GIẢI PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN CHO HẠ TẦNG CNTT TRỌNG YẾU QUỐC GIA

PGS.TS Trần Đức Sự
Giám đốc Trung tâm Công nghệ thông tin và Giám sát an ninh mạng
Ban Cơ yếu Chính phủ

Trong những năm gần đây, tình trạng mất an toàn thông tin (ATTT) hạ tầng mạng công nghệ thông tin (CNTT) trên toàn thế giới diễn ra hết sức căng thẳng và có nhiều diễn biến phức tạp. Các cuộc tấn công vào hệ thống mạng CNTT của các cơ quan nhà nước, doanh nghiệp tăng nhanh cả về số lượng, cường độ, cũng như mức độ nguy hiểm. Trước tình hình đó, nhiều quốc gia đã phải phát triển lực lượng chuyên trách sẵn sàng tham gia, đối phó với chiến tranh mạng; đây là yêu cầu cấp thiết nhằm đảm bảo ATTT trên hạ tầng mạng CNTT trọng yếu. Bài viết điểm qua tình hình mất an toàn, an ninh thông tin trên thế giới nói chung, Việt Nam nói riêng trong năm 2015 và đưa ra một số giải pháp nhằm góp phần khắc phục tình trạng trên.

Tình hình ATTT trên thế giới và Việt Nam trong năm 2015

Trong năm 2015, tình hình an ninh mạng trên thế giới có nhiều diễn biến phức tạp. Ngày 6.8.2015, hacker ở Liên bang Nga xâm nhập vào hệ thống Email Bộ Tổng tham mưu ở Lầu năm góc khiến hệ thống này dừng hoạt động gần 2 tuần. Ngày 21.8.2015, nhóm hacker APT Blue Termite đến từ Trung Quốc tấn công các tổ chức Nhật Bản, xâm hại dữ liệu của hơn 1,25 triệu người. Ngày 10.9.2015, nhóm hacker Turla APT ở Liên bang Nga đã đánh chặn, tấn công các vệ tinh thương mại, thu thập dữ liệu nhạy cảm của các tổ chức chính phủ, quân sự, ngoại giao, nghiên cứu, giáo dục của hơn 45 quốc gia, bao gồm cả Trung Quốc, Việt Nam và Hoa Kỳ. Ngày 5.11.2015, lực lượng Vệ binh cách mạng Hồi giáo Iran (IRCG) đã thực hiện các cuộc tấn công mạng nhằm vào các quan chức làm việc tại Văn phòng Bộ Ngoại giao Mỹ tại Iran và Cục Cận Đông (NEA). Ngày 9.11.2015, hacker của Nhà nước hồi giáo tự xưng IS đã tấn công hơn 54.000 tài khoản Twitter nhằm trả thù vụ máy bay không người lái của Mỹ giết hại công dân Anh ủng hộ IS, vụ tấn công này đã xâm phạm thông tin cá nhân, số điện thoại và mật khẩu của những người đứng đầu Cục Tình báo Trung ương CIA, Cục Điều tra Liên bang FBI và Cơ quan An ninh Quốc gia Hoa Kỳ. Ngày 2.12.2015, nhóm hacker đến từ Trung Quốc đã tấn công mạng của Cục Khí tượng Úc, gây thiệt hại về cơ sở dữ liệu. Ngày 4.12.2015, nhóm hacker Anonymous đã tấn công vào website Hội nghị biến đổi khí hậu (COP21) của Liên hợp quốc, đánh cắp và công khai toàn bộ thông tin cá nhân của 1.415 đại biểu tham gia sự kiện, nhằm phản đối vụ bắt giữ những người biểu tình chống lại COP21.

Theo báo cáo của Tổ chức tư vấn Grant Thornton International, trong năm 2015 các vụ tấn công mạng đã khiến các tổ chức, cá nhân thiệt hại hơn 315 tỷ USD. Trong đó, ước tính ở châu Âu thiệt hại khoảng 62,3 tỷ USD, Bắc Mỹ là 61,3 tỷ USD, tuy nhiên con số này vẫn thấp hơn nhiều so với khu vực châu Á - Thái Bình Dương (81,3 tỷ USD).

