HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

CƠ SỞ TẠI THÀNH PHỐ HỒ CHÍ MINH

KHOA CÔNG NGHỆ THÔNG TIN 2

--ᔕ📖ᔓ--

BÁO CÁO CUỐI KỲ

MÔN: QUẢN LÝ AN TOÀN THÔNG TIN

Giảng viên hướng dẫn	**:**	Nguyễn Hữu Nguyên
Người thực hiện	**:**	Bùi Đức Phú
Mã số sinh viên	**:**	N20DCAT042
Lớp	**:**	D20CQAT01-N
Khoá	**:**	2020 – 2025
Hệ	**:**	ĐẠI HỌC CHÍNH QUY

Hồ Chí Minh – 31/05/2024

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……
……

Điểm:

TP. Hồ Chí Minh, tháng 5 năm 2024

XÁC NHẬN CỦA GIÁO VIÊN HƯỚNG DẪN

(Ký, ghi rõ họ tên)

NGUYỄN HỮU NGUYÊN

MỤC LỤC

GIẢ ĐỊNH

Giả sử bạn vừa được một công ty Z đồng ý tuyển vào vị trí công việc triển khai đảm bảo an toàn cho công ty. Công ty Z giao nhiệm vụ trong 2 tháng thử việc là lập và đề xuất kế hoạch/các công việc cần triển khai đảm bảo an toàn cho công ty, dựa trên việc triển khai khảo sát thực tế và các định hướng phát triển kinh doanh của công ty.

- Lĩnh vực kinh doanh: Dịch vụ tài chính trực tuyến.
- Thị trường: Quốc tế, tập trung vào khu vực Châu Âu và Bắc Mỹ.
- Quy mô công ty: Công ty có 150 nhân viên.
- Mô hình tổ chức của bộ phận công nghệ thông tin an toàn thông tin hiện tại: Hiện tại công ty có 3 nhân viên IT trực thuộc giám sát mạng và hệ thống, chưa có người chịu trách nhiệm về an toàn thông tin.

Hệ thống công nghệ thông tin hiện có:

- Hệ thống trang web cung cấp dịch vụ tài chính trực tuyến, với máy chủ được đặt tại các trung tâm dữ liệu ở Châu Âu và Bắc Mỹ.

- Hệ thống máy chủ và mạng nội bộ để quản lý thông tin khách hàng và hoạt động của công ty.
- Hệ thống máy tính làm việc cho nhân viên.

- Định hướng:

- Mở rộng thị trường sang khu vực Châu Á và Úc.
- Tăng cường bảo mật hệ thống để đảm bảo an toàn thông tin khách hàng và giao dịch tài chính.
- Phát triển các biện pháp chống giả mạo và gian lận tài chính.
- Tuyển dụng thêm nhân sự chuyên môn về an ninh mạng và bảo mật thông tin để thành lập phòng An ninh thông tin và tổ Bảo mật thông tin trực thuộc phòng Công nghệ thông tin.

KẾ HOẠCH ĐẢM BẢO AN TOÀN THÔNG TIN CHO CÔNG TY Z.

1. Đánh giá rủi ro an toàn thông tin

1.1. Xác định tài sản

- Tài sản vật lý:

- Phần cứng: Máy chủ (ứng dụng, cơ sở dữ liệu, web), thiết bị mạng (switch, router, firewall), máy trạm làm việc, điện thoại di động, máy tính xách tay.
- Phần mềm: Hệ điều hành, ứng dụng kinh doanh, phần mềm chống virus, phần mềm tường lửa.
- Dữ liệu: Dữ liệu khách hàng (thông tin cá nhân, lịch sử giao dịch), dữ liệu kinh doanh (doanh thu, chi phí, báo cáo tài chính), mã nguồn phần mềm.
- Môi trường: Văn phòng làm việc, trung tâm dữ liệu, hệ thống điện, hệ thống điều hòa không khí.

- Tài sản con người:

- Nhân viên chính thức, nhân viên hợp đồng, thực tập sinh, nhà thầu, đối tác.

1.2. Xác định mối đe dọa

- **Mối đe dọa bên trong:**

- Nhân viên:
  - Cố ý: Trộm cắp dữ liệu, phá hoại hệ thống, cài đặt phần mềm độc hại, lừa đảo, tiết lộ thông tin mật.
  - Vô ý: Mất mát hoặc làm hỏng thiết bị, vô tình cài đặt phần mềm độc hại, nhấp vào liên kết độc hại, sử dụng mật khẩu yếu, chia sẻ thông tin đăng nhập.
- Lỗi hệ thống:
  - Lỗi phần cứng: Hỏng hóc ổ cứng, mất điện đột ngột.
  - Lỗi phần mềm: Lỗi ứng dụng, xung đột phần mềm, lỗ hổng bảo mật chưa được vá.
  - Lỗi cấu hình: Cấu hình sai tường lửa, cấu hình sai quyền truy cập.

