Bài 5. An toàn, Bảo mật trên môi trường Điện toán đám mây

Nội dung

1. Các vấn đề an toàn và bảo mật ĐTĐM
2. Một số phương pháp ATBM dịch vụ ĐTĐM
3. Thiết kế kiến trúc ĐTĐM đảm bảo ATBM

1. Các vấn đề an toàn và bảo mật ĐTĐM

- Khảo sát của IDC về quan ngại khi sử dụng ĐTĐM

Các vấn đề ATBM ĐTĐM

- ATBM trong dịch vụ phần mềm (SaaS)
- ATBM trong dịch vụ nền tảng (PaaS)
- ATBM trong dịch vụ hạ tầng (IaaS)

ATBM trong dịch vụ phần mềm

- Các dịch vụ phần mềm phổ biến: email, office, ERP, CRM,..
- Vấn đề ATBM do nhà cung cấp dịch vụ chịu trách nhiệm

Vấn đề 1. Bảo mật ứng dụng

- Người dùng thường truy cập ứng dụng qua các dịch vụ Web.
- Việc bảo mật tiến hành như bảo mật các ứng dụng web.

Vấn đề 2. Nhiều người thuê đồng thời

- Để đảm bảo tính riêng tư, các dịch vụ SaaS triển khai 3 mô hình:
- Mô hình khả mở (Scalability model):
  - Mỗi người sử dụng được cấp một thể hiện chuyên biệt của phần mềm
- Mô hình cấu hình qua siêu dữ liệu (configurability via metadata):
  - Mỗi người cũng có một thể hiện riêng nhưng dùng chung mã nguồn.
  - Sử dụng siêu dữ liệu để cấu hình cho từng người.

- Mô hình nhiều người dùng đồng thời:
  - Một thể hiện của ứng dụng được chia sẻ cho nhiều người dùng.
  - Tài nguyên được sử dụng hiệu quả
  - Dữ liệu người dùng được lưu trữ chung một CSDL nên khả năng rò rỉ cao.

Vấn đề 3. Bảo mật dữ liệu

- Dữ liệu của các ứng dụng được lưu trữ trên đám mây thường là dữ liệu rõ.
- Việc sao lưu dữ liệu có thể qua nhà cung cấp thứ ba.

Vấn đề 4. Truy cập dịch vụ

- Trong SaaS các ứng dụng có thể truy cập trên nhiều thiết bị khác nhau.
- Tạo sơ hở cho các phần mềm ăn cắp dữ liệu trên các thiết bị, qua mạng di động, wifi,...

ATBM trong dịch vụ nền tảng

- ATBM trong PaaS liên quan đến 2 khía cạnh:
  - Bảo mật trong nội tại dịch vụ PaaS
  - Bảo mật trong phần mềm của khách hàng sử dụng dịch vụ PaaS

Vấn đề 5. ATBM của bên thứ ba

- Các dịch vụ PaaS thường sử dụng các dịch vụ của bên thứ ba.

Vấn đề 6. Vòng đời của các ứng dụng

- Các ứng dụng có thể nâng cấp, sửa đổi.
- Nhà cung cấp dịch vụ PaaS phải kiểm soát tốt mỗi khi khách hàng cập nhật ứng dụng.

ATBM trong dịch vụ hạ tầng

- Khách hàng kiểm soát các dịch vụ họ thuê.
- Nhà cung cấp dịch vụ IaaS đảm bảo ATBM từ các tài nguyên cho thuê.

Vấn đề 7. Ảo hóa

- Ảo hóa sử dụng các phần mềm để quản lý việc khai thác các tài nguyên vật lý.
- Các phần mềm ảo hóa cũng có những lỗ hổng bảo mật cần kiểm soát.

Vấn đề 8. Giám sát máy ảo

- Thành phần giám sát máy ảo (VMM) có nhiệm vụ giám sát và quản lý các máy ảo.
- Các VMM cũng là nơi gây nguy cơ cho ATBM.
- Việc di trú các máy ảo từ VMM này sang VMM khác cũng gây nguy cơ.

Vấn đề 9. Tài nguyên chia sẻ

- Các máy ảo chia sẻ tài nguyên vật lý như Ram, CPU, đĩa cứng,...
- Việc chia sẻ tài nguyên làm giảm tính ATBM.
- Máy ảo này có thể ăn cắp thông tin của máy ảo khác qua tài nguyên chia sẻ.
- Giữa các máy ảo có thể có các kênh giao tiếp không theo quy tắc bảo mật của VMM.

