THẾ NÀO LÀ MỘT CHÍNH SÁCH TỐT VỀ AN NINH MẠNG?

TS. Phạm Quốc Trung, Khoa QLCN, ĐHBK Tp.HCM

Ngày nay, với sự phát triển nhanh chóng của CNTT-VT và mạng lưới Internet, các tổ chức, quốc gia đều nhận thấy những lợi ích mà hệ thống thông tin (HTTT) mang lại, như là giúp con người: làm việc nhanh hơn, hiệu quả hơn và thông minh hơn. Vì vậy, các tổ chức và quốc gia đều đẩy mạnh việc ứng dụng CNTT-VT và Internet trong việc xây dựng các HTTT của mình, như hệ thống TMĐT hay chính phủ điện tử, xem đó như là chiến lược nhằm nâng cao lợi thế cạnh tranh của tổ chức hay quốc gia. Tuy nhiên, bên cạnh lợi ích mang lại, những vấn đề đảm bảo an toàn, an ninh HTTT và dữ liệu cũng ngày càng trở nên quan trọng, bởi thông tin và HTTT đã trở thành 1 loại tài sản quý giá của tổ chức cần phải được bảo vệ. Ngày nay, các vấn đề về an toàn, an ninh HTTT có thể gặp ở khắp nơi, như: virus, trojan, tấn công mạng, tấn công từ chối dịch vụ, đánh cắp dữ liệu, thiết bị, xâm nhập CSDL trái phép, tiến hành các giao dịch trái phép… Tuy nhiên, làm thế nào để bảo vệ an toàn, an ninh HTTT, hay để đưa ra một chính sách tốt về an ninh máy tính giúp hạn chế đến mức tối thiểu các thiệt hại vẫn là 1 câu hỏi khó đối với các nhà quản lý. Bài viết này, dựa trên kinh nghiệm cá nhân của một người đang giảng dạy và nghiên cứu về lĩnh vực HTTT ở VN để đưa ra một số phân tích, nhận xét, góp ý cho các nhà quản lý về ANM. Hy vọng bài viết sẽ giúp những người ngoài ngành hiểu thêm về vấn đề khá mới và còn nhiều tranh cãi này.

Trước hết, để đơn giản, trong bài viết này, các khái niệm An ninh máy tính, An ninh thông tin, hay An ninh mạng… được xem là tương đồng nhau, cùng chỉ đến phương thức để bảo vệ sự an toàn, an ninh của các hạ tầng CNTT-VT, dữ liệu, thông tin, HTTT quan trọng… của tổ chức, đảm bảo tổ chức vận hành hiệu quả, ổn định và an toàn. Để có được chính sách an ninh thông tin tốt, người quản lý HTTT cần nhận diện các mối đe dọa đối với an toàn, an ninh của HTTT. Theo các tài liệu học thuật về HTTT (Kroenke, 2014), có ba nguồn đe dọa an ninh thông tin chính bao gồm:

- Sai lầm hoặc vi phạm (không cố ý) của con người, hoặc bất kỳ ai khi sử dụng hệ thống.
- Hành vi cố ý phá hoại của con người, chủ yếu là các hacker, hay nhân viên chống đối.
- Thảm họa từ thiên tai, như: động đất, lũ lụt, hỏa hoạn, sóng thần, sét đánh…

Trong đó, hành vi cố ý phá hoại của hacker được xem là nguy hiểm nhất. Theo các thống kê về tình hình tội phạm máy tính và Internet, với xu hướng phát triển của các công nghệ phòng chống virus và ngăn ngừa tấn công phá hoại, ngày nay, số lượng các cuộc tấn công nhỏ lẻ từ các cá nhân đã giảm xuống, nhưng mức độ nghiêm trọng và tổn hại từ các vụ tấn công mang tính tổ chức lại tăng lên. Hơn nữa, các số liệu thống kê cũng cho thấy các vấn đề an ninh nghiêm trọng gần đây liên quan đến việc đánh cắp dữ liệu, gián điệp mạng, tấn công phá hoại, hoặc chiến tranh mạng… chủ yếu đến từ các tội phạm mạng có tổ chức, hoặc được tài trợ bởi các chính phủ độc tài hay được vận hành bởi các tổ chức khủng bố quốc tế. Vì vậy, mối quan tâm về an ninh mạng hiện nay trên thế giới tập trung vào bảo vệ an toàn HTTT trước mối đe dọa từ tội phạm mạng có tổ chức là trên hết. Hơn nữa, việc tấn công mạng ngày nay còn có chiều hướng mở rộng ra các lĩnh vực khác, gây xâm phạm chủ quyền quốc gia, và có thể dẫn đến nguy cơ chiến tranh mạng. Chính vì vậy, tổng thống Obama khi đến TQ đã đề cập bóng gió đến vấn đề này.

