Bài tập Chương 6 – Chiến lược QLRR (Risk Management Strategy)

Đề bài tập: Hãy đề xuất chiến lược QLRR ATTT cho một rủi ro CNTT mà bạn biết.

Lớp: NT207.P11.ATCL
Mã số SV: 21520202
Tên SV: Hồ Hải Dương

Sinh viên soạn bài làm theo Dàn bài sau đây:

Đề xuất chiến lược QLRR ATTT đối với rủi ro bảo mật từ nhà cung cấp dịch vụ đám mây và lỗ hổng người dùng

I. NHÓM YÊU CẦU – YÊU CẦU:

Rủi ro thuộc về 3 nhóm sau:

1. **Nhóm A.15 - Quan hệ với nhà cung cấp (Supplier Relationships)**, Yêu cầu **A.15.1 - Security in supplier relationships**
2. **Nhóm A.9 - Kiểm soát truy cập (Access Control)**, Yêu cầu **A.9.4 - System and application access control**
3. **Nhóm A.6 - Tổ chức quản lý an toàn thông tin (Organization of Information Security)**, Yêu cầu **A.6.2 - Mobile devices and teleworking**

II. ĐIỀU KHOẢN VI PHẠM

Người kiểm tra ATTT đã phát hiện sự không phù hợp tại các điều khoản sau:

1. **A.15.1.1 - Security in supplier relationships**
   Control: "Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented."
2. **A.9.4.1 - Information access restriction**
   Control: "Access to information and application system functions shall be restricted in accordance with the access control policy."
3. **A.6.2.2 - Mobile devices and teleworking**
   Control: "A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites."

III. NỘI DUNG PHÁT HIỆN VI PHẠM

Tình huống/ngữ cảnh: Công ty ABC sử dụng dịch vụ đám mây từ nhà cung cấp XYZ để lưu trữ và quản lý dữ liệu nhạy cảm của khách hàng. Do chính sách bảo mật chưa được thắt chặt, một số nhân viên của công ty có quyền truy cập vào dữ liệu mà không có các biện pháp kiểm soát đầy đủ.

1. **ĐIỂM YẾU**:
   - Thiếu mã hóa dữ liệu của nhà cung cấp dịch vụ đám mây.
   - Kiểm soát truy cập lỏng lẻo từ phía nhà cung cấp.
   - Chính sách kiểm soát truy cập không rõ ràng của Công ty ABC.
   - Quyền truy cập không cần thiết của một số nhân viên vào dữ liệu nhạy cảm.
2. **MỐI ĐE DỌA**:
   - Khai thác lỗ hổng bảo mật.
3. **RỦI RO TIỀM ẨN**:
   - Rủi ro mất mát hoặc lộ dữ liệu khách hàng nếu kẻ tấn công truy cập trái phép vào hệ thống đám mây.
   - Rủi ro dữ liệu bị chỉnh sửa hoặc xóa bởi người dùng không có thẩm quyền hoặc kẻ tấn công.
   - Vi phạm các quy định pháp lý và hợp đồng bảo mật do không đảm bảo an toàn thông tin cho dữ liệu nhạy cảm của khách hàng.
4. **KHẢ NĂNG XẢY RA RỦI RO (Likelihood)**: 80%
   - Do các điểm yếu từ nhà cung cấp dịch vụ đám mây và chính sách kiểm soát truy cập chưa chặt chẽ, khả năng xảy ra rủi ro là cao.
5. **HỆ QUẢ (Impact/Consequence)**:

- Dữ liệu của khách hàng có thể bị kẻ xấu truy cập và sử dụng cho các mục đích xấu, gây thiệt hại uy tín cho Công ty ABC.
- Công ty ABC có thể bị mất các hợp đồng lớn do vi phạm yêu cầu bảo mật thông tin từ phía khách hàng.
- Khách hàng mất niềm tin vào công ty và có thể chuyển sang đối thủ cạnh tranh.
- Công ty có thể phải chịu các khoản phạt tài chính hoặc trách nhiệm pháp lý do vi phạm các quy định về bảo mật và quyền riêng tư của dữ liệu khách hàng.
- Các chi phí khắc phục sự cố và cải thiện bảo mật sau khi xảy ra vi phạm sẽ tốn kém và ảnh hưởng đến hoạt động kinh doanh của công ty.

