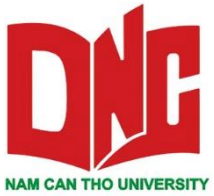
BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC NAM CẦN THƠ



ĐIỆN TOÁN ĐÁM MÂY

Chương 4:

AN TOÀN VÀ BẢO MẬT

Giảng viên: Nguyễn Trung Kiên

Các vấn đề về an toàn và bảo mật trong điện toán đám mây

- An toàn và bảo mật (ATBM) là yêu cầu tối quan trọng trong hệ thống đám mây do tính chất phân tán và trực tuyến.
- ATBM là mối lo ngại hàng đầu của các tổ chức khi chuyển dịch sang sử dụng dịch vụ đám mây (khảo sát của IDC năm 2009).

Các tầng dịch vụ trong điện toán đám mây và Những vấn đề ATBM

SaaS (Software as a Service)

- Đặc điểm: dịch vụ phần mềm được cung cấp qua đám mây, nhà cung cấp chịu trách nhiệm quản lý và bảo mật ứng dụng.
- Rủi ro bảo mật:
  - Lỗ hổng ứng dụng: các lỗ hổng bảo mật trong ứng dụng web có thể bị khai thác từ xa.
  - Quyền riêng tư dữ liệu: dữ liệu nhạy cảm có nguy cơ bị truy cập trái phép.

Các tầng dịch vụ trong điện toán đám mây và Những vấn đề ATBM (tt)

PaaS (Platform as a Service)

- Đặc điểm: cung cấp nền tảng phát triển, triển khai ứng dụng mà không cần quan tâm đến cơ sở hạ tầng bên dưới.
- Rủi ro bảo mật:
  - Dịch vụ tích hợp: sử dụng các dịch vụ từ bên thứ ba có thể dẫn đến các rủi ro về bảo mật.
  - Cập nhật và vá lỗi: các bản cập nhật phần mềm có thể vô tình tạo ra các lỗ hổng mới.

Các tầng dịch vụ trong điện toán đám mây và Những vấn đề ATBM (tt)

IaaS (Infrastructure as a Service)

- Đặc điểm: cung cấp tài nguyên hạ tầng như máy chủ ảo, mạng, lưu trữ.
- Rủi ro bảo mật:
  - Ảo hóa: tạo ra một lớp phức tạp trong quản lý bảo mật.
  - Chia sẻ tài nguyên: các máy ảo khác nhau chia sẻ cùng một hạ tầng vật lý, có thể dẫn đến rò rỉ dữ liệu giữa các máy ảo.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây

- Giao diện người sử dụng và API được cung cấp không an toàn
  - Phần lớn các nhà cung cấp dịch vụ đám mây sử dụng các giao diện HTTP, SOAP hoặc REST để cung cấp dịch vụ của mình.
  - Vấn đề bảo mật:
    - Chứng nhận sử dụng hợp lệ yếu
    - Việc kiểm tra các quyền không đủ
    - Thiếu kiểm tra tính hợp lệ của dữ liệu

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Tài nguyên phân bổ không giới hạn
  - Hệ thống có thể gặp phải tình huống dành sẵn quá nhiều tài nguyên nếu như việc đánh giá về tài nguyên sử dụng không chính xác.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Các lỗ hổng liên quan đến dữ liệu
  - Khả năng phân tách yếu cho những dữ liệu có nguồn gốc khác nhau (chẳng hạn như của đối thủ cạnh tranh hoặc của tin tặc) dẫn đến dễ bị đánh cắp.
  - Dữ liệu không được xóa hoàn toàn.
  - Dữ liệu được sao lưu bởi một bên thứ ba không tin cậy.
  - Người sử dụng thường không biết vị trí lưu trữ lữ liệu.
  - Dữ liệu thường được lưu trữ, lưu chuyển và xử lý dạng bản rõ (plain text).