Vấn đề 10. Kho ảnh máy ảo công cộng

- Máy ảo được tạo sẵn theo mẫu lưu trong các file ảnh.
- Các ảnh máy ảo thường để nơi công cộng.
- Tin tặc có thể chèn mã độc vào ảnh các máy ảo.
- Ảnh máy ảo cũng có các lỗ hổng bảo mật nếu không được cập nhật kịp thời.

Vấn đề 11. Phục hồi máy ảo

- Người sử dụng có thể phục hồi máy ảo về trạng thái đã lưu trữ trước đó.
- Nguy cơ ATBM khi máy ảo cũ chưa được vá các lỗ hổng bảo mật.

Vấn đề 12. Mạng ảo

- Mạng ảo chia sẻ tài nguyên mạng dùng chung.
- Máy ảo có thể bắt được các gói tin của máy ảo khác trên hệ thống mạng dùng chung đó.

Một số lỗ hổng bảo mật khác

- Giao diện API được cung cấp không an toàn.
- Các lỗ hổng liên quan đến dữ liệu lưu trữ trên đám mây từ khách hàng.
- Tin tặc tấn công qua các máy ảo

Liên minh ATBM trong ĐTĐM

- Cloud Security Alliance – CSA: Thành lập 11/2008
- Nhận diện các vấn đề về ATBM trên ĐTĐM
- Chia sẻ kinh nghiệm, giải pháp hỗ trợ đảm bảo ATBM
- Các nhà cung cấp dịch vụ ĐTĐM và các công ty liên quan tham gia.

9 nguy cơ ATBM

- Năm 2013 CSA công bố 9 nguy cơ ATBM trên ĐTĐM
  1. Rò rỉ dữ liệu
  2. Mất mát dữ liệu
  3. Bị đánh cắp tài khoản hoặc thất thoát dịch vụ
  4. Giao diện API không an toàn
  5. Tấn công từ chối dịch vụ (DDOS)
  6. Nguy cơ từ bên trong
  7. Sự lạm dụng dịch vụ đám mây
  8. Khảo sát không đầy đủ
  9. Lỗ hổng công nghệ sử dụng chung

Một số phương pháp đảm bảo ATBM cho ĐTĐM

Quy trình ATBM

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 ATBM

- Lập kế hoạch:
  - Nhận định nguy cơ ATBM
  - Xác định cơ chế kiểm soát ATBM
  - Lên kế hoạch thực hiện
- Triển khai:
  - Cài đặt cấu hình cho cơ chế kiểm soát ATBM
- Đánh giá:
  - Đánh giá cơ chế kiểm soát đã triển khai có đảm bảo ATBM
- Duy trì:
  - Thường xuyên theo dõi, cập nhật thông tin mới về ATBM

Bảo mật trung tâm dữ liệu

- Bảo mật mức vật lý:
  - Chính sách trong thiết kế, xây dựng và vận hành trung tâm dữ liệu.
  - Truy cập vật lý được bảo vệ nghiêm ngặt và chuyên nghiệp
  - Hệ thống phân tích nhật ký hoạt động thường xuyên

- Kiểm soát truy cập:
  - Kiểm soát những đối tượng có thể truy cập các dịch vụ đám mây.
  - Xác nhận bằng hóa đơn thanh toán
  - Kiểm tra định danh qua điện thoại
  - Giấy phép truy cập
  - Khóa truy cập
  - Cặp khóa

- Bảo mật dữ liệu và mạng:
  - Bảo mật hệ điều hành: bảo mật cho HĐH máy chủ vật lý và máy ảo.
  - VD: Amazon sử dụng khóa SSH
  - Bảo mật mạng: dùng tường lửa truy cập từ bên ngoài và tường lửa nội bộ.
  - Bảo mật cho các hệ thống giám sát: dùng giấy phép X.509 và SSL.
  - Bảo mật lưu trữ dữ liệu:
    - Kiểm soát quyền truy cập trong một danh sách ACL – access control list
    - Mã hóa dữ liệu quan trọng

