn tài nguyên mạng như băng thông, bộ nhớ... và làm mất khả năng xử lý các yêu cầu dịch vụ từ người sử dụng khác.

***Các nguy cơ từ các sản phẩm phần mềm*:** Do tính "công cộng" (public) của hệ thống, các phần mềm được các TVĐT sử dụng đa phần là những sản phẩm thương mại, không được bảo hiểm về ATTT. Hệ thống thông tin TVĐT dễ bị tổn thương bởi một loạt các phần mềm độc hại (Malware) và các phần mềm gián điệp (Spyware) như: trojan, virus, worms, adware, keylogger, rootkit [17]. Các phần mềm thư viện khi được thiết kế thường ít chú trọng đến các lỗi bảo mật và thường không có các bản vá lỗi (servise park) nên trong quá trình sử dụng dễ bị hacker khai thác các lỗi bảo mật như: "SQL injection", Cross-site Scripting (XSS), các lỗi lập trình… Một trong những tác hại của lỗi phần mềm là phá hoại tính toàn vẹn của dữ liệu như: đánh cắp một cách bất hợp pháp quyền sử dụng dữ liệu, xóa, sửa, thêm dữ liệu hoặc phát lại một số thông tin quan trọng nhằm thực hiện một số mục đích của kẻ tấn công. Một trong những công cụ quan trọng nhất để đảm bảo tính toàn vẹn dữ liệu là sử dụng các công cụ mật mã như các hàm băm một chiều (OWHF). Hiện nay, các giải thuật được sử dụng phổ biến là MD5, SHA1, SHA2.

***Các nguy cơ do người dùng*:** Xuất phát từ đặc điểm *"Công cộng"*, người dùng trong hệ thống thư viện rất đa dạng, nhận thức về ATTT không đồng nhất, điều này gây ra rất nhiều rủi ro cho hệ thống. Việc kiểm soát truy cập, quản lý chất lượng mật khẩu, kiểm soát và bảo vệ thông tin cá nhân, ngăn chặn các hành vi lấy cắp, sửa đổi nội dung thông tin đang là những thách thức cho các nhà quản trị hệ thống thư viện. Theo nhiều tài liệu nghiên cứu, có 80% nguy cơ các cuộc tấn công xuất phát từ nội bộ. Điều này cho thấy con người là khâu yếu nhất trong toàn bộ quy trình an toàn và bảo mật thông tin.

Kỹ thuật khai thác điểm yếu do người dùng phổ biến là *"social engenering"[13]*. Kỹ thuật *"social engenering" là phương pháp tấn công phi kỹ thuật, dựa trên sự thiếu hiểu biết của người dùng* để lừa gạt họ cung cấp các thông tin nhạy cảm như username, password hay các thông tin quan trọng khác. Chính vì yếu tố tấn công phi kỹ thuật dựa trên sự thiếu hiểu biết, không đề phòng của người sử dụng mà dạng tấn công này được xem là dạng tấn công nguy hiểm nhất.

Ngoài việc phòng chống bốn nhóm nguy cơ nêu trên, để đảm bảo an toàn hạ tầng TVĐT các nhà quản lý cũng cần quan tâm tới việc nâng cao nhận thức và hiểu biết về ATTT, đặc biệt cần xây dựng một bộ quy tắc, chính sách

về ATTT giúp cho việc quản lý, vận hành hệ thống được an toàn và hiệu quả.

