Điện toán đám mây

An toàn cho điện toán đám mây

TS Ngô Bá Hùng - mail:nbhung@cit.ctu.edu.vn

Tháng 03/2016

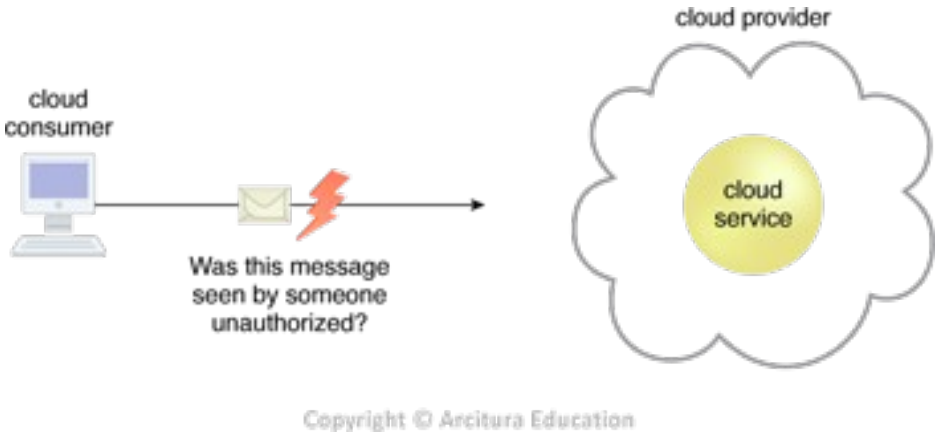
Nội dung

- Các thuật ngữ và khái niệm cơ bản
- Các tác nhân đe dọa
- Những mối đe dọa cho an ninh đám mây

Thuật ngữ và khái niệm cơ bản

Khái niệm và thuật ngữ cơ bản

- An toàn là một tập hợp phức tạp các kỹ thuật, các công nghệ, các quy tắc và các ứng xử được phối hợp với nhau để đảm bảo tính toàn vẹn trong việc truy cập vào các hệ thống máy tính và dữ liệu.
- Các biện pháp an toàn CNTT nhằm vào mục đích phòng chống lại các mối đe dọa an ninh, các quấy rối tạo ra từ những ý đồ xấu hoặc những lỗi không cố ý của người dùng



- **Tính cơ mật** (Confidentiality): Là đặc tính được tạo ra để cho phép truy cập bởi những người được phép. Đối với môi trường đám mây, tính cơ mật chủ yếu gắn liền với việc hạn chế truy cập vào dữ liệu truyền tải và lưu trữ

Khái niệm và thuật ngữ cơ bản

- **Tính toàn vẹn** (Integrity): Là đặc tính không cho phép sửa đổi bởi những người không có thẩm quyền. Đối với môi trường điện toán đám mây, thuộc tính này thể hiện ở chỗ dữ liệu được truyền bởi người tiêu dùng có đảm bảo trùng khớp với dữ liệu nhận được bởi dịch vụ đám mây hay không. Tính toàn vẹn có thể mở rộng đến cách thức mà ở đó dữ liệu được lưu trữ, xử lý và truy vấn bởi các dịch vụ đám mây và các tài nguyên CNTT dựa trên đám mây
- **Tính xác thực** (Authenticity): là đặc tính của một sự vật được cung cấp bởi một nguồn được ủy quyền.
- **Tính sẵn dùng** (Availability): là đặc tính có thể truy cập và sử dụng trong một khoảng thời gian nào đó. Trong môi trường đám mây, tính năng sẵn sàng của các dịch vụ đám mây có thể là một trách nhiệm được chia sẻ bởi nhà cung cấp đám mây và nhà cung cấp truy cập đám mây

Khái niệm và thuật ngữ cơ bản

- **Mối đe dọa** (Threat): là một sự xâm phạm an ninh tìm ẩn mà nó có thể thách thức những sự phòng vệ nhằm để vi phạm quyền riêng tư hoặc gây tổn hại
- **Tính dễ bị tổn thương** (Vulnerability): là một điểm yếu mà nó có thể bi khai thác bởi vì nó được bảo vệ bằng những biện pháp an ninh không đủ mạnh hoặc biện pháp an ninh đang tồn tại bị mất tác dụng trước một sự tấn công. Tính dễ tổn thương của các tài nguyên CNTT có thể có nhiều lý do, ví dụ như việc cấu hình không đầy đủ, những yếu kém trong chính sách an ninh, lỗi người sử dụng, hỏng hóc phần cứng hoặc phần mềm nhúng (firmware), lỗi trong phần mềm và kiến trúc an ninh nghèo nàn.
- **Rũi ro** (Risk): là khả năng bị mất hoặc hư hại xảy ra từ việc thực hiện một hoạt động. Rũi ro thường được đo dựa trên mức độ đe dọa và số lượng có thể của các điểm dễ bị tổn thương

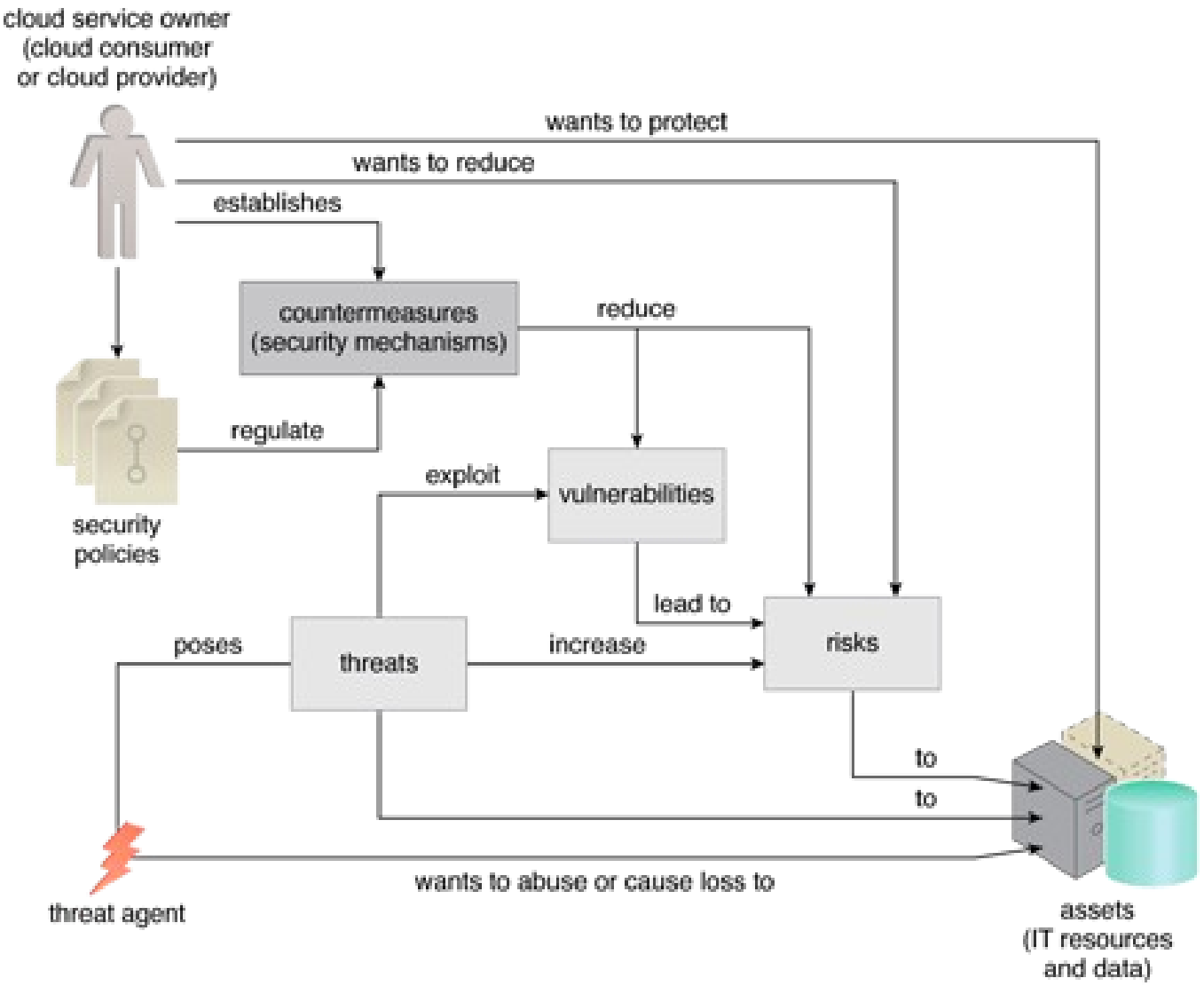
Khái niệm và thuật ngữ cơ bản

- **Kiểm soát an ninh** (Security control): là các biện pháp đối phó để ngăn ngừa hoặc đáp lại các mối đe dọa an ninh nhằm giảm thiểu hoặc phòng tránh rũi ro. Chi tiết về các biện pháp đối phó cho vấn đề an ninh thông thường được trình bày trong các chính sách an ninh, bao gồm một tập các luật và các quy định mô tả cách thức cài đặt một hệ thống, dịch vụ hoặc một kế hoạch an ninh nhằm bảo vệ tối đa các tài nguyên CNTT nhạy cảm và thiết yếu.
- **Các cơ chế an ninh** (Security mechanisms): Các biện pháp đối phó thường được mô tả dưới dạng những điều khoản của cơ chế an ninh. Các cơ chế này là những thành phần bao gồm trong một khuôn khổ phòng thủ để bảo vệ nguồn tài nguyên CNTT, thông tin và dịch vụ.
- **Các chính sách an ninh** (Security policies): Một chính sách an ninh thiết lập một tập các luật và quy tắc an ninh. Thông thường, các chính sách an ninh sẽ định nghĩa trước cách thức các luật và các quy tắc được cài đặt và áp đặt.

Các tác nhân đe dọa an ninh

Các tác nhân đe dọa

- **Tác nhân đe dọa** (Threat agent) là một thực thể mà nó đặt ra một mối đe dọa bởi vì nó có khả năng tạo ra một cuộc tấn công
- Các mối đe dọa an ninh đám mây có thể có nguồn gốc từ bên trong hoặc bên ngoài, từ con người hay từ các phần mềm.



Các tác nhân đe dọa

- **Kẻ tấn công ẩn danh** (Anonymous attacker): là người tiêu dùng dịch vụ đám mây không được tin tưởng, không được cấp phép trong đám mây. Thông thường nó tồn tại dưới dạng một chương trình phần mềm bên ngoài mà nó khởi động các cuộc tấn công trên mạng thông qua các mạng công cộng. Khi những kẻ tấn công ẩn danh có ít thông tin về chính sách an ninh và phòng thủ, chúng sẽ bị hạn chế trong việc phát động những cuộc tấn công có hiệu lực. Vì vậy những kẻ tấn công ẩn danh thường cần đến những hành động như chiếm đoạt tài khoản người dùng hoặc đánh cấp các chứng chỉ người dùng. Với những phương pháp này, một mặt chúng có thể ẩn danh mặt khác sẽ tránh để lại các dấu vết có thể bị truy tố.

Các tác nhân đe dọa

- **Tác nhân dịch vụ độc hại** (Malicious service agent): Một tác nhân dịch vụ độc hại có thể đánh chặn và chuyển tiếp giao thông trên mạng đang đổ về một đám mây. Nó là các tác nhân dịch vụ với phần xử lý bên trong bị can thiệp hoặc nhiễm độc. Đó cũng có thể là một phần mềm bên ngoài đám mây có khả năng đánh chặn từ xa và làm sai lệch nội dung các thông điệp.
- **Kẻ tấn công được tin tưởng** (Trusted attacker): Một kẻ tấn công được tin tưởng chia sẻ các tài nguyên CNTT trong cùng một môi trường đám mây như người tiêu dùng đám mây sẽ cố gắng khai thác các chứng chỉ hợp pháp nhằm vào các nhà cung cấp đám mây và các thuê bao đám mây mà chúng cùng chia sẻ các tài nguyên CNTT. Những kẻ tấn công được tin tưởng thường phát động các cuộc tấn công từ bên trong đường biên tin tưởng của một đám mây bằng cách lạm quyền của các chứng chỉ hợp lệ hoặc thông qua sự chiếm đoạt các thông tin nhạy cảm và thông tin bí mật. Những kẻ tấn công được tin tưởng (còn được gọi là các thuê bao độc hại) có thể dùng các tài nguyên CNTT dựa trên đám mây để khai thác nhiều vấn đề như thâm nhập vào các tiến trình chứng thực yếu, bẻ khóa, …

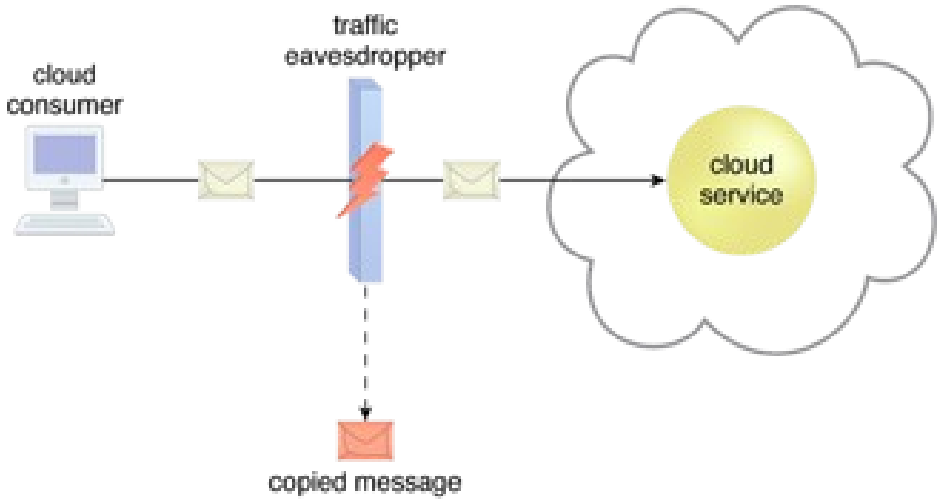
Các tác nhân đe dọa

- **Nội gian** (Malicious insider): là các tác nhân độc hại con người hành động dưới tư cách là nhà cung cấp đám mây. Họ thường là những nhân viên hiện tại hoặc trước đây hay bên thứ ba có quyền truy cập vào tài sản của nhà cung cấp dịch vụ đám mây. Tác nhân đe dọa loại này tạo ra sư thiệt hại tìm năng cực kỳ lớn.

