Trường Đại học Công nghệ Thông tin
GVHD : Nguyễn Văn Thiện
Lớp : NT207.P11.ATCL
MSSV : 21520202
Tên : Hồ Hải Dương

BÀI TẬP VỀ NHÀ

Môn: Quản lý rủi ro và an toàn thông tin trong doanh nghiệp
Chương 3 – Principles (Các nguyên tắc)
Ngày hoàn thành bài tập: 15/11/2024

MỤC LỤC

BÀI LÀM CHI TIẾT

Bài số 1 *(8đ)*

Cho ví dụ minh họa "Mục đích của QLRR là tạo ra giá trị và bảo vệ giá trị" ("The purpose of risk management is the creation and protection of value") [ISO 31000]

1.1/ Tạo giá trị

1.1.1/ Mối đe dọa: Các dữ liệu được lưu trữ trên dịch vụ đám mây. *(0đ)*

1.1.2/ Điểm yếu: Chính sách bảo mật thông tin không bao gồm các yêu cầu bảo mật liên quan đến dịch vụ đám mây mà tổ chức sử dụng. *(2đ)*

1.1.3/ Rủi ro tiềm ẩn: Dữ liệu doanh nghiệp bị rò rỉ hoặc đánh cắp, gây thiệt ại nhiều mặt về tài chính và uy tín. *(2đ)*

1.1.4/ "Công ty HHD" là người tạo giá trị dịch vụ đám mây: 120 triệu VNĐ/năm. Ban lãnh đạo công ty đã quản lý rủi ro về dữ liệu và bảo mật bằng cách đầu tư 120 triệu VNĐ mỗi năm vào dịch vụ đám mây từ AWS (Amazon Web Services) và Azure (Microsoft). Các dịch vụ này cung cấp khả năng lưu trữ an toàn, đồng bộ hóa dữ liệu và truy cập linh hoạt trên toàn cầu. *(2đ)*

1.2/ Bảo vệ giá trị *(2đ)*

Để bảo vệ giá trị 120 triệu VNĐ/năm từ các dịch vụ AWS và Azure, công ty HHD thực hiện các biện pháp sau:

- **1.2.1/** Kích hoạt xác thực đa yếu tố (MFA) cho tất cả tài khoản truy cập, đảm bảo chỉ người được ủy quyền mới có thể truy cập vào hệ thống.
- **1.2.2/** Áp dụng mã hóa dữ liệu từ phía doanh nghiệp trước khi tải lên đám mây, sử dụng các công cụ như AWS Key Management Service (KMS) và Azure Encryption Key Vault.
- **1.2.3/** Sử dụng dịch vụ Amazon GuardDuty và Microsoft Azure Sentinel để giám sát hoạt động đăng nhập và phát hiện các hành vi đáng ngờ.
- **1.2.4/** Định kỳ đánh giá và cập nhật quyền truy cập của nhân viên, chỉ cấp quyền truy cập cần thiết dựa trên vai trò công việc.
- **1.2.5/** Tổ chức các buổi đào tạo hàng quý về an toàn thông tin, đặc biệt tập trung vào nhận diện lừa đảo (phishing) và cách bảo vệ dữ liệu khi sử dụng đám mây, với chi phí 20 triệu VNĐ/năm.

1.3/ Hiệu quả kinh tế

Nhờ đầu tư 120 triệu VNĐ/năm vào AWS và Azure cùng với các biện pháp bảo vệ, công ty HHD đã:

Commented [nvt1]: *>>>Comment có thể bị rút gọn nên em nhớ Click vào khung Comment hoặc vào hình mũi tên đen (hay hình tam giác ở góc phải bên dưới) để đọc hết phần này; em đọc hết góp ý của Thầy là khi em thấy dấu "./."*

Mối đe dọa phải là KẺ TẤN CÔNG MẠNG/TIN TẶC/TỘI PHẠM MẠNG hay hành vi của những kẻ này.
Theo định nghĩa trong ISO27000 thì mối đe dọa hay "Threat" là *"potential cause of an unwanted incident, which can result in harm to a system or organization"*
Theo định nghĩa thì mối đe dọa phải là một ***'cause'*** tức là một nguyên nhân hay động cơ.

Sự cố ('inciden') mà em nêu ra là *'dữ liệu doanh nghiệp bị rò rỉ hoặc đánh cắp...'* thì mối đe dọa chỉ có thể là hành vi của 'KẺ TẤN CÔNG MẠNG/TIN TẶC/TỘI PHẠM MẠNG/kẻ xấu nội bộ/....' nghĩa là mối đe dọa phải là con người thì mới đánh cắp dữ liệu. 'Đánh cắp' là hành động của con người.
Theo môn LTHĐT, Con người là 1 đối tượng nên có thuộc tính ('properties') và cách thức hành động ('methods') đặc trưng khác với các đối tượng khác; trong đó "đánh cắp" hay "ăn cắp" chỉ một phương pháp trong nhiều phương pháp của riêng con người.