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Lỗ hổng trong máy ảo
  - Tồn tại những kênh giao tiếp không tường minh.
  - Cấp phát và giải phóng tài nguyên không hạn chế trong máy ảo.
  - Di chuyển không được kiểm soát.
  - Không kiểm soát các snapshot có thể dẫn đến rò rỉ dữ liệu.
  - Các máy ảo có IP để giám sát, do đó tin tặc có thể định vị được máy ảo cần tấn công.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Lỗ hổng trong ảnh máy ảo (VM image)
  - Ảnh máy ảo được đặt trên kho lưu trữ công cộng.
  - Ảnh máy ảo không thể được vá lỗi.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Lỗ hổng trong Hypervisor
  - Khả năng cấu hình linh động của hypervisor có thể khiến chúng bị khai tác.

Một số lỗ hổng về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Lỗ hổng trong mạng ảo
  - Lỗ hổng khi chia sẻ các cầu nối ảo giữa các máy ảo.

Những nguy cơ về an toàn và bảo mật trong các hệ thống đám mây

- Rò rỉ dữ liệu: dữ liệu của người dùng bị rò rỉ ra ngoài một cách không mong muốn.
- Mất mát dữ liệu: xảy ra khi dữ liệu bị phá hủy hoặc không thể truy cập được.
- Bị đánh cắp tài khoản hoặc thất thoát dịch vụ: hiện tượng người sử dụng bị đánh cắp tài khoản hoặc mất quyền truy cập vào dịch vụ là phổ biến trong môi trường đám mây.
- Giao diện và API không an toàn: các nhà cung cấp dịch vụ đám mây thường cung cấp các API để khách hàng quản lý và tương tác với dịch vụ. Khi các lỗ hổng trong API bị khai thác, tính an toàn của toàn bộ hệ thống sẽ bị đe dọa.

Những nguy cơ về an toàn và bảo mật trong các hệ thống đám mây (tt)

- Tấn công từ chối dịch vụ: DoS là cách thức hạn chế khả năng truy cập vào dữ liệu và ứng dụng của người sử dụng dịch vụ.
- Nguy cơ từ bên trong: nguy cơ đến từ các cá nhân có ác ý trong tổ chức cung cấp dịch vụ, như quản trị viên hệ thống đám mây.
- Sự lạm dụng dịch vụ đám mây: tin tặc có thể thuê một lượng lớn tài nguyên đám mây để thực hiện các hoạt động xấu như giải mã dữ liệu, tấn công DDoS, hoặc phát tán mã độc.
- Khảo sát không đầy đủ: nhiều doanh nghiệp chuyển sang sử dụng dịch vụ đám mây mà không đánh giá đầy đủ các rủi ro.
- Lỗ hổng trong các công nghệ sử dụng chung: hệ thống đám mây thường chia sẻ hạ tầng, nền tảng và ứng dụng; nhưng một số thành phần như bộ đệm CPU, GPU không được thiết kế cho việc chia sẻ.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây

Giai đoạn	Hoạt động
Lập kế hoạch	Phân loại tài nguyên thông tin Chọn cơ chế kiểm soát an toàn và bảo mật Đánh giá rủi ro
Triển khai	Cài đặt cơ chế kiểm soát
Đánh giá	Đánh giá Xem xét định kỳ

Quy trình quản lý rủi ro về an toàn và bảo mật

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

- **Bước 1 - Lập kế hoạch:** nhận định những nguy cơ về an toàn và bảo mật; xác định các cơ chế kiểm soát an toàn và bảo mật hiệu quả nhằm giải quyết các nguy cơ; lên kế hoạch cho việc thực hiện các cơ chế kiểm soát an toàn và bảo mật.
- **Bước 2 - Triển khai:** bao gồm việc cài đặt và cấu hình cho các cơ chế kiểm soát an toàn và bảo mật.
- **Bước 3 - Đánh giá:** đánh giá tính hiệu quả của của các cơ chế kiểm soát và định kỳ xem xét tính đầy đủ của cơ chế kiểm soát.
- **Bước 4 - Duy trì:** khi hệ thống và các cơ chế kiểm soát đã vận hành, cần thường xuyên cập nhật những thông tin mới về các nguy cơ ATBM.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật trung tâm dữ liệu

Bao gồm cả bảo mật vật lý và quản lý các thành phần phần mềm.

