ISSN 2354-0575

NGHIÊN CỨU VÀ TRIỂN KHAI HỆ THỐNG GIÁM SÁT MẠNG CHO BỘ Y TẾ

Vũ Xuân Thắng, Trần Đỗ Thu Hà, Đặng Vân Anh
Trường Đại học Sư phạm Kỹ thuật Hưng Yên

Ngày tòa soạn nhận được bài báo: 06/03/2018
Ngày phản biện đánh giá và sửa chữa: 02/05/2018
Ngày bài báo được chấp nhận đăng: 05/06/2018

Tóm tắt:
Bài báo này chúng tôi trình bày quá trình nghiên cứu một số các lỗ hổng bảo tại hệ thống mạng trong bộ Y tế. Từ các kết quả nghiên cứu, nhóm báo đề xuất các giải pháp triển khai hệ thống giám sát mạng phục vụ cho đảm bảo an toàn hệ thống mạng.
Từ khoá: *Network monitoring, IDS protected, IDS Snort.*

1. Đặt vấn đề

Giải pháp hệ thống quản trị mạng (Network Management System) nhằm xây dựng ứng dụng giám sát các hệ thống mạng đang được triển khai và vận hành, với tiêu chí giám sát toàn diện, linh hoạt và thời gian thực hỗ trợ tối ưu cho các nhà vận hành và giám sát hệ thống, thông báo kịp thời các vấn đề xảy ra trọng mạng để hiệu quả hoạt động là tốt nhất.

Với nhiều quốc gia đang phát triển - trong đó có Việt Nam – vấn đề trao đổi dữ liệu y tế giữa các bệnh viện trong nước và với các bệnh viện quốc tế là một vấn đề khá mới mẻ. "Mạng y tế" được hiểu là một hệ thống kết nối nhiều thiết bị y tế với nhau nhằm mục đích truyền dữ liệu y tế giữa các hệ thống trong cùng một bệnh viện, giữa các cơ sở y tế khác nhau, thậm chí giữa các quốc gia trên thế giới. Với đặc thù của ngành, môi trường thông tin trong ngành y tế là một môi trường phức tạp và đa dạng. Ngoài các thông tin hành chính (gồm: các văn bản, quy chế, các quyết định, thông báo, hướng dẫn...) còn có các thông tin phục vụ khám chữa bệnh cũng phải được quản lý như: [1]

• Thông tin về quản lý hành chính, quản lý nhân sự, quản lý đội ngũ y bác sĩ, quản lý vật tư, quản lý tài chính...

• Thông tin bệnh viện: hồ sơ bệnh án (xét nghiệm huyết học, sinh hoá, vi sinh, tế bào...)

• Thông tin về chẩn đoán chức năng (Điện tim ECG, điện não EEG, hô hấp...), thông tin về hình ảnh (X-quang, siêu âm, CT, MRI...)

Để đội ngũ làm nhiệm vụ phản ứng với các sự cố hệ thống hay các chuyên gia về bảo mật có thể thực hiện các công việc cần có sự trợ giúp từ các hệ thống giám sát mạng. Một giải pháp của hệ thống giám sát mạng cần đáp ứng được những tiêu chí và cung cấp các chức năng chính sau [4, 5]:

• Giám sát liên tục và thống nhất: Các vấn đề, giám sát tính sẵn sàng và dung lượng tài nguyên (Event, performance, topology, inventory…), báo cáo thống kê.

• Giám sát các chương trình phần mềm, dịch vụ hoạt động trên hệ thống.

• Giám sát hiệu năng hoạt động của máy chủ cơ sở dữ liệu, máy chủ email.

• Xác định nguồn lưu lượng đi ra/vào hệ thống, thu thập thông tin cụ thể, chính xác.

• Thực hiện quản lý và giám sát các hệ thống máy chủ ảo hoá.

• Liên kết sự kiện và phân tích nguồn gốc lỗi: tự động thu thập các thông tin về sự kiện, phân tích lỗi thông qua các sự kiện và cảnh báo từ các nguồn giám sát.

• Giải pháp tích hợp: các thành phần của giải pháp có khả năng mở rộng và tích hợp với các thành phần khác (reporting, trouble ticket…)

2. Nội dung cần giám sát đối với hệ thống thông tin trong y tế

2.1. Khái quát tình hình an toàn bảo mật của các hệ thống CNTT tại Việt Nam

Theo báo cáo của các cơ quan chức năng, tình hình an toàn bảo mật mạng của các hệ thống công nghệ thông tin tại Việt Nam tiếp tục diễn biến phức tạp. Báo cáo của hãng bảo mật Kaspersky và Symantec cho thấy, Việt Nam đứng thứ 3 (3,96%) sau Nga (40%) và Ấn Độ (8%) về số dùng di động bị mã độc tấn công nhiều nhất trên thế giới, thứ 6 trên thế giới về số lượng địa chỉ IP trong nước được dùng trong các mạng máy tính ma tấn công nước khác; thứ 7 trên thế giới về phát tán tin nhắn rác và đứng thứ 12 trên thế giới về các hoạt động tấn công mạng (2013) [6]. Trong năm 2012-2013, Bộ Công an đã phát hiện gần 6.000 lượt cổng thông tin, trang tin điện tử của Việt Nam.

