AN TOÀN THÔNG TIN TRONG BỐI CẢNH GIA TĂNG TẤN CÔNG MẠNG: THỰC TRẠNG, CÁCH TIẾP CẬN

NGUYỄN LINH GIANG, HUỲNH QUYẾT THẮNG, VŨ THỊ HƯƠNG GIANG
Viện Công nghệ thông tin và Truyền thông, Trường Đại học Bách khoa Hà Nội

Hiện nay, an ninh mạng không chỉ liên quan tới vấn đề an ninh thông tin cá nhân hay dữ liệu kinh doanh của các tổ chức, doanh nghiệp mà còn liên quan đến chủ quyền, an ninh quốc gia. Trong bài viết này, các tác giả đề cập đến bối cảnh an toàn thông tin (ATTT) mạng trên thế giới nói chung và ở Việt Nam nói riêng trong những năm gần đây, từ đó đưa ra những phương hướng và giải pháp tổng thể nhằm đảm bảo an toàn, an ninh không gian mạng quốc gia.

Mở đầu

Theo báo cáo thường niên về tình trạng an toàn, an ninh hệ thống thông tin trên thế giới cũng như ở Việt Nam do các tổ chức ATTT trên thế giới cũng như trong khu vực, từ năm 2010 tới nay, tình trạng tấn công mạng, các hình thức tội phạm mạng đã tăng khá nhanh. Các dạng tấn công phổ biến bao gồm: sử dụng mã độc để ăn trộm thông tin, tấn công từ chối dịch vụ, tấn công vào các hệ thống quản trị dữ liệu. Vấn đề đặt ra là làm sao có thể xây dựng được một hệ thống giải pháp đồng bộ để đảm bảo ATTT quốc gia, đảm bảo không bị rò rỉ các thông tin kinh tế - xã hội, bảo đảm hoạt động của các hệ thống thông tin cung cấp dịch vụ cũng như các hệ thống chuyên biệt, đảm bảo sự lành mạnh cho hệ thống thông tin kinh tế - xã hội của Việt Nam. Để làm được việc đó, cần có những giải pháp từ tổng thể đến cụ thể, cho phép xây dựng hệ thống đảm bảo an ninh thông tin quốc gia với nhiều tầng bảo vệ khác nhau. Trong khuôn khổ bài viết này, chúng tôi trình bày tổng quan về tình trạng ATTT ở Việt Nam những năm gần đây, phương hướng và giải pháp bảo mật thông tin ở nước ta trong điều kiện hiện nay.

Bối cảnh ATTT tại Việt Nam và trên thế giới

Trong những năm vừa qua, trên thế giới cũng như trong nước đã xảy ra hàng ngàn vụ tấn công vào hệ thống mạng, hệ thống máy tính, gây nên nhiều thiệt hại. Những tấn công này tập trung vào những vụ việc gây mất mát, rò rỉ thông tin bí mật quốc gia, đánh cắp thông tin kinh tế tài chính, tấn công vào tính sẵn sàng của các hệ thống mạng thông tin, hệ thống cung cấp dịch vụ, hệ thống tác nghiệp của các cơ quan, tổ chức, doanh nghiệp. Những tấn công này đặc biệt nguy hiểm đối với những hệ thống mạng thông tin mang tính sống còn của quốc gia. Số liệu của các Trung tâm Ứng cứu khẩn cấp máy tính (CERT) trên thế giới và trong khu vực cho thấy, số lượng các vụ tấn công vào các trang web cơ quan chính quyền của Đài Loan tăng mạnh trong năm 2012-2013; tấn công vào cổng thông tin các cơ quan, tổ chức của Nhật Bản cũng tăng mạnh trong những năm gần đây. Các hình thức tấn công mạng tập trung nhiều vào những dạng: xâm nhập trái phép, tấn công từ chối dịch vụ, tấn công lấy trộm thông tin quan trọng thông qua các mã độc...

