BÀI TẬP

TIỂU LUẬN 2 (NHÓM)

Các yêu cầu hoàn thành

Mark as done

Opened: Thursday, 4 April 2024, 12:00 AM

Due: Wednesday, 24 April 2024, 12:30 PM

Làm nhóm, nộp một file PDF hoặc Word (ít nhất 2 trang) và một file PPT (dưới 10 slide) ngắn gọn.

Đề xuất giải pháp tăng cường an toàn thông tin cho một hệ thống cụ thể.

Gợi ý:

- Tiêu đề: Ví dụ "Giải pháp ABC cho hệ thống XYZ".

- Tìm chọn và giới thiệu một hệ thống thông tin cụ thể, mô tả các chức năng hoặc thông tin hoặc dữ liệu của hệ thống.

- Nêu thực trạng an toàn thông tin của hệ thống đó.

- Đề xuất một giải pháp để tăng cường an toàn thông tin cho thực trạng trên.

- Kết luận

- Tài liệu tham khảo

- Chuẩn bị tài liệu họp nhóm: Phúc Lâm
- Ngày chuẩn bị: 16/04/2024
- Ngày họp nhóm: 17/04/2024
- Địa điểm: lớp học V6.0x
- Thời gian: tiết 7-9 lúc 12h30 đến 2h30
- Nội dung họp: lựa chọn đề tài để thực hiện tiểu luận 2 của nhóm
- Phân chia công việc

MỤC LỤC

TIÊU ĐỀ 1: "GIẢI PHÁP ABC CHO HỆ THỐNG QUẢN LÝ THÔNG TIN BỆNH NHÂN"

Mô tả hệ thống:

Hệ thống quản lý thông tin bệnh nhân là một ứng dụng web được sử dụng bởi các bệnh viện và cơ sở y tế để lưu trữ, truy xuất và quản lý thông tin về các bệnh nhân. Hệ thống này chứa các thông tin như hồ sơ bệnh án, lịch sử điều trị, kết quả xét nghiệm, đơn thuốc và các thông tin liên quan đến sức khỏe của bệnh nhân.

Thực trạng an toàn thông tin:

Hiện tại, hệ thống quản lý thông tin bệnh nhân đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Thiếu hệ thống bảo mật mạnh mẽ: Thiếu các biện pháp bảo vệ dữ liệu nhạy cảm của bệnh nhân như mã hóa dữ liệu, kiểm soát truy cập và xác thực người dùng.
- Nguy cơ rò rỉ thông tin: Dữ liệu bệnh nhân có thể bị đánh cắp hoặc rò rỉ do các lỗ hổng bảo mật trong hệ thống.
- Thiếu cơ chế giám sát và phát hiện xâm nhập: Khả năng phát hiện các hoạt động đáng ngờ trên hệ thống còn hạn chế.

Giải pháp tăng cường an toàn thông tin:

Để tăng cường an toàn thông tin cho hệ thống quản lý thông tin bệnh nhân, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai mã hóa dữ liệu**: Áp dụng mã hóa dữ liệu cho thông tin nhạy cảm của bệnh nhân như số CMND, thông tin y tế, để đảm bảo dữ liệu được bảo vệ khi truyền và lưu trữ.
2. **Thiết lập các chính sách kiểm soát truy cập**: Thiết lập các chính sách và quy trình kiểm soát truy cập chi tiết để chỉ cho phép người dùng được ủy quyền truy cập vào các loại thông tin nhất định theo nguyên tắc của sự cần thiết.
3. **Đầu tư vào giải pháp phát hiện xâm nhập và giám sát**: Đưa vào hoạt động các công cụ giám sát liên tục để phát hiện và ngăn chặn các hành vi xâm nhập, bao gồm cả các cảnh báo sớm về các hành vi không bình thường trên hệ thống.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý thông tin bệnh nhân, đảm bảo tính bảo mật, toàn vẹn và quyền riêng tư của thông tin bệnh nhân. Đây là bước quan trọng trong việc nâng cao chất lượng dịch vụ y tế và đáp ứng các tiêu chuẩn an toàn thông tin trong lĩnh vực y tế.