Hiệp hội An toàn thông tin Việt Nam (VNISA) đã công bố báo cáo Kết quả khảo sát thực trạng an toàn thông tin Việt Nam năm 2015 và đưa ra Chỉ số An toàn thông tin Việt Nam 2015 - VNISA Index

2015. Theo đó, chỉ số trung bình của Việt Nam là 46,5%, tuy ở dưới mức trung bình và vẫn còn sự cách biệt với các nước như Hàn Quốc (hơn 60%), song so với năm 2014 thì đã có bước tiến rõ rệt (tăng 7,4%).[2]

Về việc sử dụng các công nghệ, biện pháp kỹ thuật để bảo đảm ATTT, các TC/DN thường sử dụng một trong những biện pháp sau đây: hệ thống phòng chống tấn công DoS/DDoS; hệ thống phát hiện xâm nhập (IDS/IPS) trong mạng; tường lửa (Network Firewall), phần mềm chống virus, lọc nội dung Web; bộ lọc chống thư rác (Anti-Spam), kiểm soát truy cập; bảo mật mạng không dây, hệ thống quản lý sự kiện ATTT (Security Incident & Event Management - SIEM). Trong các biện pháp trên, việc sử dụng phần mềm chống virus (Anti-Virus) được các TC/DN sử dụng nhiều nhất, với 22% các TC/DN. [6]

2.2. Hiện trạng việc ứng dụng CNTT trong Y tế

Trong những năm qua công nghệ thông tin trong ngành y tế đã đạt được một số thành quả quan trọng như: ứng dụng công nghệ thông tin vào quản lý bệnh viện, các hệ trợ giúp ra quyết định lâm sàng, khám chữa bệnh từ xa (telemedicine)... Tuy nhiên việc ứng dụng, nghiên cứu và đào tạo công nghệ thông tin y tế trong những năm qua vẫn chưa đáp ứng được nhu cầu phát triển ngày càng tăng của công nghệ thông tin y tế ở Việt Nam. Các thành quả ứng dụng công nghệ thông tin chủ yếu tập trung ở các đơn vị tuyến trung ương, tại các đơn vị tuyến dưới việc ứng dụng Công nghệ Thông tin còn rất hạn chế.

2.2.1. Hạ tầng kỹ thuật CNTT trong ngành

**** Tại cơ quan Bộ Y tế***

Tất cả các Vụ, Cục, Văn phòng Bộ, Tổng cục đã kết nối mạng nội bộ và kết nối Internet tốc độ cao: đạt 100%; Hệ thống đường truyền Internet tốc độ cao: 06 (trong đó 02 là FTTH: 10 MB, 02 là SHDSL 2MB và 4 MB); Tỷ lệ trung bình máy tính/CBCC: 100% (trừ khối hành chính - quản trị - bảo vệ). Các đơn vị được trang bị từ ngân sách nhà nước và tài trợ của các dự án trong và ngoài nước; Chưa kết nối mạng diện rộng WAN;

Hệ thống website: Bộ Y tế đã đưa vào sử dụng cổng thông tin điện tử nâng cấp từ trang tin điện tử www.moh.gov.vn.

**** Tại các đơn vị sự nghiệp y tế***

Tại Trung ương, cơ sở y tế thuộc Bộ Y tế đã có 100% các đơn vị trực thuộc Bộ có mạng LAN và kết nối Internet tốc độ cao, bình quân mỗi mạng có trên 110 máy tính, 74% cán bộ y tế sử dụng máy tính thông thạo trong công việc, 58% có hệ thống e-mail riêng và 43% có hệ thống bảo mật, 53% có hệ thống backup dữ liệu;

Tại các tỉnh: 95,3% Văn phòng Sở có mạng LAN và kết nối được Internet tốc độ cao, 61% cán bộ của Sở Y tế có hệ thống e-mail riêng, 26% có hệ thống bảo mật và 24% có hệ thống lưu trữ dữ liệu; Trong 280 bệnh viện địa phương được điều tra có 151 (52,9%) bệnh viện tỉnh có LAN và 81% kết nối được Internet tốc độ cao, 37,2% bệnh viện huyện có mạng LAN và 65% kết nối Internet;

Tại các trạm y tế: số lượng trạm có máy tính phục vụ tra cứu thông tin là 8% và đã nối mạng Internet đạt 0,05%; Đường truyền: Một số ít cơ sở y tế (chiếm 2%) có đường truyền riêng, trên 70% đơn vị sử dụng đường truyền ADSL và còn nhiều nơi vẫn truy cập Internet bằng Dial-up; 100% các trường Đại học, Cao đẳng Y - Dược có mạng LAN, kết nối Internet và Website;

Trang thông tin điện tử: 16% Sở Y tế có địa chỉ website trên Internet, 27% đơn vị trực thuộc Bộ Y tế có trang web. Các cơ sở y tế địa phương kết nối Internet ước đạt 30%; gần 80 đơn vị trực thuộc các sở y tế có Web- site trên Internet.