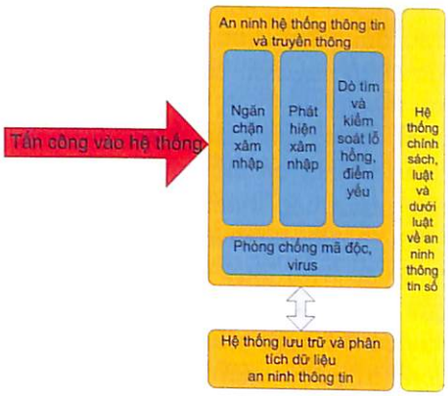
Ở Việt Nam, tình trạng tấn công của tin tặc vào trang web của các cơ quan, tổ chức cũng xảy ra với tần suất cao. Thực tế, hệ thống máy chủ dịch vụ tại các cơ quan Chính phủ, Nhà nước còn tồn tại nhiều lỗ hổng hệ thống, nếu bị lợi dụng sẽ gây mất mát thông tin quan trọng và gây nhiều thiệt hại cho quốc gia. Theo số liệu thống kê của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT), trong các năm 2011-2013, số lượng các vụ tấn công của tin tặc ngày càng tăng mạnh. Trong năm 2013, số lượng các vụ tấn công đã ghi nhận được là 6379 vụ, tăng gấp 3 lần so với năm 2012 và gấp gần 25 lần so với năm 2010. Trong đó, số vụ tấn công bằng mã độc chiếm gần một phần ba với 2142 vụ, tấn công lừa đảo với 2469 vụ và tấn công phá hoại với 1603 vụ. Đây chỉ là số liệu được báo cáo và thống kê, trên thực tế con số này có thể còn lớn hơn nhiều lần. Theo Sách trắng về công nghệ thông tin và truyền thông năm 2013, 2014, các chỉ số về ATTT của Việt Nam năm 2013 là xấp xỉ 37,5%; năm 2014 cao hơn một chút, nhưng vẫn thấp hơn nhiều so với các nước trong khu vực, đặc biệt là Hàn

Quốc với 62%. Tỷ lệ các đơn vị, cơ quan, tổ chức có sử dụng các biện pháp đảm bảo ATTT và truyền thông còn thấp (tỷ lệ cao nhất đối với khả năng nhận biết dạng tấn công mã độc vào khoảng 32%, các dạng tấn công xâm nhập trái phép khoảng 8,9%, tấn công làm giảm hiệu năng và tấn công từ chối dịch vụ vào khoảng 12,5%...).

Như vậy có thể thấy rằng, ở các đơn vị, cơ quan trong nước, khả năng đảm bảo an toàn cho hệ thống thông tin và dữ liệu số còn thấp, do đó ảnh hưởng nhiều tới an ninh kinh tế - xã hội. Để nâng cao tính bảo mật, ATTT trong phạm vi cả nước, cần phải có những giải pháp tổng thể, đồng bộ, từ nhận thức của người sử dụng, sở hữu thông tin đến mức an toàn, an ninh cho hạ tầng thông tin, truyền thông và các hệ thống ứng dụng nền tảng. Trong phần sau, một số cách tiếp cận tới bài toán tổng thể sẽ được trình bày dựa trên tư tưởng chủ đạo là xây dựng một hệ thống tích hợp, có thể triển khai ở các Nhà cung cấp dịch vụ Internet (ISP), Nhà cấp phép trang tin điện tử (ICP), cũng như trong hệ thống mạng Internet quốc gia. Hệ thống này có nhiệm vụ ngăn chặn, giám sát, kiểm soát các truy cập vào - ra không gian mạng của Việt Nam. Cụ thể là cần xây dựng một ranh giới của Việt Nam trong không gian mạng toàn cầu, mọi truy cập vào - ra không gian mạng đó sẽ được kiểm soát chặt chẽ và triệt để. Trong những năm gần đây, khái niệm biên giới quốc gia trên mạng Internet đã dần được hình thành rõ nét hơn, nhưng việc xây dựng nó vẫn vấp phải nhiều khó khăn và cần được thảo luận, xem xét về logic cũng như tính khả thi.

Phương hướng và giải pháp tăng cường ATTT ở Việt Nam

Biên giới quốc gia về ATTT trên Internet có thể hiểu một cách đơn giản là một hệ thống ngăn chặn, kiểm soát mọi luồng thông tin, dữ liệu trao đổi giữa các hệ thống mạng bên trong Việt Nam và bên ngoài. Hệ thống này sẽ lọc, phân tích và đưa ra những biện pháp cần thiết để xử lý các luồng thông tin tương tác có hại tới an ninh quốc gia cũng như an ninh kinh tế - xã hội. Những người sử dụng và các hệ thống đầu - cuối phát sinh ra những luồng thông tin trao đổi cũng phải được xác thực và kiểm soát tương tự như một người xuất - nhập cảnh qua biên giới quốc gia. Trong trường hợp có những thỏa thuận cấp cao giữa các bên liên quan, biên giới an ninh thông tin lúc này được coi là vô hình, mọi luồng thông tin hợp lệ sẽ "trong suốt" khi đi qua những biên giới đó, tạo cảm giác không bị kiểm soát. Việc xây dựng một biên giới kiểm soát thông tin như vậy yêu cầu một hệ thống giải pháp tổng thể, đồng bộ giữa các cơ quan, tổ chức và doanh nghiệp ở Việt Nam. Nhìn chung, hệ thống này sẽ bao gồm những thành phần sau: *một là,* hệ thống ngăn chặn và lọc các luồng dữ liệu trên các tầng tại các cổng giao tiếp của hệ thống mạng trục quốc gia và Internet. *Hai là,* hệ thống phát hiện những xâm nhập trái phép qua biên giới an ninh thông tin quốc gia. *Ba là,* hệ thống lọc và kiểm soát những thông tin độc hại, xuyên tạc, mã độc trước khi cho đi qua biên giới an ninh quốc gia. *Bốn là,* hệ thống kiểm soát mã độc hại, virus phát tán qua mạng. *Năm là,* xây dựng và bổ sung hệ thống các chính sách, luật liên quan tới biên giới an ninh Internet. *Sáu là,* ngoài vấn đề an ninh, những vấn đề liên quan tới hải quan, kiểm soát và chống gian lận thương mại nội dung số cũng có thể được đặt ra khi các hoạt động thương mại dựa trên dữ liệu số, đa phương tiện được thực hiện thông qua biên giới an ninh Internet quốc gia.



Hình 1: các thành phần trong hệ thống đảm bảo an toàn hệ thống thông tin

Xây dựng các hệ thống lọc chặn luồng dữ liệu

Các hệ thống lọc, chặn luồng dữ liệu có nhiệm vụ kiểm soát mọi luồng dữ liệu xâm nhập vào biên giới an ninh quốc gia, bản chất là những hệ thống tường lửa với tốc độ xử lý và băng thông lớn, cho phép xử lý thời gian thực những luồng dữ liệu với tốc độ hàng chục Gb/s. Nếu xét trên tầng mạng, những hệ thống này sẽ lọc các gói tin và ngăn chặn những truy cập trái phép, không được ủy quyền; còn những luồng dữ liệu hợp lệ sẽ được nó cho phép đi qua. Trên các tầng cao hơn, những hệ thống lọc, chặn luồng dữ liệu sẽ phân tích nội dung các gói tin, xác định các giao thức ở tầng trên hoặc các ứng dụng phát sinh ra các gói tin đó, xác định đối tượng truy cập vào các hệ thống bên trong biên giới an ninh. Từ đó, kiểm soát, kiểm tra, xác thực các đối tượng thông tin, ứng dụng, cá nhân này khi đi qua biên giới an ninh Internet quốc gia. Có thể hình dung, những hệ thống lọc, chặn này giống như các trạm kiểm soát xuất - nhập cảnh trên biên giới quốc gia. Tại đây, ở mức cao, những hệ thống lọc chặn có thể phân tích nội dung dữ liệu, phát hiện những tác nhân độc hại, mã độc hay virus để ngăn chặn sớm những tấn công vào bên trong biên giới an ninh quốc gia.

Đối với các hình thức thương mại, trao đổi dữ liệu số, những hệ thống lọc chặn này còn có thể mở rộng để kết nối với hệ thống hải quan và kiểm soát những gian lận thương mại nội dung số. Ta có thể hình dung, chức năng của các thành phần hệ thống kiểm soát lọc chặn luồng dữ liệu giống như các hình thức kiểm soát tại các cửa khẩu biên giới. Những hệ thống này có thể được triển khai tại các ISP, cổng truy cập Internet quốc gia; giúp kiểm soát nội dung dữ liệu số, tính hợp lệ của các nội dung đó và phát hiện những gian lận, giả mạo ảnh hưởng tới an ninh kinh tế - xã hội quốc gia, và phải đáp ứng được yêu cầu xử lý thời gian thực các luồng dữ liệu ở tốc độ cao để không làm giảm hiệu năng của toàn bộ hệ thống mạng.

Xây dựng các hệ thống phát hiện và ngăn chặn xâm nhập trái phép qua biên giới thông tin quốc gia

Trong nhiệm vụ của các hệ thống đảm bảo an ninh biên giới thông tin Internet, việc phát hiện và ngăn chặn kịp thời những tấn công xâm nhập vào hệ thống thông tin, hệ thống mạng của Việt Nam đóng vai trò quan trọng sống còn. Những hệ thống này giám sát các luồng thông tin, dữ liệu trao đổi nội tại trong phạm vi biên giới an ninh và phân tích những dữ liệu thu thập được, dựa vào đó phát hiện những hành vi, luồng trao đổi thông tin không bình thường, những tác động không bình thường vào những hệ thống, kho dữ liệu cũng như các máy trạm quan trọng. Từ các kết quả phân tích, hệ thống có thể đưa ra những biện pháp ngăn chặn phù hợp hoặc đưa ra những cảnh báo, giúp cho người quản trị lựa chọn được những cách giải quyết tối ưu.

Với các kết nối, trao đổi dữ liệu có tốc độ từ hàng trăm Mb/s đến hàng Gb/s, các hệ thống phát hiện và ngăn chặn xâm nhập trái phép gặp nhiều thách thức trong quản lý, giám sát các luồng dữ liệu trao đổi. Các dạng tấn công DoS/DDoS với mục tiêu làm cho các đối tượng bị tấn công gặp khó khăn khi cung cấp dịch vụ, hoặc mất khả năng truy cập, khai thác và hoạt động hiệu quả [1]. Trong đó, dạng tấn công DDoS có thể có những tác động như: làm tiêu hao tài nguyên hệ thống; làm tiêu hao băng thông của hệ thống mạng; làm máy chủ ngừng cung cấp dịch vụ hoặc bị sập nhờ sử dụng các lỗ hổng tiềm ẩn trong hệ thống. Ngoài ra, nhiều dạng tấn công khác có thể có những tác động: giả mạo các gói tin trong mạng; chiếm quyền điều khiển các hệ thống máy chủ quan trọng; xâm nhập qua các lỗ hổng bảo mật và lấy cắp dữ liệu quan trọng.

Nói chung, có nhiều cách tấn công vào hệ thống, những tấn công này làm hệ thống không thể đáp ứng được các yêu cầu dịch vụ hoặc là hoạt động rất chậm. Thông thường, các hệ thống ngăn chặn xâm nhập như tường lửa (firewall) hoặc ngăn chặn xâm nhập IPS hoạt động khá hiệu quả khi ngăn chặn các dạng tấn công, xâm nhập đã biết, nhưng lại trở nên không hiệu quả đối với những dạng tấn công chưa biết. Một trong những cách tiếp cận để giải quyết một phần bài toán này là giám sát mạng, hệ thống theo thời gian thực và từ các dữ liệu thu nhận được tìm ra những đặc trưng của các dạng tấn công này bằng phương pháp tự động hoặc bán tự động. Tuy nhiên, việc xây dựng và triển khai giải pháp này gặp nhiều thách thức trong bối cảnh bùng nổ phát triển các công nghệ nền tảng mới như: công nghệ tính toán lưới, điện toán đám mây, công nghệ di động và mạng Internet vạn vật. Đối với các hệ thống dịch vụ điện toán đám mây, việc phát hiện xâm nhập gặp thách thức do việc giao tiếp giữa các nút tham gia vào đám mây thường được phát triển trên các kênh truyền thông được bảo vệ. Can thiệp vào các kênh truyền thông này là khó khăn, phức tạp nếu không có sự cho phép từ nhà cung cấp dịch vụ cũng như có những điều luật được điều chỉnh tương ứng. Trong trường hợp hệ thống mạng Internet vạn vật và di động, vấn đề nảy sinh là lượng dữ liệu thu nhận được rất lớn, do đó cần phải phát triển những phương pháp phân tích và xử lý thích hợp với sự gia tăng mạnh dữ liệu. Tóm lại, những hệ thống giám sát và phát hiện bất thường phải có cơ chế theo dõi và dò vết theo các luồng dữ liệu trong mạng trao đổi dữ liệu, điều đó phụ thuộc nhiều vào cơ chế ghi nhật ký hoạt động của hệ thống tổng thể và từng thành phần riêng lẻ, ngoài ra còn phải có khả năng xử lý thời gian thực dữ liệu lớn ở tốc độ cao vì những số liệu mạng thu thập được là vô cùng lớn theo thời gian.