- **Mối đe dọa bên ngoài:**

- Hacker:
  - Tấn công mạng: Tấn công từ chối dịch vụ (DoS/DDoS), tấn công vào ứng dụng web, tấn công vào hệ thống mạng.
  - Lừa đảo trực tuyến: Lừa đảo qua email (phishing), lừa đảo qua điện thoại (vishing), lừa đảo qua tin nhắn (smishing).
- Phần mềm độc hại:
  - Virus: Lây lan qua tệp tin đính kèm, liên kết độc hại.
  - Worm: Tự động lây lan qua mạng.
  - Trojan: Giả dạng phần mềm hợp pháp để đánh cắp thông tin hoặc cài đặt phần mềm độc hại khác.
  - Ransomware: Mã hóa dữ liệu và yêu cầu tiền chuộc để giải mã.
- Gian lận tài chính:
  - Thực hiện các giao dịch giả mạo.

- Rửa tiền.
- Lừa đảo chiếm đoạt tài sản.

- Thiên tai:
  - Lũ lụt, hỏa hoạn, động đất, bão, lốc xoáy.

1.3. Xác định lỗ hổng

- Lỗ hổng kỹ thuật:
- Lỗ hổng trong hệ điều hành, phần mềm ứng dụng, thiết bị mạng.
- Thiếu các bản vá lỗi bảo mật.
- Cấu hình sai tường lửa, IDS/IPS.
- Mật khẩu yếu, không sử dụng xác thực hai yếu tố.
- Thiếu mã hóa dữ liệu.
- Lỗ hổng quy trình:
- Quy trình quản lý thay đổi chưa được kiểm soát.
- Quy trình quản lý sự cố chưa hiệu quả.
- Quy trình sao lưu và phục hồi dữ liệu chưa đầy đủ.
- Thiếu chính sách và quy định về an toàn thông tin.
- Lỗ hổng con người:
- Thiếu nhận thức về an toàn thông tin.
- Không tuân thủ các chính sách và quy trình an toàn thông tin.
- Bị lừa đảo bởi các cuộc tấn công lừa đảo trực tuyến.

1.4. Đánh giá rủi ro

- Phân tích định tính:
- Đánh giá mức độ nghiêm trọng của từng rủi ro dựa trên khả năng xảy ra (cao, trung bình, thấp) và tác động (cao, trung bình, thấp).
- Sử dụng ma trận rủi ro để đánh giá mức độ rủi ro tổng thể của từng tài sản.
- Phân tích định lượng:
- Tính toán giá trị tài sản (AV – Asset Value).
- Ước tính tần suất xảy ra tổn thất hàng năm (ARO – Annualized Rate of Occurrence).
- Ước tính mức độ tổn thất khi xảy ra rủi ro (SLE – Single Loss Expectancy).
- Tính toán kỳ vọng tổn thất hàng năm (ALE – Annualized Loss Expectancy) theo công thức: ALE = SLE x ARO.

1.5. Xử lý rủi ro

- Giảm thiểu (Mitigation): Triển khai các biện pháp kiểm soát để giảm khả năng xảy ra hoặc tác động của rủi ro (ví dụ: cài đặt phần mềm chống virus, tường lửa, đào tạo nhân viên).

- Chuyển giao (Transfer): Chuyển giao rủi ro cho bên thứ ba (ví dụ: mua bảo hiểm an ninh mạng).
- Tránh (Avoidance): Tránh các hoạt động có thể dẫn đến rủi ro (ví dụ: không lưu trữ dữ liệu nhạy cảm trên các thiết bị di động).
- Chấp nhận (Acceptance): Chấp nhận rủi ro nếu chi phí xử lý rủi ro cao hơn lợi ích mang lại.

2. Xây dựng và ban hành chính sách an toàn thông tin

2.1. Tổng quan về hệ thống chính sách an toàn thông tin

Xây dựng hệ thống chính sách an toàn thông tin dựa trên các tiêu chuẩn và thông lệ tốt nhất về an toàn thông tin, bao gồm ISO 27001 và NIST Cybersecurity Framework. Hệ thống chính sách này bao gồm các chính sách cấp cao, chính sách cấp bộ phận và các hướng dẫn, quy trình..

2.2. Chính sách cấp cao

- Chính sách An toàn Thông tin (Information Security Policy - ISP): Đây là chính sách cốt lõi, xác định các nguyên tắc, mục tiêu và cam kết của công ty đối với việc bảo vệ thông tin. Chính sách này cũng xác định rõ trách nhiệm của ban lãnh đạo, các phòng ban và từng cá nhân trong việc đảm bảo an toàn thông tin.
- Chính sách Quản lý Rủi ro An toàn Thông tin (Information Security Risk Management Policy): Chính sách này quy định quy trình đánh giá và quản lý rủi ro an toàn thông tin, bao gồm việc xác định, đánh giá, xử lý và giám sát rủi ro.
- Chính sách Phân loại Thông tin (Information Classification Policy): Chính sách này xác định các loại thông tin (như thông tin mật, thông tin nội bộ, thông tin công khai) và mức độ bảo vệ tương ứng cho từng loại.
- Chính sách Sử dụng Tài nguyên Công nghệ Thông tin (Acceptable Use Policy - AUP): Chính sách này quy định cách thức sử dụng các tài nguyên CNTT của công ty một cách có trách nhiệm và tuân thủ pháp luật, bao gồm cả việc sử dụng email, internet, mạng xã hội và các thiết bị di động.
- Chính sách Chống Giả mạo và Gian lận (Anti-Fraud and Anti-Money Laundering Policy): Chính sách này quy định các biện pháp phòng ngừa và phát hiện các hành vi giả mạo và gian lận tài chính, bao gồm cả việc xác minh danh tính khách hàng, giám sát giao dịch và báo cáo các hoạt động đáng ngờ.

2.3. Chính sách cấp bộ phận

- Chính sách An ninh Mạng (Network Security Policy): Quy định các biện pháp bảo vệ mạng máy tính của công ty, bao gồm cả tường lửa, hệ thống phát hiện xâm nhập và các biện pháp kiểm soát truy cập.
- Chính sách Bảo mật Dữ liệu (Data Protection Policy): Quy định các biện pháp bảo vệ dữ liệu cá nhân và dữ liệu nhạy cảm khác của công ty, bao gồm cả việc mã hóa, sao lưu và quản lý truy cập.
- Chính sách Quản lý Sự cố An toàn Thông tin (Incident Response Policy): Quy định quy trình xử lý các sự cố an toàn thông tin, từ việc phát hiện, báo cáo, điều tra đến khắc phục và phòng ngừa.

- Chính sách Quản lý Thay đổi (Change Management Policy**):** Quy định quy trình quản lý các thay đổi đối với hệ thống CNTT của công ty, nhằm đảm bảo rằng các thay đổi được thực hiện một cách an toàn và không gây ảnh hưởng đến hoạt động kinh doanh.

2.4. Hướng dẫn và quy trình thực hiện

- Hướng dẫn về Mật khẩu Mạnh (Strong Password Guidelines): Hướng dẫn nhân viên cách tạo và sử dụng mật khẩu mạnh.
- Quy trình Báo cáo Sự cố An toàn Thông tin (Incident Reporting Procedure): Hướng dẫn nhân viên cách báo cáo các sự cố an toàn thông tin.
- Quy trình Sao lưu và Phục hồi Dữ liệu (Backup and Recovery Procedure): Hướng dẫn quy trình sao lưu và phục hồi dữ liệu.
- Quy trình Quản lý Bản vá Lỗi (Patch Management Procedure): Hướng dẫn quy trình cập nhật các bản vá lỗi bảo mật cho phần mềm và hệ thống.
- Quy trình Xác minh Danh tính Khách hàng (Customer Identification Procedure): Hướng dẫn quy trình xác minh danh tính của khách hàng để ngăn chặn giả mạo.
- Quy trình Giám sát Giao dịch (Transaction Monitoring Procedure): Hướng dẫn quy trình giám sát các giao dịch tài chính để phát hiện các hoạt động đáng ngờ.

2.5. Triển khai và duy trì

- Ban hành: Các chính sách và hướng dẫn được ban hành bởi Ban Giám đốc và được phổ biến đến toàn thể nhân viên.
- Đào tạo: Tổ chức các buổi đào tạo về an toàn thông tin cho nhân viên để nâng cao nhận thức và hiểu biết về các chính sách và quy trình.
- Xem xét định kỳ: Thường xuyên xem xét và cập nhật các chính sách và hướng dẫn để đảm bảo tính phù hợp với môi trường kinh doanh và công nghệ luôn thay đổi.

2.6. Thực thi và giám sát

- Thực thi: Các chính sách và quy trình được thực thi một cách nghiêm túc và nhất quán.
- Giám sát: Thường xuyên giám sát việc tuân thủ các chính sách và quy trình, đồng thời xử lý kịp thời các vi phạm.

2.7. Cải tiến liên tục

- Thu thập phản hồi: Thu thập phản hồi từ nhân viên và các bên liên quan để cải tiến hệ thống chính sách.
- Đánh giá hiệu quả: Thường xuyên đánh giá hiệu quả của hệ thống chính sách và thực hiện các điều chỉnh cần thiết.