2.2.2. Yêu cầu về đảm bảo an toàn thông tin đối với dữ liệu Y tế

Để đảm bảo an toàn, các hệ thống công nghệ thông tin y tế phải được kiểm tra, thử nghiệm trước khi được áp dụng trong bệnh viện và sau khi áp dụng sẽ được đánh giá để đảm bảo an toàn và chất lượng trong chăm sóc và điều trị người bệnh. Công nghệ thông tin y tế có thể cải thiện một cách đáng kể an toàn người bệnh thông qua khả năng tự động hóa và hỗ trợ sự kết nối trong công việc, giúp truyền các thông tin về sức khỏe người bệnh một cách dễ dàng, liên tục và cung cấp các cơ chế an toàn giúp giảm nguy cơ sai sót.

Với tầm quan trọng và nhạy cảm của cơ sở dữ liệu ngành Y tế, cũng như để bảo vệ an toàn cho hạ tầng công nghệ thông tin và các phần mềm nghiệp vụ của ngành y. Ngày 29/12/2014 Bộ Y tế ban hành Thông tư 53/2014/TT-BYT về Quy định điều kiện hoạt động y tế trên môi trường mạng. Trong đó nhấn mạnh: Có chính sách về an toàn, bảo mật thông tin phù hợp với quy định về an toàn, bảo mật hệ thống công nghệ thông tin của Nhà nước và quy chế an toàn bảo mật thông tin của cơ quan. Vấn đề an ninh, an toàn mạng trong nội bộ cơ quan, đơn vị ngành cần đảm bảo các vấn đề:

• Bảo đảm có biện pháp kỹ thuật cho phép kiểm soát các truy cập đối với hệ thống mạng;

• Có biện pháp phát hiện và phòng chống xâm nhập, phòng chống phát tán mã độc hại cho hệ thống;

• Có chính sách cập nhật định kỳ các bản vá lỗi hệ thống, cập nhật cấu hình cho các thiết bị;

• Có biện pháp bảo đảm an toàn thông tin

cho các máy trạm khi kết nối với môi trường mạng;

• Bảo đảm an toàn, an ninh về mặt vật lý tại vị trí đặt các hệ thống máy chủ;

• Các trang thiết bị mạng, an ninh, bảo mật, phần mềm chống virus, công cụ phân tích....

Trong trường hợp hệ thống gặp sự cố về vấn đề kĩ thuật hay do điều kiện ngoại cảnh tác động như bị hacker tấn công, mã độc lây nhiễm…quản trị viên hệ thống cần đưa ra những biện pháp khắc phục kịp thời và điều tra nguyên nhân, nguồn gốc xảy ra sự cố để có phương án triệt để. Thông tư của Bộ Y tế cũng quy định các đơn vị trong ngành cần thiết lập:

• Quy trình quản lý sự cố, trong đó phải quy định rõ trách nhiệm của các bộ phận liên quan, trường hợp hạ tầng công nghệ thông tin được thuê ngoài thì đơn vị cung cấp dịch vụ phải cung cấp quy trình xử lý sự cố;

• Định kỳ rà soát, cập nhật các sự cố và phương án xử lý cho quy trình quản lý sự cố;

• Áp dụng các giải pháp kỹ thuật để phát hiện, xử lý kịp thời các cuộc tấn công vào hệ thống mạng;

• Có biện pháp phòng chống rủi ro và thảm họa công nghệ thông tin.

2.3. Mục tiêu việc giám sát hệ thống thông tin trong Y tế

**** Quản lý tập trung:***

Nhiều tổ chức triển khai hệ thống giám sát mạng với một mục đích duy nhất: tập hợp các dữ liệu thông qua một giải pháp nhật ký tập trung.

Một ưu điểm khi sử dụng các hệ thống giám sát đó là: các hệ thống này đều hỗ trợ sẵn các mẫu báo cáo phù hợp với các chuẩn quốc tế như Health Insurance Portability and Accountability Act (HIPAA) cho Y tế, Payment Card Industry Data Security Standard (PCI DSS) và Sarbanes-Oxley Act (SOX).

