Trường đại học công nghệ - Đại học quốc gia Hà Nội

**Khoa công nghệ thông tin**

Báo cáo tìm hiểu bài báo khoa học đề tài

**Một cách tiếp cận thực dụng để mở rộng quy mô bảo mật trong điện toán đám mây**

Thời gian thực hiện 9/2014

Hà Nội, 13/9/2014

Cloud đang trở thành xu hướng công nghệ phục vụ phát triển cơ sở hạ tầng ảo. Các nhà phát triển dịch vụ và quản trị đang tìm cách cấp quyền truy cập và quản lí ở cấp độ quy mô lớn. Security và Cloud là hai thứ luôn đi liền với nhau. Phương pháp truyền thống để đảm bảo an toàn thông tin không làm việc tốt trong các đám mây. Mô hình bảo mật điện toán đám mây là sẵn sang chấp nhận một cách tiếp cận mới, một cách làm việc mới. An ninh thông tin ngày càng nhanh chóng trở thành các chủ đề thường xuyên hơn do những thách thức từ những xâm nhập thông tin.

Dưới đây là những vấn đề an ninh thông tin trong điện toán đám mây :

# Chia sẻ trách nhiệm

Mô hình an ninh cho [cloud](http://azure.microsoft.com/en-us/support/trust-center/), [service](http://aws.amazon.com/security/) và [providers](https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf) hoạt động theo. Thách thức của mô hình này là nó tác động tới việc bảo mật của bạn với vai trò tiếp cận của họ. An ninh hiện đại với sự linh hoạt và hiểu được vai trò của nó trong mô hình chia sẻ trách nhiệm bạn có thể xây dựng nó thành công.

# The Model

Nhà cung cấp đám mây chịu trách nhiệm về sự an toàn cho các vấn đề : cơ sở vật lý, cơ sở hạ tầng vật lý, cơ sở hạ tầng mạng, lớp ảo hóa. Bạn chịu trách nhiệm về : hệ điều hành, dữ liệu và các ứng dụng. Mô hình đã phân chia chức năng. Nó tăng cường an ninh cho bạn bằng cách di chuyển đến các đám mây công cộng. Và giảm một nửa khối lượng công việc bảo mật.

[Big](http://aws.amazon.com/solutions/case-studies/), [name](https://cloud.google.com/customers/) và [organizations](http://azure.microsoft.com/en-us/case-studies/) đang di chuyển khối lượng công việc nhạy cảm vào các đám mây. Chia sẻ khối lượng công việc cho phép cung cấp an ninh chất lượng cao với cùng một nguồn lực.

# Tin tưởng nhưng cần xác minh

Bạn cần xác minh nhà cung cấp đang nắm giữ thỏa thuận và cung cấp dịch vụ an ninh. Bạn không phải là khách hang duy nhất của nhà cung cấp dịch vụ. Các nhà lãnh đạo dịch vụ này áp dụng cách minh bạch về chia sẻ thông tin gần. Họ cung cấp thông tin về dịch vụ bảo mật và tuân thủ. Những công cụ của nhà cung cấp giúp bạn an toàn trong khu vực trách nhiệm của bạn. FireWall điều khiển máy ảo và bạn phải triển khai đúng cách.

# Trong thực tế

Ví dụ một PCI kiểm toán, bạn cần cung cấp một dịch vụ đám mây cho việc kiểm toán của mình. Bạn cần xác nhận quyền điều khiển của họ. Bây giờ, bạn không phải là khách hàng duy nhất. Bạn có thể kiểm tra bảo mật áp dụng cho hệ điều hành, ứng dụng và dữ liệu của bạn. Đây là mô hình chia sẻ trách nhiệm hành động. Nó làm đơn giản hóa cách thức thủ tục di chuyển lên đám mây.

# Shifting Controls

Chúng ta cố gắng tìm kiếm và thể hiện kinh nghiệm với những thách thức mới, triển khai cùng một bộ kiểm soát an ninh theo công thức dành cho thảm họa an ninh.

# The Wall

Thiết kế “[zones](https://www.cse-cst.gc.ca/its-sti/publications/itsg-csti/itsg22-eng.html)” cho tạo ra bức tường mạnh mẽ xung quanh dữ liệu. Dữ liệu được duy trì bảo mật cao ở một môi trường đầy biến động. An ninh trong đám mây là di chuyển điều khiển tương tự cho máy ảo. Cho phép sử dụng quy tắc nhỏ hơn để thiết lập sự kiểm soát khi nó đang chạy. Di chuyển điều khiển cho máy ảo cho phép triển khai phong phú hơn các chính sách điều khiển, là điều quan trọng trong môi trường biến động theo minute-to-minute.

# Giữ Tabs

Khi di chuyển lên đám mây, chúng ta đã chuyển một số ít các điều khiển đến hàng trăm, hàng ngàn các điều khiển. Điều này tạo ra hai xu hướng : triển khai và quản lý.

# Triển khai

Trong đám mây, thách thức vật lý đã biến mất, bạn có thể triển khai một hay hàng ngàn ứng dụng. Bạn cũng cần đơn giản hóa cách thức triển khai ứng dụng trong các đám mây để tránh trường hợp rối. Bạn cần ưu tiên triển khai ( an ninh nên là điều áp dụng đầu tiên ) thay vì tạo ra thách thức mới.

# Quản lý

Bạn cần phải có một phương thức quản lý từ đơn vị trung tâm. Đội ngũ an ninh của bạn chỉ cần xem xét vấn đề an ninh của một máy chủ web thay vì hàng trăm máy chủ web. Tập trung và quản lí tự động là phương pháp hợp lí để giải quyết thách thức kiểm soát an ninh.

# Nhanh hơn, mạnh hơn

Hệ thống máy tính làm tốt nhiệm vụ tự động. Bạn hãy tận dung điều này và tự động hóa triển khai và kiểm soát an ninh, điều này cho phép bạn tập trung vào phân tích và tăng khả năng kiểm soát an ninh.

Tóm tắt từ bài viết của tác giả : Mark Nunnikhoven, phó chủ tịch Cloud and Emerging Technologies tại Trend Micro. *Tham khảo tại :* [*InfoQ.com*](http://www.infoq.com/articles/cloud-security-at-scale)