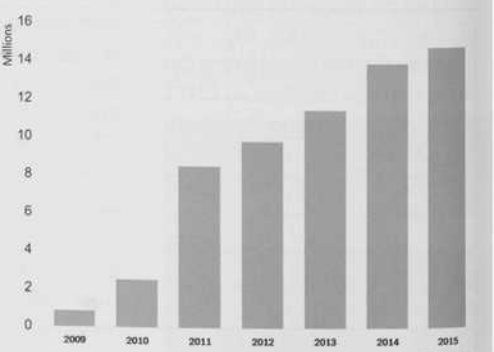
Quản lý an ninh mạng hợp tác

DƯƠNG THỊ THANH TÚ,
NGUYỄN TUẤN NGỌC,
NGUYỄN THỊ BÍCH PHƯỢNG

TRONG MỘT THỜI GIAN DÀI, CHÍNH SÁCH AN NINH VÀ KỸ THUẬT BẢO MẬT MẠNG LÀ MỘT CHỦ ĐỀ NGHIÊN CỨU LỚN CHO CÁC NHÀ NGHIÊN CỨU. TUY NHIÊN, VIỆC TÌM HIỂU VỀ VẤN ĐỀ QUẢN LÝ AN NINH MẠNG, ĐẶC BIỆT LÀ QUẢN LÝ BẢO MẬT TRONG MÔI TRƯỜNG MẠNG MỞ ÍT ĐƯỢC QUAN TÂM. BÀI BÁO ĐỀ CẬP ĐẾN VẤN ĐỀ NÀY, QUA ĐÓ GIỚI THIỆU GIẢI PHÁP QUẢN LÝ AN NINH MẠNG HỢP TÁC TRONG MÔI TRƯỜNG MẠNG MỞ NHƯ HIỆN NAY.

1. Giới thiệu chung

Trong những năm gần đây lĩnh vực CNTT và Truyền thông đã có nhiều bước tiến mạnh mẽ. Tốc độ truyền dẫn dữ liệu ngày một nhanh hơn, khả năng kết nối ngày một mạnh mẽ hơn, khả năng tính toán và lưu trữ dữ liệu cũng ngày càng được nâng cao, đặc biệt là trong trí tuệ nhân tạo. Những bước tiến đáng kể ấy đang đáp ứng được tốt các yêu cầu từ phía người dùng trong thời điểm hiện tại. Tuy nhiên, khi các yêu cầu của người dùng về dung lượng và tốc độ đã được đáp ứng một cách đầy đủ thì một yêu cầu khác lại nảy sinh và ngày càng cấp thiết hơn: an ninh và quản lý an ninh trong môi trường mạng mở.



Hình 1: Thống kê số lượng mã độc được phát hiện trong giai đoạn 2009 - 2015 theo Kaspersky Lab

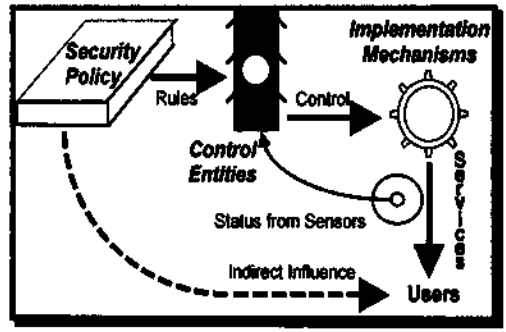
Gần đây tỉ lệ gia tăng của các mã độc ngày càng mạnh mẽ, như theo thống kê của Kapersky Lab (Hình 1) số lượng mã độc tăng 1600% từ năm 2009 đến năm 2015, gây mất an toàn thông tin không chỉ cho các cá nhân mà rất nhiều tổ chức, doanh nghiệp phải đau đầu [1]. Hơn thế nữa, sự tấn công của các tin tặc cũng ngày càng gia tăng và nguy hiểm. Có thể liệt kê hàng loạt vụ nghiêm trọng không chỉ liên quan đến an ninh thông tin mà còn ảnh hưởng đến an ninh chính trị, kinh tế, xã hội như vụ tấn công ngày 29/7/2016 gây mất an toàn, anh ninh sân bay Nội Bài và Tân Sơn Nhất; vụ việc Mossack Fonseca làm rò rỉ 2,6 TB dữ liệu liên quan tới tài sản và thuế của nhiều nhân vật nổi tiếng; hay vụ bê bối do lộ các email của ứng cử viên tổng thống Mỹ Hillary Clinton... Chính vì thế, quản lý an ninh để đảm bảo an ninh thông tin là một công việc tối quan trọng khi con người đang ngày cố gắng số hoá toàn bộ thông tin có được, để thuận tiện cho quá trình lưu trữ và truyền tải trên môi trường mạng công cộng, chia sẻ.

