AN TOÀN THÔNG TIN TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

GS. TS. Võ Xuân Vinh –Viện Nghiên cứu Kinh doanh – UEH

Tóm tắt

Trong kỷ nguyên số, an ninh mạng đã trở thành một trong những thách thức quan trọng nhất, đặc biệt trong bối cảnh chuyển đổi số, sự phổ biến của IoT và các công nghệ mới như 5G. Tình hình toàn cầu cho thấy sự gia tăng mạnh mẽ của các cuộc tấn công mạng, từ tấn công ransomware đến đánh cắp thông tin cá nhân, đòi hỏi các quốc gia phải xây dựng hệ thống an ninh mạng toàn diện. Tại Việt Nam, thực trạng an ninh mạng vẫn đối mặt với nhiều nguy cơ, bao gồm tấn công từ chối dịch vụ (DDoS), lừa đảo trực tuyến và các lỗ hổng bảo mật trong dịch vụ điện toán đám mây. Để ứng phó, bài tham luận đề xuất các giải pháp như quản lý tài sản công nghệ thông tin thông qua danh sách chi tiết và cập nhật định kