ĐIỆN TOÁN ĐÁM MÂY - MÔ HÌNH MẠNG MÁY TÍNH internet trong tương lai

TIẾN THÀNH

Mô hình điện toán đám mây dường như ngày càng được ưa chuộng. Tuy nhiên, nghiên cứu gần đây cho thấy vấn đề về bảo mật là rào cản lớn nhất quyết định liệu điện toán đám mây có được sử dụng rộng rãi nữa hay không. Điện toán đám mây hay điện toán máy chủ ảo là mô hình điện toán sử dụng các công nghệ máy tính và phát triển dựa vào mạng Internet. Thuật ngữ "*đám mây*" ở đây chính là mạng Internet và các kết cấu hạ tầng bên trong.

Trên thực tế, điện toán đám mây đơn giản chỉ là một bước tiến khác trong cách mạng công nghệ thông tin. Mô hình đám mây được phát triển dựa trên 3 yếu tố cơ bản gồm máy tinh trung ương, máy chủ/khách và ứng dụng Web. Nhưng bản chất của 3 thành phần này đều tồn tại các vấn đề về bảo mật.

Các vấn đề bảo mật vẫn không ngăn được sự bùng nổ công nghệ cũng như sự ưa chuông điện toán đám mây bởi khả năng giải quyết và đáp ứng các nhu cầu bức thiết trong kinh doanh. Để đảm bảo an toàn cho đám mây điện toán, chúng ta cần nắm được vai trò của nó trong sự phát triển công nghệ. Rất nhiều câu hỏi tồn tại xung quanh những ưu và khuyết điểm khi sử dụng điện toán đám mây trong đó tính bảo mật, hữu dụng và quản lí luôn được chú ý xem xét kĩ lưỡng. Bảo mật là đề tài được thắc mắc nhiều nhất và sau đây là 10 vấn đề hàng đầu được đặt ra để quyết định liệu việc triển khai điện toán đám mây có phù hợp hay không?

1. Khả năng rủi ro khi triển khai mô hình điện toán đám mây?

Dù mang tính chất cá nhân hay công cộng thì chúng ta vẫn không thể hoàn toàn quản lí được môi trường, dữ liệu và kể cả con người. Những thay đổi trong mô hình có thể làm tăng hoặc giảm rủi ro. Những ứng dụng đám mây cung cấp thông tin rõ ràng, các công cụ thông báo tiên tiến và tích hợp với hệ thống sẵn có sẽ làm giảm rủi ro. Tuy nhiên, một vài ứng dụng khác lại không thể điều chỉnh các trạng thái bảo mật, không phù hợp với hệ thống sẽ làm gia tăng rủi ro.

2. Cần phải làm gì để chắc chắn chính sách bảo mật hiện tại tương thích với mô hình đám mây?

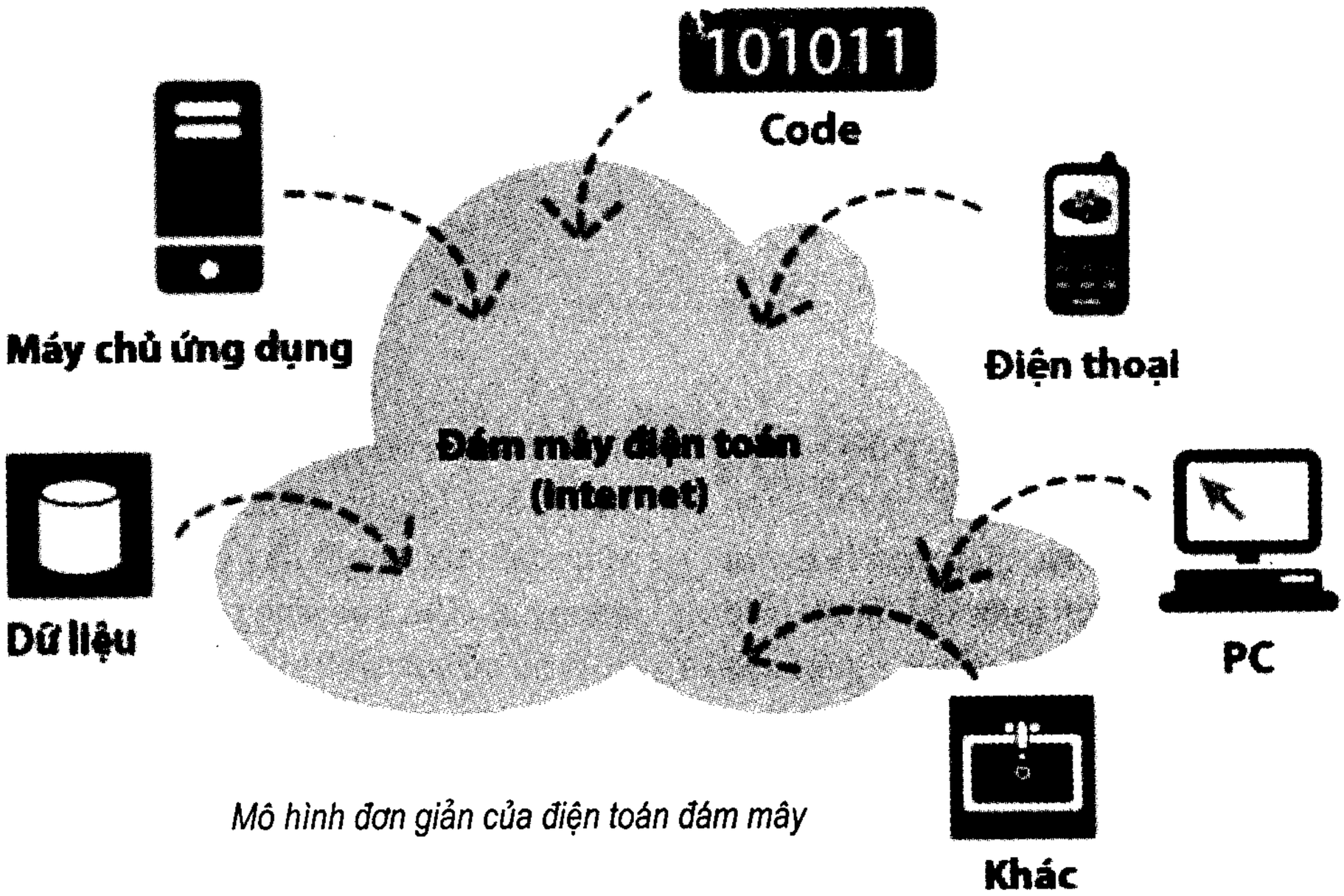
Mỗi thay đổi trong mô hình là mỗi dịp để ta cải thiện tình trạng và chính sách bảo mật. Vì người sử dụng sẽ tác động và điểu khiển mô hình đám mây nên chúng ta không nên tạo ra chính sách bảo mật mới. Thay vào đó là mở rộng chính sách hiện thời để tương thích với các nền tảng kèm theo. Để tay đổi chính sách bảo mật thì ta cần xem xét các yếu tố tương quan như: dữ liệu sẽ được lưu ở đâu, bảo vệ như thế nào, ai được phép truy cập, và cần tuân theo những quy tắc và thỏa hiệp gì.

3. Việc triển khai mô hình đám mây có đáp ứng được yêu cầu ủy thác?

Triển khai mô hình đám mây tác động đến tỉnh rủi ro và ảnh hưởng đến khả năng đáp ứng các quy tắc khác nhau. Một vài ứng dụng đám mây có khả năng thông báo hay báo cáo tình trạng hoạt động mạnh mẽ đồng thời được thiết lập để đáp ứng những yêu cầu thích ứng riêng biệt. Trong khi một số lại quá chung chung và không thể đáp ứng được những yêu cầu chi tiết. Ví dụ như khi chúng ta truy xuất dữ liệu, một thông báo hiện ra cho biết dữ liệu chỉ được lưu trữ trong phạm vi lãnh thổ (server trong nước) thì chúng ta không thể truy xuất được bởi các nhà cung cấp dịch vụ không thể thực hiện yêu cầu này.