IV. CHIẾN LƯỢC QUẢN LÝ RỦI RO ATTT

1. Chọn chiến lược nào trong 4 chiến lược sau đây:

- Chấp nhận rủi ro ☐
- Giảm nhẹ rủi ro ☑
- Tránh né rủi ro ☐
- Chuyển giao rủi ro ☐

2. Giải thích:

a) Lý do chọn chiến lược:
- Nhà cung cấp dịch vụ đám mây có thể không thực hiện đủ biện pháp bảo mật, gây nguy cơ mất dữ liệu và xâm phạm quyền riêng tư.
- Chính sách kiểm soát truy cập không rõ ràng và quyền truy cập không cần thiết của một số nhân viên làm gia tăng rủi ro.

b) Mục tiêu:
- Đảm bảo an toàn và bảo mật dữ liệu của tổ chức khi sử dụng dịch vụ đám mây, giảm thiểu khả năng mất dữ liệu và xâm phạm quyền riêng tư.

c) Biện pháp kiểm soát để kiểm soát rủi ro và thực hiện chiến lược:
- Yêu cầu nhà cung cấp dịch vụ đám mây triển khai mã hóa dữ liệu và áp dụng các biện pháp xác thực đa yếu tố (MFA) để bảo vệ quyền truy cập.
- Thiết lập các chính sách kiểm soát truy cập rõ ràng, chỉ cấp quyền truy cập cần thiết cho nhân viên dựa trên vai trò công việc.
- Thực hiện giám sát và đánh giá định kỳ để phát hiện và xử lý kịp thời các hoạt động truy cập trái phép.

V. KẾ HOẠCH THỰC HIỆN ('Plan of Action'):

Các công việc (hoặc các bước) sẽ triển khai biện pháp kiểm soát rủi ro (hay phương án xử lý rủi ro) được thực hiện theo kế hoạch sau	Dự kiến nguồn lực, chi phí để thực hiện	Đơn vị/ cá nhân thực hiện	Lịch trình triển khai	Thời hạn hoàn thành
1. Chiến lược giảm nhẹ rủi ro - Triển khai mã hóa và kiểm soát truy cập cho dịch vụ đám mây • **Bước 1**: Làm việc với nhà cung cấp dịch vụ đám mây để thiết lập các biện pháp mã hóa toàn bộ dữ liệu. Điều này bao gồm việc mã hóa dữ liệu trong quá trình lưu trữ và khi truyền tải qua mạng. Mã hóa giúp bảo vệ dữ liệu khỏi truy cập trái phép ngay cả khi có vi phạm bảo mật. • **Bước 2**: Yêu cầu nhà cung cấp dịch vụ đám mây triển khai xác thực đa yếu tố (MFA) cho tất cả các tài khoản truy cập vào hệ	**Công ty cung cấp dịch vụ**: Sử dụng dịch vụ từ Amazon Web Services (AWS) với các tính năng bảo mật tích hợp như mã hóa và MFA. **Chi phí thực hiện**: Khoảng 5,000 USD/tháng cho dịch vụ bảo mật dữ liệu và xác thực đa yếu tố (bao gồm cả chi	Phòng IT của Công ty ABC phối hợp với AWS, công ty cung cấp dịch vụ đám mây, để triển khai các biện pháp mã hóa và kiểm soát truy cập.	Triển khai bắt đầu từ ngày 01/11/2024.	1 tuần.

