

Một số vấn đề bảo mật và an toàn thông tin trong nhà trường

Lê Thanh Phúc*

*ThS, Phòng Công nghệ thông tin, Học viện Ngân hàng

Received: 16/04/2024; Accepted: 26/04/2024; Published: 15/5/2024

Abstract: In the context of strong development of information technology, properly processing and protecting information becomes more difficult. Therefore, finding appropriate and effective solutions for information security in schools is an urgent issue that requires attention and investment from educational organizations.

Keywords: information security , safety

1. Đặt vấn đề

Trong bối cảnh phát triển mạnh mẽ của công nghệ thông tin, việc xử lý và bảo vệ thông tin đúng cách trở nên khó khăn hơn. Do đó, việc tìm ra giải pháp phù hợp và hiệu quả cho bảo mật thông tin trong nhà trường là vấn đề cấp bách đòi hỏi sự chú trọng và đầu tư từ phía các tổ chức giáo dục.

2. Nội dung nghiên cứu

2.1. Khái niệm cơ bản về bảo mật và an toàn thông tin

Bảo mật thông tin là quá trình đảm bảo rằng thông tin được bảo vệ khỏi sự truy cập trái phép, sử dụng trái phép, tiết lộ trái phép, sửa đổi trái phép và phá hủy trái phép. Nó bao gồm cả việc bảo vệ thông tin cá nhân và thông tin doanh nghiệp. Cụ thể, có một số khái niệm cơ bản liên quan đến an toàn thông tin:

Tính bảo mật: Đảm bảo thông tin được bảo mật chặt chẽ, chỉ cho phép những người được phân quyền truy cập thông tin

Tính toàn vẹn: Bảo vệ sự hoàn chỉnh toàn diện cho hệ thống thông tin, đảm bảo thông tin không bị sửa đổi trái phép³.

Tính chính xác: Thông tin phải chính xác, đầy đủ và không vi phạm bản quyền nội dung.

An toàn thông tin trong thời đại số là quan trọng hơn bao giờ hết. Việc bảo vệ thông tin trở thành một yêu cầu không thể thiếu trong mọi hoạt động nói chung và hoạt động điện tử nói riêng. Tam giác CIA (Confidentiality, Integrity, Availability) là khái niệm cơ bản, cốt lõi của an toàn thông tin. Nó bao gồm tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin.

2.2. Tầm quan trọng của bảo mật và an toàn thông tin trong ngành giáo dục

Bảo mật và an toàn thông tin trong ngành giáo dục đóng vai trò quan trọng để đảm bảo tính bí mật, toàn vẹn và sẵn sàng của thông tin. Dưới đây là một số điểm nổi bật:

Bảo vệ dữ liệu học sinh và giáo viên: Thông tin cá nhân của học sinh và giáo viên cần được bảo vệ khỏi việc truy cập trái phép hoặc lộ ra ngoài. Hệ thống quản lý thông tin phải tuân thủ các quy định về bảo mật dữ liệu.

Phòng ngừa việc sao chép trái phép: Bảo mật thông tin giúp ngăn chặn việc sao chép trái phép tài liệu giảng dạy, bài kiểm tra và đề thi. Điều này đảm bảo tính công bằng và độ tin cậy của quá trình học tập.

Bảo vệ hệ thống mạng và cơ sở hạ tầng công nghệ: Các trường học cần đầu tư vào việc bảo vệ hệ thống mạng, máy tính và dữ liệu. Điều này giúp tránh tình trạng tấn công mạng, lây nhiễm mã độc và mất dữ liệu quan trọng.

Đào tạo về an toàn thông tin cho cộng đồng giáo dục: Giáo viên, học sinh và nhân viên cần được đào tạo về an toàn thông tin. Hiểu biết về cách phòng ngừa rủi ro và xử lý sự cố là quan trọng để duy trì môi trường học tập an toàn.

Tóm lại, việc thực hiện các biện pháp bảo mật và an toàn thông tin trong ngành giáo dục giúp bảo vệ thông tin quan trọng và đảm bảo môi trường học tập hiệu quả và an toàn.

