Mục lục

I. Nội dung

1.Tổng quan về an toàn thông tin (ATTT).

** Khái niệm:*

An toàn thông tin (ATTT) là lĩnh vực tập trung vào việc bảo vệ thông tin khỏi các mối đe dọa, bao gồm truy cập trái phép, sử dụng sai mục đích, tiết lộ, sửa đổi, phá hủy hoặc mất mát. ATTT đóng vai trò quan trọng trong việc bảo vệ các tài sản thông tin của tổ chức và cá nhân, như là:

- **Dữ liệu**: thông tin được lưu trữ trong các hệ thống máy tính, chẳng hạn như dữ liệu khách hàng, tài chính, nhân sự,…
- **Hệ thống**: các thiết bị và phần mềm được sử dụng để xử lý và lưu trữ dữ liệu, chẳng hạn như máy tính, máy chủ, mạng,…
- **Mạng:** các kết nối giữa các thiết bị và hệ thống, chẳng hạn như mạng internet, mạng nội bộ,…

**** Mục tiêu của ATTT: đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin.***

- ***Tính bảo mật:*** bảo vệ thông tin khỏi truy cập trái phép, sử dụng sai mục đích, tiết lộ hoặc sửa đổi.
- ***Tính toàn vẹn:*** đảm bảo thông tin là chính xác, đầy đủ và đáng tin cậy.
- ***Tính sẵn sàng:*** đảm bảo thông tin có sẵn cho người dùng được phép khi cần thiết.

** Các mối đe dọa đối với ATTT rất đa dạng, bao gồm:*

- Tấn công mạng: các nỗ lực truy cập trái phép vào hệ thống hoặc mạng để đánh cắp dữ liệu hoặc gây ra thiệt hại.
- Phần mềm độc hại: các chương trình độc hại có thể gây hại cho hệ thống hoặc dữ liệu.

- Lỗi con người: những sai lầm do con người gây ra có thể dẫn đến vi phạm ATTT.
- Thiên tai: các sự kiện như hỏa hoạn, lũ lụt hoặc động đất có thể gây thiệt hại cho hệ thống thông tin.

** Để đảm bảo ATTT, cần thực hiện một số biện pháp, bao gồm:*

- Kiểm soát truy cập: chỉ cho phép những người dùng được phép truy cập vào thông tin.
- Mã hóa dữ liệu: bảo vệ dữ liệu khỏi truy cập trái phép bằng cách mã hóa nó.
- Sao lưu dữ liệu: tạo bản sao lưu của dữ liệu để có thể khôi phục trong trường hợp mất mát.
- Nâng cao nhận thức về ATTT: đào tạo nhân viên về các mối đe dọa ATTT và cách thức bảo vệ thông tin.
- Thực hiện các biện pháp phòng ngừa: triển khai các biện pháp kỹ thuật và tổ chức để bảo vệ hệ thống và dữ liệu.

ATTT là một lĩnh vực quan trọng cần được quan tâm bởi tất cả các tổ chức và cá nhân. Bằng cách thực hiện các biện pháp phù hợp, có thể bảo vệ thông tin khỏi các mối đe dọa và đảm bảo tính bảo mật, tính toàn vẹn và tính sẵn sàng của thông tin.

2. Hệ thống thông tin (một trang web) của một tổ chức

** Hệ thống thông tin quản lý trường học (IUH)*

Ví dụ: Hệ thống thông tin quản lý trường học ở Trường đại học Công Nghiệp TP.Hồ Chí Minh (IUH)

- Chức năng:

- Quản lý học sinh: Đăng ký nhập học, quản lý hồ sơ sinh viên, theo dõi điểm số và kết quả học tập, thanh toán học phí.

- Quản lý giảng viên: Lập lịch giảng dạy, quản lý bài giảng, chấm điểm bài tập và thi cử.
- Quản lý nhân sự: Quản lý hồ sơ nhân viên, thanh toán lương, đánh giá hiệu quả công việc.
- Quản lý tài chính: Theo dõi thu chi, lập ngân sách, thanh toán hóa đơn.
- Quản lý thư viện: Tìm kiếm sách và tài liệu, mượn và trả sách, quản lý tài nguyên thư viện.

- Lợi ích:

- Tăng hiệu quả hoạt động: tự động hóa các quy trình thủ công, tiết kiệm thời gian và chi phí.
- Cải thiện khả năng ra quyết định: cung cấp dữ liệu chính xác và kịp thời để hỗ trợ việc ra quyết định.
- Tăng cường giao tiếp: tạo kênh thông tin liên lạc hiệu quả giữa các ban ngành, phụ huynh và học sinh.
- Nâng cao chất lượng giáo dục: cung cấp môi trường học tập hiệu quả cho học sinh và giảng viên.