- Bảo mật mức vật lý:
  - Đặt trung tâm dữ liệu ở những cơ sở khó nhận biết với bảo vệ chặt chẽ.
  - Nhân viên phải trải qua xác thực hai bước và khách tham quan phải được hộ tống.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật trung tâm dữ liệu (tt)

- Bảo mật dữ liệu:
  - Kiểm soát truy cập dữ liệu thông qua danh sách kiểm soát truy nhập (ACL).
  - Mã hóa dữ liệu trước khi truyền tải và lưu trữ để đảm bảo an toàn.
- Phòng chống xâm nhập và thảm họa tự nhiên:
  - Phát hiện và ngăn chặn sự thâm nhập trái phép vào trung tâm dữ liệu.
  - Bảo vệ trung tâm dữ liệu khỏi các thảm họa tự nhiên như động đất, lũ lụt.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật trung tâm dữ liệu (tt)

- Quản lý định danh và truy cập:
  - Quản lý định danh là chìa khóa để đảm bảo an toàn cho hệ thống.
  - Cần có cơ chế kiểm soát để đảm bảo tính bí mật và toàn vẹn của thông tin định danh.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Chứng nhận SAS 70

- Phần lớn các đám mây công cộng đều cần chứng nhận này.
- Chứng nhận này không phải là một danh mục để kiểm tra tại một thời điểm. Nó yêu cầu các tiêu chuẩn phải được duy trì trong ít nhất 6 tháng kể từ khi bắt đầu đăng ký.
- Chi phí để đạt được chứng nhận này rất lớn.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập

- Xác nhận bằng hóa đơn thanh toán:
  - Nhiều dịch vụ thương mại điện tử sử dụng hóa đơn thanh toán cho mục đích xác thực với người dùng.
  - Ở môi trường trực tuyến, hóa đơn thanh toán thường gắn liền với thẻ tín dụng của khách hàng. Tuy nhiên, thẻ tín dụng thì thường không có nhiều thông tin gắn với khách hàng nên một số biện pháp khác có thể được áp dụng.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập (tt)

- Kiểm tra định danh qua điện thoại:
  - Phải xác định đúng đối tượng truy cập.
  - Để tránh rủi ro trong việc xác nhận, một hình thức xác nhận qua các kênh liên lạc khác như điện thoại là cần thiết. Thông thường nhà cung cấp sẽ liên hệ với khách hàng và yêu cầu khách hàng trả lời số PIN được hiển thị trên trình duyệt.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập (tt)

- Giấy phép truy nhập:
  - Hình thức giấy phép truy nhập đơn giản nhất chính là mật khẩu. Khách hàng có thể lựa chọn một mật khẩu mạnh, hoặc có thể lựa chọn những giấy phép truy nhập nhiều bước như RSA SecurID.
  - Người sử dụng cần dùng giấy phép truy nhập khi họ muốn sử dụng dịch vụ trực tiếp. Trong trường hợp người sử dụng dịch vụ qua API, cần phải có khóa truy nhập.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập (tt)

- Khóa truy nhập:
  - Để gọi bất kỳ API nào của hệ thống đám mây, người sử dụng phải có một khóa truy nhập. Khóa này được cung cấp cho người sử dụng trong quá trình thiết lập tài khoản.
  - Người sử dụng cần bảo vệ khóa truy nhập này để tránh sự rò rỉ dịch vụ.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập (tt)

- Giấy phép X.509:
  - Dựa trên ý tưởng về hạ tầng khóa công khai (PKI). Một giấy phép X.509 bao gồm một giấy phép (chứa khóa công khai và nội dung cấp phép) và một khóa bí mật.
  - Giấy phép được sử dụng mỗi khi sử dụng dịch vụ, trong đó khóa bí mật được sử dụng để sinh ra chữ ký số cho mỗi yêu cầu dịch vụ. Khóa này cần phải được giữ kín và không được phép chia sẻ.
  - Khi yêu cầu dịch vụ, người sử dụng sinh chữ ký số bằng khóa bí mật của mình, sau đó gắn chữ ký số, giấy phép với yêu cầu dịch vụ. Khi hệ thống nhận được yêu cầu, nó sẽ sử dụng khóa công khai trong giấy phép để giải mã chữ ký số và chứng thực người dùng. Hệ thống cũng sử dụng giấy phép để xác nhận các yêu cầu là hợp lệ.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Các biện pháp kiểm soát truy cập (tt)

