PHENIKAA UNIVERSITY

ĐIỆN TOÁN ĐÁM MÂY

L6. An toàn và bảo mật

Nguyễn Thành Trung
trung.nguyenthanh@phenikaa-uni.edu.vn

Điện toán đám mây có thực sự an toàn ?

Nhà cung cấp dịch vụ và người dùng phải đối mặt với những vấn đề gì

2022

Công ty bảo mật Splunk và SNG đã tiến hành phỏng vấn 1.227 lãnh đạo bảo mật hoặc IT thuộc

- 11 nước trên thế giới (Úc, Canada, Pháp, Đức, Ấn Độ, Nhật Bản, Hà Lan, New Zealand, Singapore, Vương quốc Anh, Hoa Kỳ),
- 15 ngành khác nhau: hàng không, quốc phòng, tiêu dùng, giáo dục, tài chính, chính quyền, chăm sóc sức khỏe, công nghệ, khoa học, sản xuất, truyền thông, năng lượng, bán lẻ, viễn thông, vận tải, tiện ích

STT	Số lãnh đạo đồng ý	Phân loại thách thức	Diễn giải thách thức
01	39%	Con người/ Chính sách	Nhận biết các cấu hình không được tuân thủ, bao gồm cả những cấu hình không tuân thủ theo các thông lệ tốt nhất trong ngành hoặc theo khuôn khổ quy định
02	32%	Hệ thống	Xác định lỗ hổng của các phần mềm
03	29%	Chính sách/ Hệ thống	Truy vết, theo dõi các hoạt động của người dùng và hoạt động tài khoản dịch vụ (ví dụ: Các phiên người dùng thực hiện dòng lệnh tương tác, quyền truy cập vào bảng điều khiển điện toán đám mây, v.v.)
04	28%	Chính sách	Cấu hình của các nhóm bảo mật (ví dụ: Việc cấu hình cho cả cụm máy chủ phục vụ tương tác với bên ngoài)
05	25%	Hệ thống	Nguy cơ tiềm ẩn từ các hoạt động cấp hệ điều hành (ví dụ: Xử lý hoặc thay đổi tệp hệ thống)
06	23%	Hệ thống	Khả năng phát hiện phần mềm độc hại

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
4. Chi phí
5. Thời gian ngừng hoạt động (Downtime)
6. Thiếu nguồn lực
7. Quản lý môi trường đa đám mây

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
   - Khách hàng phụ thuộc vào các nhà cung cấp đám mây
   - Vấn nạn lấy cắp dữ liệu
   - Sự ảnh hưởng bởi phần mềm độc hại

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
   - Quyền truy cập từ xa >=< tính bảo mật.

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
   - Đảm bảo dữ liệu được cung cấp cho đám mây không bị rò rỉ ra ngoài
   - Dịch vụ cần được theo dõi và giám sát, với tính hiệu suất cao, tính mạnh mẽ

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
4. Chi phí
   - tổ chức quy mô nhỏ
   - chuyển dữ liệu

Thách thức

Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
4. Chi phí
5. Thời gian ngừng hoạt động (Downtime)
   - Thách thức chung của điện toán đám mây
   - Khó có thể đảm bảo mang lại một nền tảng không có downtime