- Ví dụ về cách sử dụng:

+ Sinh viên: sử dụng hệ thống để đăng ký học phần, xem điểm số, thanh toán học phí,...

+ Giảng viên: sử dụng hệ thống để đăng tải bài giảng, chấm điểm bài tập, theo dõi tiến độ học tập của sinh viên,...

+ Nhân viên văn phòng: sử dụng hệ thống để quản lý hồ sơ học sinh, nhân viên, tài chính,...

+ Ban lãnh đạo: sử dụng hệ thống để theo dõi hoạt động của nhà trường, ra quyết định về chiến lược phát triển,...

4. Giải thích 3 tính cần thiết (CIA) của ATTT đối với hệ thống đó, nêu ví dụ minh họa cho mỗi tính cần thiết.

** Tam giác bảo mật CIA bao gồm:*

- Tính bảo mật (Confidentiality):

+ Là nguyên tắc đảm bảo kiểm soát truy cập thông tin. Thông tin chỉ được phép truy cập bởi những đối tượng (người, chương trình máy tính…) được cấp phép.

+ Ví dụ: Trong hệ thống ngân hàng, một khách hàng được phép xem thông tin số dư tài khoản của mình nhưng không được phép xem thông tin của khách hàng khác.

- Tính toàn vẹn (Integrity):

+ Là sự đảm bảo dữ liệu là đáng tin cậy và chính xác. Thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được phép và phải đảm bảo rằng thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

+ Ví dụ: Trong hệ thống ngân hàng, không cho phép khách hàng tự thay đổi thông tin số dư của tài khoản của mình.

- Tính sẵn dùng (Availability):

+ Là sự đảm bảo liên tục và mức độ đáp ứng kịp thời của hệ thống khi có yêu cầu truy cập dữ liệu hoặc thao tác từ người dùng. Đảm bảo thông tin/dịch vụ luôn sẵn sàng khi những người dùng hoặc ứng dụng được ủy quyền cầu.

+ Ví dụ: Trong hệ thống quản lý thông tin ngân hàng, cần đảm bảo rằng chủ tài khoản có thể truy vấn/giao dịch thông tin tài khoản của mình bất cứ lúc nào.

**** Ba khái niệm thể hiện các mục tiêu cốt lõi an toàn cho cả thông tin và dịch vụ của hệ thống thông tin. Bên cạnh bộ ba CIA, trong lĩnh vực an toàn còn khái niệm quan trọng cần có:***

- Tính xác thực (Authenticity): việc xác thực nguồn gốc của thông tin trong hệ thống (thuộc sở hữu của đối tượng nào) để đảm bảo thông tin đến từ một nguồn đáng tin cậy.

- Tính chống thoái thác (Non-repudiation): Khả năng ngăn chặn việc từ chối một hành vi đã làm. Bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với các bên khác.

Ví dụ: Trong hệ thống ngân hàng, có khả năng cung cấp bằng chứng để chứng minh một hành vi khách hàng đã thực hiện và người thực hiện đó có hợp pháp không, như giao dịch thanh toán, giao dịch chuyển khoản....

5. Giải thích tại sao tổ chức đó cần phải có các biện pháp khác nhau để đảm bảo tính an toàn thông tin.

- Tổ chức cần phải có các biện pháp khác nhau để đảm bảo tính an toàn thông tin vì:

+ Đa dạng của thông tin: Tổ chức lưu trữ và xử lý nhiều loại thông tin khác nhau, bao gồm thông tin nhạy cảm, thông tin tài chính, thông tin khách hàng, v.v. Mỗi loại thông tin có yêu cầu bảo mật và kiểm soát riêng biệt.

+ Mức độ đe dọa đa dạng: Tổ chức phải đối mặt với các mối đe dọa từ các hành vi tấn công mạng, tin tặc, gián điệp, hỏng hóc kỹ thuật, v.v. Để chống lại các mối đe dọa này, tổ chức cần triển khai các biện pháp bảo mật phù hợp như tường lửa, phần mềm diệt virus, hệ thống giám sát và phát hiện xâm nhập.

+ Tuân thủ quy định và tiêu chuẩn: Tổ chức phải tuân thủ các quy định pháp luật về bảo mật thông tin, chẳng hạn như quy định về quyền riêng tư, bảo vệ dữ liệu cá nhân, và quy định ngành công nghiệp. Các biện pháp an ninh cần phải tuân thủ các tiêu chuẩn và quy định tương ứng để đảm bảo tuân thủ pháp luật.

6. Chỉ ra ba mối đe dọa ảnh hưởng đến an toàn thông tin đến tổ chức và cá nhân.

- Hành động vô ý (Inadvertent Acts).

+ Là những hành động mà xảy bởi lỗi nào đó, người thực hiện không cố ý.