Bảng dưới đây tóm tắt một số vấn đề về an toàn, an ninh HTTT mà các tổ chức thường gặp, như là: rò rỉ dữ liệu, chỉnh sửa sai dữ liệu, dịch vụ báo lỗi, từ chối dịch vụ, và mất mát thiết bị... Kết

nối các vấn đề này với ba nguồn đe dọa đã được nhận diện trên đây sẽ giúp mọi người dễ hình dung hơn về các vấn đề mà một chính sách an toàn, an ninh HTTT nên chú ý.

Bảng 1. Các vấn đề an ninh HTTT và những nguồn đe dọa (Kroenke, 2014)

		Source		
		Human error	**Malicious activity**	**Natural disasters**
Problem	**Unauthorised data disclosure**	Procedural mistakes	Pretexting Phishing Spoofing Sniffing Computer crime	Disclosure during recovery
	Incorrect data modification	Procedural mistakes Incorrect procedures Ineffective accounting controls System errors	Hacking Computer crime	Incorrect data recovery
	Faulty service	Procedural mistakes Development and installation errors	Computer crime Usurpation	Service improperly restored
	Denial of service	Accidents	DOS attacks	Service interruption
	Loss of infrastructure	Accidents	Theft Terrorist activity	Property loss

Theo Viện Quốc gia về Chuẩn và Công nghệ (NIST) của Mỹ (https://www.nist.gov/), một chính sách an ninh thông tin tốt cần có các đặc tính sau:

1. Cần hỗ trợ nhiệm vụ, mục tiêu của tổ chức
2. Cần tích hợp chặt chẽ với các hoạt động quản trị khác
3. Cần tiết kiệm chi phí
4. Trách nhiệm và tính giải trình cần được chỉ rõ
5. Cần xem xét tính liên đới với an toàn an ninh bên ngoài hệ thống
6. Cần một cách tiếp cận tích hợp và toàn diện
7. Cần được tái đánh giá theo định kỳ
8. Cần tuân theo các ràng buộc và quy chuẩn xã hội

Từ những thông tin trên, hãy cùng nhìn lại luật An ninh mạng (ANM) mà Quốc hội Việt Nam vừa thông qua 12/6/2018, và sẽ có hiệu lực từ 1/1/2019 để xem đó có phải là 1 chính sách tốt về an ninh thông tin hay không. Đầu tiên, cần nhận thấy luật an ninh mạng vừa được thông qua chưa thể xem là tốt bởi nó chưa đáp ứng đầy đủ các đặc tính trên. Cụ thể là, luật ANM của Việt Nam đã không thỏa mãn các đặc tính: 3 (tiết kiệm), 4 (trách nhiệm và giải trình), 6 (tiếp cận toàn diện), và 8 (tuân theo các ràng buộc xã hội). Hãy cùng tìm hiểu vì sao nhé!