Thách thức

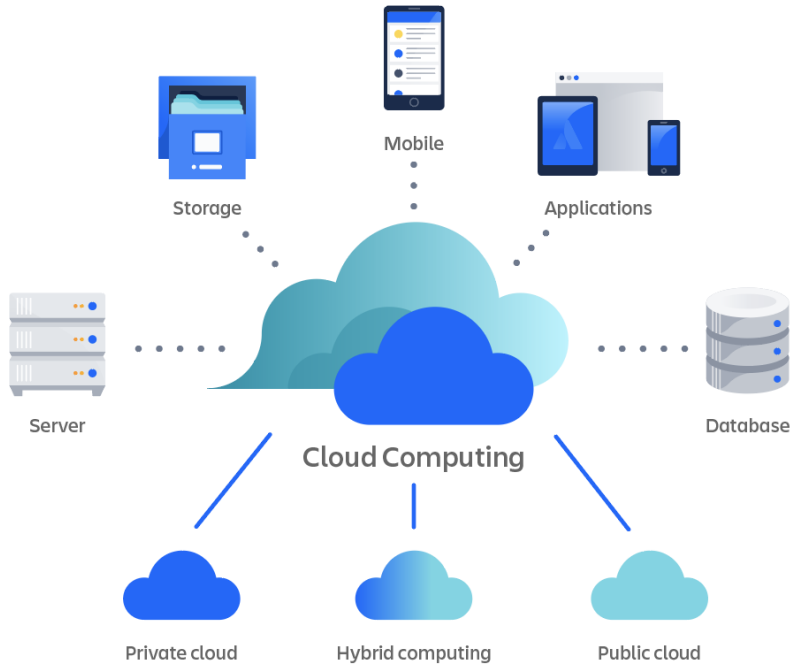
Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
4. Chi phí
5. Thời gian ngừng hoạt động (Downtime)
6. Thiếu nguồn lực

Thách thức

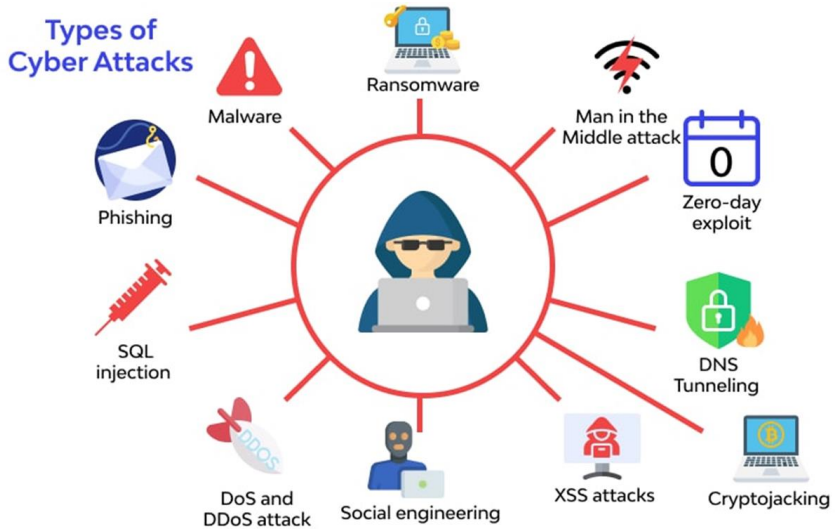
Các rủi ro và thách thức của Điện toán đám mây

1. Bảo mật & Quyền riêng tư
2. Khả năng tương tác và tính di động
3. Mức độ đáng tin cậy và tính linh hoạt
4. Chi phí
5. Thời gian ngừng hoạt động (Downtime)
6. Thiếu nguồn lực
7. Quản lý môi trường đa đám mây
   - Trung bình một công ty đang sử dụng 4,8 đám mây công cộng (Public Cloud) và đám mây riêng tư (Private Cloud) khác nhau



An toàn và bảo mật

- Information System Security: Trong một hệ thống thông tin, an toàn và bảo mật (ATBM) là sự đảm bảo tính bí mật, tính toàn vẹn và tính sẵn dùng của hệ thống dưới những đe dọa đến từ các sự cố phần cứng/phần mềm hoặc đến từ sự tấn công có chủ đích của con người
- Cloud Security: việc tập hợp các công nghệ kiểm soát được thiết kế để duy trì tính bảo mật và bảo vệ thông tin, giúp bảo mật dữ liệu và tất cả các ứng dụng được liên kết với nó.