Quản lý an ninh lâu nay đã được coi là một chức năng phụ của quản lý mạng, là một trong năm khu chức năng được định nghĩa trong khuôn khổ quản lý OSI (Open System Interconnection). Theo truyền thống, quản lý an ninh đã được xem như là một trường hợp đặc biệt của mạng lưới quản lý. Tuy nhiên, trong thực tế, bảo mật và quản lý phụ thuộc lẫn nhau bởi bản chất của chúng, mỗi đối tượng cần các dịch vụ khác nhau. Quản lý an ninh và bảo mật của quản lý là các khía cạnh khác nhau của cùng một vấn đề. Bảo mật của quản lý là một điều kiện tiên quyết, đảm bảo độ tin cậy cao cho các ứng dụng an toàn, đặc biệt là quản lý của bảo mật. Đây gọi là an ninh quản lý trước khi quản lý các yêu cầu an ninh. Trong khi đó, quản lý an ninh là để đảm bảo rằng các biện pháp an ninh hoạt động cân bằng với điều kiện hiện nay và tuân theo các chính sách bảo mật [2].

2. Thách thức trong việc quản lý an ninh mạng

Giải pháp an ninh chung là cố gắng thiết lập chu vi hoặc lớp bảo vệ để lọc những dữ liệu đi vào hoặc ra. Nhiều lớp và điểm truy cập làm cho mạng lưới an ninh mạnh hơn. Mức độ của mối đe dọa đến nguồn tài nguyên và dữ liệu trong một hệ thống làm cho hoạt động quản lí an ninh trở nên quan trọng với nhiệm vụ phân phối hoạt động.

Một chương trình bảo mật mạnh hay yếu phụ thuộc vào sự đúng đắn, đầy đủ và độ tin cậy của ba thành phần liên quan. Đó là chính sách bảo mật, cơ chế thực hiện và các biện pháp đảm bảo. Hình 2 cho thấy các mối quan hệ giữa các thành phần và các người dùng đầu cuối. Chính sách bảo mật thiết lập các hướng dẫn quy trình hoạt động và kỹ thuật bảo mật chống lại rủi ro an ninh với các điều khiển và biện pháp bảo vệ. Chính sách an ninh đã trực tiếp tác động đến các quy tắc và lập chính sách hành động để đảm bảo các hoạt động đúng đắn khi thực hiện cơ chế. Chính sách này có ảnh hưởng gián tiếp đến người sử dụng, họ thấy an ninh ứng dụng và truy cập vào dịch vụ, chứ không phải truy cập các chính sách.



Hình 2: Các thành phần bảo mật

Mục tiêu của quản lý bảo mật là để áp dụng và thực thi chính sách an ninh phù hợp trên ranh giới của hệ thống và trong suốt với người dùng. Đầu tiên, một đặc điểm kỹ thuật đầy đủ và phù hợp cho chính sách phải được xác định, độc lập với việc thực hiện. Thứ hai là một kế hoạch thống nhất để thực thi các chính sách bảo mật áp dụng bằng cách sử dụng công cụ có sẵn, quy trình và cơ chế. Nhiệm vụ khó khăn trong việc đạt được một trạng thái "bảo mật" không phải việc thu thập các công cụ cần thiết mà

là việc lựa chọn và lồng ghép những quyền để cung cấp một chuỗi toàn diện và đáng tin cậy về an ninh.

Sự phát triển nhanh chóng của ngoại cảnh nguy hiểm, ngoài những thay đổi trong mạng lưới và kiến trúc an ninh, khiến việc quản lý an ninh mạng ngày nay trở lên khó khăn và phức tạp hơn so với vài năm trước đây. Chính sách quản lý bảo mật trong những môi trường phức tạp có thể bị lỗi và tốn quá nhiều thời gian, đặc biệt nếu giải pháp quản lý làm việc chậm, hoặc hạn chế trong việc kiểm soát và mức độ chi tiết thấp. Việc quản lý chính sách kém có thể dẫn đến sai cấu hình bảo mật, làm cho mạng dễ bị ảnh hưởng bởi các mối đe dọa phức tạp và không tuân thủ quy định. Chính vì thế, việc triển khai nhất quán các chính sách bảo mật, cũng như áp dụng phương thức quản lý hiệu quả từ mức ứng dụng đến cơ sở hạ tầng, có ý nghĩa rất quan trọng trọng việc đảm bảo an ninh cho hệ thống [3].