- *Về chi phí triển khai*: Theo nhiều phân tích trong và ngoài nước, khi triển khai luật này, chi phí cho các DN hoạt động trong lĩnh vực CNTT-VT và các tổ chức kiểm tra, giám sát sẽ tăng lên rất lớn khi phải trang bị các hạ tầng phần cứng, phần mềm, CSVC liên quan và con người để có thể lưu trữ dữ liệu, quản lý vận hành hệ thống ở Việt Nam. Đó là chưa kể đến chi phí của các DN ngoài ngành có sử dụng các phần mềm, ứng dụng do các DN nước ngoài cung cấp. Theo luật này, họ sẽ phải chuyển đổi sang nhà cung cấp khác, nếu các DN phần mềm nước ngoài không đáp ứng các yêu cầu đặt ra của luật an ninh mạng của VN. Nhìn chung, chi phí (cả vô hình và hữu hình) của DN và các cơ quan nhà nước sẽ tăng vọt khi triển khai. Theo tôi được biết, luật ANM ở Trung Quốc tuy đã được thông qua, nhưng vẫn chưa thể đi vào triển khai trên thực tế, chính vì yêu cầu kỹ thuật về việc dời các trung tâm lưu trữ dữ liệu và kiểm tra, giám sát một lượng lớn dữ liệu là không thể đáp ứng được và làm phát sinh chi phí quá lớn khi đi vào vận hành thực tế. Điều này, trái với nguyên tắc tiết kiệm, và các nhà quản lý ANM phải cân nhắc đánh đổi giữa an ninh và hiệu quả/ thuận tiện khi vận hành. Đôi khi, để tiết kiệm chi phí, DN cần phải chấp nhận 1 mức độ rủi ro ở chừng mực nào đó, chứ không thể đảm bảo an toàn, an ninh 100%.
- *Về trách nhiệm và giải trình*: luật ANM cũng trao quyền rất lớn cho các cơ quan an ninh trong việc thu thập dữ liệu khách hàng từ các DN, mà không có các yêu cầu tương ứng về tính minh bạch và trách nhiệm giải trình, điều này sẽ dẫn đến sự lạm quyền, và có khả năng chồng chéo, và vi phạm đến các quyền riêng tư, và tự do kinh doanh, tự do ngôn luận đã được quy định trong các bộ luật khác. Ngay cả ở phạm vi tổ chức, chính sách an ninh tốt cần ngăn ngừa cả sự lạm quyền của người quản trị mạng, admin… để tránh việc vi phạm quyền riêng tư của nhân viên. Điều này đã được thảo luận và gây tranh cãi trong nhiều tình huống, bởi có những hành vi có thể không vi phạm quy định về an toàn an ninh nhưng sẽ vi phạm vấn đề đạo đức, và xâm phạm quyền riêng tư, tự do cá nhân. Các bộ luật tương tự ở các nước phát triển đều nhấn mạnh đến trách nhiệm bảo vệ an toàn dữ liệu và đảm bảo quyền riêng tư, và tự do truy cập của người sử dụng. Ở đây, cần nhấn mạnh sự cân bằng giữa an ninh và an toàn dữ liệu/ thông tin. Luật ANM của VN quá chú trọng vào an ninh, tính dễ kiểm soát, mà xem nhẹ tính an toàn, riêng tư, và thuận tiện của người sử dụng.
- *Về tiếp cận tích hợp và toàn diện*: luận ANM của VN chưa xem xét vấn đề an toàn an ninh thông tin dưới nhiều góc nhìn của các bên liên quan, mà chỉ quan tâm đến góc nhìn của cơ quan quản lý, mà cụ thể là Bộ Công An. Điều này, sẽ bỏ qua những góc nhìn khác cũng rất quan trọng trong tổng thể bức tranh về an ninh mạng, như: cá nhân, nhà kỹ thuật, nhà khoa học, doanh nghiệp, Hiệp hội doanh nghiệp, Bộ Công thương (Cục TMĐT), Bộ KH-CN (Cục SHTT)… Theo cá nhân tôi, bộ luật này đòi hỏi sự hiểu biết sâu về CNTT-VT, một lĩnh vực có sự thay đổi rất nhanh chóng, vì vậy, cần có sự tham gia ý kiến, tư vấn và phối hợp của các bộ ngành, đặc biệt là Bộ KH-CN, hiệp hội CNTT, doanh nghiệp và người tiêu dùng… thì mới đảm bảo tính tích hợp và toàn diện của các chính sách đề ra, cũng như hạn chế sự chồng lấn của luật ANM với các bộ luật hiện hành có liên quan.
- *Về tuân theo các ràng buộc xã hội*: bất kỳ luật mới nào được ban hành cũng cần phù hợp với các ràng buộc đã có trước đây, và phải tương thích với các thỏa thuận VN đã ký với quốc tế. Trái với tinh thần hội nhập quốc tế và tự do hóa thương mại, luật ANM của VN đã hạn chế sự tự do kinh doanh, tự do biểu đạt và tự do truy cập, mà LHQ đã xem là