3. Triển khai các biện pháp kỹ thuật

3.1. Bảo vệ hệ thống mạng

- Tường lửa ứng dụng web (Web Application Firewall - WAF): Cài đặt WAF để bảo vệ hệ thống trang web khỏi các cuộc tấn công như SQL injection, cross-site scripting (XSS) và các lỗ hổng khác.
- Hệ thống phát hiện và ngăn chặn xâm nhập (Intrusion Detection and Prevention System - IDPS): Triển khai IDPS để giám sát lưu lượng mạng theo thời gian thực, phát hiện và ngăn chặn các cuộc tấn công mạng, đồng thời cung cấp cảnh báo kịp thời cho đội ngũ an ninh.
- Phân đoạn mạng (Network Segmentation): Chia mạng nội bộ thành các phân đoạn nhỏ hơn dựa trên chức năng hoặc mức độ nhạy cảm của dữ liệu, giúp cô lập các cuộc tấn công và hạn chế thiệt hại.
- Kiểm soát truy cập mạng (Network Access Control - NAC): Triển khai NAC để kiểm soát và giới hạn quyền truy cập vào mạng dựa trên các tiêu chí như danh tính người dùng, loại thiết bị và trạng thái bảo mật.

3.2. Bảo vệ máy chủ và thiết bị đầu cuối

- Hệ thống phòng chống xâm nhập máy chủ (Host-based Intrusion Prevention System - HIPS): Cài đặt HIPS trên các máy chủ để giám sát và ngăn chặn các hoạt động đáng ngờ, bảo vệ máy chủ khỏi các cuộc tấn công từ bên trong và bên ngoài.
- Phần mềm diệt virus và chống phần mềm độc hại (Endpoint Protection Platform - EPP): Triển khai EPP trên các máy trạm và thiết bị đầu cuối để bảo vệ chúng khỏi virus, phần mềm độc hại, ransomware và các mối đe dọa khác.
- Quản lý bản vá lỗi (Patch Management): Thực hiện quy trình quản lý bản vá lỗi chặt chẽ, tự động cập nhật các bản vá lỗi bảo mật cho hệ điều hành, phần mềm ứng dụng để vá các lỗ hổng bảo mật.
- Quản lý cấu hình an toàn (Security Configuration Management - SCM): Xây dựng và duy trì các cấu hình an toàn chuẩn cho các máy chủ, thiết bị mạng và thiết bị đầu cuối, đảm bảo chúng được cấu hình đúng cách và tuân thủ các tiêu chuẩn bảo mật.
- Kiểm soát thiết bị (Device Control): Giới hạn các loại thiết bị có thể kết nối vào mạng công ty và kiểm soát việc sử dụng các thiết bị lưu trữ di động để ngăn chặn việc mất mát hoặc đánh cắp dữ liệu.

3.3. Bảo vệ dữ liệu

- Mã hóa dữ liệu (Data Encryption): Sử dụng các thuật toán mã hóa mạnh mẽ như AES-256 để mã hóa dữ liệu nhạy cảm khi lưu trữ và truyền tải, đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập và đọc dữ liệu.
- Quản lý khóa mã hóa (Key Management): Triển khai hệ thống quản lý khóa mã hóa an toàn để bảo vệ các khóa mã hóa và đảm bảo tính toàn vẹn của chúng.

- Sao lưu và phục hồi dữ liệu (Backup and Disaster Recovery): Thực hiện sao lưu dữ liệu thường xuyên và lưu trữ bản sao lưu ở một vị trí an toàn, tách biệt với hệ thống chính, để đảm bảo khả năng phục hồi dữ liệu trong trường hợp xảy ra sự cố.
- Phân loại dữ liệu (Data Classification): Phân loại dữ liệu theo mức độ nhạy cảm và áp dụng các biện pháp bảo vệ phù hợp cho từng loại dữ liệu.
- Ngăn ngừa mất mát dữ liệu (Data Loss Prevention - DLP): Triển khai giải pháp DLP để giám sát và ngăn chặn việc rò rỉ dữ liệu nhạy cảm ra ngoài thông qua email, web, thiết bị di động hoặc các kênh khác.
- Tokenization: Thay thế các dữ liệu nhạy cảm bằng các mã token để giảm thiểu rủi ro trong trường hợp bị xâm nhập.