3. Các giải pháp an toàn thông tin đối với thư viện điện tử

3.1. An toàn vật lý

An toàn vật lý là đảm bảo sự an toàn của các thiết bị như máy tính, máy in, màn hình, router, switch, cáp… Các thiết bị này cần được đặt tại các vị trí an toàn, ví dụ, trong các phòng có hệ thống bảo vệ như khóa, hệ thống chống trộm, camera… nhằm ngăn chặn các hành vi ăn cắp tài sản, truy cập trái phép vào các máy chủ hệ thống, phá hoại dữ liệu, hoặc truy cập vào các nguồn tài nguyên mật của thư viện. Nói tóm lại, TVĐT cần thực hiện các biện pháp an ninh mức vật lý như các thiết bị phải được triển khai với yêu cầu giảm thiểu thâm nhập của những đối tượng bên ngoài không có trách nhiệm; các hệ thống xử lý và bảo vệ thông tin có chứa các dữ liệu quan trọng cần phải được đặt sao cho giảm thiểu khả năng thâm nhập cố tình hay hữu ý của những người không được phép; những thiết bị có yêu cầu bảo vệ đặc biệt như server chứa dữ liệu quan trọng của thư viện cần phải được cách ly; có các biện pháp bảo vệ sao cho giảm thiểu tối đa các mối đe dọa như lửa, cháy nổ, khói, nước, bụi, những tác động cơ học, các hóa chất, các bức xạ điện từ trường mạnh và tia phóng xạ…; các thiết bị cần phải được theo dõi thường xuyên và được kiểm tra định kỳ, nếu phát hiện các dấu hiệu có thể gây ra các hỏng hóc cho hệ thống cần sử dụng các phương tiện bảo vệ đặc biệt; đảm bảo an toàn hệ thống cáp; thực hiện an toàn nơi làm việc; các thông tin quý giá nếu không được sử dụng cần được lưu trữ trong môi trường được bảo vệ; các máy tính cá nhân, máy in phải được theo dõi trong thời gian xử lý thông tin và cần được bảo vệ khỏi các hành vi đánh cắp bàn phím, mật khẩu và các hành vi khác trong thời gian không có mặt người sử dụng;…

3.2. An toàn hạ tầng mạng

Trong các TVĐT, nguồn tài nguyên thông tin được truy cập thông qua Internet và mạng máy tính đóng một vai trò quan trọng trong việc kết nối các nguồn tài nguyên thông tin [14]. Hơn thế, đảm bảo tính sẵn sàng, hiệu quả và hiệu quả chi phí của việc truy cập mạng trong kỷ nguyên số sẽ là năng lực cốt lõi của các thư viện. Do đó, an ninh mạng có một vai trò vô cùng quan trọng đối với các TVĐT nhằm duy trì tính toàn vẹn của dữ liệu.

Đảm bảo an toàn hạ tầng mạng trong các TVĐT nhằm chống lại bốn nhóm nguy cơ đó là: truy cập trái phép (Non - authorized access); mất mát hay rò rỉ thông tin (information leakage/Loss Prevention); phá hoại tính toàn vẹn dữ liệu (damage to data integrity) và tấn công từ chối dịch vụ (denial of service attacks).

Các giải pháp an toàn hạ tầng mạng có thể chia thành các nhóm sau:

• *Nhóm các giải pháp ngăn chặn, chống truy cập mạng trái phép:* Nhóm giải pháp này sử dụng các công cụ phòng chống truy cập trái phép như tường lửa (FW). Tuy nhiên, FW không phát hiện ra các hành vi bất thường xảy ra trên mạng. Do đó, ngoài việc trang bị tường lửa các TVĐT cần có một loại thiết bị có khả năng theo dõi và phát hiện mọi dấu vết các hành vi của dòng thông tin đi qua FW. Thiết bị như vậy được gọi là thiết bị phát hiện và ngăn chặn tấn công (IDS/IPS). IDS/IPS làm việc như một người gác cổng phát hiện các hành vi "bất thường" (mà FW không phát hiện được) của một cuộc tấn công. Ví dụ, FW không phát hiện ra hành vi tấn công DDOS hoặc TCP/IP hijacking.

Ở nhóm giải pháp này còn có các thiết bị kiểm tra, đánh giá định kỳ, các phương tiện tìm kiếm phát hiện lỗ hổng bảo mật và vá lỗi cho toàn bộ hệ thống bao gồm: hệ điều hành, các

phần mềm ứng dụng, các dịch vụ… các TVĐT có thể sử dụng các phần mềm như: công cụ nmap để quét mạng; sử dụng các phần mềm Paros Proxy, WebScarab, Acunetix Web Vulnerability Scanner,…để quét lỗ hổng bảo mật của các ứng dụng.