Những mối đe dọa an ninh đám mây

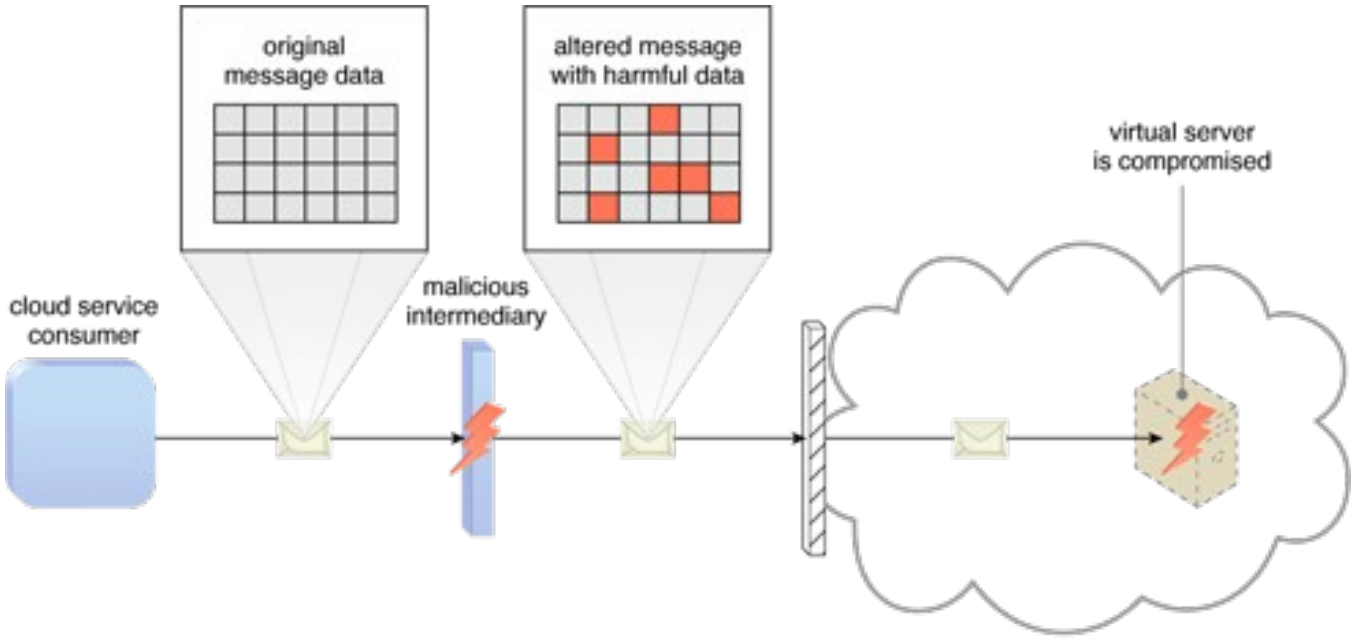
Những mối đe dọa an ninh đám mây

- **Nghe trộm thông tin** (traffic eavesdropping): Nghe trộm thông tin xảy ra khi dữ liệu được truyền tải đến hoặc trong một đám mây bị chặn một cách thụ động bởi một tác nhân dịch vụ độc hại nhằm mục đích thu thập thông tin một cách bất hợp pháp. Mục đích của loại tấn công này là đánh cắp các dữ liệu bí mật và có thể là sự bí mật về mối quan hệ giữa người tiêu dùng và nhà cung cấp đám mây.



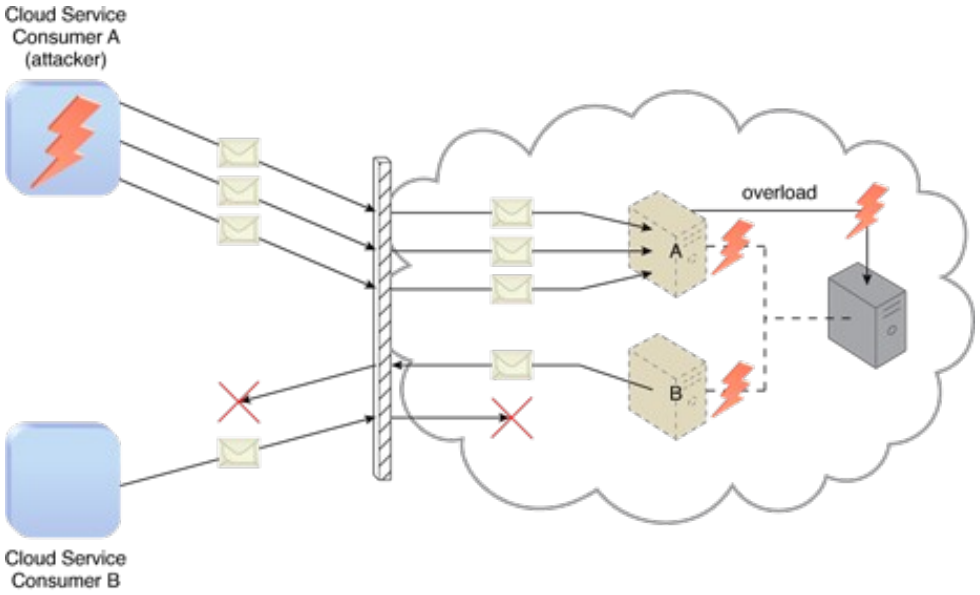
Những mối đe dọa an ninh đám mây

- **Trung gian độc hại** (Malicious intermediary): Mối đe dọa về trung gian độc hại nảy sinh khi các thông điệp bị chặn và thay đổi bởi một tác nhân dịch vụ độc hại, tạo ra một vi phạm về tính mật và tính toàn vẹn của dữ liệu. Nó cũng có thể cài đặt thêm các dữ liệu có hại vào các thông điệp trước khi chuyển tiếp chúng về nơi nhận



Những mối đe dọa an ninh đám mây

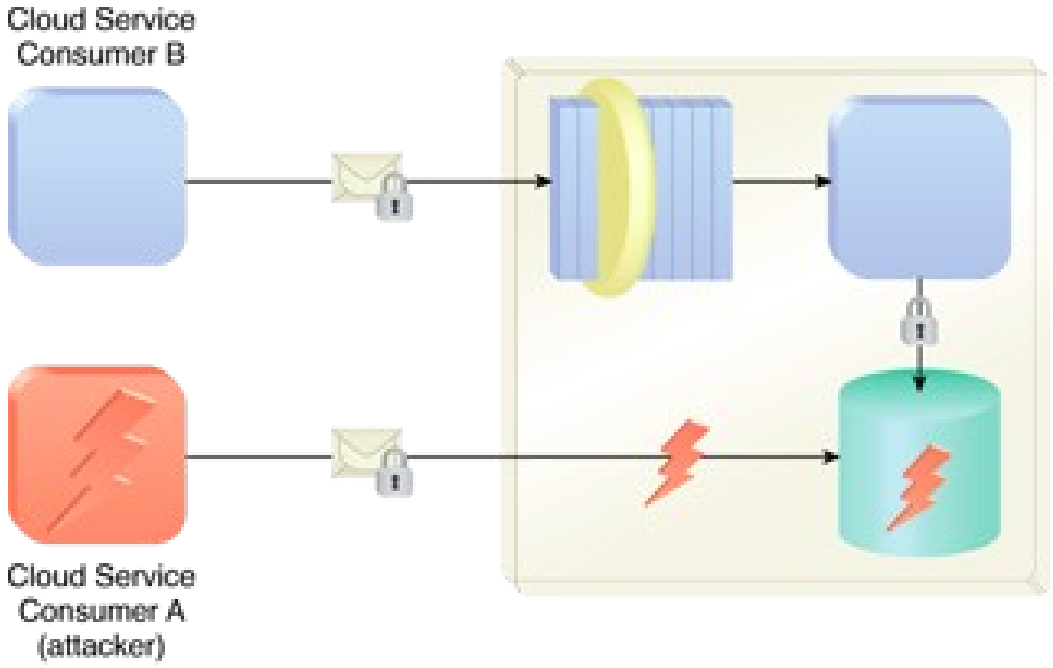
- **Từ chối dịch vụ** (Denial of service): Mục đích của loại tấn công này là làm quá tải các tài nguyên CNTT để chúng không thể vận hành một cách đúng đắng. Các cách khởi tạo loại tấn công này:
  - Tải trên các dịch vụ đám mây bị tăng lên một cách nhân tạo với những thông điệp bắt chước hoặc các yêu cầu truyền thông được lặp lại
  - Mạng bị quá tải để giảm đáp ứng và tác động tiêu cực đến hiệu năng
  - Nhiều yêu cầu dịch vụ đám mây được gởi, mỗi yêu cầu thì được thiết kế để tiêu thụ vượt mức bộ nhớ và tài nguyên tính toán



Những mối đe dọa an ninh đám mây

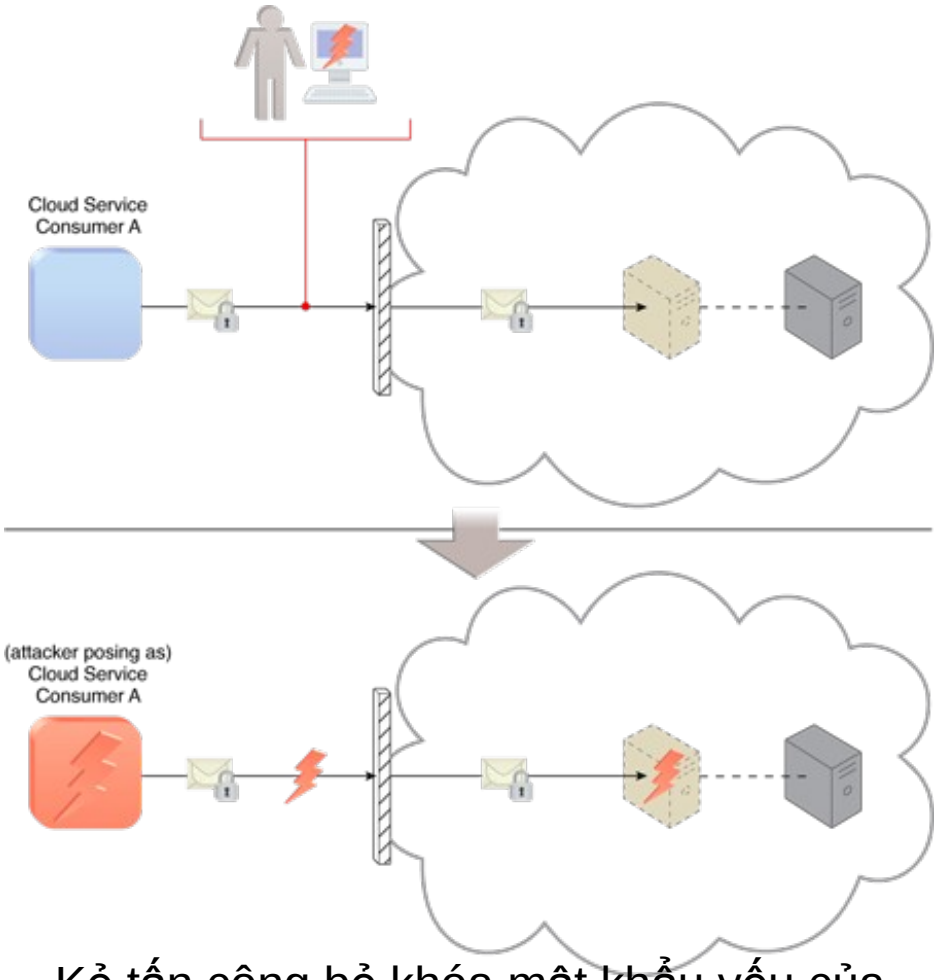
- **Ủy quyền không phù hợp** (Unsufficient authorization): tấn công loại này xảy ra khi việc truy cập được gán cho một kẻ tấn công một cách sai lầm và quá rộng dẫn đến việc kẻ tấn công có thể truy cập được các tài nguyên CNTT mà thông thường thì các tài nguyên này được bảo vệ.