+ Kẻ tấn công không có ác ý.

+ Các hành động lỗi của con người, sai lệch từ chất lượng dịch vụ, truyền thông lỗi là các hành động vô ý.

+ Nhân viên hoặc người dùng hệ thống cũng là mối đe dọa nội bộ hệ thống.

- Hành động cố ý (Delierate Acts)

+ Là các hành động được thực hiện bởi người của tổ chức làm tổn hại đến thông tin.

+ Các kẻ tấn công có một ý định xấu và muốn ăn cắp hoặc phá hủy dữ liệu.

+ Bao gồm các hành động như gián điệp, hacking, Cracking.

- Thảm họa tự nhiên (Natural Disaster)

+ Sức mạnh của thiên nhiên là rất nguy hiểm bởi vì chúng là điều không ngờ và xuất hiện đôi khi không có cảnh báo.

+ Chúng phá vỡ cuộc sống của con người nhưng cũng gây nguy hại đến thông tin được lưu vào trong máy tính.

+ Các mối đe dọa này có thể tránh nhưng chúng ta phải có những biện pháp phòng ngừa cần thiết.

- Lỗi về kỹ thuật (Technical Failures)

+ Lỗi về phần cứng: Nó xảy ra khi nhà sản xuất phân phối thiết bị có lỗi mà nhà sản xuất có thể biết hoặc không biết.

+ Lỗi phần mềm kỹ thuật: Những lỗi này có thể khiến hệ thống hoạt động theo cách không mong muốn hoặc bất ngờ. Một số trong số này là không thể phục hồi trong khi một số xảy ra định kỳ.

- Lỗi trong quản lý (Management Failure)

+ Quản lý phải luôn luôn cập nhật về diễn biến và công nghệ hiện tại.

+ Kế hoạch phù hợp phải được thực hiện bởi nhà quản lý để bảo vệ tốt thông tin.

+ Các chuyên gia CNTT cũng phải giúp ban quản lý trong việc bảo vệ thông tin, bằng cách hỗ trợ ban quản lý nâng cao công nghệ mới nhất.

7. Các tình huống và ví dụ minh họa có thể gây ra các rủi ro từ các mối đe dọa nêu trên và phân tích hậu quả nếu xảy ra.

a. Các tình huống và ví dụ minh họa.

**** Hành động vô ý (Inadvertent Acts):***

- Cá nhân:

+ Mở email lạ, nhấp vào liên kết độc hại hoặc tải xuống tệp đính kèm bị nhiễm virus.

+ Chia sẻ thông tin nhạy cảm trên mạng xã hội hoặc các diễn đàn trực tuyến.

+ Sử dụng mật khẩu yếu hoặc dễ đoán cho các tài khoản trực tuyến.

- Tổ chức:

+ Cán bộ nhân viên không được đào tạo về an toàn thông tin, dẫn đến việc xử lý dữ liệu sai cách.

+ Hệ thống máy tính không được cập nhật các bản vá bảo mật mới nhất.

+ Mất mát hoặc thất lạc thiết bị lưu trữ dữ liệu.

*** Hành động cố ý (Deliberate Acts):**

- Cá nhân:

+ Trộm cắp hoặc đánh cắp thông tin cá nhân.

+ Gây ra các cuộc tấn công mạng như tấn công lừa đảo, tấn công từ chối dịch vụ (DDoS), v.v.

+ Phá hoại hệ thống máy tính hoặc mạng lưới.

- Tổ chức:

+ Các cuộc tấn công mạng từ các đối thủ cạnh tranh hoặc tội phạm mạng.

+ Lỗ hổng bảo mật trong hệ thống thông tin của tổ chức bị khai thác.

+ Rò rỉ dữ liệu do nhân viên nội bộ cố ý.

*** Thảm họa tự nhiên (Natural Disaster):**

- Ví dụ: Một trận động đất/lũ lụt gây thiệt hại vật chất cho trung tâm dữ liệu, làm hỏng các hệ thống lưu trữ dữ liệu và làm mất dữ liệu quan trọng.

*** Lỗi về kỹ thuật (Technical Failures):**

- Lỗi về phần cứng:

+ Ổ đĩa cứng trên máy chủ chứa dữ liệu quan trọng bị hỏng, dẫn đến mất dữ liệu hoặc ngừng hoạt động.

+ Công ty bán lẻ trực tuyến gặp sự cố với hệ thống thanh toán trực tuyến do máy chủ quan trọng bị hỏng, dẫn đến việc các giao dịch bị gián đoạn.

- Lỗi về phần mềm:

+ Lỗ hổng bảo mật trong phần mềm hệ thống bị kẻ tấn công tận dụng và xâm nhập vào hệ thống một cách không ủy nhiệm.