• *Nhóm giải pháp kiểm soát truy cập:* Kiểm soát truy cập là xác định quyền truy cập đến từng phần của hệ thống cho từng loại người dùng; xác nhận và xác thực người dùng và khi cần thiết phải xác thực thiết bị (địa chỉ mạng, mã số của terminal,…) cần truy cập; ghi lại tất cả cuộc truy cập thành công và không thành công; nếu dùng mật khẩu để xác thực hệ thống, cần sử dụng các mật khẩu có chất lượng cao và khi cần thiết cần phải hạn chế số lượng người truy cập đồng thời vào mạng. Cần đảm bảo tài nguyên thông tin của các TVĐT chỉ có thể truy cập bởi những cá nhân được xác thực. Quá trình truy cập tài nguyên hệ thống thông tin TVĐT của người dùng cần thông qua các bước:

- Identification: Quá trình nhận dạng người dùng, người dùng cung cấp các thông tin cho hệ thống nhận dạng.

- Authentication: Xác thực là quá trình chứng minh *"Tôi chính là tôi"*. Để xác thực người dùng, ta cần có những yếu tố sau:

+ Something you KNOW**:** Dựa vào một vài yếu tố bạn biết (ví dụ: username/password)

+ Something you HAVE **-** Dựa vào một yếu tố bạn có (vd: bạn phải có một thẻ từ)

+ Something you ARE - Dựa vào một yếu tố thuộc về bạn (ví dụ : vân tay, giọng nói, võng mạc hay DNA)

- Authorization: Thẩm quyền truy cập tài nguyên được hệ thống cấp cho người dùng sau khi xác thực Authentication. Authorization thể hiện các quyền mà người dùng có thể thực thi trên hệ thống. Authorization làm việc trực tiếp với điều khiển truy cập Access Control.

• *Nhóm các giải pháp nhằm phục hồi dữ liệu sau sự cố*: như chống thất thoát dữ liệu, sao lưu (backup). nhằm mục đích đảm bảo tính liên tục (sẵn sàng) làm việc của hệ thống thông tin TVĐT. Nó giúp các TVĐT nhanh chóng và chủ động đưa hệ thống vào sử dụng sau khi bị sự cố. Có thể áp dụng một trong các phương pháp lưu trữ sau:

- Backup liên tục (working backup): Là một dạng backup toàn phần (full backup)-thực hiện liên tục nhằm mục đích phục hồi hệ thống một cách tức thì.

- Cất giữ tại chỗ (Onsite Storage):Thực hiện bên trong hệ thống.

- Cất giữ bên ngoài (Offsite Storage). Được thực hiện bên ngoài hệ thống, thường tại các văn phòng ở xa (remote office) hoặc tại một trung tâm được bảo vệ an toàn.

• *Xây dựng chính sách an ninh mạng*: Tổng hợp các quy tắc, quy trình vận hành ATTT và các giải pháp để thực thi ATTT trong cơ quan thông tin - thư viện. Là bước hoàn thiện một môi trường làm việc và hoạt động theo chuẩn bảo mật. Hiện nay nước ta có rất nhiều đơn vị đang xây dựng chính sách ATTT theo chuẩn ISO 17799/27001, sử dụng mô hình ISMS.

3.3. An toàn dữ liệu

Thuật ngữ "an toàn dữ liệu" có nghĩa là các hệ CSDL cần phải được bảo vệ chống truy nhập nhằm sửa đổi hay phá hoại một cách chủ định hay không chủ định. Như vậy, các hệ thống cơ sở dữ liệu phải được quản trị, bảo vệ tập trung, nhằm bảo đảm được tính toàn vẹn và an toàn dữ liệu khi thực hiện cập nhật, sửa đổi hay bổ sung thông tin trong các CSDL. Việc bảo vệ tuyệt đối các hệ CSDL khỏi truy nhập là không thể, nhưng các TVĐT phải có các biện pháp đủ mạnh để ngăn chặn hầu hết truy cập trái phép vào CSDL.