Người tiêu dùng dịch vụ đám mây A giành được quyền truy cập vào cơ sở dữ liệu đã được thiết kế với giả định rằng cơ sở dữ liệu này chỉ có thể được truy cập trực tiếp thông qua một web service với một hợp đồng dịch vụ được công bố công công (như trường hợp người tiêu dùng dịch vụ B)



Những mối đe dọa an ninh đám mây

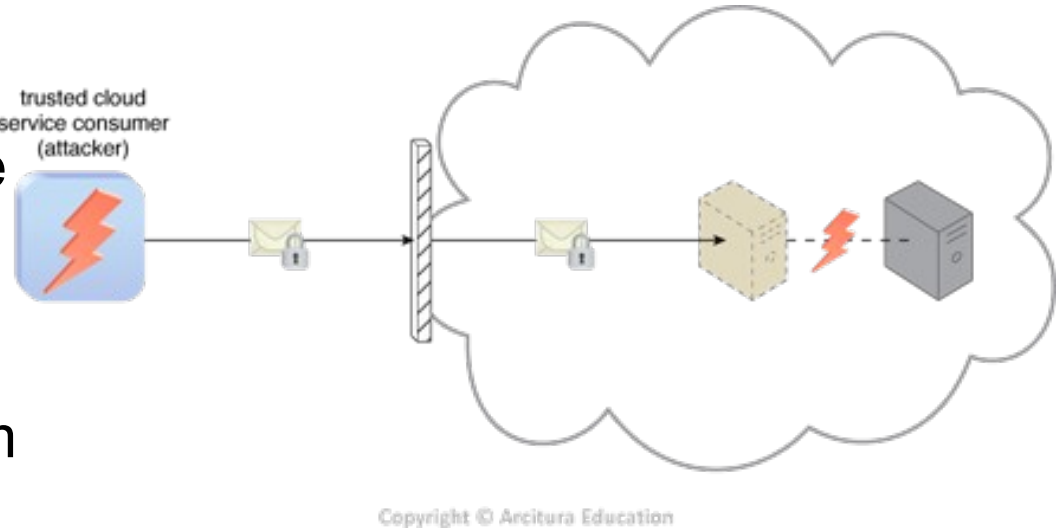
- **Ủy quyền không phù hợp** (Unsufficient authorization):
  - Một biến thể khác của hình thức này là *ủy quyền yếu* có thể xảy ra khi các mật khẩu được đặt đơn giản hoặc các tài khoản dùng chung được dùng để bảo vệ các tài nguyên CNTT. Với môi trường đám mây loại này có thể dẫn đến những tác động đáng quan tâm tùy thuộc vào phạm vi các tài nguyên CNTT bị truy cập và phạm vi quyền đối với các tài nguyên mà kẻ tấn công có được.