thống. MFA đảm bảo rằng chỉ những người được ủy quyền mới có thể truy cập vào dữ liệu quan trọng, giảm thiểu nguy cơ từ việc đánh cắp mật khẩu hoặc truy cập trái phép qua tài khoản. • **Bước 3**: Thực hiện phân quyền truy cập theo vai trò cụ thể của nhân viên, đảm bảo rằng chỉ những nhân viên thực sự cần thiết mới có quyền truy cập vào dữ liệu nhạy cảm. Điều này bao gồm việc thiết lập các cấp độ truy cập khác nhau cho từng vai trò công việc, từ đó kiểm soát chặt chẽ quyền truy cập vào thông tin quan trọng và hạn chế nguy cơ từ việc lạm dụng quyền truy cập. • **Bước 4**: Thiết lập hệ thống giám sát hoạt động đăng nhập và truy cập vào dịch vụ đám mây để phát hiện và cảnh báo các hành vi đáng ngờ, chẳng hạn như truy cập từ các vị trí địa lý bất thường hoặc nhiều lần đăng nhập không thành công. Việc giám sát này giúp phát hiện kịp thời các hành vi truy cập trái phép và ngăn chặn các cuộc tấn công trước khi chúng gây ra thiệt hại.	phí quản lý và duy trì dịch vụ). Chi phí này bao gồm mã hóa dữ liệu, MFA, giám sát đăng nhập và hỗ trợ kỹ thuật từ AWS.			
2. Chiến lược giám sát rủi ro - Kiểm tra định kỳ và đánh giá tuân thủ • **Bước 1**: Lên lịch kiểm tra và đánh giá bảo mật định kỳ hàng tháng cho toàn bộ hệ thống đám mây, tập trung vào các yếu tố quan trọng như mã hóa dữ liệu, kiểm soát truy cập, và giám sát đăng nhập. Việc kiểm tra định kỳ này sẽ đảm bảo các biện pháp bảo mật luôn được duy trì và tuân thủ các tiêu chuẩn an toàn thông tin của ISO 27001:2013. • **Bước 2**: Báo cáo kết quả kiểm tra định kỳ và xử lý ngay lập tức bất kỳ lỗ hổng hoặc sự cố bảo mật nào được phát hiện. Việc xử lý nhanh chóng giúp bảo vệ hệ thống và dữ liệu khỏi các rủi ro tiềm ẩn, đảm bảo rằng các biện pháp bảo mật luôn được cập nhật và hiệu quả.	**Công ty cung cấp dịch vụ**: AWS cung cấp dịch vụ giám sát bảo mật và đánh giá tuân thủ. **Chi phí thực hiện**: Khoảng 2,500 USD/tháng cho các dịch vụ kiểm tra và đánh giá định kỳ, bao gồm giám sát an ninh, phân tích lỗ hổng và hỗ trợ bảo mật từ AWS.	Phòng IT của Công ty ABC phối hợp với AWS, công ty cung cấp dịch vụ đám mây, để thực hiện kiểm tra và đánh giá định kỳ.	Thực hiện định kỳ hàng tháng, bắt đầu từ ngày 01/12/2024.	Đến khi hết thời hạn theo hợp đồng.

• **Bước 3**: Thực hiện đánh giá lại chính sách kiểm soát truy cập và phân quyền mỗi quý, nhằm đảm bảo rằng quyền truy cập của nhân viên được quản lý chặt chẽ và phù hợp với vai trò công việc hiện tại. Đánh giá này giúp giảm thiểu nguy cơ lạm dụng quyền truy cập và đảm bảo dữ liệu nhạy cảm luôn được bảo vệ. • **Bước 4**: Tổ chức các buổi họp định kỳ với nhà cung cấp dịch vụ đám mây để đánh giá các biện pháp bảo mật hiện có và thảo luận các cải tiến cần thiết. Việc phối hợp chặt chẽ với nhà cung cấp giúp đảm bảo rằng hệ thống đám mây của công ty luôn tuân thủ các yêu cầu bảo mật cao nhất và thích ứng nhanh chóng với các mối đe dọa mới.				

(*)Xem Bài tập mẫu có tên (Sample)BaiLamBaiTapCaNhan_Ch.06(RMStrategy).pdf để tìm hiểu cách điền thông tin cho nội dung Kế hoạch thực hiện./.