3. Giải pháp quản lý an ninh mạng hợp tác

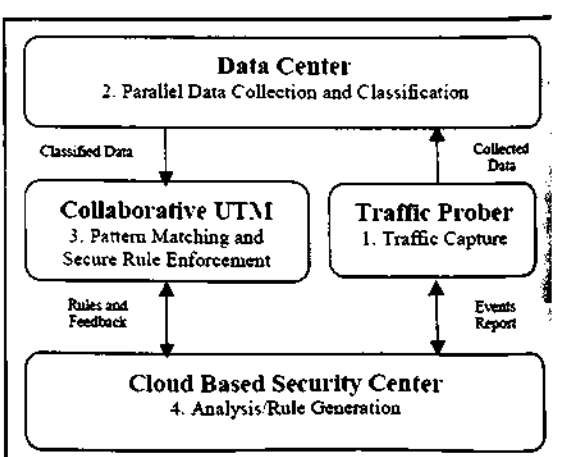
Quản lý an ninh có hai vai trò quan trọng là giám sát và kiểm soát. Giám sát liên quan đến việc thu thập dữ liệu, nhằm cung cấp cái nhìn sâu sắc đối với hệ thống cho dù hoạt động an ninh đạt được chính sách bảo mật theo yêu cầu bởi thiết kế hệ thống. Trạng thái biểu diễn có thể ở dạng thời gian thực. Tần số và độ chi tiết của dữ liệu thu thập nhất thiết phải cân bằng với khối lượng dữ liệu của lưu lượng mạng và khả năng xử lý của thành phần giám sát. Kiểm soát trong quản lý an ninh là cung cấp một phương tiện để điều chỉnh mức độ giám sát an ninh và biện pháp bảo vệ hoạt động nếu chính sách hiện thời không phù hợp với chính sách bảo mật hoặc mức độ rủi ro mong muốn.

Nhằm cung cấp giải pháp quản lý mạng an toàn và hiệu quả trong môi trường hệ thống mở, hệ thống quản lý bảo mật mạng hợp tác [4] là một giải pháp khá hiệu quả với sự kết hợp của ba hệ thống: Quản lý sự đe dọa hợp nhất UTM (Unified Threat Management); Hệ thống thăm dò lưu lượng; và Trung tâm an ninh dựa trên cơ sở điện toán đám mây.

Hệ thống quản lý an ninh mạng hợp tác ra đời với mục đích nâng cao năng lực quản lý an ninh mạng bằng việc kết hợp các hệ thống UTM như NetSecu của Palo Alto hay Juniper trong kiến trúc 3 lớp tích hợp. Trong đó, các nút NetSecu cơ bản nằm ở lớp thứ 3. Lớp thứ 2 quản lý miền NetSecu, còn lớp 1 là miền quản lý trung tâm, lưu trữ, thiết lập và sử lý các qui tắc, chính sách đảm bảo an ninh cho hệ thống. Hình 3 minh họa toàn bộ thủ tục trong tiến trình quản lý các sự kiện nhằm đảm bảo an ninh mạng. Hệ thống thăm dò lưu lượng được kết hợp với các UTM để nắm bắt dữ liệu về lưu lượng sau đó chuyển tới trung tâm dữ liệu. Trung tâm dữ liệu sẽ phân loại riêng rẽ các dữ liệu lưu lượng này rồi truyền chúng đồng thời tới UTM để đánh giá các sự kiện hoạt động và các yếu tố liên quan đến chính sách bảo mật. Các bản tin vận hành từ các bộ thăm dò và NetSecu sẽ được thu thập và gửi ngược lại trung tâm bảo mật dựa trên cơ sở điện toán đám mây để phân tích và đánh giá nhanh chóng các hành vi nhằm ngăn chặn các tình huống gây mất an toàn có thể xảy ra.