**** Giám sát an toàn mạng:***

Hệ thống này có thể phát hiện ra các sự cố mà các thiết bị thông thường không phát hiện được. Thứ nhất, rất nhiều thiết bị đầu cuối có phần mềm ghi lại sự kiện an ninh nhưng không tích hợp khả năng phát hiện sự cố. Bên cạnh đó còn cho thấy sự tương quan sự kiện giữa các thiết bị. Bằng cách thu thập sự kiện của toàn tổ chức, hệ thống giám sát có thể thấy được nhiều phần khác nhau của các cuộc tấn công thông qua nhiều thiết bị và sau đó tái cấu trúc lại chuỗi sự kiện và xác định cuộc tấn công ban đầu là gì và nó đã thành công hay chưa.

**** Tăng cường khả năng xử lý sự cố***

Một lợi ích khác của các hệ thống giám sát trong mạng đó là gia tăng đáng kể hiệu quả việc xử lý sự cố, tiết kiệm đáng kể thời gian và nguồn lực cho các nhân viên xử lý sự cố.

2.4. Giải pháp đảm bảo bảo an toàn hệ thống mạng cho bộ Y tế

2.4.1. Các giải pháp đảm bảo tính bảo mật và toàn vẹn của thông tin

Hàm băm mật mã

Hàm băm là nền tảng cho nhiều ứng dụng mã hóa. Có nhiều thuật toán để thực hiện hàm băm, trong số đó, phương pháp SHA-1 và MD5 thường được sử dụng khá phổ biến từ thập niên 1990 đến nay [4].

Hàm băm mật mã phải có khả năng chống lại các loại tấn công mật mã, tối thiểu phải đảm bảo có 3 tính chất sau:

● Kháng tiền ảnh (Pre-image resistance): Với một mã băm h bất kỳ, khó tìm được một thông điệp m nào mà h = hash(m).

● Kháng tiền ảnh thứ hai (Second pre-image resistance): Với một thông điệp m_1 bất kỳ, khó tìm được một thông điệp thứ hai m_2 sao cho $m_1 \neq m_2$ và $hash(m_1) = hash(m_2)$.

● Kháng xung đột (Collision resistance): Khó tìm được một cặp thông điệp m_1 và m_2 sao cho $m_1 \neq m_2$ và $hash(m_1) = hash(m_2)$.

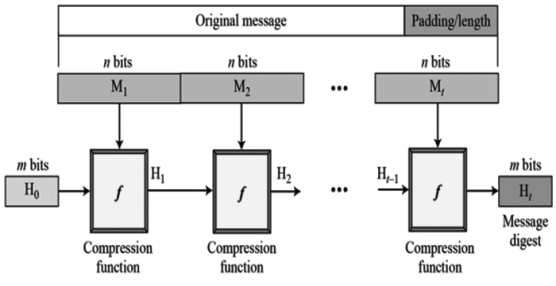
Thực hiện:

Bước 1: Gọi H là trạng thái có kích thước n bit, f là "hàm nén" thực hiện thao tác trộn khối dữ liệu với trạng thái hiện hành.

Bước 2: Khởi gán H_0 bằng một vector khởi tạo nào đó.

Bước 3: $H_i = f(H_{i-1}, M_i)$ với i = 1, 2, 3, …,s

Khi đó: H_s chính là thông điệp rút gọn của thông điệp M ban đầu.



Hình 2.1. *Sơ đồ Merkel-Damgard*

Giải thuật mạng neuron nhân tạo một đầu vào

Mạng neuron được đề cập ở đây là mạng neuron nhân tạo (Artificial Neural Network) là một mô phỏng xử lý thông tin được nghiên cứu ra từ hệ thống thần kinh của sinh vật giống như bộ não để xử lý thông tin.

Việc thu thập tự động thông tin từ các tín hiệu điều khiển trên mạng thông qua việc theo dõi các cổng giao tiếp, quá trình giải mã các file Long để tập hợp dữ liệu đầu vào:

Đầu vào vô hướng p được nhân với trọng số w cho wp tạo thành một số hạng gửi đến bộ cộng (Σ). Một đầu vào khác là 1 được nhân với độ chênh b rồi chuyển đến bộ cộng. Đầu ra của bộ cộng thường được xem như là net-input trở thành đầu vào cho hàm truyền f sinh ra đầu ra neuron là:

a: a = f(wp + b)

Bias giống trọng số ngoại trừ luôn có đầu vào hằng số là 1. Có thể bỏ qua bias nếu thấy không cần thiết.

Giải thuật mạng neuron nhân tạo nhiều đầu vào

Các đầu vào độc lập p_1, p_2, p_3, ... ,p_R được gán trọng số bởi các thành phần w_{11}, w_{12},..., w_{1R} của ma trận trọng số W.