TIÊU ĐỀ 2: "GIẢI PHÁP ABC CHO HỆ THỐNG QUẢN LÝ TÀI LIỆU CÔNG TY XYZ"

Mô tả hệ thống: Hệ thống quản lý tài liệu của công ty XYZ là một ứng dụng nội bộ được sử dụng để lưu trữ và quản lý các tài liệu quan trọng của công ty, bao gồm hợp đồng, báo cáo tài chính, bản vẽ kỹ thuật, tài liệu quản lý và các thông tin nhạy cảm khác.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống quản lý tài liệu của công ty XYZ đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Thiếu hệ thống bảo mật mạnh mẽ: Dữ liệu quan trọng của công ty chưa được mã hóa hoặc bảo vệ đầy đủ, dễ bị truy cập trái phép.
- Rủi ro mất dữ liệu: Thiếu cơ chế sao lưu và phục hồi dữ liệu định kỳ, dễ gây mất mát thông tin quan trọng.
- Nguy cơ rò rỉ thông tin: Dữ liệu nhạy cảm có thể bị rò rỉ do thiếu kiểm soát truy cập hoặc các lỗ hổng bảo mật.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống quản lý tài liệu của công ty XYZ, chúng tôi đề xuất các giải pháp sau:

1. **Mã hóa dữ liệu:** Áp dụng mã hóa đối với các tài liệu nhạy cảm như hợp đồng, báo cáo tài chính để đảm bảo tính bảo mật khi truyền và lưu trữ.
2. **Thiết lập kiểm soát truy cập:** Đặt ra các chính sách và quy trình kiểm soát truy cập chặt chẽ để chỉ những người được ủy quyền mới có thể truy cập và chỉnh sửa các tài liệu quan trọng.
3. **Sao lưu dữ liệu định kỳ:** Thiết lập kế hoạch sao lưu định kỳ và phục hồi dữ liệu để đảm bảo tính sẵn sàng và phòng trường hợp mất dữ liệu.

Kết luận: Việc triển khai các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý tài liệu của công ty XYZ, đảm bảo tính bảo mật, toàn vẹn và quyền riêng tư của dữ liệu quan trọng của công ty. Đây là bước quan trọng trong việc nâng cao chất lượng quản lý thông tin và đảm bảo sự an toàn thông tin trong công ty.

TIÊU ĐỀ 3: "GIẢI PHÁP ABC CHO HỆ THỐNG QUẢN LÝ THÔNG TIN SINH VIÊN CỦA ĐẠI HỌC IUH"

Mô tả hệ thống: Hệ thống quản lý thông tin sinh viên của Đại học IUH là một ứng dụng web được sử dụng để lưu trữ, quản lý và truy xuất thông tin liên quan đến sinh viên của trường. Hệ thống này bao gồm các thông tin về hồ sơ sinh viên, điểm thi, lịch học, đăng ký học phần, hồ sơ tốt nghiệp và các thông tin khác về hoạt động học tập của sinh viên.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống quản lý thông tin sinh viên của Đại học IUH đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Thiếu kiểm soát truy cập: Một số thông tin nhạy cảm của sinh viên như điểm thi chưa được bảo vệ và kiểm soát truy cập chặt chẽ.
- Nguy cơ rò rỉ thông tin: Dữ liệu sinh viên có thể bị rò rỉ do thiếu cơ chế bảo mật hoặc các lỗ hổng trong hệ thống.
- Thiếu giám sát và phát hiện sớm các hành vi không mong muốn trên hệ thống.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống quản lý thông tin sinh viên của Đại học IUH, chúng tôi đề xuất các giải pháp sau:

1. **Cải thiện kiểm soát truy cập:** Thiết lập các chính sách và quy trình kiểm soát truy cập chi tiết để chỉ những người được ủy quyền mới có thể truy xuất thông tin nhạy cảm của sinh viên.
2. **Triển khai mã hóa dữ liệu:** Áp dụng mã hóa đối với các thông tin quan trọng như điểm thi, hồ sơ tốt nghiệp để đảm bảo tính bảo mật khi truyền và lưu trữ.
3. **Đầu tư vào giải pháp giám sát và phát hiện xâm nhập:** Đưa vào hoạt động các công cụ giám sát liên tục để phát hiện và ngăn chặn các hành vi không mong muốn trên hệ thống, bao gồm cả các cảnh báo sớm về các hoạt động bất thường.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý thông tin sinh viên của Đại học IUH, đảm bảo tính bảo mật và quyền riêng tư của thông tin sinh viên. Đây là bước quan trọng trong việc nâng cao chất lượng quản lý thông tin và đảm bảo sự tin cậy của hệ thống trong môi trường đại học.

