CHƯƠNG 2: Tìm hiểu An toàn bảo mật trong công nghệ đám mây

**2.1. Khái niệm về an ninh thông tin**

An ninh thông tin (Information Security) là một lĩnh vực quan trọng trong công nghệ thông tin và quản lý dữ liệu. Nó liên quan đến bảo vệ thông tin quan trọng và đảm bảo tính bí mật, toàn vẹn, và sẵn sàng của thông tin trước mọi mối đe dọa và rủi ro. Dưới đây là một số khái niệm quan trọng trọng liên quan đến an ninh thông tin:

+Tính bí mật (Confidentiality): Đảm bảo rằng thông tin chỉ được truy cập và sử dụng bởi những người có quyền truy cập. Điều này đòi hỏi sử dụng các biện pháp như mã hóa dữ liệu và quản lý quyền truy cập.

+Tính toàn vẹn (Integrity): Đảm bảo rằng thông tin không bị sửa đổi hoặc biến đổi một cách trái phép. Bất kỳ thay đổi nào cũng phải được theo dõi và kiểm tra.

+Tính sẵn sàng (Availability): Đảm bảo rằng thông tin có sẵn cho người dùng khi cần thiết, và không bị tấn công hoặc gặp sự cố gì đó làm gián đoạn hoạt động thông tin.

+Tính quản lý rủi ro (Risk Management): Đánh giá và quản lý các rủi ro liên quan đến an ninh thông tin, bao gồm việc đề xuất các biện pháp bảo mật để giảm thiểu rủi ro.

+Các biện pháp bảo mật (Security Measures): Đây là các biện pháp và công nghệ được sử dụng để bảo vệ thông tin, bao gồm tường lửa (firewalls), mã hóa dữ liệu, chính sách bảo mật, và giám sát hệ thống.

+Chính sách an ninh thông tin (Information Security Policies): Đây là tập hợp các quy tắc và hướng dẫn mà tổ chức sử dụng để đảm bảo an ninh thông tin, và chúng thường định rõ quyền và trách nhiệm của người dùng trong việc bảo vệ thông tin.

**2.2.Một số tiêu chuẩn về an ninh thông tin**

*2.2.1.Tiêu chuẩn về hệ thống quản lý an ninh*

Bộ Tiêu chuẩn ISO 27001 là hệ thống tiêu chuẩn về hệ thống bảo mật & quản lý an ninh thông tin. Thông tin rất quan trọng của mỗi tổ chức và ISO 27001; đưa ra các phưong pháp đánh giá việc theo dõi; bảo vệ và quản lý hệ thống thông tin, dữ liệu. Việc mất thông tin trong bất cứ trường hợp nào; dù ít hay nhiều cũng gây ra thiệt hại cho tổ chức. Thậm chí có thể khiến tổ chức sụp đổ.

Tiêu chuẩn ISO 27001 là hệ thống tiêu chuẩn của Anh về hệ thống quản lý an ninh thông tin. Tiêu chuẩn ISO 27001 giúp quản lý an ninh thông tin một cách hiệu quả nhất. Thông tin ở đây bao gồm những dữ liệu được lưu lại dưới dạng điện tử; hoặc dữ liệu đã được in ra – dữ liệu mềm và dữ liệu cứng.

Thông qua việc áp dụng ISO 27001. Các tổ chức sẽ xác định được loại thông tin và xác định các mối nguy, rủi ro có thể xảy ra. Sau đó thiết lập hệ thống, thiết lập sự kiểm soát cũng như các quy trình để giảm thiểu các rủi ro đó. ISO 27001 phù hợp với mọi quy mô của tổ chức; các công ty – doanh nghiệp và nó được áp dụng ở mọi lĩnh vực kinh tế khác nhau.

2.2.2.Tiêu chuẩn an ninh thông tin về điện toán đám mây

ISO/IEC 27017 là một tiêu chuẩn quốc tế cung cấp hướng dẫn về an ninh thông tin liên quan đến việc sử dụng dịch vụ điện toán đám mây. Tiêu chuẩn này được phát triển bởi Tổ chức Tiêu chuẩn Hóa Quốc tế (ISO) và Tổ chức Tiêu chuẩn Điện tử Quốc tế (IEC).