Kẻ tấn công bẻ khóa mật khẩu yếu của người tiêu dùng dịch vụ A. Sau đó người tiêu dùng dịch vụ B do kẻ tấn công thiết kế sẽ dùng mật khẩu của A để tìm cách truy cập vào máy chủ ảo

Những mối đe dọa an ninh đám mây

- **Tấn công ảo hóa** (Virtualization attack): Vì nhà cung cấp đám mây gán quyền quản trị cho người tiêu dùng để truy cập vào các tài nguyên CNTT ảo hóa (như máy chủ ảo), điều này dẫn đến rũi ro gắn liền là người tiêu dùng đám mây có thể lạm dụng truy cập này để tấn công vào các tài nguyên CNTT vật lý phía dưới.

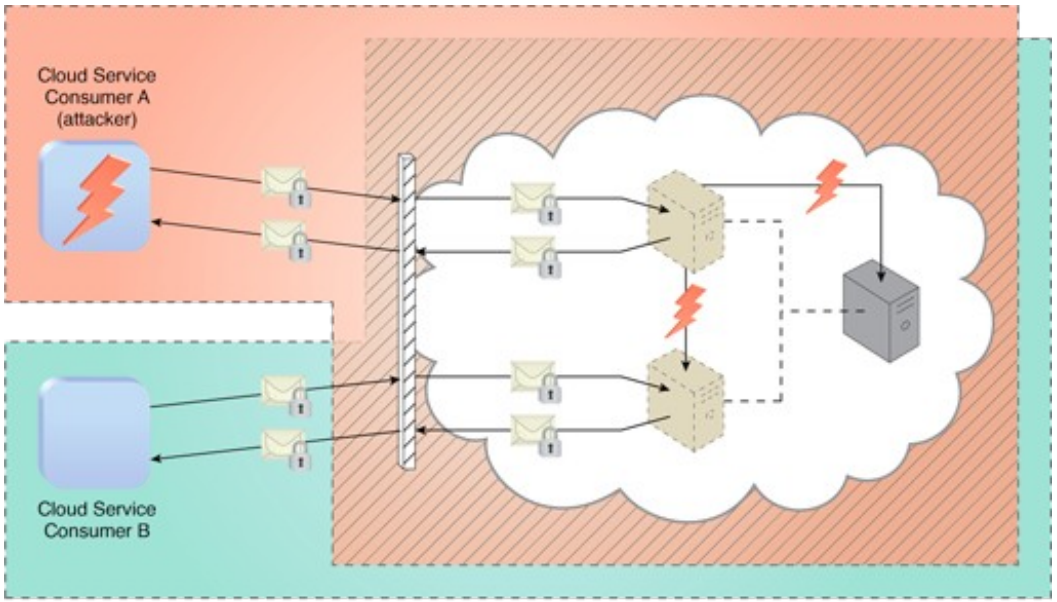


Loại tấn công này khai tác những điểm dễ tổn thương trong các nền tảng ảo hóa để gây nguy hại đến tính riêng tư, sự toàn vẹn và khả năng sẵn dùng của nền tảng đám mây.

Vì trên nền tảng ảo hóa có nhiều người tiêu dùng, loại tấn công này có tác động lan truyền lớn

Những mối đe dọa an ninh đám mây

- **Chồng lấn vùng tin tưởng** (Overlapping trust boundaries):
  - Nếu các tài nguyên CNTT vật lý của một đám mây được chia sẻ bởi nhiều người tiêu dùng dịch vụ đám mây khác nhau thì những người dùng dịch vụ đám mây này có vùng tin tưởng bị chồng lấn.
  - Những người tiêu dùng dịch vụ đám mây độc hại có thể nhắm vào các nguồn tài nguyên CNTT mà chúng chia sẻ cùng vùng tin tưởng.



  - Kết quả là một phần hay toàn bộ người tiêu dùng dịch đám mây khác có thể bị ảnh hưởng bởi cuộc tấn công và những kẻ tấn công có thể sử dụng các tài nguyên CNTT ảo đã thu được để tấn công tác tài nguyên khác trong cùng một vùng tin tưởng

Cám ơn đã lắng nghe !