những quyền căn bản của con người. Chính vì vậy, các tổ chức quốc tế và chuyên gia về an ninh mạng cũng đã có những kiến nghị với chính phủ VN về khả năng vi phạm các cam kết quốc tế khi VN thông qua luật ANM. Vừa rồi, chúng ta đã thấy các cuộc biểu tình ôn hòa của người dân ở cả 3 miền đất nước để phản đối luật đặc khu và an ninh mạng, điều này phản ánh mối quan tâm rất lớn của xã hội đối với 2 vấn đề này. Đặc biệt, cả 2 vấn đề đều ít nhiều liên quan đến Trung Quốc, một thế lực đang gây đe dọa cho thế giới về an ninh cả trên thế giới thực và thế giới ảo. Luật ANM này được cho là bản sao chép từ luật ANM của Trung Quốc, bởi sự giống nhau đến kinh ngạc của 2 bộ luật. Không lo sao được khi cả Mỹ và Úc đều chỉ ra các thiết bị viễn thông sản xuất bởi Huawei (TQ) là có chip gián điệp, trong khi hầu hết các thiết bị ở VN đều sử dụng linh kiện của Huawei. Các trung tâm phân tích dữ liệu từ các cuộc tấn công mạng, lấy cắp dữ liệu… gần đây đều cho thấy chúng được thực hiện từ TQ bởi các tổ chức thân chính phủ hoặc được tài trợ bởi chính phủ TQ. Cần phải xem xét những quan tâm của người dân, xã hội trong việc ban hành và xây dựng luật ANM thì nó mới có thể đi vào cuộc sống, giúp đảm bảo mọi người tuân theo và đạt được mục tiêu của bộ luật ANM là xây dựng 1 không gian mạng an toàn, lành mạnh.

Hơn nữa, một chính sách đầy đủ về an toàn an ninh máy tính trong 1 tổ chức thường bao gồm 3 thành phần như sau:

1. Một phát biểu chung về chương trình an ninh máy tính của tổ chức.
2. Các chính sách gắn với từng vấn đề cụ thể.
3. Các chính sách gắn với từng hệ thống thông tin cụ thể.

Luật ANM hiện nay của VN vừa được thông qua dường như chưa đi vào các vấn đề cụ thể đang còn gây tranh cãi, hay các hệ thống cụ thể. Điều này có lẽ do nhóm soạn thảo cũng chưa có đủ thông tin về các vấn đề ANM mà VN đang gặp phải, hoặc phải cần thêm nhiều thông tư, văn bản hướng dẫn đi kèm. Để có thể đưa ra được các chính sách cho từng vấn đề cụ thể, đòi hỏi nhóm soạn thảo luật ANM cần phải phân tích dữ liệu về các vấn đề an toàn, an ninh thông tin hiện nay ở VN và trên thế giới một cách kỹ lưỡng. Trên cơ sở đó, mới có được các chính sách phù hợp với bối cảnh VN, và đảm bảo theo kịp tốc độ phát triển nhanh chóng của lĩnh vực này. Chỉ có trên cơ sở phân tích các vấn đề rủi ro có thể gặp, các thành phần của HTTT dễ bị tổn thương, tần suất xuất hiện, mức độ nghiêm trọng, chi phí cài đặt các giải pháp ngăn ngừa… nhà quản lý mới sắp được thứ tự ưu tiên của các vấn đề cần quan tâm, từ đó, hình thành nên các chính sách chung và riêng phù hợp, giúp đảm bảo sự phát triển lành mạnh của không gian mạng, làm nền tảng vững chắc cho sự phát triển kinh tế và xã hội trong thời đại kỹ thuật số.

Hơn nữa, luật hay chính sách cần phải đi kèm với các biện pháp kỹ thuật phần cứng, phần mềm, con người và hạ tầng phù hợp. Với đà tiến triển như vũ bão của CMCN 4.0, chúng ta cần những chuyên gia am hiểu về các khái niệm mới, như: dữ liệu lớn, điện toán đám mây, internet của vạn vật, thực tại ảo, kinh tế số… Trong thời đại kỹ thuật số, luật ANM là rất cần thiết, và nên được xây dựng một cách kỹ lưỡng bởi những người am hiểu. Nếu những người đề xuất và bấm nút thông qua luật ANM mà thiếu sự am hiểu cần thiết về lĩnh vực này, thì đó sẽ là một sự rủi ro rất lớn cho đất nước về an toàn, an ninh mạng trong tương lai. Hy vọng, bài viết này sẽ góp phần giúp chúng ta hiểu thêm về một số khái niệm liên quan và nhận thức được tầm quan trọng của vấn đề ANM. Nếu may mắn, thì biết đâu những góp ý này sẽ góp phần giúp VN có được một bộ luật ANM tốt hơn cho đất nước. Mong lắm thay!