Phạm vi ứng dụng: ISO/IEC 27017 tập trung vào việc xác định và thực hiện các biện pháp bảo mật cụ thể cho dịch vụ điện toán đám mây. Nó cung cấp hướng dẫn về việc bảo vệ thông tin và dữ liệu khi sử dụng các dịch vụ cloud hoặc triển khai hệ thống trong môi trường điện toán đám mây. ISO/IEC 27017 không chỉ áp dụng cho các nhà cung cấp dịch vụ điện toán đám mây mà còn cho người dùng dịch vụ này. Nó giúp xác định các trách nhiệm và yêu cầu bảo mật của cả hai bên. Tiêu chuẩn này xác định các yêu cầu cụ thể về an ninh thông tin trong các khía cạnh quan trọng của điện toán đám mây, bao gồm quản lý quyền truy cập, quản lý rủi ro, quản lý quá trình và quản lý dữ liệu. SO/IEC 27017 hỗ trợ việc đánh giá và quản lý rủi ro bảo mật trong môi trường điện toán đám mây. Nó cung cấp các hướng dẫn về việc đánh giá và xử lý rủi ro liên quan đến việc sử dụng dịch vụ điện toán đám mây. ISO/IEC 27017 giúp cung cấp một khung làm việc cụ thể cho an ninh thông tin trong môi trường điện toán đám mây và giúp tổ chức và nhà cung cấp dịch vụ cloud đảm bảo rằng thông tin và dữ liệu của họ được bảo vệ một cách tốt nhất trong môi trường này.

2.2.3.Tiêu chuẩn an ninh thông tin về dữ liệu

ISO/IEC 27001 là tiêu chuẩn quốc tế về quản lý an ninh thông tin, và nó áp dụng cho việc bảo vệ dữ liệu cũng như hệ thống thông tin liên quan.Tiêu chuẩn này tập trung vào việc thiết lập, triển khai, duy trì và cải thiện hệ thống quản lý an ninh thông tin (ISMS) trong một tổ chức. Nó không chỉ liên quan đến công nghệ thông tin mà còn áp dụng cho tất cả các khía cạnh của tổ chức, bao gồm quản lý quy trình, nguồn nhân lực, và quản lý rủi ro. ISO/IEC 27001 đặt ra các yêu cầu cơ bản cho việc quản lý an ninh thông tin, bao gồm việc xác định rủi ro, thiết lập các biện pháp kiểm soát bảo mật, và xây dựng một quy trình liên tục để cải thiện an ninh thông tin. Tuân thủ ISO/IEC 27001 không bắt buộc, nhưng nó cung cấp một cơ cấu và hướng dẫn cho việc triển khai an ninh thông tin trong tổ chức. Nếu một tổ chức muốn chứng minh tuân thủ tiêu chuẩn này, nó có thể đăng ký cho việc chứng nhận bởi một cơ quan chứng nhận độc lập.

2.3.Phân loại về an ninh thông tin trong điện toán dám mây

2.3.1.Theo các nhóm vấn đề

+Bảo mật Dữ liệu:

Bảo vệ dữ liệu: Đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của dữ liệu trong khi lưu trữ, truyền tải và xử lý trên môi trường đám mây.

Mã hóa dữ liệu: Sử dụng mã hóa để bảo vệ dữ liệu khi nó đang được truyền hoặc lưu trữ trong điện toán đám mây.

+Quản lý Rủi ro:

Đánh giá rủi ro: Xác định và đánh giá các rủi ro tiềm ẩn cho an ninh thông tin trong môi trường điện toán đám mây.

Quản lý rủi ro: Phát triển và triển khai biện pháp để giảm thiểu hoặc quản lý các rủi ro đã được xác định.

+Quản lý Truy cập:

Quản lý quyền truy cập: Đảm bảo rằng chỉ những người có quyền mới có thể truy cập dữ liệu và tài nguyên trong điện toán đám mây.

Xác thực và ủy quyền: Xác định người dùng và cung cấp quyền truy cập dựa trên vai trò và chính sách quản lý.

Bảo mật Hệ thống:

Bảo mật mạng: Đảm bảo mạng và kết nối mạng được bảo vệ khỏi các mối đe dọa mạng.

Bảo mật ứng dụng: Đảm bảo tính bảo mật của ứng dụng và dịch vụ đám mây.