- Cặp khóa:
  - Là yếu tố quan trọng nhất trong việc truy nhập vào các thể hiện của AWS.
  - Mỗi dịch vụ cần một cặp khóa riêng biệt. Cặp khóa cho phép hệ thống đảm bảo người dùng hợp lệ.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật dữ liệu và mạng

- Bảo mật hệ điều hành
  - Bảo mật cho hệ điều hành của máy chủ vật lý.
  - Bảo mật cho hệ điều hành của các máy ảo chạy trên nó.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật dữ liệu và mạng (tt)

- Bảo mật môi trường cộng sinh
  - Là các biện pháp và chiến lược bảo mật được thiết kế để bảo vệ một môi trường mà nhiều hệ thống hoặc máy chủ cùng tồn tại và chia sẻ tài nguyên. Môi trường này thường bao gồm các máy ảo, dịch vụ và ứng dụng chạy trên nền tảng đám mây, nơi mà sự tách biệt và bảo mật giữa các thực thể là vô cùng quan trọng để đảm bảo an toàn.
  - Các yếu tố bảo mật chính: cách ly giữa các thực thể, quản lý truy cập, mã hóa, giám sát và phát hiện xâm nhập, tuân thủ và tiêu chuẩn hóa.

Một số phương pháp đảm bảo an toàn cho dịch vụ đám mây (tt)

Bảo mật dữ liệu và mạng (tt)

- Bảo mật lưu trữ dữ liệu
  - Kiểm soát quyền truy nhập dữ liệu thông qua một danh sách kiểm soát truy nhập (ACL - access control list). Với ACL, người sử dụng có toàn quyền kiểm soát tới những đối tượng được phép sử dụng dịch vụ của họ.
  - Một vấn đề bảo mật khác là dữ liệu có thể bị đánh cắp trong quá trình truyền giữa máy của người sử dụng dịch vụ và đám mây. Khi đó các API được bảo vệ bởi SSL sẽ là giải pháp cần thiết.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật

Thiết kế kiến trúc là bước quan trọng trong quy trình xây dựng một hệ thống phức tạp. Mục tiêu chính là xác định được một (hoặc nhiều) cấu trúc tổng thể của hệ thống với những thành phần và mối quan hệ giữa chúng.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây

- Yêu cầu bảo mật mức vật lý
  - Phát hiện và phòng chống sự thâm nhập trái phép vào trung tâm dữ liệu, các thiết bị phần cứng.
  - Bảo vệ hệ thống khỏi các thảm họa tự nhiên như động đất, lũ lụt.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống
  - Quản lý định danh:
    - Đảm bảo bí mật, toàn vẹn và sẵn sàng của thông tin định danh.
    - Chứng thực người dùng (thường với tải yêu cầu cao).
  - Quản lý truy cập:
    - Chứng thực nhiều bước cho các thao tác yêu cầu mức ưu tiên cao.
    - Thiết lập danh sách trắng (white list IP) cho quản trị viên.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống (tt)
  - Quản lý khóa:
    - Kiểm soát và giới hạn truy cập vào khóa mã hóa.
    - Đảm bảo việc hủy bỏ khóa có hiệu lực ngay lập tức trên các trung tâm dữ liệu.
  - Ghi nhận sự kiện và thống kê:
    - Ghi nhận sự kiện: tự động ghi lại các sự kiện quan trọng trong hệ thống. Lưu trữ nhật ký hệ thống cho các hoạt động kiểm tra và giám sát.
    - Thống kê: phân tích dữ liệu từ các sự kiện để phát hiện xu hướng bất thường. Báo cáo tình trạng bảo mật định kỳ.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống (tt)
  - Giám sát bảo mật:
    - Khai thác các thông tin ghi nhận (logs), thông tin giám sát mạng hay thông tin bảo mật từ hệ thống giám sát vật lý.
    - Một số chức năng chính: cảnh báo sự cố bảo mật dựa trên phân tích tự động các thông tin thu thập được. Gửi cảnh báo bằng nhiều phương tiện như email, SMS. Cho phép khách hàng có thể tự xây dựng cơ chế cảnh báo khi sử dụng PaaS hoặc IaaS.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống (tt)
  - Quản lý sự cố:
    - Có quy trình đầy đủ cho việc phát hiện, ghi nhận và xử lý sự cố.
    - Có các cơ chế hỗ trợ người sử dụng thông báo về sự cố.
    - Việc kiểm tra sự cố cần được thực hiện thường xuyên.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống (tt)
  - Kiểm soát mạng và hệ thống:
    - Áp dụng cho cả các hạ tầng vật lý và hạ tầng ảo.
    - Đảm bảo khả năng cô lập, khả năng cấu hình và tính bảo mật cho các thành phần bảo mật.
    - Đảm bảo khả năng cô lập về mạng cho các vùng chức năng của hệ thống đám mây.
    - Phân tách truy nhập thiết bị vật lý với thiết bị ảo.
    - Phân tách vùng thiết bị ảo của các khách hàng khác nhau.
    - Đảm bảo tính nhất quán của máy ảo, hệ điều hành,... cho ứng dụng của khách hàng.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Những yêu cầu an toàn và bảo mật cho kiến trúc đám mây (tt)