Để đảm bảo an toàn dữ liệu cán bộ công nghệ thông tin của các TVĐT cần phân chia một cách rõ ràng quyền hạn của từng đối tượng khi sử dụng hệ CSDL, với các quyền: đọc (read), chèn (insert), sửa đổi (modify), xóa (delete) dữ liệu, cần xác định rõ ai sẽ có tất cả các quyền trên, ai chỉ có một số quyền hạn nhất định. Bên cạnh đó cần sử dụng mật mã để đảm bảo an toàn dữ liệu. Mật mã là phương pháp bảo vệ thông tin bằng việc mã hóa chúng (encrypting) thành một dạng mà chỉ có thể đọc bởi người có thẩm quyền với hệ thống đó hay một người dùng cụ thể. Việc sử dụng và tạo hệ thống đó gọi là mật mã (cryptography). Có thể sử dụng các phương thức mã hóa cơ bản sau:

- Hàm băm - HASH ((MD5, SHA1, SHA2);

- Mã hóa đối xứng - Symmetric (một số thuật toán mã hóa đối xứng phổ biến hiện nay như DES, 3DES và AES);

- Mã hóa bất đối xứng - Asymmetric (RSA, ECC, Diffie-Helman …).

3.4. An toàn người sử dụng

Người sử dụng TVĐT bao gồm nhiều đối tượng khác nhau có tương tác với thư viện [19]. An toàn người sử dụng có mối liên hệ mật thiết với các vấn đề về an toàn cơ sở hạ tầng kỹ thuật, an toàn dữ liệu được trình bày ở phần trên. Tuy nhiên, an toàn người sử dụng thường đề cập tới vấn đề kiểm soát truy cập nhằm đảm bảo tính bảo mật và xác thực.

An toàn người sử dụng bao hàm hai vấn đề chính, là: đảm bảo ATTT của người sử dụng và xác thực người dùng khi tiếp cận hệ thống.

An toàn thông tin người sử dụng: Với sự giúp sức của máy tính điện tử và mạng máy tính, các thông tin của người sử dụng (thông tin cá nhân, lịch sử tìm kiếm, giao dịch, mượn - trả,…) đều được ghi lại và được lưu trữ trong hệ thống. Câu hỏi đặt ra là thông tin của người sử dụng được các thư viện lưu trữ như thế nào? Có đảm bảo rằng những thông tin này không rò rỉ ra ngoài, gây ảnh hưởng tới người sử dụng. An toàn ở đây đề cập tới quyền riêng tư và bảo mật.

Quyền riêng tư (privacy) là thuật ngữ liên quan chặt chẽ đến ATTT người sử dụng. Riêng tư tức là quyền được giữ kín, giữ riêng và không công bố các thông tin cá nhân, là quyền được giữ bí mật cá nhân, được bảo vệ bí mật cá nhân, không bị xâm phạm bí mật cá nhân, bảo vệ cá nhân trước việc bị mạo danh và giả mạo thông tin [21, 22].

Bảo mật (Confidentiality) nghĩa là các thông tin giao dịch, tìm kiếm, download, lĩnh vực người dùng quan tâm… khi sử dụng thư viện phải được giữ bí mật.

Các thông tin của người sử dụng có thể bị đánh cắp phục vụ cho nhiều mục đích khác nhau, như: lợi dụng tài khoản người dùng để truy cập bất hợp pháp hệ thống, tấn công HTTT thư viện, cung cấp thông tin người sử dụng cho bên thứ ba,... Do đó, các TVĐT cần có những biện pháp cụ thể để đảm bảo ATTT người sử dụng, và cần được thể hiện trong chính sách ATTT cụ thể.

Xác thực người dùng: Khi nói về hệ thống các biện pháp tổng hợp nhằm bảo đảm an toàn cho việc trao đổi thông tin trên mạng máy tính, người ta thường nhắc đến AAA (Authentication - xác thực; Authorization - phân quyền và Accounting - tính toán), trong đó xác thực là công đoạn đầu tiên và quan trọng nhất. Tương tự như vậy, trong các TVĐT, để đảm bảo an toàn, người sử dụng cần phải trải qua bước xác thực trước khi sử dụng các sản phẩm - dịch vụ thư viện. Hiện nay, đa phần các TVĐT đều yêu cầu xác thực thông qua username và password mà người sử dụng được cấp.

Kết luận

TVĐT là một hệ thống thông tin hoàn chỉnh, chịu sự tác động của các yếu tố gây mất ATTT. Các nguy cơ này có thể đến từ cơ sở hạ tầng kỹ thuật, từ các giao thức mạng, đến từ các sản phẩm phần mềm và đến từ chính người sử dụng. Để đảm bảo ATTT trong TVĐT cần tiến hành đồng thời nhiều giải pháp khác nhau, từ các giải pháp về quản lý đến các hướng dẫn thực thi ATTT và cuối cùng là lựa chọn các giải pháp công nghệ để thực hiện.

