Nguyên Tắc An Toàn Bảo Mật Thông Tin Trong Thông Tin - Thư Viện

Bảo mật thông tin – thư viện

Nếu như trước đây việc đảm bảo an toàn thông tin chỉ được các thư viện và cơ quan thông tin quan tâm ở vấn đề phòng chống trộm cắp tài liệu, trang thiết bị và các vấn đề liên quan đến trật tự, thì hiện nay các thư viện và cơ quan thông tin quan tâm đến vấn đề này ở các mức độ sâu hơn trong công tác xây dựng nguồn thông tin điện tử và tổ chức dịch vụ trực tuyến cho NDT. Một quy luật dễ nhận thấy là: thư viện càng "mở" thì việc bảo đảm an toàn thông tin càng khó khăn và phức tạp.

Vì vậy, đảm bảo ATTT trong thư viện chính là việc bảo vệ thông tin và hệ thống thông tin khỏi các truy cập, chỉnh sửa, đánh cắp hoặc sử dụng thông tin trái phép. Việc đảm bảo ATTT trong thư viện là đảm bảo 3 yêu cầu: bí mật, toàn vẹn và sẵn sàng sử dụng.

1. Nguyên tắc an toàn bảo mật thông tin trong thông tin - thư viện

- Bí mật: Không được truy cập, sử dụng hoặc tiết lộ khi không được phép

- Bảo mật thông tin người sử dụng
- Bảo mật thông tin về lịch sử mượn – trả tài liệu của người sử dụng

- Toàn vẹn: đảm bảo sự chính xác, không thay đổi đối với thông tin gốc

- Thông tin thư mục trong CSDL
- Thông tin trên Website Trung tâm

- Sẵn sàng: thông tin ở trạng thái sẵn sàng cho việc truy cập và sử dụng

- Hệ thống OPAC
- Các nguồn tin điện tử

Theo Banjerjee, có nhiều nguyên nhân để hệ thống thông tin của các thư viện bị đe dọa (các cuộc tấn công từ bên ngoài vào thông qua mạng internet). Có 3 nguyên nhân chính là:

- Lợi dụng tài nguyên phần cứng, chiếm không gian đĩa cứng, CPU, …để lưu trữ và truyền bá các văn hóa phẩm đồi trụy, các tài liệu vi phạm bản quyền nhằm tránh sự kiểm soát của các cơ quan chức năng.
- Lợi dụng máy chủ hoặc các máy trạm khác trong mạng để làm bàn đạp tấn công các hệ thống thông tin khác.
- Đánh cắp thông tin về bạn đọc, thay đổi hoặc xóa bỏ thông tin trong các cơ sở dữ liệu của thư viện.
- Những người phụ Trung tâm cũng đã sớm quan tâm đến vấn đề ATTT và an ninh mạng và đã tiến hành một số công việc nhằm đảm bảo ATTT như:
- Cài đặt chương trình phòng và diệt virút Kaspersky Anti-Virus 6.0.4.1611 cho tất cả các máy tính trong Trường;
- Thiết lập hệ thống tường lửa;
- Đóng băng cấu hình các máy tính thuộc Phòng truy cập Internet không cho phép cài đặt phần mềm, không cho truy cập và thay đổi các tham số cấu hình của hệ điều hành;
- Sử dụng phần mềm XXX quản lý thời gian sử dụng máy tính đối với NDT;
- Khóa cổng USB, khóa ổ CD/DVD;
- Định kỳ sao lưu dự phòng các thông tin và CSDL;

- Máy trạm tra cứu chỉ sử dụng một màn hình cảm ứng hạn chế tối đa quền can thiệp vào cấu hình của máy.