3.4. Bảo vệ các ứng dụng web

- Kiểm thử an ninh ứng dụng web (Web Application Security Testing - WAST): Thực hiện kiểm thử an ninh ứng dụng web thường xuyên, bao gồm cả kiểm thử tĩnh (Static Application Security Testing - SAST) và kiểm thử động (Dynamic Application Security Testing - DAST), để phát hiện và khắc phục các lỗ hổng bảo mật.
- Quản lý danh tính và truy cập (Identity and Access Management - IAM): Triển khai giải pháp IAM để quản lý danh tính người dùng, xác thực và ủy quyền truy cập vào các ứng dụng và dữ liệu, đảm bảo rằng chỉ những người dùng được phép mới có thể truy cập vào các tài nguyên cần thiết.
- Xác thực đa yếu tố (Multi-Factor Authentication - MFA): Bắt buộc sử dụng MFA cho việc đăng nhập vào các ứng dụng quan trọng để tăng cường bảo mật.
- Kiểm soát phiên làm việc (Session Management): Quản lý phiên làm việc của người dùng một cách an toàn để ngăn chặn tấn công chiếm quyền điều khiển phiên làm việc.

4. Nâng cao nhận thức về an toàn thông tin

Do công ty chưa có bộ phận an toàn thông tin, cũng như chưa có nhân viên phụ trách mảng này nên việc nâng cao nhận thức về an toàn thông tin là rất cần thiết. Cần thực hiện các biện pháp sau:

- Đào tạo:

- Đào tạo cơ bản**:** Tổ chức các khóa đào tạo về an toàn thông tin cho tất cả nhân viên, bao gồm cả nhân viên mới và nhân viên hiện tại.
- Nội dung đào tạo bao gồm các kiến thức cơ bản về an toàn thông tin, các mối đe dọa phổ biến (đặc biệt là các cuộc tấn công lừa đảo trực tuyến nhắm vào khách hàng), cách nhận diện và phòng tránh các cuộc tấn công lừa đảo, cách sử dụng mật khẩu mạnh và bảo vệ thông tin cá nhân.
- Đào tạo chuyên sâu**:** Tổ chức các buổi đào tạo chuyên sâu về an toàn thông tin cho các nhân viên làm việc trong các bộ phận có nguy cơ cao như IT, tài chính.
- Nội dung đào tạo nâng cao bao gồm kiến thức về các biện pháp bảo mật chuyên sâu, cách phát hiện và xử lý sự cố an ninh, cách quản lý rủi ro và tuân thủ các quy định pháp luật về bảo mật thông tin.

- Kiểm tra:

- Thực hiện các bài kiểm tra định kỳ để đánh giá kiến thức và kỹ năng về an toàn thông tin của nhân viên.
- Sử dụng các bài kiểm tra mô phỏng các cuộc tấn công lừa đảo để đánh giá khả năng nhận diện và phòng tránh của nhân viên.

- Khuyến khích:

- Khuyến khích nhân viên báo cáo các sự cố an toàn thông tin và đưa ra các đề xuất cải tiến.
- Thiết lập hệ thống khen thưởng cho các nhân viên có đóng góp tích cực cho việc nâng cao an toàn thông tin của công ty.

- Xây dựng văn hóa an toàn thông tin:

- Lồng ghép các thông điệp về an toàn thông tin vào các hoạt động truyền thông nội bộ của công ty.
- Tổ chức các sự kiện và cuộc thi về an toàn thông tin để tạo sự hứng thú và tăng cường nhận thức cho nhân viên.
- Xây dựng một môi trường làm việc mà mọi người đều nhận thức được tầm quan trọng của an toàn thông tin và sẵn sàng thực hiện các biện pháp bảo vệ.

5. Ứng phó sự cố an toàn thông tin

- Xây dựng quy trình ứng phó sự cố:

- Xác định các loại sự cố an toàn thông tin có thể xảy ra:
  - Sự cố về an ninh mạng: Tấn công mạng, xâm nhập trái phép, mã độc, rò rỉ dữ liệu.
  - Sự cố về hệ thống: Mất điện, hỏng hóc phần cứng, lỗi phần mềm.
  - Sự cố về con người: Mất mát hoặc đánh cắp thiết bị, lỗi thao tác của nhân viên.
  - Sự cố về gian lận tài chính: Giao dịch giả mạo, rửa tiền, lừa đảo.
  - Sự cố về thiên tai: Cháy nổ, lũ lụt, động đất.
- Xác định các bước cần thực hiện khi xảy ra sự cố:
  - Phát hiện: Phát hiện sự cố thông qua hệ thống giám sát, báo cáo của nhân viên hoặc các kênh thông tin khác.
  - Đánh giá: Đánh giá mức độ nghiêm trọng của sự cố và xác định phạm vi ảnh hưởng.
  - Thông báo: Thông báo cho các bên liên quan, bao gồm ban lãnh đạo, đội ngũ an ninh, nhân viên và khách hàng (nếu cần).
  - Chặn đứng: Thực hiện các biện pháp để ngăn chặn sự cố lan rộng và giảm thiểu thiệt hại.
  - Khắc phục: Khôi phục hệ thống và dữ liệu về trạng thái hoạt động bình thường.
  - Điều tra: Điều tra nguyên nhân gốc rễ của sự cố và xác định các biện pháp phòng ngừa.
  - Báo cáo: Lập báo cáo về sự cố và các biện pháp đã thực hiện.
- Phân công trách nhiệm cho từng thành viên trong đội ứng phó sự cố:
  - Trưởng nhóm: Điều phối các hoạt động ứng phó sự cố, đưa ra quyết định và báo cáo cho ban lãnh đạo.
  - Chuyên viên kỹ thuật: Phân tích sự cố, thực hiện các biện pháp khắc phục kỹ thuật.