Ở đây: $W = [w_{11}, w_{12},..., w_{1R}]$; $p = [p_1, p_2, p_3, ... ,p_R]$

Như vậy:

$n = w_{11}p_1+w_{12}p_2+w_{13}p_3+ ...+w_{1R}p_R+b = Wp+b$ (2.1)

Trong đó ma trận W cho trường hợp 1 neuron chỉ có một hàng. Vậy:

a = f(n) = f(Wp + b). (2.2)

Quy ước chỉ số của các thành phần w_{ij} của ma trận trọng số như sau: Chỉ số đầu (i) biểu thị neuron đích được gán trọng số; chỉ số sau (j) biểu thị tín hiệu nguồn cung cấp cho neuron. Như vậy w_{ij} nói lên rằng trọng số này kết nối đến neuron thứ i từ tín hiệu nguồn thứ j (từ p_j → neuron i).

Thuật toán Rabin Fingerprint

Thuật toán Rabin Fingerprint là một trong nhiều thuật toán Fingerprint thực hiện khóa công khai sử dụng các đa thức trên một trường giới hạn [10].

Thuật toán được sử dụng trong hệ thống như sau:

- Đầu vào: Tài liệu (trang web công khai)
- Đầu ra: Dấu vân tay tài liệu (các giá trị băm của tài liệu đó)

Bước 1: Bắt đầu.

Bước 2: Xử lý văn bản, xoá hết tất cả khoảng trắng và các kí tự đặc biệt (như: <,>, %,!, …).

Bước 3: Chia khối văn bản đã xử lý đó thành các chuỗi con có độ dài K.

// Số lượng chuỗi con có độ dài K và số lượng giá trị băm (mã băm) bằng (m-K+1), với m là kích thước của tài liệu.

Bước 4: Tính toán giá trị băm đối với mỗi chuỗi con bằng cách tính H(P) như sau:

// H(P) là một tuyến tính trong n (n là độ dài của P)

Bước 5: Lưu lại tất cả các giá trị băm của văn bản.

Bước 6: Kết thúc.

Thuật toán Rabin Fingerprint cải tiến

Thuật toán cải tiến được đề xuất trong hệ thống như sau:

Đầu vào: Tài liệu (trang web công khai)

Đầu ra: Dấu vân tay tài liệu (các giá trị băm của tài liệu đó)

Bước 1: Bắt đầu.

Bước 2: Xử lý văn bản, xoá hết tất cả khoảng trắng và các kí tự đặc biệt (như: <, >, %, !, …) từ mã HTML (mã trang web) để thu được một khối văn bản thuần túy (pure text block).

Bước 3: Chia văn bản M thành K khối, mỗi khối con có kích thước là n. K = m/n với m là kích thước của văn bản M, n là số nguyên dương cho trước là kích thước của mỗi chuỗi con.

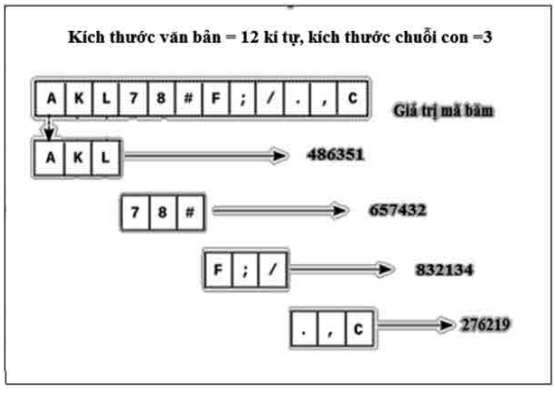
Bước 4: Tính mã băm H(P) cho các chuỗi con như sau:

Khởi tạo:

$T_r = T_{[r..r+n-1]}$;
K=0;
$H_{(S)} = S_{(n)} + 2*S_{(n-1)} + 4*S_{(n-2)} + \ldots + (2n-1)*S_{(1)}$;
While (K<m/n)
{
for (r=K*n; r<=(K*n+n); r++){
$Hp(T_r) = (Hp(T_r) + T_{(r)}) \bmod p$
//Tính gt băm cho các chuỗi con, p là nt lớn.
}
K++;
}

Bước 5: Lưu lại tất cả các giá trị băm của văn bản.

Bước 6: Kết thúc.



Hình 2.2. *Minh hoạ cải tiến giải thuật*

2.4.2. Giám sát hệ thống máy chủ

Để thực hiện công việc giám sát máy chủ, các quản trị viên hệ thống thường sử dụng các phần mềm chuyên dụng được cài đặt trên các máy chủ để theo dõi và gửi thông báo khi sự cố bất thường xảy đến như: chương trình ứng dụng hay dịch vụ bị

ngưng hoạt động, phần mềm bị lỗi, chỉ số CPU tăng quá cao, tỉ lệ sử dụng RAM quá lớn, nhiệt độ của máy chủ tăng quá cao… Một số hình thức giám sát máy chủ phổ biến hiện nay như:

• Giám sát theo thời gian thực: Hình thức này sử dụng các công cụ hiển thị chuỗi liên tục các thông số, mô tả hệ thống.

• Giám sát bằng nhật ký: Hình thức giám sát này cung cấp các thông tin tương tự như giám sát thời gian thực.