- Yêu cầu bảo mật với các thành phần hệ thống (tt)
  - Quản lý cấu hình:
    - Việc duy trì một danh sách thông tin về các tài nguyên của hệ thống và cấu hình của chúng là cần thiết.
    - Sử dụng một hệ thống cơ sở dữ liệu cấu hình CMDB.
    - Phân loại các tài nguyên theo chức năng, tính nhạy cảm, độ quan trọng,…

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Các yếu tố kiến trúc và mẫu bảo mật

- Phòng ngự chiều sâu (defence in-depth)
  - Sử dụng nhiều tầng kiểm soát bảo mật để tạo nên một giải pháp đầy đủ, hoàn chỉnh.
  - Trên quan điểm kiến trúc, có thể được xem như một mẫu thiết kế hiệu quả cho vấn đề bảo mật. Ứng dụng của mẫu này có thể thấy ở nhiều hệ thống thực tiễn.
  - Ví dụ: phòng ngự chiều sâu cho phân hệ kiểm soát truy nhập bao gồm nhiều lớp: lớp 1 - mạng riêng ảo (VPN); lớp 2 - bộ định tuyến cổng vào với cơ chế lọc IP; lớp 3 - token bảo mật.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Các yếu tố kiến trúc và mẫu bảo mật (tt)

- Hũ mật ong (honeypots)
  - Tạo nên một hệ thống không tồn tại hoặc không có giá trị, nhằm thu hút sự tấn công. Khi đã thu hút thành công, “hũ mật ong” lại được sử dụng để quan sát, phân tích và cảnh báo.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Các yếu tố kiến trúc và mẫu bảo mật (tt)

- Hộp cát (sandbox)
  - Là một lớp trừu tượng nằm giữa phần mềm với hệ điều hành, nhằm tạo môi trường độc lập cho việc thực thi ứng dụng.
  - Hệ thống có thêm một tầng bảo vệ theo mô hình phòng ngự chiều sâu.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Các yếu tố kiến trúc và mẫu bảo mật (tt)

- Cô lập máy ảo
  - Hạ tầng chuyển mạch trong một hệ thống đám mây không thể cô lập được các gói tin truyền thông giữa các máy ảo nằm trên cùng một môi trường phần cứng. Nếu các gói tin không được mã hóa, máy ảo có thể theo dõi, quan sát các gói tin gửi đến/gửi đi từ máy ảo khác trong cùng một mạng.
  - Cô lập máy ảo là kỹ thuật:
    - Ứng dụng công nghệ ảo hóa để cô lập các máy ảo trong cùng một mạng vật lý
    - Mã hóa các gói tin gửi đến/gửi đi từ máy ảo
    - Kiểm soát truy cập đến máy ảo, đặc biệt là các cổng dịch vụ
    - Lọc gói tin đến máy ảo qua các cơ chế tường lửa