- Chuyên viên truyền thông: Thông báo cho các bên liên quan, quản lý thông tin và truyền thông về sự cố.
- Chuyên viên pháp lý: Tư vấn về các vấn đề pháp lý liên quan đến sự cố.

- Thành lập đội ứng phó sự cố:

- Lựa chọn các thành viên có kiến thức và kinh nghiệm về an toàn thông tin, CNTT, quản lý rủi ro và truyền thông.
- Đảm bảo đội ngũ có đủ nguồn lực và khả năng làm việc 24/7 để ứng phó với các sự cố bất ngờ.
- Tổ chức các buổi đào tạo và huấn luyện định kỳ để nâng cao kỹ năng và kiến thức của đội ngũ.

- Diễn tập ứng phó sự cố:

- Xây dựng các kịch bản sự cố thực tế và đa dạng để đánh giá khả năng ứng phó của đội ngũ.
- Thực hiện diễn tập định kỳ (hàng quý hoặc hàng năm) để đảm bảo đội ngũ luôn sẵn sàng và có thể phản ứng nhanh chóng khi xảy ra sự cố thực tế.
- Sau mỗi buổi diễn tập, đánh giá kết quả, rút ra bài học kinh nghiệm và cập nhật quy trình ứng phó sự cố.
- Phát triển các công cụ và quy trình hỗ trợ:
- Xây dựng hệ thống giám sát và cảnh báo sớm để phát hiện các dấu hiệu bất thường và các cuộc tấn công tiềm ẩn.
- Phát triển các công cụ phân tích và xử lý sự cố để hỗ trợ quá trình điều tra và khắc phục sự cố.
- Thiết lập các kênh liên lạc an toàn và hiệu quả để đảm bảo thông tin được truyền đạt nhanh chóng và chính xác trong quá trình ứng phó sự cố.

6. Đánh giá và cải tiến

- Đánh giá định kỳ:

- Tần suất**:** Thực hiện đánh giá định kỳ hàng năm hoặc khi có sự thay đổi đáng kể về môi trường kinh doanh, công nghệ hoặc quy định pháp luật.
- Phạm vi**:** Đánh giá toàn bộ hệ thống quản lý an toàn thông tin, bao gồm các chính sách, quy trình, biện pháp kỹ thuật và con người.
- Phương pháp**:** Sử dụng các phương pháp đánh giá khác nhau như phỏng vấn, khảo sát, kiểm tra hồ sơ, kiểm tra kỹ thuật (ví dụ: kiểm tra thâm nhập, đánh giá lỗ hổng).
- Kết quả**:** Xác định các điểm mạnh, điểm yếu và đưa ra khuyến nghị cải tiến cụ thể để nâng cao tính hiệu quả của hệ thống an toàn thông tin.

- Cải tiến liên tục:

- Theo dõi và giám sát**:** Liên tục theo dõi và giám sát các hoạt động an toàn thông tin để phát hiện sớm các rủi ro và sự cố. Sử dụng các công cụ SIEM (Security Information and Event Management) để thu thập, phân tích và tương quan các bản ghi sự kiện bảo mật từ các nguồn khác nhau.
- Cập nhật và nâng cấp**:** Thường xuyên cập nhật và nâng cấp các chính sách, quy trình, công nghệ và giải pháp bảo mật để đáp ứng với sự thay đổi của môi trường và các mối đe dọa mới. Thực hiện các bài kiểm tra an ninh định kỳ để đánh giá tính hiệu quả của các biện pháp bảo mật hiện có.