Xây dựng hệ thống lọc thông tin độc hại

Trên Internet có những thông tin có ích nhưng cũng nhiều thông tin độc hại, xuyên tạc có thể ảnh hưởng tới an ninh kinh tế - xã hội. Việc lọc và đảm bảo sự lành mạnh về thông tin trong không gian mạng nội địa của Việt Nam có vai trò quan trọng trong việc đảm bảo an ninh kinh tế - xã hội. Tuy việc lọc bỏ hay ngăn chặn những luồng thông tin này là hết sức khó khăn do tính mở của Internet, nhưng ở một khía cạnh nào đó, có thể xây dựng những hệ thống lọc làm giảm bớt những thông tin độc hại, giữ cho đời sống thông tin của xã hội được lành mạnh. Trên thực tế, những hệ thống lọc thông tin độc hại có thể được tích hợp vào hệ thống lọc chặn như tường lửa, proxy, hệ thống phát hiện xâm nhập mạng để tạo thành hệ thống kiểm soát liên hoàn. Một ví dụ cụ thể về dạng hệ thống này là hệ thống lọc thư rác [2]. Việc trao đổi thư điện tử là hoạt động diễn ra thường xuyên trong giao tiếp trên Internet, vì vậy những hình thức tấn công mạng, giả mạo để xâm nhập hệ thống và đánh cắp dữ liệu thông qua hình thức thư điện tử cũng tăng nhanh trong những năm gần đây. Điển hình là dạng tấn

công từ chối dịch vụ DDoS như: phát tán thư rác với số lượng lớn; phát tán sâu Internet, virus, các phần mềm độc hại, mã độc qua thư điện tử; phát tán các thông tin độc hại tới an ninh kinh tế - xã hội thông qua hệ thống thư điện tử và thư rác... Do đó, việc phát hiện, phân loại và lọc những thư rác trong hệ thống thư điện tử là một trong những bài toán quan trọng để đảm bảo ATTT quốc gia, và hiện nay, việc này đang được đẩy mạnh nghiên cứu cả trong và ngoài nước.

Kiểm soát các mã độc, phần mềm độc hại và virus mạng

Vấn đề kiểm soát mã độc, phần mềm độc hại, virus phát tán qua mạng có thể hoạt động trên nhiều mức. Ở tầng thấp nhất, các hệ thống kiểm soát sẽ lọc các gói tin phát tán qua mạng, phân tích các giao thức sử dụng và từ đó đưa ra những biện pháp xử lý sớm. Tuy vậy, trong nhiều trường hợp, những tác nhân độc hại này chỉ có thể phát hiện khi thực hiện phân tích trên tầng ứng dụng. Các hệ thống phân tích sẽ kiểm soát tại những trạm nhận tin, như các máy chủ mail, các proxy, tường lửa của tầng ứng dụng; những hệ thống kiểm soát và diệt virus Internet có thể được triển khai để thực hiện chức năng này. Với sự bùng nổ của trao đổi thông tin qua Internet như hiện nay, cần phải nghiên cứu, phát triển những hệ thống kiểm soát hiệu năng cao, có khả năng phân tích, phát hiện và ngăn chặn những tác nhân độc hại tác động vào hệ thống thông tin.

Xây dựng hệ thống các luật, chính sách an ninh biên giới thông tin quốc gia

Việc đảm bảo an ninh cho biên giới an ninh Internet quốc gia không thể thành công nếu không có những điều chỉnh phù hợp với những dạng hành vi mới trong không gian mạng [3]. Để đảm bảo về mặt luật pháp, cần phải hoàn thiện, bổ sung, sửa đổi những điều luật, văn bản dưới luật, các chính sách để bao phủ những hành vi này. Đặc biệt, phải có những quy định cụ thể về các hạ tầng mạng trọng yếu cần được tăng cường bảo vệ như: chính phủ, quốc phòng, năng lượng, giao thông, y tế, ngân hàng và bảo hiểm..., theo đó, hạ tầng của các mạng này phải đạt tiêu chuẩn an ninh thông tin tối thiểu. Mặt khác, các doanh nghiệp viễn thông cũng phải nâng cao năng lực bảo đảm an ninh, ATTT đối với các công nghệ và dịch vụ ứng dụng cho người dùng; có trách nhiệm thông báo cho khách hàng khi phát hiện nguy cơ mất ATTT.