Tuy nhiên cũng còn nhiều hạn chế và việc đảm bảo ATTT, an ninh mạng chưa đạt được nhiều kết quả như:

- Chưa có sự phân quyền cụ thể cho mỗi nhóm cán bộ sử dụng
- Chưa có sự phân công cán bộ CNTT phụ trách các vấn đề liên quan đến ATTT
- Chưa có kế hoạc thực hiện khi sự cố xảy ra (nếu có)
- Trung tâm chỉ có duy nhất một máy chủ để sử dụng cho nhiều dịch vụ khác nhau nên nếu xảy ra rủi ro (máy chủ bị tấn công) sẽ ảnh hướng đến toàn bộ hệ thống.
- Sao lưu CSDL chỉ được lưu trữ trong môt ổ cứng gắn ngoài dễ xảy ra tình trạng mất mát, hư hỏng.
- Chưa khóa một số chức của trình duyệt Web, các ứng dụng cũng như hạn chế các trang Web đen.
- Chưa có kế hoạch kiểm tra định kỳ nhật ký truy cập và sử dụng máy tính của bạn đọc tại các máy tính cá nhân (PC) trong Phòng truy cập internet.
- Chưa đào tọa bạn đọc, cung cấp cho họ những kiến thức về ATTT trong thư viện cũng như phổ biến các nội quy, quy định về sử dụng máy tính, quyền truy cập, sử dụng máy tính và các nguồn tin.

Ngoài những yếu điểm trên việc quan tâm đào tạo kiến thức ATTT cho CBTV cũng rất cần thiết. Các máy tính trạm dùng cho CBTV chưa được quản lý chặt chẽ và sử dụng một cách hợp lý. Các máy tính này thường được trang bị đầy đủ các thiết bị phần cứng cũng như không (hoặt ít) bị giới hạn trong việc cài đặt phần mềm, thay đổi các thiết lập và cài đặt sẵn có của hệ điều hành, được phép truy cập nhiều nguồn tin khác nhau có khả năng gây nên những rủi ro ngoài mong muốn.

Do vậy, ngoài công việc Trung tâm đã triển khai đạt kết quả, Trung tâm cũng cần phải:

- Khóa các chức năng không cần thiết trên một số máy tính làm công tác nghiệp vụ (tải về và cài đặt phần mềm)
- Kiểm tra định kỳ nhật ký truy caaph và sử dụng máy tính của CBTV theo nội quy, quy định của Trung tâm nói riêng và Quy định của pháp luật nói chung.
- Thường xuyên sao lưu sự phòng các dữ liệu cần thiết (nhất là các dữ liệu không được sao lưu trên máy chủ)

2. An toàn thông tin trong thư viện điện tử

2.1. Khái niệm an toàn thông tin

An toàn thông tin (ATTT) giờ đây không chỉ còn là mối quan tâm của các công ty, tổ chức liên quan đến tài chính, ngân hàng mà nó cũng là mối quan tâm của các thư viện. Đặc biệt là các thư viện điện tử, thư viện số nơi mà các hoạt động thư viện đang dần được tự động hóa, mục lục truyền thống được thay thế bằng mục lục điện tử, cùng với đó là các dịch vụ trực tuyến dựa trên web được cung cấp cho người sử dụng

2.2. Các mục tiêu cơ bản của an toàn thông tin trong thư viện điện tử

Khi phân tích một hệ thống bảo mật, chúng ta cần xuất phát từ những tính chất cơ bản của ATTT. Có vùng dữ liệu yêu cầu tính bảo mật của thông tin, có vùng dữ liệu cần tính toàn vẹn, tất cả các dữ liệu đó đều phải được đáp ứng khi yêu cầu đó là tính sẵn sàng của hệ thống. Trong đó:

- **Tính bảo mật (confidentiality):** đảm bảo thông tin chỉ được truy cập bởi người dùng hợp pháp. Giảm thiểu tối đa mọi hành vi ăn cắp, khai thác thông tin bất hợp pháp.
- **Tính sẵn sàng (availability):** đảm bảo những người dùng hợp pháp mới được truy cập các thông tin và tài sản liên quan khi có yêu cầu. Hệ thống cần được sẵn sàng phục vụ và đứng vững trước mọi rủi ro khách quan và chủ quan.
- **Tính toàn vẹn (integrity):** bảo vệ tính chính xác, đầy đủ của thông tin cũng như các phương pháp xử lý. Ngăn ngừa các hành vi sửa đổi, giả mạo thông tin.