- Đào tạo và nâng cao nhận thức**:** Tiếp tục đào tạo và nâng cao nhận thức về an toàn thông tin cho nhân viên để đảm bảo họ luôn có kiến thức và kỹ năng cần thiết để bảo vệ thông tin của công ty. Tổ chức các buổi đào tạo định kỳ về các mối đe dọa mới nhất và các kỹ thuật phòng chống tấn công.
- Quản lý thay đổi**:** Thiết lập quy trình quản lý thay đổi chặt chẽ để đảm bảo rằng tất cả các thay đổi đối với hệ thống CNTT đều được đánh giá rủi ro bảo mật và được phê duyệt trước khi triển khai.
- Đánh giá rủi ro thường xuyên**:** Thực hiện đánh giá rủi ro an toàn thông tin định kỳ để xác định và đánh giá các rủi ro mới phát sinh, từ đó cập nhật và điều chỉnh các biện pháp kiểm soát rủi ro phù hợp.
- Hợp tác với các chuyên gia an ninh mạng**:** Cân nhắc hợp tác với các chuyên gia an ninh mạng bên ngoài để được tư vấn và hỗ trợ trong việc đánh giá, cải tiến và triển khai các biện pháp bảo mật hiệu quả hơn.

7. Hợp tác với các đối tác công nghệ

- Lựa chọn đối tác:

- Tiêu chí lựa chọn: Ưu tiên các đối tác có uy tín, kinh nghiệm trong lĩnh vực an toàn thông tin, tài chính ngân hàng, tuân thủ các tiêu chuẩn bảo mật quốc tế (ví dụ: ISO 27001, PCI DSS) và có kinh nghiệm triển khai các dự án bảo mật cho các tổ chức tài chính.
- Đánh giá đối tác**:** Thực hiện đánh giá rủi ro an ninh đối với các đối tác tiềm năng, xem xét các báo cáo đánh giá độc lập và đánh giá của khách hàng khác.

- Thỏa thuận về an toàn thông tin:

- Hợp đồng: Ký kết hợp đồng chi tiết về các yêu cầu bảo mật, trách nhiệm của mỗi bên trong việc bảo vệ thông tin, quy trình xử lý sự cố và các biện pháp bồi thường nếu xảy ra vi phạm.
- Đánh giá định kỳ: Thường xuyên đánh giá lại hoạt động bảo mật của đối tác và yêu cầu cung cấp các báo cáo về an ninh.
- Trao đổi thông tin và hợp tác:
- Chia sẻ thông tin về mối đe dọa: Thiết lập kênh trao đổi thông tin về các mối đe dọa an ninh mạng mới nhất, các lỗ hổng bảo mật và các biện pháp phòng ngừa.
- Hợp tác ứng phó sự cố: Xây dựng quy trình hợp tác ứng phó sự cố an ninh mạng với các đối tác, bao gồm cả việc chia sẻ thông tin, phối hợp điều tra và khắc phục sự cố.

- Kiểm tra an ninh:

- Kiểm tra sản phẩm/dịch vụ: Yêu cầu đối tác cung cấp các báo cáo kiểm tra an ninh sản phẩm/dịch vụ từ các tổ chức độc lập.
- Kiểm tra định kỳ: Tiến hành kiểm tra an ninh định kỳ đối với các sản phẩm/dịch vụ của đối tác được sử dụng trong hệ thống của công ty.
- Bảo mật trong quá trình chia sẻ dữ liệu:
- Mã hóa dữ liệu: Sử dụng các phương pháp mã hóa mạnh mẽ để bảo vệ dữ liệu khi trao đổi với đối tác.

- Thỏa thuận về quyền truy cập dữ liệu: Xác định rõ quyền truy cập và sử dụng dữ liệu của từng bên trong hợp đồng.
- Giám sát việc truy cập dữ liệu**:** Thực hiện giám sát việc truy cập và sử dụng dữ liệu của đối tác để đảm bảo tuân thủ các thỏa thuận về bảo mật.