4. Liệu các nhà cung cấp dịch vụ sử dụng các chuẩn bảo mật hay theo thực tế kinh nghiệm (SAML, WSTrust, ISO, v.v..)?

Các tiêu chuẩn có vai trò quan trọng trong điện toán đám mây như một sự tương kết giữa các dịch vụ và ngăn tình trạng độc quyền dịch vụ bảo mật. Rất



Mô hình đơn giản của điện toán đám mây

nhiều tổ chức được thành lập nhằm khởi tạo và mở rộng để hỗ trợ trong bước khởi đầu triển khai mô hình.

5. Điều gì sẽ xảy ra nếu vi phạm và xử lý như thế nào?

Khi lên chương trình bảo mật cho mô hình, chúng ta cũng cần lên kế hoạch giải quyết các lỗi vi phạm và tình trạng mất dữ liệu. Đây là yếu tố quan trọng trong các điều khoảng của nhà cung cấp và được thực hiện bởi cá nhân. Chúng ta buộc phải đáp ứng những chính sách và điều lệ do nhà cung cấp đề ra để đảm bảo được hổ trợ kịp thời nếu gặp sự cố.

6. Ai sẽ quan sát và chịu trách nhiệm bảo đảm an toàn cho dữ liệu?

Trên thực tế thì trách nhiệm bảo mật được chia sẻ. Tuy nhiên, ngày nay vai trò này lại thuộc về hệ thống thu thập dữ liệu mà không phải nhà cung cấp. Chúng ta có thể đàm phán để giới hạn trách nhiệm đối với viêc mất mát dữ liệu cụ thể là chia sẻ vai trò này với nhà cung cấp. Nhưng cuối cùng, chúng ta vẫn là người chịu trách nhiệm.

7. Làm thế nào để chắc chắn rằng những dữ liệu phù hợp đã được chuyển vào mô hình?

Để biết được dữ liệu nào đã được chuyển vào đám mây, chúng ta phải hiểu dữ liệu là gì và xây dựng một hệ thống bảo mật phù hợp dựa trên dữ liệu và các ứng dụng. Quy trình này tốn nhiều thời gian để bắt đầu và rất nhiều công ty sử dụng công nghệ chống rò rỉ dữ liệu để phân loại và theo dõi dữ liệu.

8. Làm thế nào để chắc chắn những nhân viên, đối tác và khác hàng được ủy quyền có thể truy xuất dữ liệu và ứng dụng?

Vấn đề về quản lí thông tin truy cập và truy xuất dữ liệu là một thách thức trong bảo mật. Các công nghệ như truy cập chéo miền (federation), hệ thống ảo an toàn, và dự phòng đóng vai trò quan trọng trong bảo mật điện toán đám mây. Hổ trợ đám mây bằng cách mở rộng và bổ sung môi trường có thể giúp giải quyết thách thức này.

9. Dữ liệu và ứng dụng được đăng tải như thế nào, công nghệ bảo mật nào thực hiện công việc này?

Các nhà cung cấp đám mây sẽ cung cấp thông tin này cũng như trực tiếp tác động đến khả năng đáp ứng các yêu cầu của một tổ chức hay cá nhân. Do đó, yếu tố rõ ràng là rất cần thiết đối với chúng ta trước khi đưa ra quyết định.

10. Yếu tố nào khiến chúng ta có thể tin tưởng vào nhà cung cấp?

Rất nhiều yếu tố đề ra để đánh gía độ tin cậy của một nhà cung cấp như: kỳ hạn dịch vụ, hình thức hợp đồng, thủ tục SLAs (Service Level Agreements) thỏa hiệp hợp đồng dịch vụ, chính sách bảo mật, tiểu sử hoạt động, chiến lược, và danh tiếng. Tuy nhiên, vẫn chưa có câu trả lời chính xác cho câu hỏi trên.

T.T