+ Lỗ hổng bảo mật trong một ứng dụng di động phổ biến cho phép tin tặc truy cập vào thông tin cá nhân của người dùng, dẫn đến rủi ro về việc mất mát dữ liệu.

**** Lỗi về quản lý (Management):***

- Ví dụ: Công ty đa quốc gia không triển khai chính sách bảo mật hoặc huấn luyện nhân viên không đầy đủ về các biện pháp bảo mật, dẫn đến việc xảy ra các lỗ hổng bảo mật hoặc hành động không an toàn từ phía nhân viên và tổ chức.

b. Hậu quả:

- Dẫn đến việc mất mát niềm tin từ phía khách hàng, tiềm ẩn rủi ro pháp lý.
- Mất cắp dữ liệu quan trọng: thông tin nhân viên, thông tin khách hàng, sản phẩm, chiến lược kinh doanh, bí mật thương mại/công nghệ.
- Dẫn đến việc mất mát niềm tin từ phía khách hàng.
- Gây ra mất mát tài chính và thông tin cá nhân hoặc tổ chức.
- Bị đánh cắp thông tin tài khoản ngân hàng và thẻ tín dụng.
- Gây mất mát doanh thu do gián đoạn dịch vụ hoặc quá trình sản xuất, làm giảm sự hài lòng của khách hàng.
- Có thể bị kiện tụng hoặc phạt tiền từ phía cơ quan quản lý hoặc cá nhân, do vi phạm các quy định về bảo vệ dữ liệu cá nhân hoặc bảo mật thông tin.
- Gây tổn thất tài chính công ty, doanh thu và dẫn đến thô lỗ nặng.

8. Đề xuất một số biện pháp phòng ngừa

- Triển khai các chính sách, quy trình, và hướng dẫn an ninh thông tin rõ ráng và cụ thể để hướng dẫn cá nhân, tổ chức về an toàn thông tin.

- Cung cấp đào tạo định kỳ về an toàn thông tin cho cá nhân, tổ chức nhằm giúp nhận biết và phòng chống các mối đe dọa, đánh cắp thông tin, cũng như biết phản ứng đúng đắn khi xẩy ra sự cố.
- Thực hiện kiểm tra bảo mật định kỳ và cập nhận bản vá an ninh mới nhất cho tất cả hệ thống và phần mềm, giảm thiểu nguy cơ từ các lỗ hỏng bảo mật.
- Sao lưu dữ liệu định kỳ và lưu trữ sao lưu tại nhiều địa điểm khác nhau để đảm bảo dữ liệu qua trọng có sẵn khi cần thiết.
- Triển khai phần mềm bảo mật và công cụ giám sát mạng, giúp phát hiện và ngăn chặn các mối đe dọa mạng, cũng như giám sát hoạt động của người dùng để phát hiện các hành vi không bình thường.
- Tạo ra một môi trường làm việc an toàn và trách nhiệm, khuyến khích việc báo cáo các sự cố an toàn thông tin và thiết lập các cơ chế phản hồi nhanh chóng.
- Thực hiện nguyên tắc lưỡng cực trong việc quản lý quyền truy cập vào dữ liệu, chỉ cho phép người dùng truy cập vào những thông tin mà họ cần để làm việc.
- Thực hiện kiểm tra rủi ro định kỳ để đánh giá và định vị các vấn đề an toàn thông tin tiềm ẩn, từ đó đưa ra biện pháp phòng ngừ và cải tiến liên tục.

9. Kết luận

- An toàn thông tin là quá trình bảo vệ thông tin quan trọng khỏi sự truy cập trái phép, sử dụng trái phép, tiết lộ không đúng đắn, sửa đổi không đúng đắn hoặc phá hủy thông tin.
- Mục tiêu của An Toàn Thông Tin: Bảo vệ tính bảo mật, tính toàn vẹn và tính sẵn dùng, tính xác thực, tính chống thoái thác của thông tin. Đảm bảo rằng thông tin chỉ được truy cập bởi những người được ủy quyền, không bị sửa đổi hoặc mất mát trong quá trình truyền tải, và có sẵn khi cần thiết.

- Mối đe dọa được phận loại: hành động vô ý, hành động cố ý, thảm họa tự nhiên, lỗi kỹ thuật và lỗi quản lý.
- Hậu quả tiềm ẩn của mỗi loại mối đe dọa, từ mất mát dữ liệu đến gián đoạn hoạt động kinh doanh và rủi ro pháp lý.
- Biện pháp phòng: triển khai chính sách và quy trình an ninh thông tin, đào tạo nhân viên, kiểm tra và cập nhật hệ thống, và quản lý quyền truy cập. Các biện pháp này giúp xây dựng hệ thống an toàn thông tin và giảm thiểu nguy cơ từ các mối đe dọa.