An toàn và bảo mật

- Nguyên do:
  - tính chất phân tán và trực tuyến
  - tích hợp nhiều tầng dịch vụ với nhiều công nghệ đặc thù

⇒ **nhiều nguy cơ mới về ATBM**

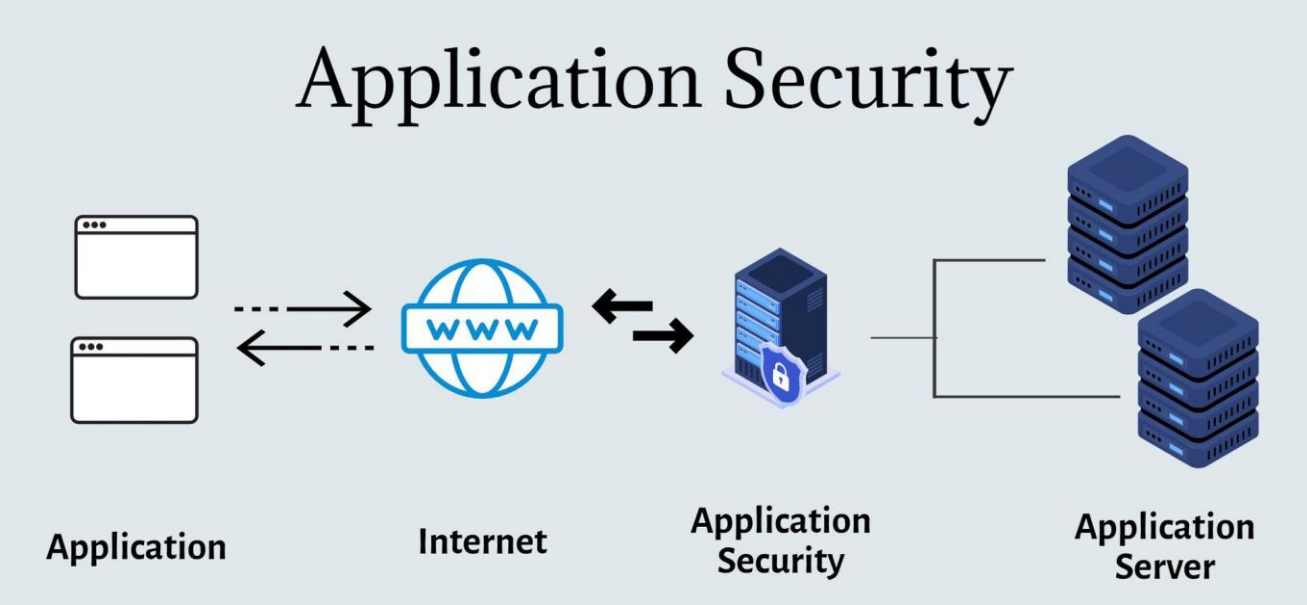
⇒ các vấn đề bảo mật:
  - nhà cung cấp dịch vụ đám mây phải đối mặt
  - khách hàng phải đối mặt

An toàn và bảo mật trong SaaS

- Vấn đề 1. Bảo mật ứng dụng
  - Người sử dụng thường truy nhập các ứng dụng ĐTĐM thông qua trình duyệt web.

  ⇒Sai sót trong các trang web có thể tạo nên những lỗ hổng của dịch vụ SaaS.

  ⇒Tin tặc có thể tấn công tới các máy tính của người dùng
  - ATBM trong dịch vụ SaaS không khác với trong các ứng dụng web thông thường.

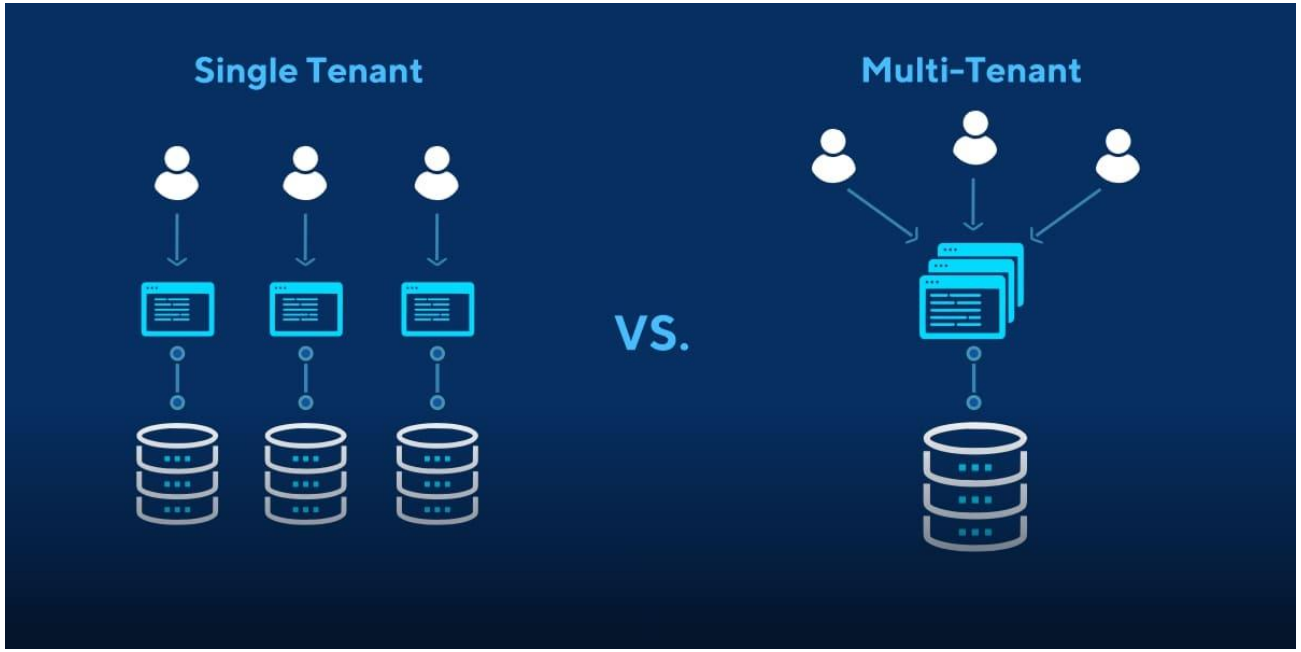


An toàn và bảo mật trong SaaS

- Vấn đề 2. Nhiều người thuê đồng thời (multi-tenancy)
  - ứng dụng được chia sẻ cho nhiều người thuê.

  ⇒tài nguyên sẽ được sử dụng hiệu quả (mặc dù tính khả mở sẽ giảm đi).

  ⇒dữ liệu của cácngười dùng được lưu trữ trên cùng một cơ sở dữ liệu nên nguy cơ về rò rỉ dữ liệu có thể xảy ra



An toàn và bảo mật trong SaaS

- Vấn đề 3. Bảo mật dữ liệu
  - Nhà cung cấp dịch vụ SaaS sẽ 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 ĐTĐM 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.

An toàn và bảo mật trong SaaS

- Vấn đề 4. 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 ứng dụng không an toàn,…

An toàn và bảo mật trong PaaS

- Vấn đề 5. An toàn và bảo mật của bên thứ ba
  - Dịch vụ PaaS thường không chỉ cung cấp môi trường phát triển ứng dụng của nhà cung cấp dịch vụ mà còn cho phép sử dụng những dịch vụ mạng của bên thứ ba.

⇒Những dịch vụ này thường được đóng gói dưới dạng thành phần trộn (mashup).

⇒ATBM trong các dịch vụ PaaS cũng phụ thuộc vào ATBM của chính các mashup này

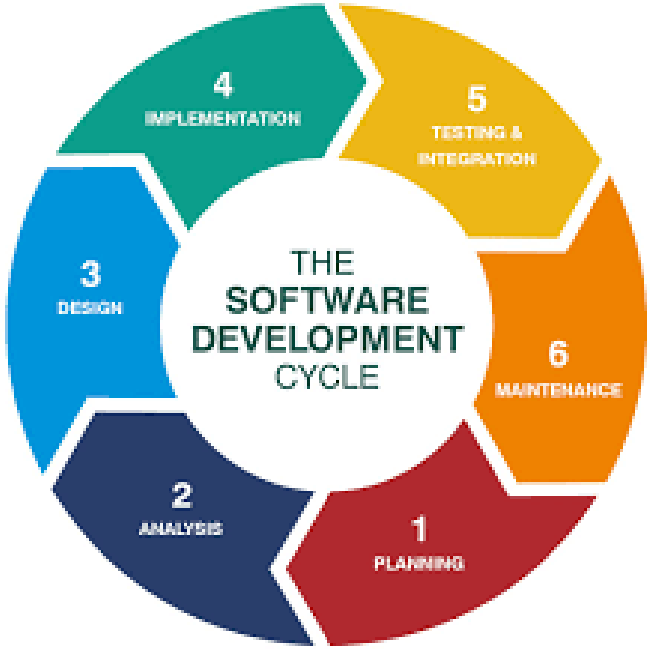
An toàn và bảo mật trong PaaS

- Vấn đề 6. Vòng đời của ứng dụng
  - Các ứng dụng trên dịch vụ ĐTĐM cũng có vòng đời

  ⇒liên tục nâng cấp.

  ⇒đòi hỏi nhà cung cấp dịch vụ PaaS phải hỗ trợ tốt cho những thay đổi của ứng dụng.

  ⇒sự thay đổi của các thành phần ứng dụng trong quá trình nâng cấp đôi khi gây ra vấn đề về ATBM



An toàn và bảo mật trong IaaS

- Vấn đề 7. Ảo hóa
  - Công nghệ ảo hóa cho phép dễ dàng tạo lập, sao chép, chia sẻ, di trú và phục hồi các máy ảo trên đó thực thi các ứng dụng.

  ⇒Công nghệ này tạo nên một tầng phần mềm mới trong kiến trúc phần mềm của hệ thống.

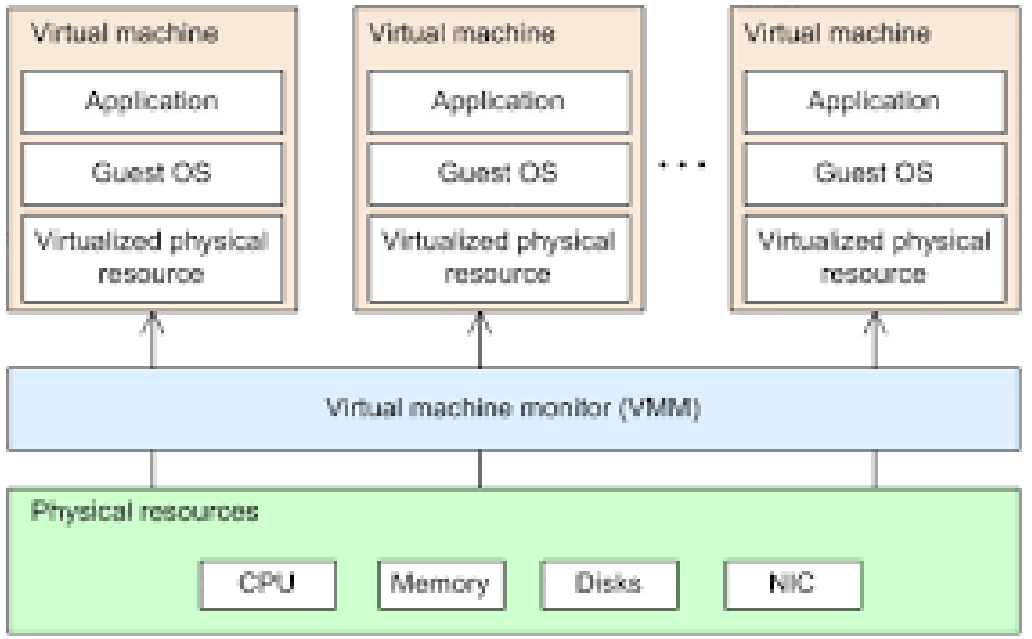
  ⇒Chính vì vậy nó cũng mang đến những nguy cơ mới về ATBM.

An toàn và bảo mật trong IaaS

- Vấn đề 8. Giám sát máy ảo
  - Thành phần giám sát máy ảo (virtual machine monitor – VMM) hay còn gọi là supervisor có trách nhiệm giám sát và quản lý các máy ảo được tạo trên máy vật lý.