Nếu con mèo hay con chó thì người ta không dùng từ "đánh cắp" mặc dù nó có thể làm theo cách thức tương tự. Trước khi "đánh cắp", con người thường có ý tưởng rồi mới quan sát, theo dõi, chọn thời điểm phù hợp rồi ra tay lén lút v.v. Từ ý tưởng đến một loạt các hành vi như vậy thì con thú không hội đủ năng lực như vậy.

Bản thân dữ liệu được lưu trữ trên đám mây không thể mà mối đe dọa ngoại trừ dữ liệu này đã bị nhiễm mã độc hay không còn duy trì tính 'integrity' ban đầu và đang bị tin tặc điều khiển và kiểm soát.

Theo cách chấm điểm áp dụng cho BT Ch.03 Bài 1 mà tất cả bài làm của sinh viên trong lớp bị ảnh hưởng thì EM mất 2 điểm ở đây./.

- Giảm thiểu nguy cơ rò rỉ dữ liệu, tránh thiệt hại tài chính ước tính 1 tỷ VNĐ mỗi năm do vi phạm bảo mật.
- Đảm bảo tính liên tục trong hoạt động kinh doanh, giảm thiểu gián đoạn dịch vụ với tỷ lệ sẵn sàng 99.99% từ AWS và Azure.
- Củng cố niềm tin của khách hàng và đối tác nhờ vào việc bảo vệ dữ liệu an toàn và tuân thủ các tiêu chuẩn bảo mật quốc tế.

Bài số 2 *(8,25đ)*

Cho ví dụ minh họa nội dung CẢI TIẾN LIÊN TỤC trong 2 slides cuối (26 và 27) của giáo trình Chương 3 (QLRRATTT_Principles_Ch.03_v1.pdf)

Ở bài số 2 này em sử dụng ngữ cảnh là: **"Sử dụng các dịch vụ đám mây (AWS hoặc Azure) để phát hiện và quản lý rủi ro an ninh thông tin trong dữ liệu khách hàng"**.

BẢNG PHÂN TÍCH NỘI DUNG CẢI TIẾN LIÊN TỤC		
STT	**BƯỚC**	**NỘI DUNG CHI TIẾT**
1	**Tạo giá trị + Đo lường (Measure)** *(1.5đ+1.5đ)*	Trong việc quản lý rủi ro khi sử dụng dịch vụ đám mây, công ty sử dụng **AWS CloudTrail** và **Azure Security Center** để đo lường các chỉ số quan trọng. Hệ thống này có thể ghi nhận trung bình **100,000 sự kiện mỗi ngày** trên các tài khoản và dịch vụ. Việc giám sát giúp phát hiện các hành vi bất thường, chẳng hạn như **5-10 truy cập trái phép mỗi tháng** và **khoảng 50 sự cố bảo mật nhỏ** mỗi quý.
2	**Phân tích (Analyse)** *(1.5đ)*	Dữ liệu đo lường được phân tích kỹ càng qua **Amazon GuardDuty** và **Azure Sentinel** để nhận diện các mẫu bất thường trong truy cập và thao tác dữ liệu. Chẳng hạn, việc phân tích đã phát hiện các hành vi truy cập từ địa chỉ IP lạ xảy ra trung bình **2 lần mỗi tuần** và các thao tác bất thường vào giờ cao điểm xảy ra khoảng **3 lần/tháng**. Những phân tích này giúp nhận diện các lỗ hổng có thể bị khai thác, từ đó giảm thiểu nguy cơ vi phạm bảo mật dữ liệu.
3	**Quản lý (Manage)** *(1.5đ)*	Sau khi phát hiện lỗ hổng, công ty thực hiện các biện pháp quản lý rủi ro bao gồm mã hóa dữ liệu và kiểm soát truy cập. Sử dụng **AWS Key Management Service (KMS)** và **Azure Key Vault**, toàn bộ dữ liệu quan trọng được mã hóa với chi phí trung bình **20 triệu VNĐ/năm**. Ngoài ra, việc quản lý quyền truy cập và xác thực đa yếu tố (MFA) cho toàn bộ nhân viên đã giúp giảm thiểu đến **90% nguy cơ rò rỉ dữ liệu** do truy cập trái phép.

Commented [nvt2]:
>>>Comment có thể bị rút gọn nên em nhớ Click vào khung Comment hoặc vào hình mũi tên đen (hay hình tam giác ở góc phải bên dưới) để đọc hết phần này; em đọc hết góp ý của Thầy là khi em thấy dấu "./."

Bài làm của Em chưa nêu ra được Rủi ro tiềm ẩn là gì trong bài này.
Ví dụ:
Rủi ro tiềm ẩn là tin tặc có thể tấn công (truy cập trái phép) vào dịch vụ đám mây, xâm phạm dữ liệu và gây tổn hại các thuộc tính C.I.A cho dữ liệu của Công ty. Theo cách chấm điểm BT Ch.03 Bài 2 thì:
Em mất 1 điểm ở đây.