An ninh cho các hệ thống điện toán đám mây

Một trong những xu hướng phát triển nền tảng tính toán hiện nay là sự phát triển mạnh mẽ của công nghệ điện toán đám mây. Điều này đã tạo ra những thách thức mới trong việc đảm bảo an toàn dữ liệu trên các hệ thống điện toán đám mây, cần những thay đổi lớn về quan niệm cũng như các biện pháp đảm bảo an toàn an ninh. Ngoài việc đảm bảo an toàn cho dữ liệu, kiểm soát các đối tượng truy cập vào các hệ thống đám mây, phát hiện xâm nhập, ngăn chặn tấn công vào hệ thống điện toán đám mây, phải có những chính sách, quy định khi quản lý dữ liệu trên các hệ thống điện toán đám mây của các nhà cung cấp trong và ngoài nước, đặc biệt về tính riêng tư và quyền sở hữu dữ liệu.

An ninh cho mạng Internet vạn vật (Internet of Things - IoT)

Với sự phát triển của các công nghệ di động, hệ thống mạng Ad-hoc, mạng cảm biến, các công nghệ thông minh, mạng Internet sẽ mở rộng tới các thiết bị và điều này sẽ tạo ra những thách thức lớn về mặt kiểm soát, cũng như vấn đề đảm bảo an ninh cho mạng vạn vật. Ngoài yêu cầu về hiệu năng xử lý của thiết bị, những vấn đề liên quan tới định tuyến an toàn, chống dạng tấn công từ chối dịch vụ DDoS trong mạng Internet vạn vật, các bài toán đảm bảo an toàn mạng khi chuyển sang mạng vạn vật cần phải có những điều chỉnh hợp lý do sự hạn chế của các thiết bị về khả năng tính toán, sự phụ thuộc năng lượng. Ví dụ, các cơ chế xác thực khi sử dụng chứng thư số cần phải được điều chỉnh để phù hợp với khả năng tính toán của các thiết bị này. Một trong những vấn đề nảy sinh là lượng dữ liệu cần xử lý rất lớn, có thể nói là bùng nổ dữ liệu khi xây dựng những hệ thống kiểm soát, phân tích an toàn an ninh mạng, đặc biệt trong bối cảnh phát triển mạng Internet vạn vật. Những vấn đề này dẫn tới phải giải quyết những bài toán xử lý dữ liệu lớn, các hệ thống phân tích, khai phá dữ liệu với hiệu năng cao. Đây là những vấn đề nóng, đang được đẩy mạnh nghiên cứu trong những năm gần đây.

Kết luận

Bài báo đã trình bày một cách nhìn tổng quan tới việc đảm bảo an toàn, an ninh không gian mạng quốc gia. Những vấn đề trình bày ở đây không thể nói rằng đã bao phủ mọi vấn đề của bài toán, tuy vậy cũng có thể đưa ra được một cách tiếp cận tổng thể để tìm ra những hướng giải quyết phù hợp đối với bài toán đảm bảo an ninh không gian mạng quốc gia ✍

Tài liệu tham khảo

[1] Ihsan Ullah, Naveed Khan, Hatim A. Aboalsamh (2013), Survey on botnet: its architecture: detection, prevention and mitigation, *IEEE*.

[2] Fernando Sanchez and Zhenhai Duan (2012), A Sender-Centric Approach to Detecting Phishing Emails, *CyberSecurity 2012. 2012 International Conference on Cyber Security*, pp. 33-39.

[3] Vũ Quốc Khánh, Tăng cường đảm bảo ATTT tại Việt Nam, *Báo cáo tại Hội thảo Ngày An toàn thông tin Việt Nam 2013*, VNCERT, Bộ Thông tin và Truyền thông.