*** UTM hợp tác:**

Như đã trình bày ở trên, NetSecu là ví dụ điển hình cho hệ thống quản lý đe dọa hợp nhất UTM. Nó đảm



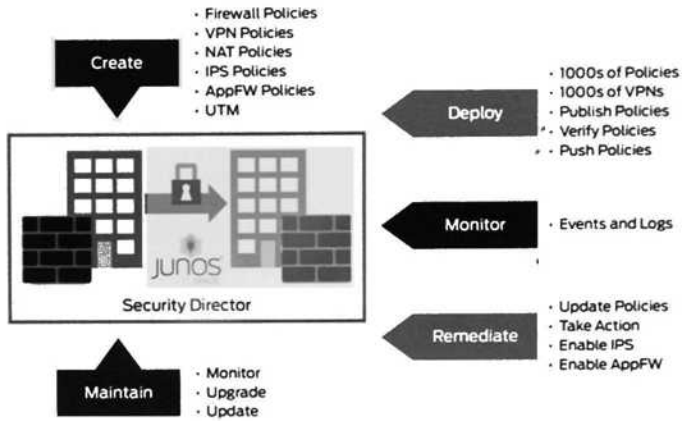
Hình 3: Mô hình hoạt động của hệ thống quản lý mạng hợp tác trong môi trường điện toán đám mây

hiệm vai trò bảo mật mạng
ợp tác: phát hiện được các
ấn công phân tán kết hợp với
iều khiển lưu lượng. Về bản
hất, NetSecu là một khối các
ệ thống bảo mật mạng được
ên kết với nhau, nhằm nhận
iện các sự kiện liên quan
ến bảo mật và phản ứng để
hống lại các cuộc tấn công
heo một cách nhất quán và
hống nhất.

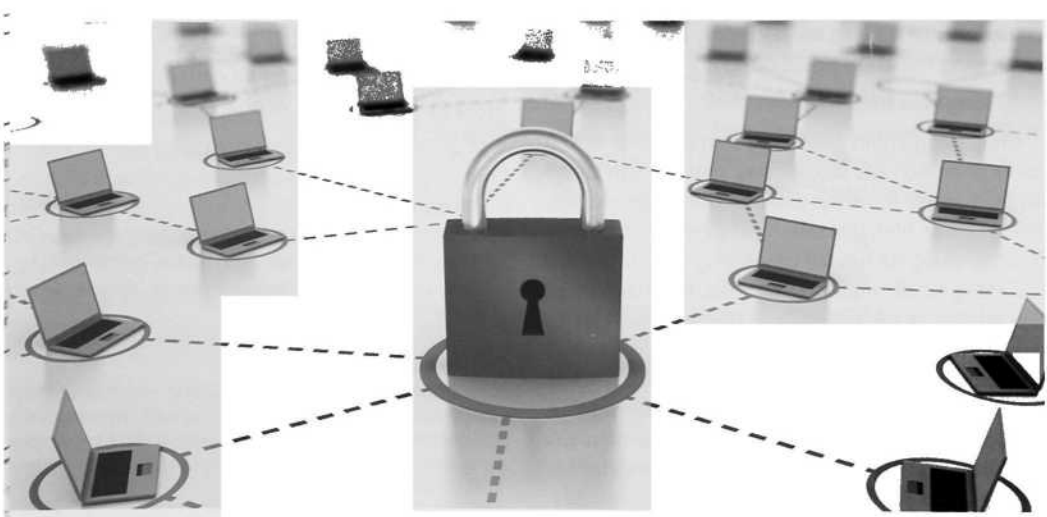
Tính năng: Một nút NetSecu bao gồm các tính năng cơ bản sau:

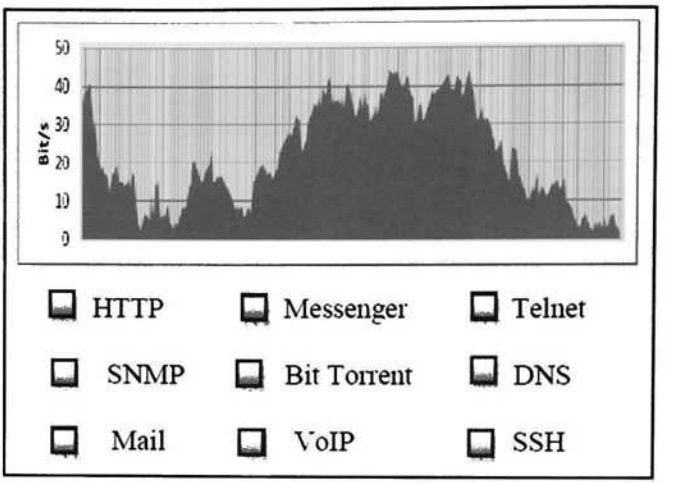
- Truyền lan các phần tử bảo mật.
- Tự động kích hoạt, vô hiệu hóa hay nâng cấp các chức năng an ninh.
- Xây dựng các chính sách hợp tác bảo mật trên miền Internet.