⇒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 ATBM



An toàn và bảo mật trong IaaS

- Vấn đề 9. 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,…

  ⇒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.

An toàn và bảo mật trong IaaS

- Vấn đề 10. Kho ảnh máy ảo công cộng
  - Trong môi trường IaaS, ảnh máy ảo là một mẫu sẵn có để tạo nên các máy ảo.

  $\Rightarrow$người dùng có thể dễ dàng tạo nên máy ảo theo nhu cầu của mình.

  $\Rightarrow$tạo nên một nguy cơ về bảo mật khi tin tặc tải lên những ảnh máy ảo có chứa mã độc. Ảnh máy ảo cũng tạo ra nguy cơ về bảo mật khi chúng không được vá lỗi giống như các hệ thống đang vận hành

An toàn và bảo mật trong IaaS

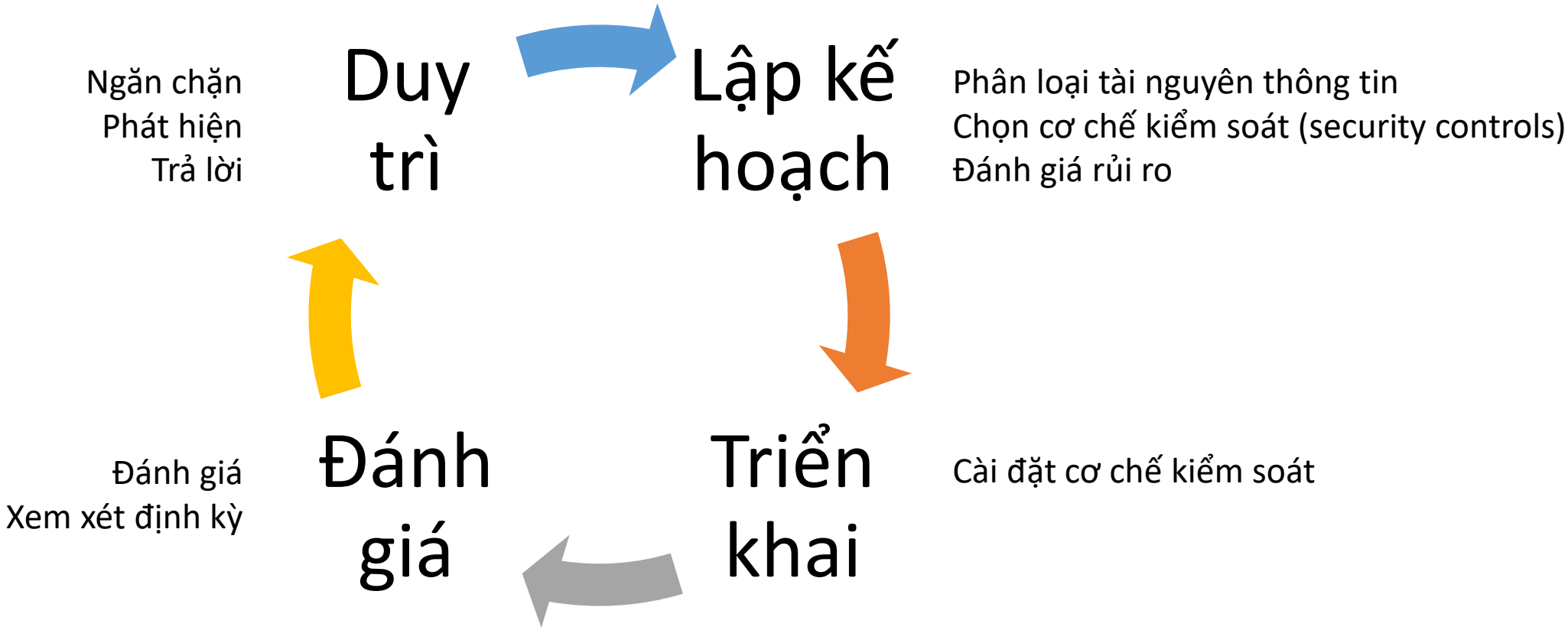
- Vấn đề 11. Phục hồi máy ảo
  - Người sử dụng có thể phục hồi máy ảo về một trạng thái được lưu trữ trước đó.
  - Tuy nhiên, nguy cơ về ATBM lại phát sinh khi những lỗi được vá mới không áp dụng cho trạng thái máy ảo cũ.