2.3. Các mối đe dọa phổ biến đối với bảo mật và an toàn thông tin trong nhà trường

Tại các nhà trường, bảo mật và an toàn thông tin đóng vai trò quan trọng để đảm bảo tính bí mật, toàn vẹn và sẵn sàng của thông tin. Dưới đây là một số mối đe dọa phổ biến mà các nhà trường cần quan tâm:

Tấn công mạng: Các cuộc tấn công mạng có thể nhắm vào hệ thống mạng, máy tính, và dữ liệu của trường học. Điều này gây nguy cơ mất thông tin quan trọng và gián đoạn hoạt động học tập.

Phần mềm độc mã hóa dữ liệu tống tiền (Ransomware): Ransomware mã hóa dữ liệu và yêu

cầu tiền chuộc để giải mã. Trường học có thể bị tấn công bằng loại mã độc này, gây thiệt hại về dữ liệu và tài chính¹.

Lừa đảo trực tuyến và lây nhiễm phần mềm độc hại: Các cuộc tấn công qua email giả mạo, lừa đảo thông tin đăng nhập, hoặc lây nhiễm phần mềm độc hại từ các trang web độc hại có thể ảnh hưởng đến hệ thống và thông tin của trường học².

Mất an toàn từ các mối đe dọa sẵn có: Các thiết bị không được bảo mật, việc sử dụng mật khẩu yếu, và việc không cập nhật phần mềm đều tạo ra mối đe dọa cho an toàn thông tin.

Tấn công mạng vào hạ tầng quan trọng của cơ quan nhà nước: Các hệ thống quản lý học tập, thông tin học sinh, và dữ liệu khác có thể bị tấn công, ảnh hưởng đến hoạt động của trường học¹.

2.3. Các giải pháp cụ thể dành cho các vấn đề bảo mật thông tin cụ thể trong nhà trường

2.3.1. Giải pháp cho việc bảo vệ dữ liệu cá nhân

Giải pháp bảo vệ dữ liệu cá nhân

Bảo vệ dữ liệu cá nhân là vấn đề ngày càng quan trọng trong thời đại công nghệ số, khi mà thông tin cá nhân của chúng ta được lưu trữ và sử dụng rộng rãi trên mạng internet. Dưới đây là một số giải pháp để bảo vệ dữ liệu cá nhân:

*** Biện pháp kỹ thuật:**

Mã hóa dữ liệu: Mã hóa dữ liệu sẽ chuyển đổi thông tin sang dạng không thể đọc được nếu không có khóa giải mã. Đây là biện pháp hiệu quả để bảo vệ dữ liệu nhạy cảm như mật khẩu, thông tin tài chính, v.v.

Sử dụng phần mềm bảo mật: Cài đặt phần mềm chống virus, chống phần mềm độc hại, tường lửa và cập nhật thường xuyên để bảo vệ thiết bị của bạn khỏi các mối đe dọa an ninh mạng.

Cài đặt mật khẩu mạnh: Sử dụng mật khẩu khác nhau cho các tài khoản trực tuyến khác nhau và thay đổi mật khẩu thường xuyên. Tránh sử dụng thông tin cá nhân dễ đoán như ngày sinh, tên thú cưng, v.v. trong mật khẩu.

Cẩn thận khi chia sẻ thông tin cá nhân: Hạn chế chia sẻ thông tin cá nhân trên mạng xã hội hoặc các trang web không uy tín. Cẩn thận khi nhấp vào các liên kết hoặc tệp đính kèm trong email hoặc tin nhắn từ người lạ.

*** Biện pháp tổ chức:**

Tìm hiểu về chính sách bảo mật dữ liệu: Đọc kỹ chính sách bảo mật dữ liệu của các trang web và ứng dụng mà bạn sử dụng trước khi cung cấp thông tin cá nhân.

Chỉ cung cấp thông tin cá nhân khi cần thiết: Hạn

chế cung cấp thông tin cá nhân hơn mức cần thiết cho mục đích sử dụng.

Yêu cầu xóa dữ liệu cá nhân: Bạn có quyền yêu cầu các tổ chức xóa dữ liệu cá nhân của bạn nếu họ không còn cần thiết cho mục đích sử dụng hoặc thu thập dữ liệu trái phép.

*** Biện pháp pháp lý:**

Luật bảo vệ dữ liệu cá nhân: Việt Nam đã có Luật Bảo vệ dữ liệu cá nhân có hiệu lực từ ngày 1/7/2023, quy định các quyền và nghĩa vụ của tổ chức và cá nhân trong việc bảo vệ dữ liệu cá nhân.