Tình trạng mất an toàn, an ninh thông tin ở Việt Nam năm 2015 chịu tác động trực tiếp từ tình hình an toàn, an ninh thông tin trên thế giới. Nhiều mạng CNTT của các tổ chức, doanh nghiệp ở Việt Nam đã và đang trở thành mục tiêu của các cuộc tấn công mạng. Đối với các mạng CNTT trọng yếu của các cơ quan Đảng và Chính phủ Việt Nam cũng ghi nhận nhiều cuộc tấn công lớn nhỏ xuất phát từ một số nước trong khu vực và trên thế giới. Báo cáo tổng kết năm 2015 của Trung tâm Ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) đã ghi nhận 5.898 vụ tấn công Phishing, 8.850 vụ tấn công Deface, 16.837 vụ tấn công Malware (tăng 1,7 lần so với năm 2014), và có hơn 200 website giả mạo (giả mạo giấy phép do Bộ Thông tin và Truyền thông cấp, giả mạo webmail VNN, VDC, giả mạo website Ngân hàng Nhà nước…), 1.451.997 lượt địa chỉ IP trên cả nước bị nhiễm mã độc từ các mạng máy tính ma Botnet (tăng 1,6 lần so với năm 2014).

Ban Cơ yếu Chính phủ và Bộ Ngoại giao ký thỏa thuận phối hợp trong lĩnh vực bảo mật và ATTT

Theo thống kê của BKAV, trong năm 2015 nước ta có 62.863 dòng virus máy tính mới xuất hiện, 61,7 triệu lượt máy tính đã bị lây nhiễm virus, gây thiệt hại khoảng 8.700 tỷ đồng. Cũng trong năm 2015, có 5.226 website của các cơ quan, doanh nghiệp tại Việt Nam bị hacker xâm nhập, trong đó có 340 website của cơ quan Chính phủ và tổ chức giáo dục. Ngoài ra, nhiều tổ chức, đơn vị bị tấn công và ăn cắp dữ liệu quan trọng nhưng không dám công bố do lo ngại ảnh hưởng đến uy tín của mình. Còn theo báo cáo tổng kết năm 2015 của Kaspersky, Việt Nam là quốc gia bị tấn công mã độc nhiều thứ 4 trên thế giới, với 30,5% số lượng thiết bị CNTT bị nhiễm Malware. Đồng thời, nước ta cũng xếp thứ 3 trên thế giới và thứ 2 ở châu Á về số lượng phát tán thư rác, với 694 máy chủ bị tấn công với mục đích gửi thư rác.

Giải pháp đảm bảo ATTT cho hạ tầng CNTT trọng yếu

Trước thực tế nhiều hệ thống mạng CNTT của các cơ quan nhà nước bị tấn công trong những năm gần đây, cùng với xu thế chung của thế giới, Đảng và Nhà nước đã đưa ra nhiều chủ trương, định hướng phát triển CNTT gắn liền với việc đảm bảo an toàn, an ninh thông tin. Là cơ quan mật mã quốc gia, quản lý chuyên ngành về cơ yếu, sử dụng mật mã để thực hiện nhiệm vụ bảo mật thông tin phục vụ sự lãnh đạo, chỉ đạo của Đảng và Nhà nước, thời gian qua Ban Cơ yếu Chính phủ đã triển khai một số công việc trọng tâm bao gồm: (1) Triển khai các hệ thống bảo vệ thông tin bí mật nhà nước dùng mật mã; (2) Triển khai hệ thống chứng thực điện tử và chữ ký số (CA) phục vụ các cơ quan thuộc hệ thống chính trị; (3) Triển khai giám sát ATTT trên mạng CNTT trọng yếu của Đảng và Chính phủ; (4) Quản lý mật mã phục vụ hoạt động phát triển kinh tế - xã hội, kiểm định và quản lý chất lượng sản phẩm mật mã, đánh giá an ninh thiết bị mật mã.

Trong quá trình phối hợp với các cơ quan, tổ chức để thực hiện nhiệm vụ được giao, Ban Cơ yếu Chính phủ nhận thấy một số vấn đề còn tồn tại trong hầu hết các mạng CNTT của các cơ quan nhà nước, đó là: triển khai các giải pháp đảm bảo ATTT, bảo mật còn yếu và chưa đồng bộ; đội ngũ chuyên trách đảm bảo ATTT còn thiếu và chưa được đào tạo chuyên sâu, nhận thức của người dùng về ATTT còn chưa cao, dễ dẫn đến nguy cơ lộ/lọt, mất ATTT; quy chế, chính sách về ATTT còn chưa đồng bộ, chưa thực hiện và giám sát một cách toàn diện, triệt để, hầu hết các chính sách ATTT chưa chú trọng đến vai trò của con người, trách nhiệm về ATTT của từng tổ chức... Giải quyết được các vấn đề nêu trên sẽ góp phần đắc lực trong công tác bảo đảm ATTT trên hạ tầng CNTT. Để làm điều đó đòi hỏi phải có hệ thống giải pháp tổng thể về chính sách, kỹ thuật và đào tạo nguồn nhân lực.