TIÊU ĐỀ 4: "GIẢI PHÁP ABC CHO HỆ THỐNG QUẢN LÝ THÔNG TIN CỦA NGÂN HÀNG"

Mô tả hệ thống: Hệ thống quản lý thông tin của ngân hàng là một ứng dụng được sử dụng để lưu trữ, quản lý và truy xuất các thông tin liên quan đến khách hàng, tài khoản, giao dịch và các dịch vụ ngân hàng khác. Hệ thống này bao gồm các thông tin như hồ sơ khách hàng, số dư tài khoản, lịch sử giao dịch, các khoản vay, thông tin thẻ tín dụng và các dịch vụ tài chính khác.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống quản lý thông tin của ngân hàng đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Rủi ro bảo mật cao: Dữ liệu nhạy cảm của khách hàng và tài khoản ngân hàng có nguy cơ bị đánh cắp hoặc truy cập trái phép.
- Đe dọa từ các cuộc tấn công mạng: Ngân hàng phải đối mặt với các cuộc tấn công mạng từ các hacker và phần mềm độc hại.
- Yêu cầu nghiêm ngặt về bảo mật và tuân thủ quy định: Ngân hàng phải tuân thủ các tiêu chuẩn và quy định an toàn thông tin của ngành ngân hàng.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống quản lý thông tin của ngân hàng, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai các biện pháp bảo mật cơ bản:** Áp dụng mã hóa dữ liệu, kiểm soát truy cập chặt chẽ, xác thực hai yếu tố và giám sát liên tục để đảm bảo tính bảo mật của hệ thống.
2. **Đầu tư vào giải pháp phòng ngừa và phát hiện xâm nhập:** Xây dựng một hệ thống phòng ngừa và phát hiện xâm nhập hiệu quả để ngăn chặn các cuộc tấn công mạng và các hành vi không mong muốn trên hệ thống.
3. **Đảm bảo tuân thủ các quy định và tiêu chuẩn:** Tuân thủ các quy định an toàn thông tin của ngành ngân hàng, đảm bảo rằng hệ thống luôn tuân thủ các tiêu chuẩn bảo mật quốc tế.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý thông tin của ngân hàng, đảm bảo tính bảo mật và sự tin cậy của thông tin khách hàng và tài khoản ngân hàng. Đây là bước quan trọng trong việc bảo vệ thông tin nhạy cảm và duy trì uy tín của ngân hàng trong ngành công nghiệp tài chính.

TIÊU ĐỀ 5: "GIẢI PHÁP ABC CHO ĐẢM BẢO AN TOÀN THÔNG TIN CHO HỆ THỐNG CHỨNG KHOÁN SSI"

Mô tả hệ thống: Hệ thống chứng khoán SSI là một ứng dụng web và dịch vụ trực tuyến được sử dụng để giao dịch chứng khoán, cung cấp thông tin thị trường và các dịch vụ tài chính liên quan đến chứng khoán. Hệ thống này chứa các thông tin về giao dịch chứng khoán, tài sản của khách hàng, danh mục đầu tư, thông tin tài chính và các thông tin thị trường.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống chứng khoán SSI đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Nguy cơ bị tấn công mạng: Hệ thống chứng khoán thường là mục tiêu của các cuộc tấn công mạng từ các hacker và phần mềm độc hại.
- Đe dọa từ các hoạt động gian lận: Các hoạt động gian lận và giao dịch không hợp lệ có thể xảy ra do thiếu kiểm soát và giám sát chặt chẽ.
- Sự cần thiết của tính bảo mật và quyền riêng tư: Khách hàng yêu cầu tính bảo mật cao và sự bảo vệ thông tin cá nhân khi giao dịch trực tuyến.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống chứng khoán SSI, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai các biện pháp bảo mật tiên tiến:** Áp dụng mã hóa dữ liệu, kiểm soát truy cập nghiêm ngặt, xác thực hai yếu tố và giám sát liên tục để đảm bảo tính bảo mật của hệ thống.
2. **Đầu tư vào giải pháp phòng ngừa và phát hiện xâm nhập:** Xây dựng các giải pháp phòng ngừa và phát hiện xâm nhập hiệu quả để ngăn chặn các cuộc tấn công mạng và các hành vi gian lận.
3. **Đảm bảo tuân thủ các tiêu chuẩn quốc tế về an toàn thông tin:** Đảm bảo rằng hệ thống tuân thủ các tiêu chuẩn an toàn thông tin của ngành chứng khoán và quy định của cơ quan quản lý.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống chứng khoán SSI, đảm bảo tính bảo mật của thông tin giao dịch chứng khoán và tài sản của khách hàng. Đây là bước quan trọng trong việc đáp ứng yêu cầu bảo mật cao của ngành chứng khoán và tăng cường sự tin cậy của hệ thống trong thị trường tài chính.