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

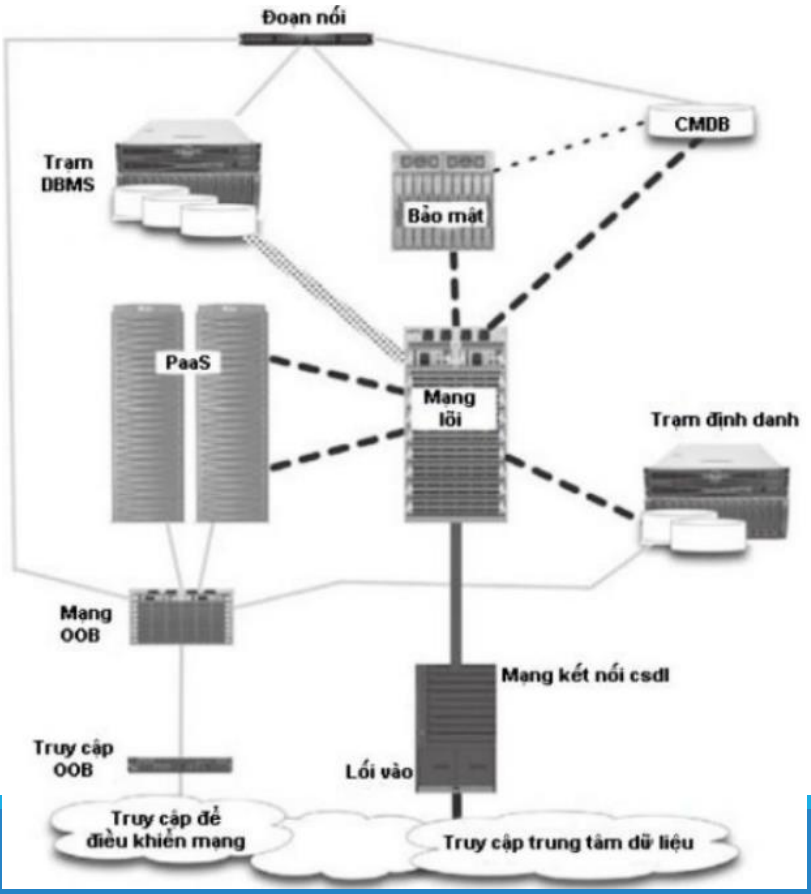
Các yếu tố kiến trúc và mẫu bảo mật (tt)

- Tạo dư thừa (redundant) và đảm bảo tính sẵn sàng (availability)
  - Tạo dư thừa cho những thành phần hệ thống, bao gồm máy chủ, thiết bị mạng,… Tùy thuộc vào mức độ đảm bảo tính sẵn sàng mà kiến trúc có thể thiết lập dư thừa tương ứng.
  - Hệ quả: tăng chi phí, tăng độ phức tạp của hệ thống.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Một số kiến trúc đám mây điển hình đáp ứng yêu cầu an toàn và bảo mật