Tổ cáo vi phạm: Bạn có thể tố cáo các hành vi vi phạm Luật Bảo vệ dữ liệu cá nhân với cơ quan chức năng nhà nước có thẩm quyền.

Ngoài ra, bạn cũng cần nâng cao nhận thức về tầm quan trọng của việc bảo vệ dữ liệu cá nhân và cập nhật thường xuyên kiến thức về an ninh mạng để tự bảo vệ bản thân tốt hơn.

2.3.2. Giải pháp cho việc ngăn chặn tấn công mạng

Với sự gia tăng của các mối đe dọa an ninh mạng, việc bảo vệ hệ thống mạng khỏi các cuộc tấn công mạng là vô cùng quan trọng. Dưới đây là một số giải pháp hiệu quả để ngăn chặn tấn công mạng:

*** Biện pháp phòng ngừa:**

Cập nhật phần mềm: Thường xuyên cập nhật hệ điều hành, phần mềm ứng dụng và trình duyệt web lên phiên bản mới nhất để vá các lỗ hổng bảo mật.

Cài đặt phần mềm bảo mật: Sử dụng phần mềm chống virus, chống phần mềm độc hại, tường lửa và cập nhật thường xuyên để bảo vệ thiết bị của bạn khỏi các mối đe dọa an ninh mạng.

Sử dụng mật khẩu mạnh: Sử dụng mật khẩu khác nhau cho các tài khoản trực tuyến khác nhau và thay đổi mật khẩu thường xuyên. Tránh sử dụng thông tin cá nhân dễ đoán như ngày sinh, tên thú cưng, v.v. trong mật khẩu.

Cẩn thận khi chia sẻ thông tin cá nhân: Hạn chế chia sẻ thông tin cá nhân trên mạng xã hội hoặc các trang web không uy tín. Cẩn thận khi nhấp vào các liên kết hoặc tệp đính kèm trong email hoặc tin nhắn từ người lạ.

Sao lưu dữ liệu: Sao lưu dữ liệu thường xuyên và lưu trữ bản sao lưu ở nơi an toàn để có thể khôi phục dữ liệu trong trường hợp bị tấn công.

*** Biện pháp phát hiện:**

Hệ thống giám sát mạng: Triển khai hệ thống giám sát mạng để theo dõi lưu lượng truy cập mạng và phát hiện các hoạt động bất thường có thể là dấu hiệu của tấn công mạng.

Phần mềm phát hiện xâm nhập: Sử dụng phần mềm phát hiện xâm nhập (IDS) để quét hệ thống

mạng và phát hiện các hành vi xâm nhập trái phép.

Hệ thống phòng chống xâm nhập: Triển khai hệ thống phòng chống xâm nhập (IPS) để ngăn chặn các cuộc tấn công mạng trước khi chúng gây ra thiệt hại.

*** Biện pháp ứng phó:**

Kế hoạch ứng phó sự cố: Lập kế hoạch ứng phó sự cố để xác định các bước cần thực hiện trong trường hợp bị tấn công mạng.

Đào tạo nhân viên: Đào tạo nhân viên về an ninh mạng để họ có thể nhận biết các dấu hiệu của tấn công mạng và biết cách xử lý trong trường hợp bị tấn công.

Hợp tác với các chuyên gia an ninh mạng: Hợp tác với các chuyên gia an ninh mạng để được hỗ trợ trong việc điều tra và ứng phó với các cuộc tấn công mạng.

Lưu ý: Các giải pháp ngăn chặn tấn công mạng cần được triển khai một cách đồng bộ và phù hợp với nhu cầu cụ thể của mỗi tổ chức. Doanh nghiệp và cá nhân cần thường xuyên cập nhật kiến thức về an ninh mạng để nâng cao hiệu quả phòng chống tấn công mạng.

Ngoài ra, bạn có thể tham khảo thêm các giải pháp an ninh mạng tiên tiến như:

Hệ thống phòng thủ mạng chủ động (APT): Bảo vệ hệ thống mạng khỏi các cuộc tấn công có chủ đích tinh vi.

Giải pháp bảo mật đám mây: Bảo vệ dữ liệu và ứng dụng được lưu trữ trên đám mây.