Tuân thủ Quy định:

Tuân thủ pháp luật: Đảm bảo rằng tổ chức tuân thủ các quy định về quyền riêng tư và bảo mật dữ liệu, như GDPR, HIPAA, hoặc các quy định khác liên quan đến lĩnh vực của họ.

+Quản lý Khẩn cấp và Sự cố:

Quản lý khẩn cấp: Xác định và lập kế hoạch cho các biện pháp khẩn cấp và phục hồi dự phòng trong trường hợp sự cố.

Phản ứng sự cố: Đáp ứng và ứng phó với các sự cố bảo mật và xác minh vụ việc bất thường.

Bảo mật Vật lý:

Bảo mật trung tâm dữ liệu: Đảm bảo tính bảo mật của trung tâm dữ liệu và cơ sở hạ tầng vật lý.

Quản lý thiết bị và tài sản: Đảm bảo bảo mật thiết bị và tài sản vật lý liên quan đến hệ thống đám mây.

+Giám sát và Kiểm tra:

Giám sát hệ thống: Theo dõi hoạt động của hệ thống để phát hiện và phản ứng sớm đối với các hoạt động không bình thường.

Kiểm tra bảo mật: Thực hiện

2.3.1.Các nguy cơ hàng đầu về an ninh

+Nguy cơ về Bảo mật Dữ liệu:

Rò rỉ dữ liệu: Nguy cơ dữ liệu nhạy cảm bị rò rỉ hoặc truy cập trái phép.

Mất mát dữ liệu: Rủi ro mất mát dữ liệu quan trọng do sự cố hệ thống hoặc hành vi người dùng sai lầm.

+Nguy cơ về Quản lý Rủi ro:

Rủi ro không được đánh giá đúng cách: Sự thiếu sót trong việc xác định và đánh giá các rủi ro tiềm ẩn.

Rủi ro không được quản lý: Không có biện pháp cụ thể để giảm thiểu hoặc quản lý các rủi ro đã xác định.

+Nguy cơ về Quản lý Truy cập:

Truy cập trái phép: Nguy cơ người dùng không được ủy quyền truy cập dữ liệu hoặc tài nguyên.

Mã hóa yếu: Sự thiếu sót trong việc triển khai mã hóa dữ liệu hoặc quá trình xác thực.

Nguy cơ về Bảo mật Hệ thống:

Tấn công Mạng: Rủi ro về các cuộc tấn công mạng, bao gồm tấn công từ phía ngoài và từ bên trong.

Lỗ hổng ứng dụng: Các lỗ hổng trong phần mềm và ứng dụng có thể bị tận dụng bởi tin tặc.

Nguy cơ về Tuân thủ Quy định:

Sự thiếu sót trong Tuân thủ: Không tuân thủ các quy định và quy tắc bảo mật và quyền riêng tư liên quan đến lĩnh vực hoạt động của tổ chức.

Khiếu nại và Trách nhiệm pháp lý: Nguy cơ xuất phát từ việc không đáp ứng yêu cầu pháp lý hoặc khiếu nại từ người dùng.

+Nguy cơ về Quản lý Khẩn cấp và Sự cố:

Sự cố không được phản ứng kịp thời: Không có kế hoạch hoặc khả năng phản ứng nhanh chóng trong trường hợp sự cố bảo mật.

Thất bại khôi phục: Không khôi phục dữ liệu hoặc dịch vụ sau sự cố.

+Nguy cơ về Bảo mật Vật lý:

Truy cập trái phép vào trung tâm dữ liệu: Rủi ro truy cập trái phép vào trung tâm dữ liệu hoặc cơ sở hạ tầng vật lý.

Mất mát hoặc hỏng thiết bị: Sự mất mát hoặc hỏng thiết bị vật lý quan trọng.

Nguy cơ về Giám sát và Kiểm tra:

Không theo dõi các hoạt động đáng ngờ: Không phát hiện được các hoạt động không bình thường trong hệ thống.

Không kiểm tra bảo mật định kỳ: Không thực hiện kiểm tra bảo mật định kỳ để xác định và khắc phục các lỗ hổng.