Các thành phần cơ bản: Một nút NetSecu sẽ chứa Bộ thăm dò lưu lượng để ghi lại lưu lượng Internet ở các mức kết nối khác nhau. Bộ điều khiển lưu lượng sẽ điều khiển lưu lượng Internet thông qua các yêu cầu về chất lượng dịch vụ và định dạng giao thức ứng dụng. Phần tử hợp tác sẽ quản lý các phần tử bảo mật dựa trên chương trình lệnh của Trung tâm an ninh. Chương trình báo cáo sẽ thu thập các File log cũng như các sự kiện tiềm ẩn mối đe dọa, đưa ra báo cáo dưới các hình thức đa dạng và thân thiện để người quản lý dễ dàng nắm bắt. Bên cạnh đó, một NetSecu cũng có trình quản lý nội bộ giúp vận hành hệ thống cũng như quản lý các phần tử bảo mật.



Hình 4: Ví dụ về hệ thống quản lý mạng của Juniper





Hình 5: Lưu lượng được giám sát và thu thập tại bộ thăm dò lưu lượng

Nhiệm vụ chính của UTM hợp tác:

• *Bảo vệ liên mạng:* Các lưu lượng trao đổi giữa Internet và mạng riêng của các Doanh nghiệp sẽ được giám sát, lọc bằng các tính năng tiên tiến như tường lửa thế hệ mới, phát hiện xâm nhập và chống vi rút.

• *Bảo vệ máy chủ:* Để bảo vệ nguồn dữ liệu, hệ thống tường lửa được thiết lập, bên cạnh đó là các chính sách truy nhập tới hệ thống máy chủ từ cả phía mạng ngoài lẫn người dùng nội bộ.

*** Trung tâm bảo mật:**

Chức năng chính của Trung tâm bảo mật là khả năng phân tích lưu lượng cũng như các vấn đề về an ninh mạng thu thập được từ Trung tâm dữ liệu. Trung tâm an ninh dựa trên cơ sở điện toán đám mây được sử dụng để lưu trữ một lượng lớn các dữ liệu lưu lượng từ các nguồn khác nhau, tiến hành phân tích để đưa ra các bộ qui luật bảo mật mới cho sự thực thi tại UTM, nhằm quản lý thông tin giữa bot và botmaster. Các qui luật mới sau khi được thực thi sẽ được phản hồi lại hệ thống, phân tích, đánh giá để loại bỏ những qui luật thiếu giá trị, nâng cao hiệu quả của hệ thống. Sau đó tiếp tục được phân phối lại.

*** Bộ thăm dò lưu lượng:**

Là một hệ thống thu gom lượng Internet tại các mức kế khác nhau, khi cần thiết, bộ thă lưu lượng có thể được thiết kế đ trung vào một loại lưu lượng c phát sinh bởi một sự kiện bảo nào đó. Hình 5 mô tả một ví d lưu lượng dữ liệu mẫu được lấy t khoản lưu lượng HTTP. 512MB khối dữ liệu thu thập được kh 40K HTTP URL.

4. Kết luận

Sự mở rộng của Inte kéo theo một số lượng các dụng nhạy cảm yêu cầu bảo mạnh mẽ dẫn đến một sự t trưởng trong nhu cầu về khả n quản lý an ninh. Cũng giống như thương mại t tử, bảo mật thông tin và các ứng dụng phát t nhanh chóng là cần thiết, trong khi cũng cho p sự linh hoạt và mở rộng kiểm soát bảo mật. Tr khi một năng lực quản lý bảo mật hiệu quả có được phát triển và kiểm chứng trên thực tế, bài giới thiệu một giải pháp quản lý an ninh mạng tác sử dụng điện toán đám mây có khả năng p hiện sự tấn công của các mã độc cũng như dễ d phát hiện ra các lỗ hổng an ninh nhờ sự xử lý s song dữ liệu thu thập và phân loại bởi mô hình L hợp tác.

Tài liệu tham khảo:

1. SANTIAGO PONTIROLI, ROBERTO MARTINEZ, "The Tao of and Powershell Malware Analysis", Virus Bulletin Conference, 201

2. PHILIP C. HYLAND, "Management of Network Sec Application", Semantic Scholar, 2016.

3. SUSHMA SETHURAM, "Network Security Manager Juniper Network, September 2016.

4. KRISHNAKUMAR L, NISHA MARIAM VARUGHESE, " Speed Classification of Vulnerabilities in Cloud Computing L Collaborative Network Security Management", 2013 Internat Conference on Advanced Computing and Communication Sys (ICACCS -2013),2013.