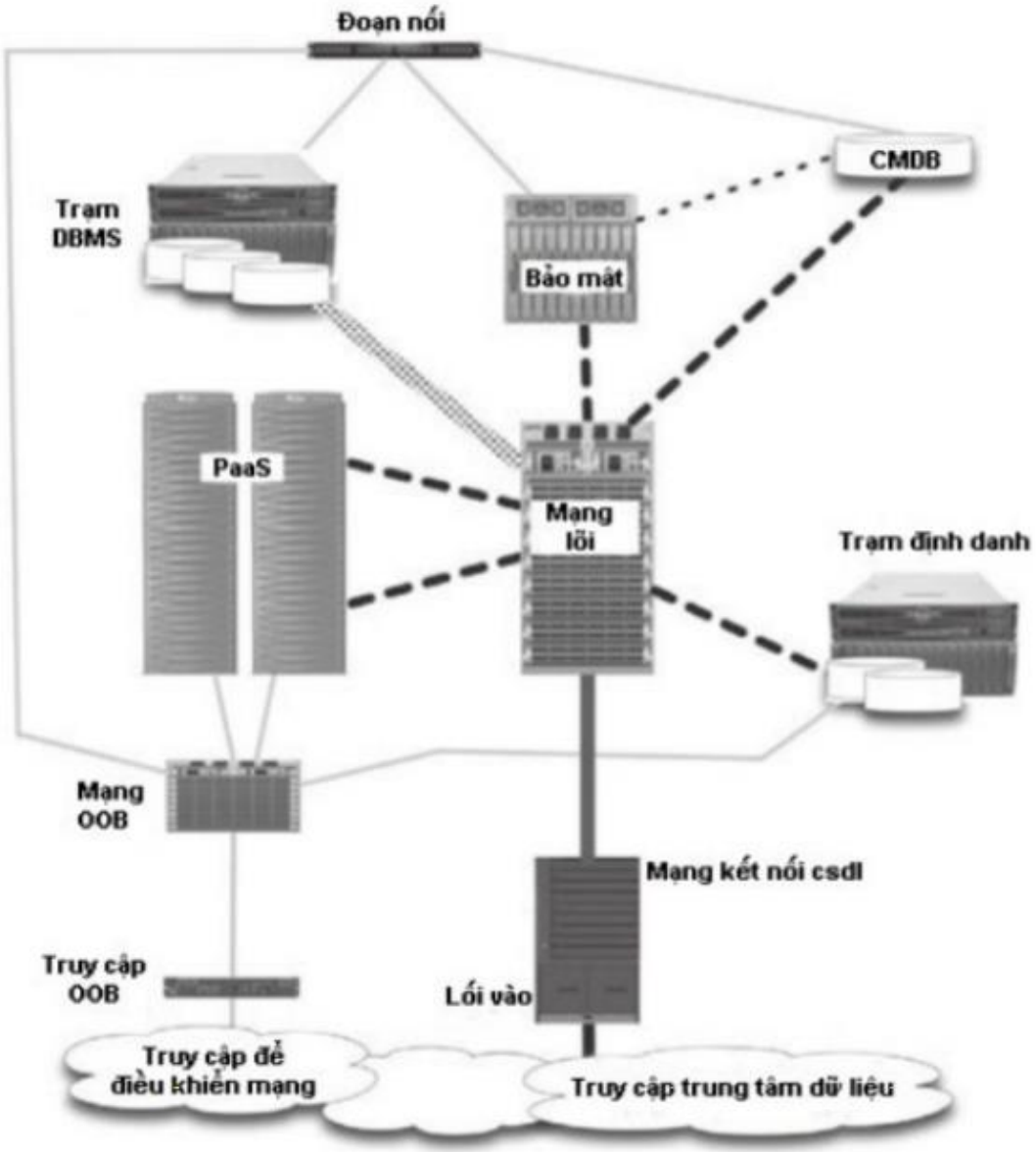
Thiết kế kiến trúc ĐTĐM đảm bảo ATBM

Những yêu cầu cho kiến trúc

- Yêu cầu bảo mật mức vật lý:
  - Chống truy cập trái phép
  - Bảo vệ hệ thống khỏi các thảm họa thiên nhiên
- Yêu cầu bảo mật các thành phần hệ thống:
  - Quản lý định danh
  - Quản lý truy cập
  - Quản lý khóa
  - Ghi nhận sự kiện và thống kê
  - Giám sát bảo mật
  - Quản lý sự cố
  - Kiểm tra an toàn và vá lỗi
  - Kiểm soát mạng và hệ thống
  - Quản lý cấu hình