Đối với vấn đề chính sách: trong những năm qua, vấn đề chính sách đối với công tác đảm bảo ATTT trên mạng CNTT đã được Đảng và Nhà nước quan tâm đúng mức, thông qua việc ban hành: Chỉ thị 28-CT/TW của Ban Bí thư Trung ương Đảng về việc tăng cường các công tác đảm bảo ATTT mạng; Luật ATTT mạng; Chỉ thị 897/CT-TTg của Thủ tướng Chính phủ về tăng cường triển khai các hoạt động đảm bảo ATTT số; Chỉ thị 15/CT-TTg của Thủ tướng Chính phủ về tăng cường đảm bảo an toàn, an ninh thông tin mạng trong thời kỳ mới; Quy chế phối hợp giữa các Bộ Thông tin và Truyền thông, Công an, Quốc phòng về đảm bảo an toàn, an ninh thông tin trên mạng CNTT…

Tuy nhiên, để các chính sách về ATTT trên mạng CNTT phát huy tác dụng, trong thời gian tới, các cơ quan chức năng cần phải tiếp tục hoàn thiện các văn bản dưới luật nhằm phát huy hiệu quả thực thi của Luật ATTT mạng. Bên cạnh đó, các bộ/ngành, địa phương cũng cần xây dựng kế hoạch cụ thể của mình nhằm thực hiện hiệu quả Quyết định số 26/QĐ-TTg của Thủ tướng Chính phủ về việc ban hành Chương trình hành động về ATTT theo Nghị quyết 36-NQ/TW nhằm đẩy mạnh ứng dụng, CNTT đáp

ứng yêu cầu phát triển bền vững và hội nhập quốc tế. Ngoài ra, các cơ quan có sử dụng mạng CNTT cần hoàn thiện quy chế về bảo đảm ATTT, để áp dụng và thực thi triệt để tại đơn vị mình.

Về các giải pháp kỹ thuật: các hệ thống hạ tầng mạng CNTT cần tập trung triển khai các giải pháp công nghệ, kỹ thuật bao gồm: giải pháp giám sát ATTT trên mạng CNTT; giải pháp chứng thực chữ ký số và các giải pháp về bảo mật khác.

Giải pháp giám sát ATTT là một trong những giải pháp quan trọng nhất và cần thiết nhất trong việc phòng chống, đối phó và ngăn chặn các cuộc tấn công mạng, nhất là đối với các mạng CNTT của các cơ quan nhà nước. Việc giám sát ATTT cho phép cảnh báo sớm được các cuộc tấn công, điểm yếu, lỗ hổng bảo mật, đồng thời đưa ra được phương án tối ưu để khắc phục và ngăn chặn các cuộc tấn công này. Từ năm 2014, Chính phủ đã giao nhiệm vụ giám sát ATTT các mạng CNTT trọng yếu của Đảng và Chính phủ cho Ban Cơ yếu Chính phủ; theo đó phê duyệt cho Ban Cơ yếu Chính phủ đầu tư, xây dựng Trung tâm giám sát ATTT quốc gia nhằm phục vụ nhu cầu về ATTT không ngừng gia tăng ở các cơ quan, đơn vị trọng yếu của Đảng và Chính phủ.

Theo số liệu thống kê về các vụ tấn công mạng trong năm 2015 của hệ thống giám sát ATTT do Ban Cơ yếu Chính phủ triển khai tại các bộ, ngành, địa phương trên cả nước, đã có 19.569 lượt tấn công khai thác lỗ hổng máy chủ, hệ thống; 221.941 lượt tấn công dò quét cổng hệ thống máy chủ, mật khẩu; phát hiện 1.512 máy bị nhiễm mã độc; 2.537 lượt vi phạm chính sách an toàn… Nhờ thực hiện nghiêm chỉnh quy định về giám sát ATTT, Trung tâm đã sớm phát hiện nhiều vụ tấn công nhằm vào các mạng trọng yếu, kịp thời đưa ra cảnh báo cùng phương án xử lý để các cơ quan nêu trên ngăn ngừa, phòng chống, giúp giảm thiểu nguy cơ gây mất ATTT tại các đơn vị trọng yếu của Đảng và Chính phủ.