Giải pháp phân tích an ninh mạng: Phân tích dữ liệu an ninh mạng để phát hiện các mối đe dọa mới và nâng cao hiệu quả phòng chống tấn công mạng.

Việc lựa chọn giải pháp ngăn chặn tấn công mạng phù hợp sẽ giúp bảo vệ hệ thống mạng của bạn khỏi các mối đe dọa an ninh mạng ngày càng gia tăng.

2.4. Những thách thức và cơ hội trong việc thúc đẩy bảo mật và an toàn thông tin trong giáo dục

***Thách thức:**

Sự gia tăng sử dụng công nghệ: Việc sử dụng ngày càng phổ biến các thiết bị di động, máy tính bảng và internet trong giáo dục dẫn đến nguy cơ cao hơn về vi phạm dữ liệu, tấn công mạng và lạm dụng thông tin.

Thiếu nhận thức: Nhiều học sinh, giáo viên và phụ huynh không nhận thức được đầy đủ về các mối đe dọa an ninh mạng và cách bảo vệ bản thân khỏi những mối đe dọa này.

Thiếu nguồn lực: Các trường học thường thiếu nguồn lực tài chính và nhân sự để đầu tư vào các biện pháp bảo mật và an toàn thông tin đầy đủ.

Chính sách và quy định: Việc thiếu các chính

sách và quy định rõ ràng về bảo mật và an toàn thông tin trong giáo dục có thể khiến việc thực thi các biện pháp bảo vệ trở nên khó khăn.

Môi trường học tập mở: Môi trường học tập mở, nơi học sinh và giáo viên chia sẻ thông tin và truy cập internet, tạo điều kiện cho các mối đe dọa an ninh mạng lây lan dễ dàng.

***Cơ hội:**

Nâng cao nhận thức: Nâng cao nhận thức về tầm quan trọng của bảo mật và an toàn thông tin thông qua các chương trình giáo dục và đào tạo cho học sinh, giáo viên và phụ huynh.

Đầu tư vào công nghệ: Đầu tư vào các công nghệ bảo mật tiên tiến như tường lửa, phần mềm chống virus và hệ thống phát hiện xâm nhập để bảo vệ hệ thống mạng và dữ liệu của trường học.

Phát triển chính sách: Phát triển các chính sách và quy định rõ ràng về việc sử dụng công nghệ, thu thập dữ liệu và bảo mật thông tin trong giáo dục.

Hợp tác: Hợp tác giữa các trường học, cơ quan chính phủ và các tổ chức tư nhân để chia sẻ thông tin về các mối đe dọa an ninh mạng và phát triển các giải pháp chung.

Sử dụng công nghệ để nâng cao an toàn: Sử dụng các công nghệ như xác thực hai yếu tố và mã hóa dữ liệu để bảo vệ thông tin cá nhân của học sinh và giáo viên.

3. Kết luận

Bảo mật và an toàn thông tin trong nhà trường là vấn đề phức tạp và đòi hỏi sự nỗ lực chung từ phía các bên liên quan. Việc xây dựng chính sách bảo mật thông tin phù hợp, đầu tư vào công nghệ bảo mật, nâng cao nhận thức về an ninh mạng cho học sinh, giáo viên và cán bộ quản lý là những giải pháp cần được ưu tiên. Bên cạnh đó, việc phối hợp với các cơ quan chức năng, các đơn vị bảo mật để chia sẻ thông tin, ứng dụng các giải pháp công nghệ tiên tiến và thường xuyên cập nhật kiến thức về an ninh mạng là điều cần thiết để nâng cao hiệu quả bảo mật và an toàn thông tin trong nhà trường.

Tài liệu tham khảo

1. Bảo mật an toàn thông tin- Bạn cần biết những thông tin gì?. <https://viettelco.net/bao-mat-an-toan-thong-tin-ban-can-biet-nhung-thong-tin-gi/>.
2. Khái niệm bảo mật thông tin là gì? - Công ty Luật ACC. <https://accgroup.vn/bao-mat-thong-tin-la-gi>.

3. Những khái niệm cơ bản về An toàn thông tin mạng - Security Daily. <https://hvn.edu.vn/ttcntt/vi/cong-nghe-hop-tac/nhung-khai-niem-co-ban-ve-an-toan-thong-tin-mang-security-daily-293.html>.