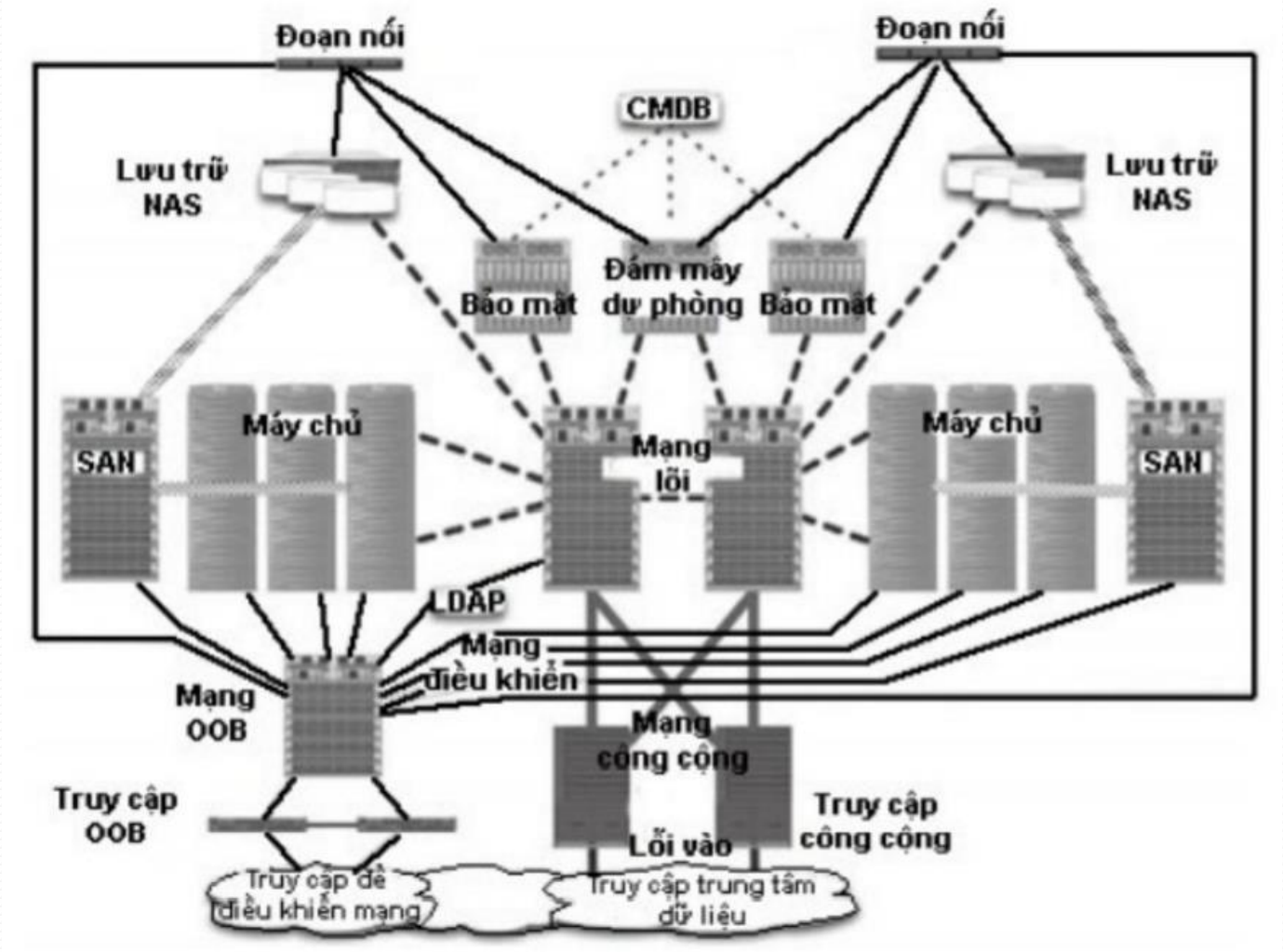
Kiến trúc đám mây PaaS

- Mạng riêng biệt OOB (out-of-band): cung cấp dải IP để truy cập từ bên ngoài
- CMDB: cơ sở dữ liệu cấu hình.



- Hệ thống mạng cục bộ chia làm ba mạng chính:
  - 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.

Kiến trúc đám mây dịch vụ tính toán lưu trữ



- LDAP(Lightweight Directory Access Protocol): giao thức truy cập thư mục.
- Cần tài nguyên dành sẵn để đảm bảo tính sẵn sàng
- Tạo mạng riêng ảo cho phép quản trị viên truy cập trực tiếp vào máy chủ để quản lý.
- Trung tâm điều hành bảo mật:
  - Cho phép giám sát các vấn đề liên quan tới an toàn bảo mật.
  - Ghi nhật ký về các sự kiện của hệ thống và cảnh báo nếu có.
  - Giám sát thông tin mạng

Tổng kết

- Việc đảm bảo ATBM trên môi trường điện toán đám mây rất quan trọng.
- Để đảm bảo ATBM trên ĐTĐM cần kết hợp của:
  - Kế hoạch
  - Kiến trúc
  - Kỹ thuật
- Các giải pháp ATBM phải đạt các tiêu chuẩn.

Câu hỏi

- Tìm hiểu các chuẩn quy định thời gian hoạt động và thời gian dừng hệ thống của các dịch vụ điện toán đám mây.