- Kiến trúc một hệ thống đám mây cung cấp các dịch vụ PaaS

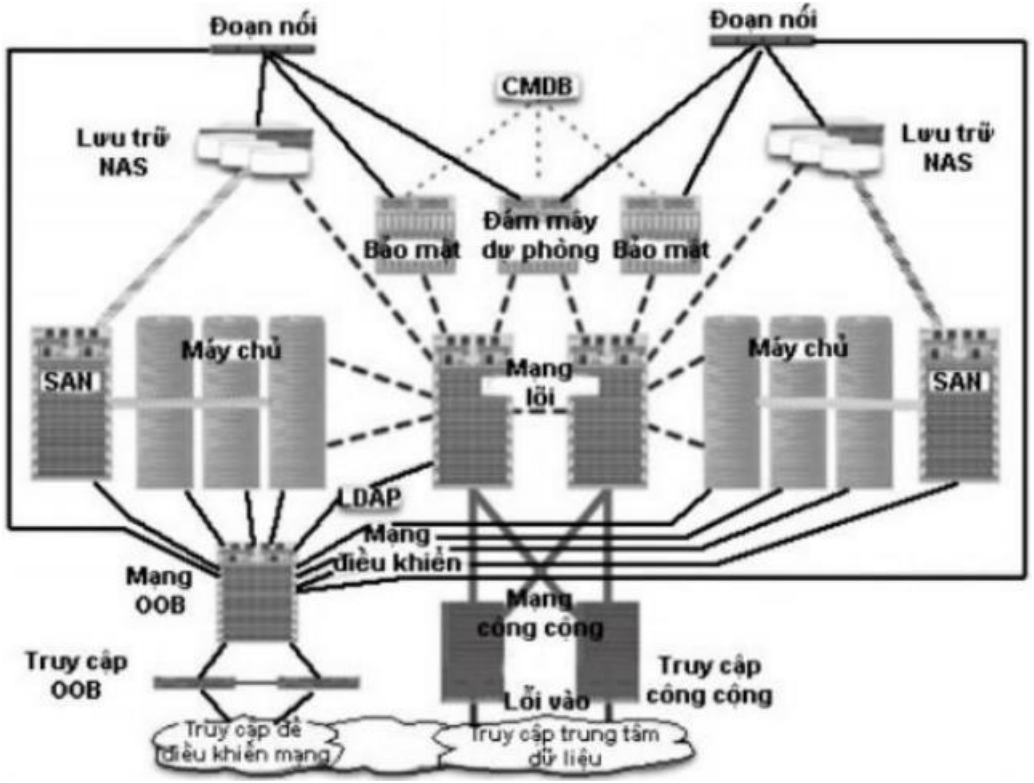


- Người sử dụng truy nhập dịch vụ của hệ thống thông qua mạng công cộng. Hệ thống cũng cung cấp một mạng riêng biệt - mạng OOB (out-of-band) nhằm phục vụ công tác quản trị. Việc kiểm soát truy nhập vào mạng OOB có thể được thực hiện thông qua một whitelist IP - IP của các quản trị viên hệ thống. Thêm vào đó, quản trị viên cần thực hiện xác thực mỗi khi thao tác. Cơ chế xác thực hai bước (token và PIN) có thể giúp hệ thống trở nên an toàn.
- Đây cũng là ví dụ về việc áp dụng cơ chế phòng ngự chiều sâu:
  - Mạng OOB: sử dụng để quản trị các thành phần khác trong hệ thống.
  - Mạng lõi: sử dụng để cung cấp dịch vụ.
  - Mạng kết nối với cơ sở dữ liệu: bao gồm nhiều kết nối đảm bảo tính sẵn sàng.

Thiết kế kiến trúc hệ thống đám mây nhằm đảm bảo an toàn bảo mật (tt)

Một số kiến trúc đám mây điển hình đáp ứng yêu cầu an toàn và bảo mật (tt)

- Kiến trúc đám mây cung cấp dịch vụ tính toán và lưu trữ



- Hệ thống cung cấp một số lượng lớn tài nguyên tính toán được ảo hóa trên các máy chủ, cũng như các kho lưu trữ trên các thiết bị SAN.
- Hỗ trợ tính sẵn sàng cao thông qua việc tạo lập dư thừa cho mạng kết nối công cộng và mạng OOB. Để đảm bảo tính sẵn sàng cho việc truy nhập vào kho lưu trữ SAN, mạng SAN được thiết lập với các kết nối giữa kho lưu trữ SAN và các máy chủ tính toán. Bản thân các máy chủ và kho lưu trữ SAN cũng được thiết kế dư thừa.
- Với các tài nguyên tính toán, để đảm bảo khả năng đáp ứng tốt cho dịch vụ, hệ thống có những thiết kế cho việc dành sẵn tài nguyên (provision). Các máy chủ phục vụ cho việc này được thiết kế độc lập. Việc dành sẵn tài nguyên này cũng đòi hỏi sự kiểm soát và quản lý của một phân hệ quản lý cấu hình tài nguyên CMDB.
- Hai phân hệ bảo mật được thiết kế theo mẫu dư thừa.
  - Cho phép tạo các mạng riêng ảo.
  - Cho phép giám sát các vấn đề liên quan tới an toàn bảo mật, quét các lỗi bảo mật của hệ thống, phân tích nguyên nhân và báo cáo.
  - Ghi nhật ký về các sự kiện của hệ thống và cảnh báo nếu có.
  - Giám sát thông tin mạng.