Các phân hệ cần được giám sát trên hệ thống máy chủ bao gồm: Bộ vi xử lý, bộ nhớ, việc sử dụng đĩa cứng, trạng thái hoạt động của mạng.

Các thông tin quan trọng mà quản trị viên hệ thống cần quan tâm như:

• Xác thực (Authentication): Các bản tin về sự kiện đăng nhập, đăng ký.

• Phân quyền (Authorization): Thông tin lưu trữ sẽ ghi lại quyền truy cập vào các dịch vụ đặc quyền hoặc hành động đặc quyền.

• Trạng thái các tiến trình: Thực hiện việc lưu trữ sự kiện của quá trình hoạt động của các tiến trình trên một hệ thống.

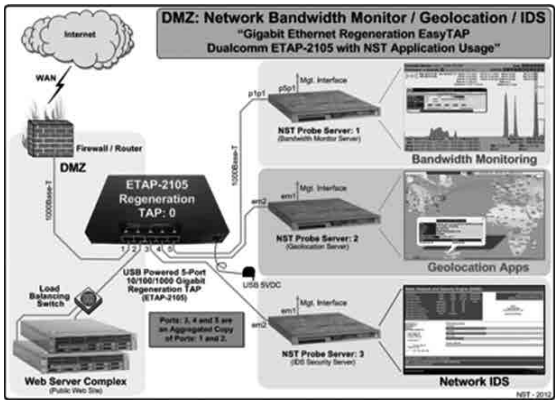
2.4.3. Giám sát hệ thống mạng

Hệ thống giám sát an toàn mạng đóng vai trò quan trọng, không thể thiếu trong hạ tầng công nghệ thông tin (CNTT) của các cơ quan, đơn vị, tổ chức. Hệ thống này cho phép thu thập, chuẩn hóa, lưu trữ và phân tích tương quan toàn bộ các sự kiện an toàn mạng được sinh ra trong hệ thống CNTT của tổ chức. Ngoài ra, hệ thống giám sát an toàn mạng phát hiện kịp thời các tấn công mạng, các điểm yếu, lỗ hổng bảo mật của các thiết bị, ứng dụng và dịch vụ trong hệ thống.Để xây dựng giải pháp hợp lý cho hệ thống giám sát an toàn mạng, các tổ chức, đơn vị có thể triển khai theo một trong ba giải pháp sau:

• Giải pháp quản lý thông tin an ninh.

• Giải pháp quản lý sự kiện an ninh.

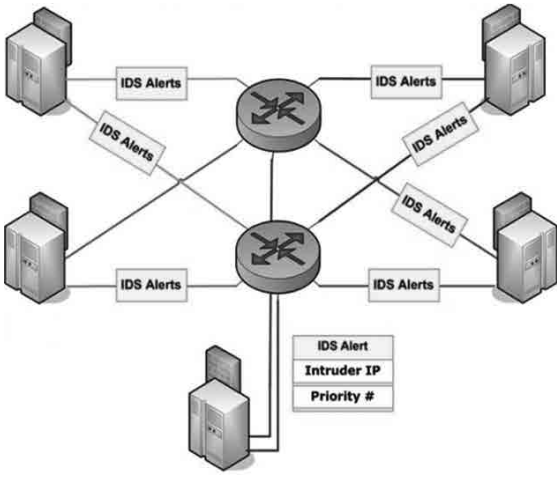
• Giải pháp quản lý và phân tích sự kiện an ninh.



Hình 2.3. *Giải pháp quản lý và phân tích sự kiện an ninh*

2.4.4. Giám sát phát hiện xâm nhập trái phép

Để thực hiện việc giám sát xâm nhập trái phép vào một hệ thống mạng, có nhiều giải pháp đang được các tổ chức áp dụng triển khai và cho thấy những hiệu quả cao trong việc tăng cường tính bảo mật và khả năng ứng phó sự cố của hệ thống. Một hệ thống phát hiện xâm nhập (IDS-Intrusion Detection System) là một thiết bị phần cứng hoặc phần mềm theo dõi hệ thống mạng, có chức năng giám sát lưu thông mạng, tự động theo dõi các sự kiện xảy ra trên một hệ thống mạng máy tính, phân tích để phát hiện ra các vấn đề liên quan đến an ninh, bảo mật và đưa ra cảnh báo [12]. Một số hệ thống phát hiện xâm nhập còn có thể ngăn chặn các nỗ lực xâm nhập nhưng điều này là không bắt buộc đối với một hệ thống giám sát. Khác với tường lửa, IDS không thực hiện các thao tác ngăn chặn truy xuất mà chỉ theo dõi các hoạt động trên mạng để tìm ra các dấu hiệu của tấn công và cảnh báo.