Các phần còn lại thì em đã nhập chung phần Tạo Giá trị vào phần Đo lường, em đã nêu được ý từng phần theo cách hiểu của em **nhưng có thiếu sót ở phần KIỂM SOÁT:**
Phần Tạo giá trị em không ghi rõ ràng thành 1 mục riêng nhưng đọc qua nội dung Đo lường thì có thể nhận ra là em tạo ra 3 giá trị và gộp chung vào mục Đo lường là:
Tạo giá trị:
-ghi nhận số lượng sự kiện mỗi ngày
-ghi nhận số lượng truy cấp trái phép mỗi tháng
-ghi nhận số lượng sự cố bảo mật mỗi quý
(Có thể AWS và Azure tạo ra nhiều giá trị hơn như thế nhưng 3 giá trị này cũng đủ cho bài tập)

Sự không rõ ràng này chỉ nhắc nhở, không trừ điểm.

Dựa trên việc tạo ra 3 giá trị như trên thì để cải tiến liên tục, em mới tiến hành 6 hoạt động có mối liên hệ với nhau là:
1.Đo lường:
...
2.Phân tích
...
3.Quản lý
...
4.Kiểm soát
...
5.Cải thiện
...
./.

4	**Kiểm soát (Control)** *(0.75đ)*	Để kiểm soát các biện pháp quản lý, công ty thiết lập các cảnh báo tự động trên AWS và Azure. Cảnh báo này gửi thông báo ngay khi phát hiện các hành vi xâm nhập bất thường, với chi phí kiểm soát an ninh trung bình **30 triệu VNĐ/năm**. Các hệ thống như Amazon GuardDuty và Azure Sentinel cho phép giám sát **24/7**, giúp ngăn chặn kịp thời các sự cố bảo mật, giảm nguy cơ vi phạm tới **85%** so với các hệ thống không có giám sát.
5	**Cải thiện (Improve)** *(1.5đ)*	Dựa trên dữ liệu từ các bước trên, công ty liên tục cải thiện quy trình quản lý rủi ro với các công nghệ mới nhất. Mỗi năm, công ty dành **50 triệu VNĐ** để nâng cấp các công cụ bảo mật, cập nhật chính sách và đào tạo nhân viên. Những cải tiến này đã giúp công ty giảm thêm **30% nguy cơ bị tấn công** và đảm bảo an toàn dữ liệu theo các tiêu chuẩn bảo mật quốc tế, trong đó có **ISO 27001**.

HẾT./.

Commented [nvt3]:
>>>Comment có thể bị rút gọn nên em nhớ Click vào khung Comment hoặc vào hình mũi tên đen (hay hình tam giác ở góc phải bên dưới) để đọc hết phần này; em đọc hết góp ý của Thầy là khi em thấy dấu "./."

Nội dung 4.KIỂM SOÁT là các hành động kiểm soát hoạt động QUẢN LÝ mà em đã nêu ra *"bao gồm mã hóa dữ liệu và kiểm soát truy cập".*

Em chỉ nêu ra KIỂM SOÁT để phát hiện các hành vi xâm nhập bất thường thông qua các cảnh báo tự động.

Xem lại phần Quản lý em nêu ở trên thì có ghi *"bao gồm mã hóa dữ liệu và kiểm soát truy cập"* nhưng tại đây không thấy em nói gì về kiểm soát *"mã hóa dữ liệu"*
Em mất 0.75 đ ở đây.

Nhắc bài:
Khác với Quản lý thì "Kiểm soát" (Control) có nghĩa là theo dõi hay giám sát một cái gì đó để đảm bảo nó đi đúng hướng, có hành động để đưa cái đó trở lại đúng hướng.

Nói giản dị cho dễ hiểu thì KIỂM SOÁT là quan sát+theo dõi+giám sát+hành động một cách hiệu quả để duy trì hay khởi động một trong 2 trạng thái ('enable/disable'):
- cho phép làm hay không cho làm;
- cho phép chạy hay bắt ngừng lại;
- cho phép nói hay bắt câm miệng lại;
- cho phép sử dụng hay không cho;
- Cho phép "Yes" hoặc bắt phải "No"
- v.v.

Khi viết nội dung về Kiểm soát, em phải hiểu KIỂM SOÁT là như vậy thì mới đạt yêu cầu.

Ví dụ như nếu có Admin nào đó của Azure hay AWS ***lén lút*** cấu hình đám mây bỏ chức năng kiểm soát truy cập hay cấu hình lại khác với yêu cầu của em; thì hành động lén lút này **vừa kết thúc là Em biết ngay và em có thể thực hiện can thiệp để** cho phép hay không cho phép cấu hình lén như vậy.

Hoặc

Ví dụ như em đưa một video của em có cảnh bạo lực, máu me…vào Youtube thì Youtube sẽ cắt bỏ ngay vì em vi phạm quy định của Youtube. Youtube đang kiểm soát nội dung nên ai vi phạm nó biết ngay và: Cho đăng hay không cho đăng là quyền của Youtube

Thế mới gọi là kiểm soát./.