Tài liệu tham khảo

1. Quyết định 2615/QĐ-BTC, ngày 19 tháng 10 năm 2012: Về việc đảm bảo an toàn thông tin trên môi trường máy tính và mạng máy tính.

2. Quốc hội (2006), Luật Công nghệ thông tin số 67/2006/QH11, ngày 29 tháng 6 năm 2006.

3. Quốc hội (2005), Luật Giao dịch điện tử số 51/2005/QH11, ngày 29 tháng 11 năm 2005.

4. Nghị định 63/2007/NĐ-CP, ngày 10 tháng 4 năm 2007: Qui định về xử phạt hành chính trong lĩnh vực CNTT.

5. Nghị định 64/2007/NĐ-CP, ngày 10 tháng 4 năm 2007: Về việc ứng dụng CNTT trong hoạt động các cơ quan nhà nước.

6. Nghị định 90/2008/NĐ-CP, ngày 13 tháng 8 năm 2008: Về việc chống thư rác.

7. Chỉ thị 03/2007/CT-BBCVT, ngày 23 tháng 2 năm 2007: Về việc tăng cường đảm bảo an toàn thông tin trên mạng Internet.

8. Chỉ thị 897/CT-TTg, ngày 10 tháng 6 năm 2011: Về việc tăng cường triển khai các hoạt động đảm bảo an toàn thông tin số.

9. Quốc hội (2010), Luật Bảo vệ quyền lợi người tiêu dùng số 59/2010/QH12, ngày 17/11/2010.

10. Quyết định số 63/QĐ-TTg, ngày 13 tháng 01 năm 2010, Phê duyệt Quy hoạch phát triển an toàn thông tin số quốc gia đến năm 2020.

11. Chuẩn bảo mật ISO 17799 – Toàn tập// http://vnexperts.net/bai-viet-ky-thuat/security/661-chun-bo-mt-iso-17799-toan-tp.html

12. Banerjee, K. (2003). How much security does your library need? Computers in Libraries, 23(5), 12-15. Truy cập ngày 28/04/2014, từ cơ sở dữ liệu ProQuest.

13. Mike Meyers' Certification Passport : CompTIA Security plus _Trevor Kay 2003.

14. Singh, S. (2003). Digital library: Definition to implementation. Ranganathan Research Centre: Delhi. http://www.oocities.org/esukhdev/lecture_rcc.pdf (Truy cập ngày 22/07/2014)

15. Nguyễn Thị Nhị, Mai Đại Phương (2011), Xây dựng và sử dụng TVĐT hỗ trợ dạy học vật lý trung học phổ thông, Kỷ yếu hội thảo quốc gia về giảng dạy vật lý.

16. Nguyễn Hồng Ngọc (2011), Một số vấn đề về số hóa tài liệu tại Việt Nam// http://www.lrc.ctu.edu.vn/bantin14/index.php/chuyen-de/22-chuyen-de/243-mot-so-van-de-so-hoa-tai-lieu-vn?tmpl=component&print=1&page= (Truy cập ngày 05/11/2014).

17. Prof. Dr. Christoph Meinel (2005), Internetworking with TCP/IP, NXBGD, Hà Nội.

18. Xie Wei, Chun-Hong Zhang (2009). Digital library network security technology research. Computer Knowledge and Technology, 2009,5 (4): 814-815.

19. Olson, Ingrid M and Abrams, Marshall D (2012). Information Security Policy, IEEE Explore, P.430 – 433.

20. Karin Hone and J.H.P.Eloff. Information security policy, What do international information security standards Say?

21. Nguyễn Văn Anh (2010), Nghiên cứu hệ thống quản lý an toàn thông tin theo tiêu chuẩn ISO 27001: Luận văn thạc sỹ ngành hệ thống thông tin, trường Đại học Công nghệ, ĐHQGHN.

22. Vũ Thanh Vân (2012) "Quyền riêng tư và văn hóa ứng xử của nhà báo", Kỷ yếu hội thảo: Sự nghiệp Thông tin - Thư viện Việt Nam đổi mới và hội nhập quốc tế.