Hình 2.4. *Vị trí của thết bị IDS trong hệ thống mạng*

Nhiệm vụ chính của IDS trong mạng là để phát hiện các cuộc tấn công cũng như có thể đẩy lùi các cuộc tấn công này. Cách thông thường nhất để phân loại các hệ thống IDS là dựa vào đặc điểm của nguồn dữ liệu thu thập được. Trong trường hợp này, các hệ thống IDS được chia thành các loại sau:

• Network-based IDS (NIDS): Sử dụng dữ liệu trên toàn bộ lưu thông mạng.

• Host-based IDS (HIDS): Sử dụng dữ liệu kiểm tra từ một máy trạm đơn để phát hiện xâm nhập.

2.3.5. Giám sát các phần mềm ứng dụng

Trong hoạt động tác nghiệp của bất kì tổ chức nào đều không thể thiếu được các chương trình phần mềm ứng dụng, đây có thể là những phần mềm quản lý, tính toán, lập báo cáo, hay đó

là những phần mềm ứng dụng trên máy chủ hay các dịch vụ của hệ thống. Các bản ghi lịch sử hoạt động của các phần mềm này có thể rất hữu ích để thu thập, thông tin này cung cấp dữ liệu chuyên sâu về hoạt động ứng dụng giữa người dùng và hệ thống.

**** Giám sát hoạt động của FTP, SFTP:***

Nhiều tổ chức sử dụng FTP, SFTP với chức năng để tải lên và tải về các tập tin lưu trữ trên máy chủ, vấn đề quan trọng là cần đảm bảo cho dịch vụ này hoạt động ổn định, sẵn sàng trong mọi thời điểm. Bất kỳ thời gian ngừng trệ nào của dịch vụ này có thể dẫn đến tập tin bị hỏng được tải lên hay tải về mà có thể ảnh hưởng đến hiệu suất của người dùng cuối.

Các báo cáo có thể được nhóm lại và hiển thị dựa trên khả năng sẵn sàng của hệ thống và hiệu năng hoạt động.

**** Giám sát hoạt động của DNS:***

DNS (Domain Name Service) là dịch vụ phân giải tên miền được sử dụng để chuyển đổi qua lại giữa tên miền và địa chỉ IP của máy chủ. Trong các đơn vị có duy trì hệ thống máy chủ cục bộ chạy trong hệ thống mạng LAN, với số lượng máy trạm lớn, thường xuyên truy cập, tương tác với các máy chủ, thì cần thiết có một hệ thống DNS nội bộ để giảm bớt lưu lượng mạng truy cập từ bên ngoài và giảm băng thông truy cập cần thiết. Đối với dịch vụ DNS, cơ sở dữ liệu các bản ghi DNS rất quan trọng, giúp máy chủ thực hiện tìm kiếm và trả lời truy vấn một cách nhanh chóng, chính xác. Với hệ thống giám sát DNS cần cung cấp các thông tin đầy đủ bao gồm: thời gian phản hồi, kiểu bản ghi, giá trị truy vấn, thời gian truy vấn, thời gian tìm kiếm… [14].

**** Giám sát dịch vụ email:***

Dịch vụ email nội bộ hiện được nhiều tổ chức triển khai và duy trì hoạt động do tính linh hoạt, bảo mật và nhanh chóng, thậm chí ngay cả khi không có truy cập internet thì nhân viên vẫn có thể trao đổi email trong mạng nội bộ mà không bị ảnh hưởng. Hệ thống giám sát toàn diện sẽ cần phải theo dõi các hoạt động của máy chủ email và thực hiện ghi lại lịch sử các log xảy ra trên hệ thống. Từ đó nó có thể cung cấp một loạt các công cụ theo dõi để kiểm tra tính sẵn sàng và hiệu suất của máy chủ email. Những công cụ này cho phép người quản trị hệ thống tiếp tục xác minh rằng các dịch vụ email vẫn đang hoạt động và sẵn sàng đáp ứng một cách nhanh chóng, cũng như có khả năng xác định bất kỳ vấn đề trước khi chúng ảnh hưởng đến người sử dụng trên hệ thống [15].

Bên cạnh đó, một số hệ thống giám sát mạng tiên tiến như Monitis [15] còn cũng cấp các tính năng giám sát nâng cao cho phép giám sát tính sẵn sàng và hiệu quả của một quá trình gửi email đầy đủ, để đảm bảo rằng các dịch vụ email gửi đến và gửi đi của hệ thống đang làm việc đúng và thao tác gửi/nhận kịp thời.