An toàn và bảo mật trong IaaS

- Vấn đề 12. Mạng ảo
  - Mạng ảo có thể được chia sẻ bởi nhiều người thuê trong một vùng chứa tài nguyên.
  - Các vấn đề ATBM có thể phát sinh giữa những người thuê chia sẻ chung mạng ảo này như việc một máy ảo có thể nghe trộm các bản tin gửi cho máy ảo khác trên cùng mạng

Đảm bảo ATBM trong ĐTĐM

- Quy trình



Đảm bảo ATBM trong ĐTĐM

1. Bảo mật trung tâm dữ liệu
2. Các biện pháp kiểm soát truy nhập
3. Bảo mật dữ liệu và mạng

Đảm bảo ATBM trong ĐTĐM

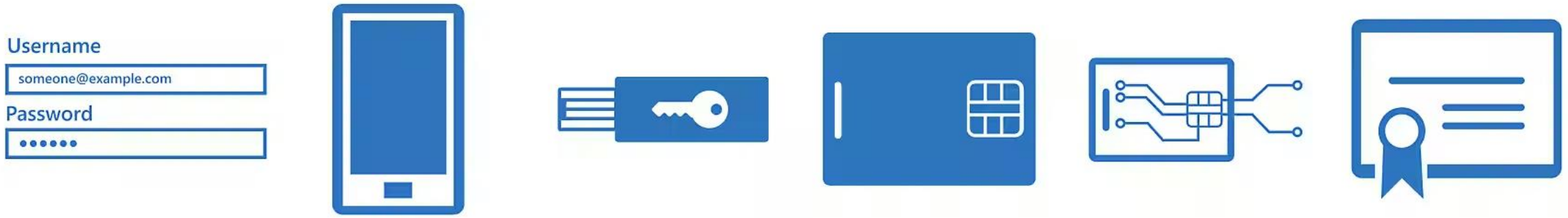
1. Bảo mật trung tâm dữ liệu
   - Bảo mật mức vật lý
   - Định danh, xác thực
   - Giám sát

Đảm bảo ATBM trong ĐTĐM

2. Các biện pháp kiểm soát truy nhập
   - Xác nhận bằng hóa đơn thanh toán
   - Kiểm tra định danh qua điện thoại
   - Giấy phép truy nhập (mật khẩu)
   - Khóa truy nhập (key)
   - Giấy phép X.509
     - bao gồm một giấy phép (chứa khóa công khai và nội dung cấp phép) và một khóa bí mật
     - Vd: xác minh trạng thái hoạt động của các giao thức, chữ ký số,…

Đảm bảo ATBM trong ĐTĐM

2. Các biện pháp kiểm soát truy nhập
   - Kết hợp nhiều phương thức (MFA - Multi-Factor Authentication)
     - bổ sung một tầng bảo vệ cho quy trình đăng nhập
     - VD: tin nhắn văn bản, cuộc gọi, sinh trắc học và mật khẩu một lần – để đáp ứng nhu cầu riêng của tổ chức và giúp bảo vệ người dùng của bạn.