8. Đảm bảo an toàn thông tin trong quá trình mở rộng kinh doanh

- Đánh giá rủi ro:
- Thực hiện đánh giá rủi ro an toàn thông tin trước khi mở rộng sang thị trường mới, đặc biệt là khu vực Châu Á và Úc.
- Xác định các rủi ro tiềm ẩn liên quan đến an toàn thông tin như các quy định pháp luật về bảo mật khác nhau, các mối đe dọa an ninh mạng đặc thù của từng khu vực và đánh giá mức độ ảnh hưởng của chúng.
- Xây dựng các biện pháp giảm thiểu rủi ro phù hợp với từng thị trường cụ thể.
- Triển khai các biện pháp bảo mật:
- Triển khai các biện pháp bảo mật phù hợp với từng thị trường mới, đặc biệt là các biện pháp chống giả mạo và gian lận tài chính.
- Xem xét các yêu cầu pháp lý và quy định về an toàn thông tin của từng quốc gia hoặc khu vực, đặc biệt là các quy định về bảo vệ dữ liệu cá nhân.
- Đảm bảo rằng các biện pháp bảo mật được tích hợp vào quy trình kinh doanh mới và được điều chỉnh để phù hợp với đặc thù của từng thị trường.
- Đào tạo nhân viên:
- Đào tạo nhân viên về các chính sách và quy trình an toàn thông tin mới, đặc biệt là các quy định và rủi ro bảo mật liên quan đến thị trường mới.
- Nâng cao nhận thức của nhân viên về các rủi ro an toàn thông tin liên quan đến hoạt động kinh doanh mới hoặc thị trường mới.
- Khuyến khích nhân viên báo cáo các sự cố và vấn đề liên quan đến an toàn thông tin.
- Quản lý nhà cung cấp:
- Đánh giá rủi ro an toàn thông tin của các nhà cung cấp dịch vụ bên thứ ba tại các thị trường mới.
- Ký kết các thỏa thuận về an toàn thông tin với các nhà cung cấp, đảm bảo các thỏa thuận này phù hợp với quy định pháp luật của từng khu vực.
- Giám sát hoạt động của các nhà cung cấp để đảm bảo họ tuân thủ các yêu cầu về an toàn thông tin.
- Giám sát và điều chỉnh:
- Thường xuyên giám sát và đánh giá hiệu quả của các biện pháp bảo mật đã triển khai tại các thị trường mới.
- Điều chỉnh và cải tiến các biện pháp bảo mật khi cần thiết để ứng phó với các thay đổi về môi trường kinh doanh, công nghệ và các mối đe dọa mới.
- Hợp tác với các cơ quan quản lý:
- Thiết lập mối quan hệ hợp tác với các cơ quan quản lý tài chính và an ninh mạng tại các thị trường mới.

- Cập nhật thông tin về các quy định pháp luật và các yêu cầu về bảo mật để đảm bảo tuân thủ.
- Hợp tác trong việc điều tra và xử lý các sự cố an ninh mạng.

9. Tuân thủ pháp luật

- Nghiên cứu và cập nhật:
- Luật An toàn thông tin mạng: Bắt buộc tuân thủ Luật An toàn thông tin mạng của Việt Nam, các quy định về an toàn thông tin trong lĩnh vực tài chính ngân hàng và các quy định liên quan tại các quốc gia Châu Âu, Bắc Mỹ, Châu Á và Úc.
- GDPR: Nếu công ty có hoạt động xử lý dữ liệu cá nhân của công dân EU, cần tuân thủ Quy định chung về bảo vệ dữ liệu (GDPR).
- Các quy định khác: Tuân thủ các quy định về bảo mật thông tin trong lĩnh vực tài chính ngân hàng tại các quốc gia mà công ty hoạt động, bao gồm các quy định về chống rửa tiền (AML) và chống tài trợ khủng bố (CFT).
- Thực hiện đánh giá tuân thủ:
- Định kỳ: Tiến hành đánh giá tuân thủ các quy định pháp luật về an toàn thông tin một cách định kỳ (ví dụ: hàng năm).
- Khi có thay đổi: Thực hiện đánh giá lại khi có sự thay đổi về quy định pháp luật hoặc hoạt động kinh doanh của công ty.
- Báo cáo: Lập báo cáo đánh giá tuân thủ và lưu trữ để chứng minh sự tuân thủ của công ty.
- Báo cáo sự cố:
- Quy trình báo cáo: Xây dựng quy trình báo cáo sự cố an toàn thông tin cho các cơ quan chức năng theo quy định của từng quốc gia.
- Thời gian báo cáo: Báo cáo sự cố trong thời gian quy định (ví dụ: trong vòng 24 giờ).
- Nội dung báo cáo: Cung cấp đầy đủ thông tin về sự cố, bao gồm nguyên nhân, tác động và biện pháp khắc phục.
- Hợp tác với các cơ quan chức năng:
- Thiết lập mối quan hệ hợp tác với các cơ quan quản lý tài chính và an ninh mạng tại các quốc gia mà công ty hoạt động.
- Cập nhật thông tin về các quy định pháp luật và các yêu cầu về bảo mật.
- Hợp tác trong việc điều tra và xử lý các sự cố an ninh mạng hoặc các vụ việc liên quan đến gian lận tài chính.

10. Kết Luận

Kế hoạch đảm bảo an toàn thông tin này chỉ ra các bước cần thiết để bảo vệ hệ thống và dữ liệu của công ty Z, đặc biệt trong quá trình mở rộng kinh doanh sang các thị trường mới. Việc thực hiện kế hoạch này sẽ giúp công ty giảm thiểu rủi ro, nâng cao uy tín và đảm bảo hoạt động kinh doanh được thông suốt, đồng thời tuân thủ các quy định pháp luật về an toàn thông tin và bảo vệ dữ liệu cá nhân.