**** Giám sát các phần mềm nghiệp vụ chung:***

Do đặc thù của mỗi ngành nên sẽ có các phần mềm chuyên dụng phục vụ công việc chuyên môn riêng. Trong ngành Y tế hiện nay, các phần mềm quản lý y bạ, quản lý thẻ bảo hiểm y tế…đang được triển khai sử dụng rộng khắp từ bệnh viện tuyến trung ương xuống địa phương. Việc vận hành và sử dụng các phần mềm đặc thù ngành này thường do bộ phận phụ trách về công nghệ thông tin quản lý và duy trì, do đó khi hệ thống phần mềm và dịch vụ hỗ trợ đi kèm phần mềm gặp trục trặc, thì để khắc phục đưa hệ thống trở lại làm việc cần có sự đánh giá và tìm ra nguyên nhân…

3. Kết luận

Trong thế giới hiện tại, việc thực hiện triển khai một hệ thống giám sát toàn bộ các thiết bị mạng là việc cấp thiết cho tất cả các doanh nghiệp, tổ chức. Việc triển khai hệ thống giám sát nhằm tối ưu hóa hệ thống mạng, tăng cường an ninh mạng, và có thể giải quyết các sự cố kịp thời. Hàng năm, công tác giám sát an ninh mạng có thêm nhiều hiệu quả hơn trong việc tìm kiếm và giảm nhẹ rủi ro an ninh. Với việc tập trung vào giám sát các hoạt động xảy ra trong hệ thống mạng, tổ chức có thể đạt được mục tiêu của mình mà không ảnh hưởng an ninh. Việc tăng cường an ninh và bảo mật cho các hệ thống đòi hỏi phải có sự đầu tư hợp lý, được tư vấn chính xác để lựa chọn được giải pháp tối ưu nhất, vừa tiết kiệm được chi phí đầu tư ban đầu, và vẫn đảm bảo được hiệu quả đề ra.

Tài liệu tham khảo

[1]. Nguyễn Thu Trang, Hệ thống thông tin y tế và tình hình ứng dụng tại Việt Nam, Luận văn thạc sĩ, 2008, tr. 46-61.

[2]. Richard Bejtlich, The Practice of Network Security Monitoring. *William Pollock*, ISBN: 1-59327-509-9, 2013, pp. 342-357.

[3]. Phạm Đức Nhơn, Xây dựng hệ thống giám sát tập trung trên cơ sở SNMP, Luận văn thạc sĩ kỹ thuật, Học viện CN BCVT, 2013. tr. 23-28.

[4].Chris Fry and Martin Nystrom, Security monitoring. *O'Reilly Media*, ISBN: 978-0-596-51816-

5, 2009, pp. 61-83.
[5]. Nguyễn Mạnh Hùng, Phát hiện và phòng chống xâm nhập trái phép mạng máy tính, Luận văn thạc sĩ, 2013, tr. 40-46.
[6]. Vikas Mishra , V.K. Vijay, S. Tazi, Intrusion Detection System with Snort in Cloud Computing: Advanced IDS. *Proceedings of International Conference on ICT for Sustainable Development*, **Vol 408** of the series Advances in Intelligent Systems and Computing, 2016, pp.457-465.
[7]. Joao Afonso, Pedro Veiga, Enhancing DNS security using dynamic firewalling with network agents. *Computer Science and Information Systems (FedCSIS) 2011 Federated Conference on*, pp. 777-782.
[8]. P. Tzerefos, C. Smythe, I. Stergiou, and S. Cvetkovic, A Comparative Study of Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP) and X.400 Electronic Mail Protocols. *Proceedings of the IEEE 1997 22nd Conference on Local Computer Networks - LCN*, pp. 545-554, 199.
[9]. Slagell A., Yurcik W., Sharing computer network logs for security and privacy: a motivation for new methodologies of anonymization. *IEEE 1st International Conference on Security and Privacy for Emerging Areas in Communication Networks*, September 2005, pp. 80-89.
[10]. Ya-Ting Fan Shiuh-Jeng Wang, Intrusion Investigations with Data-Hiding for Computer LogFile Forensics. *Proceedings of the IEEE 5th International Conference on Future Information Technology*, May 2010, pp. 1-6.
[11]. Jie wang, Xianqiang chen, Application of web usage mining in the struction of distance opening education web site, 2008, **vol. 4**, pp. 157-160.
[12]. Y. Y. Yao, H. J. Hamilton, Xuewei Wang, PagePrompter, An Intelligent Web Agent Created Using Data Mining Techniques. *Rough Sets and Current Trends in Computing*, 2002, **vol. 2475**, pp. 949-.
[13]. Ouyang Yang, Zhu Miaoliang, Effective E-Learning Environment Personalization using Web Usage Mining Technology. In *Innovations in E-learning Instruction Technology Assessment and Engineering Education*, Springer Netherlands:, 2007, pp. 311-315.

RESEARCH AND DEVELOPMENT OF THE NETWORK MONITORING SYSTEM FOR THE MINISTRY OF HEALTH

Abstract:

This report presents a process for studying some of the vulnerabilities in the Department of Health network. From the results of the research team report, the team proposed solutions to deploy network monitoring system to ensure network security.

Keywords: *Network monitoring, IDS protected, IDS Snort.*

.