Đảm bảo ATBM trong ĐTĐM

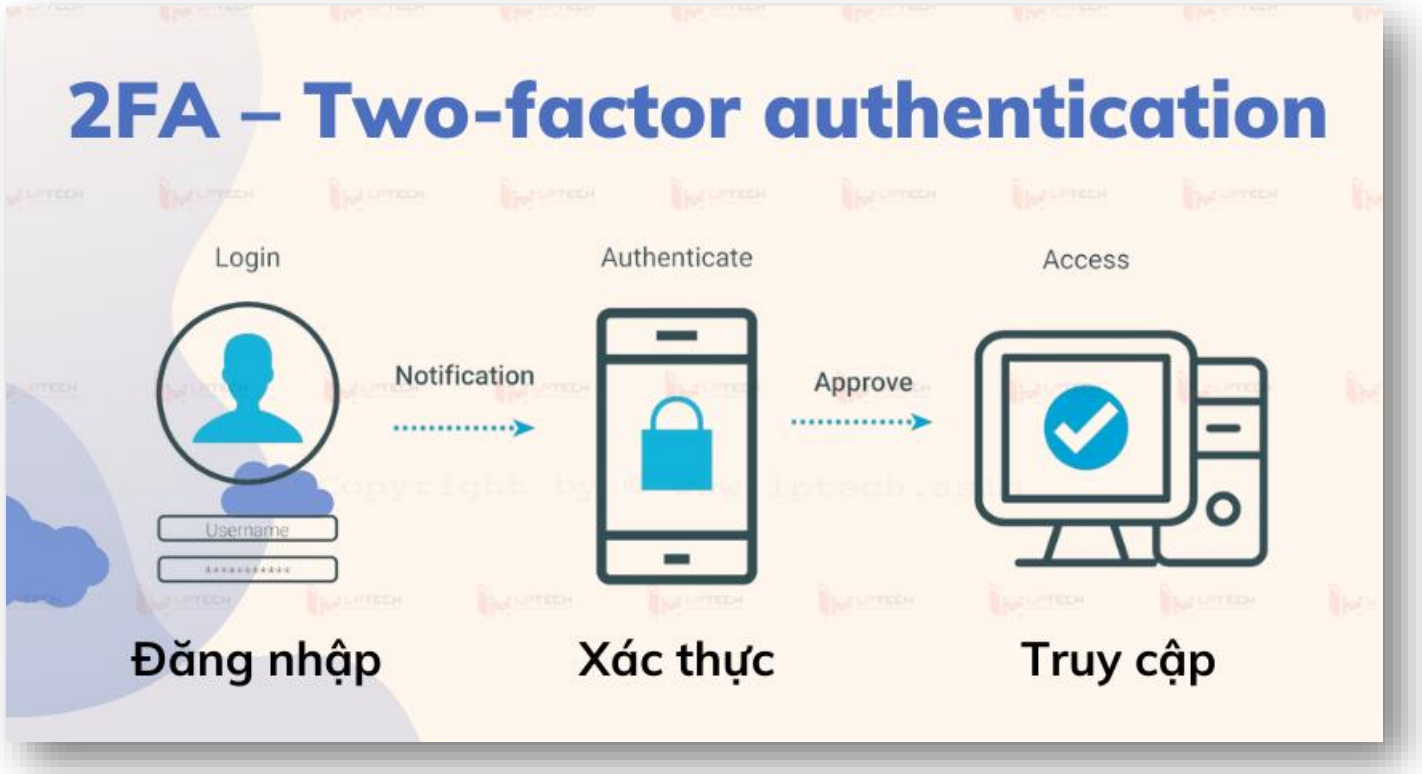
2. Các biện pháp kiểm soát truy nhập
   - Ví dụ: 2FA (Two-factor authentication)

2FA là một tính năng bảo mật giúp người dùng tránh khỏi nguy cơ bị đăng nhập vào các tài khoản mạng trái phép

Đảm bảo ATBM trong ĐTĐM

2. Các biện pháp kiểm soát truy nhập
   - Ví dụ: 2FA (Two-factor authentication)

Cách thức hoạt động



Đảm bảo ATBM trong ĐTĐM

3. Bảo mật dữ liệu và mạng
   - Bảo mật hệ điều hành
   - Bảo mật mạng
   - Bảo mật cho môi trường cộng sinh (môi trường giữa các máy ảo)
   - Bảo mật cho các hệ thống giám sát: tham số tường lửa, giấy phép X.509 cho mọi yêu cầu, mã hoá gói tin (SSL) khi dùng API,….
   - Bảo mật lưu trữ dữ liệu: kiểm soát truy nhập (ACL – access control list)