2.4.An ninh dữ liệu trong điện toán đám mây

2.4.1. Một số vấn đề về bảo vệ dữ liệu trong điện toán đám mây

-Bảo mật ứng dụng trong SaaS

Người sử dụng thường truy nhập các ứng dụng đám mây thông qua trình duyệt web. Sai sót trong các trang web có thể tạo nên những lỗ hồng của dịch vụ . Tin tặc từ đó có thể gây thương tổn tới các máy tính của người sử dụng để thực hiện các hành vi ác ý hoặc ăn trộm các thông tin nhạy cảm

-Nhiều người thuê đồng thời

Trong mô hình này, một thể hiện duy nhất của ứng dụng được chia sẻ cho nhiều người thuê. Khi đó tài nguyên sẽ được sử dụng hiệu quả. Trong mô hình này, do dữ liệu của các người dùng được lưu trữ trên cùng một cơ sở dữ liệu nên nguy cơ về rò rỉ dữ liệu có thể xảy ra.

- Bảo mật dữ liệu

Trong SaaS, dữ liệu thường được xử lý dưới dạng bản rõ và được lưu trữ trên đảm máy. Nhà cung cấp dịch vụ Sau SaaS phải chịu trách nhiệm về bảo mật dữ liệu trong khi chúng được xử lý và lưu trữ. Việc sao lưu dữ liệu rất phổ biến trong các hệ thống đảm mây cũng tạo nên những vấn đề phát sinh cho bảo mật dữ liệu, nhất là khi nhà cung cấp dịch vụ ký hợp đồng sao lưu lại với một đối tác thứ ba không đáng tin cậy.

-Truy cập dịch vụ

Việc các dịch vụ SaaS hỗ trợ khả năng truy cập thông qua trình duyệt mang lại nhiều thuận lợi, ví dụ như chúng có thể dễ dàng được truy cập từ các thiết bị kết nối mạng khác PC như điện thoại hay máy tính bảng. Tuy nhiên, điều này lại tạo nên những nguy cơ mới về ATBM như các phần mềm ăn trộm dữ liệu trên di động, mạng Wifi không an toàn, kho dụng không an toàn, ...

- Vòng đời của ứng dụng

Việc nâng cấp ứng dụng đòi hỏi nhà cung cấp dịch vụ Paas phải hỗ trợ tốt cho những thay đổi của ứng dụng. Đồng thời, Người phát triển cũng cần phải lưu ý rằng sự thay đổi của các thành phần ứng dụng trong quá trình nâng cấp đôi khi gây ra các vấn đề về ATBM

-Ảo hóa

Công nghệ ảo hóa cho phép người sử dụng dễ dàng tạo lập, sao chép, chia sẻ, di trú và phục hồi các máy áo trên đó thiện thì các ứng dụng. Công nghệ này tạo nên một tầng phần mềm mới trong kiến trúc phần mềm của hệ thống. Chính vì vậy nó cũng mang đến những nguy cơ mới về ATBM

-Giám sát máy ảo

Thành phần giám sát máy ảo (virtual machme monitor - VMM) hay còn gọi là supervisor có trách nhiệm giảm sát và quản lý các máy ảo được tạo trên máy vật lý. Chính vì vậy, nếu VMM bị tổn thương, các máy ảo do nó quản lý cũng có thể bị tổn thương. Di trú máy ảo từ một VMM này sang một VMM khác cũng tạo nên những nguy cơ mới về ATBN

- Tài nguyên chia sẻ

Các máy ảo trên cùng một hệ thống chia sẻ một số tài nguyên chung như CPU, RAM, thiết bị vào ra,... Việc chia sẻ này có thể làm giảm tính ATBM của mỗi máy ảo. Ví dụ, một máy ảo có thể đánh cắp thông tin của máy ảo khác thông qua bộ nhớ chia sẻ. Hơn nữa nếu khai thác một số kênh giao tiếp ngầm giữa các máy ảo, các máy ảo có thể bỏ qua mọi quy tắc bảo bảo mật của VMM

- Kho ảnh máy ảo công cộng

Trong môi trường IadS, ảnh máy ảo là một mẫu sẵn có để tạo nên các máy ảo. Một hệ thống đám mây có thể cung cấp một số ảnh máy ảo trong một kho công cộng để người dùng có thể dễ dàng tạo nên máy ảo theo nhu cầu của mình. Đôi khi hệ thống đám mây có thể cho phép người sử dụng tự tải ảnh máy ảo của mình lên kho công công này. Điều này tạo nên một nguy cơ về bảo mật khi tin tặc tải lên những ảnh máy ảo có chứa mã độc và người sử dụng có thể dùng những ảnh này để tạo máy ảo của họ.