Về giải pháp chứng thực chữ ký số, Ban Cơ yếu Chính phủ đã cung cấp theo yêu cầu khoảng 40.000 chứng thư số cho 20 đầu mối bộ/ngành trung ương và 37 địa phương. Tính đến nay, hầu hết các cơ quan nhà nước đã ban hành văn bản chỉ đạo, nghiêm túc triển khai thực hiện: quy định áp dụng chữ ký số trong văn bản điện tử, các văn bản hành chính chuyển qua mạng phải áp dụng chữ ký số, không dùng văn bản giấy. Một số cơ quan đạt tỷ lệ tới 80% văn bản điện tử có chữ ký số trên tổng số văn bản điện tử trao đổi chính thức; đặc biệt một số đơn vị đã thay thế hoàn toàn quy trình làm công văn giấy tờ truyền thống sang quy trình điều hành, tác nghiệp điện tử mà việc chứng thực chữ ký số là nhân tố quan trọng để đảm bảo tính xác thực và toàn vẹn của thông tin.

Trong công tác đào tạo nguồn nhân lực: phát triển, nâng cao nguồn nhân lực về đảm bảo ATTT là một điều kiện tiên quyết giúp triển khai có hiệu quả các giải pháp nêu trên. Năm 2014, Thủ tướng Chính phủ đã ký Quyết định số 99/QĐ-TTg về việc đào tạo và phát triển nguồn nhân lực an toàn, an ninh thông tin đến năm 2020, điều đó thể hiện quyết tâm của Đảng và Chính phủ trong việc đảm bảo ATTT cho hạ tầng CNTT quốc gia. Theo đó, trong thời gian tới cần tập trung nâng cao năng lực cho đội ngũ chuyên trách, xây dựng đội ngũ chuyên gia có trình độ quốc tế trong lĩnh vực ATTT. Bên cạnh đó, cần tăng cường triển khai công tác tuyên truyền, tập huấn, phổ biến kiến thức, nâng cao nhận thức trong vấn đề an toàn, an ninh thông tin cho các cán bộ làm công tác quản lý, đội ngũ lãnh đạo và toàn thể cá nhân sử dụng hệ thống.

Tóm lại, để có một hạ tầng CNTT an toàn, cần tập trung giải quyết một số yêu cầu sau: (1) Tuân thủ chặt chẽ chiến lược của các cơ quan chuyên trách đã được xác định trong các văn bản hiện hành để đảm bảo ATTT; (2) Tăng cường năng lực và phát huy vai trò của các lực lượng chuyên trách, huy động mọi nguồn lực về khoa học và công nghệ để bảo đảm ATTT theo hướng chính quy, tinh nhuệ, hiện đại, sẵn sàng ứng phó với các mối đe dọa, bảo vệ vững chắc chủ quyền quốc gia trên không gian mạng; (3) Tăng cường phối hợp giữa các lực lượng công an, quân đội, ngoại giao, cơ yếu, thông tin và truyền thông để thực hiện các biện pháp tổ chức và kỹ thuật cần thiết nhằm đối phó với các cuộc chiến tranh thông tin, làm thất bại mọi âm mưu, ý đồ sử dụng CNTT để chống phá đất nước, góp phần bảo vệ an ninh quốc gia và trật tự an toàn xã hội; (4) Xây dựng hạ tầng công nghệ đảm bảo ATTT trên cơ sở tự làm chủ, tránh lệ thuộc vào công nghệ và sản phẩm của nước ngoài; (5) Nâng cao nhận thức cho các cấp lãnh đạo, kiến thức bảo đảm ATTT cho cán bộ, nhân viên các cơ quan trong và ngoài nhà nước; (6) Thúc đẩy hợp tác quốc tế về bảo đảm ATTT để mở rộng hành lang ATTT ra khu vực và thế giới; (7) Xây dựng, hoàn thiện hạ tầng hệ thống CNTT cho các cơ quan từ trung ương đến địa phương trên cơ sở đồng bộ, được giám sát, kiểm định, đánh giá chặt chẽ về mức độ an toàn theo các tiêu chuẩn về ATTT