TIÊU ĐỀ 6: "GIẢI PHÁP ABC CHO QUẢN LÝ ĐIỂM CỦA BỘ GIÁO DỤC"

Mô tả hệ thống: Hệ thống quản lý điểm của Bộ Giáo dục là một ứng dụng phần mềm được sử dụng để lưu trữ, quản lý và xử lý điểm số của học sinh và sinh viên trong các cơ sở giáo dục trên toàn quốc. Hệ thống này chứa các thông tin về điểm thi, thành tích học tập, thông tin cá nhân của học sinh/sinh viên và các thông tin liên quan đến quá trình học tập.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống quản lý điểm của Bộ Giáo dục đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Nguy cơ rò rỉ thông tin cá nhân: Dữ liệu điểm số và thông tin cá nhân của học sinh/sinh viên có thể bị đánh cắp hoặc rò rỉ do các lỗ hổng bảo mật trong hệ thống.
- Đe dọa từ các hoạt động gian lận điểm: Các hoạt động can thiệp vào điểm số, sửa đổi dữ liệu điểm có thể xảy ra do thiếu kiểm soát và giám sát chặt chẽ.
- Sự cần thiết của tính bảo mật và toàn vẹn dữ liệu: Yêu cầu bảo mật cao và đảm bảo tính toàn vẹn của dữ liệu điểm số và thông tin học tập.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống quản lý điểm của Bộ Giáo dục, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai các biện pháp bảo mật chặt chẽ:** Áp dụng các biện pháp bảo mật như mã hóa dữ liệu, kiểm soát truy cập nghiêm ngặt và xác thực người dùng để đảm bảo tính bảo mật của hệ thống.
2. **Đầu tư vào công nghệ giám sát và phát hiện gian lận:** Xây dựng hệ thống giám sát liên tục để phát hiện và ngăn chặn các hoạt động gian lận, can thiệp vào điểm số.
3. **Tăng cường đào tạo và giám sát nhân viên:** Đào tạo nhân viên về an ninh thông tin và thực hiện giám sát chặt chẽ để đảm bảo sự tuân thủ các quy định bảo mật.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống quản lý điểm của Bộ Giáo dục, đảm bảo tính bảo mật và toàn vẹn của dữ liệu điểm số và thông tin học tập. Đây là bước quan trọng trong việc nâng cao chất lượng và độ tin cậy của hệ thống quản lý giáo dục trên cả nước.

TIÊU ĐỀ 7: "GIẢI PHÁP ABC CHO AN TOÀN THÔNG TIN HỆ THỐNG THƯƠNG MẠI ĐIỆN TỬ CỦA CÔNG TY XYZ"

Mô tả hệ thống: Hệ thống thương mại điện tử của công ty XYZ là một website được sử dụng để bán các sản phẩm như quần áo, đồ dùng cá nhân, mỹ phẩm và thực phẩm chức năng trực tuyến. Khách hàng có thể tìm kiếm, xem thông tin sản phẩm, đặt hàng và thanh toán trực tuyến thông qua website này.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống thương mại điện tử của công ty XYZ đang gặp phải các vấn đề liên quan đến an toàn thông tin:

- Nguy cơ tấn công từ phần mềm độc hại: Khách hàng có thể bị tấn công từ các phần mềm độc hại khi tương tác trực tiếp với website.
- Rủi ro về bảo mật thanh toán: Thông tin thanh toán của khách hàng có thể bị đánh cắp do thiếu cơ chế bảo mật thích hợp.
- Thiếu kiểm soát truy cập: Không có các biện pháp kiểm soát truy cập nghiêm ngặt, dẫn đến nguy cơ thông tin bị lộ.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống thương mại điện tử của công ty XYZ, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai các biện pháp bảo mật phần mềm:** Cập nhật và quản lý thường xuyên các phần mềm để ngăn chặn các tấn công từ phần mềm độc hại.
2. **Sử dụng giao thức bảo mật HTTPS:** Áp dụng giao thức HTTPS để mã hóa dữ liệu truyền tải giữa máy khách và máy chủ, đảm bảo tính bảo mật của thông tin thanh toán.
3. **Thực hiện kiểm định bảo mật:** Tiến hành kiểm định bảo mật định kỳ để phát hiện và khắc phục các lỗ hổng bảo mật trong hệ thống.
4. **Đào tạo nhân viên và khách hàng về an toàn thông tin:** Cung cấp đào tạo cho nhân viên về an ninh thông tin và cách phòng ngừa các mối đe dọa. Đồng thời, hướng dẫn khách hàng về các biện pháp an toàn khi sử dụng website.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp củng cố an toàn thông tin cho hệ thống thương mại điện tử của công ty XYZ, bảo vệ thông tin của khách hàng và đảm bảo tính bảo mật trong quá trình giao dịch trực tuyến. Đây là nền tảng quan trọng để xây dựng niềm tin và uy tín của công ty trong lĩnh vực thương mại điện tử.

TIÊU ĐỀ 8: "GIẢI PHÁP ABC CHO AN TOÀN THÔNG TIN HỆ THỐNG MÁY TÍNH PHÒNG BAN TRONG CÔNG TY TÀI CHÍNH XYZ"

Mô tả hệ thống: Hệ thống máy tính của các phòng ban trong công ty tài chính XYZ bao gồm các thiết bị máy tính và hệ điều hành được sử dụng để thực hiện các nhiệm vụ văn phòng, xử lý thông tin tài chính, và quản lý dữ liệu nội bộ của công ty.

Thực trạng an toàn thông tin của hệ thống: Hiện tại, hệ thống máy tính của các phòng ban trong công ty tài chính XYZ đang đối mặt với các vấn đề an toàn thông tin sau:

- Thiếu hệ thống bảo mật mạnh: Các máy tính không được cài đặt các biện pháp bảo vệ đầy đủ như firewall, antivirus, và các cập nhật bảo mật thường xuyên.
- Nguy cơ tấn công từ email và các tệp độc hại: Nhân viên có thể bị lừa qua email để mở các tệp đính kèm có chứa phần mềm độc hại.
- Thiếu chính sách an toàn thông tin: Công ty chưa có chính sách rõ ràng về việc sử dụng máy tính và bảo vệ dữ liệu quan trọng.

Giải pháp tăng cường an toàn thông tin: Để tăng cường an toàn thông tin cho hệ thống máy tính của các phòng ban trong công ty tài chính XYZ, chúng tôi đề xuất các giải pháp sau:

1. **Triển khai các giải pháp bảo mật nâng cao:** Cài đặt và cấu hình các firewall, antivirus, và anti-malware trên mỗi máy tính để ngăn chặn các cuộc tấn công mạng.
2. **Đào tạo nhân viên về an toàn thông tin:** Cung cấp đào tạo định kỳ về an ninh mạng và cách phòng ngừa các cuộc tấn công qua email.
3. **Thực hiện sao lưu dữ liệu định kỳ:** Thực hiện các bản sao lưu dữ liệu định kỳ để đảm bảo dữ liệu được bảo vệ và có thể khôi phục sau các sự cố.
4. **Thiết lập chính sách bảo mật thông tin:** Xây dựng và thực thi các chính sách bảo mật thông tin để đảm bảo sự tuân thủ và nhận thức của nhân viên về an toàn thông tin.

Kết luận: Việc áp dụng các giải pháp trên sẽ giúp nâng cao an toàn thông tin cho hệ thống máy tính của các phòng ban trong công ty tài chính XYZ, giảm thiểu nguy cơ tấn công mạng và đảm bảo tính bảo mật của dữ liệu nội bộ của công ty. Điều này cũng đóng góp vào sự hiệu quả và tin cậy của hoạt động của công ty.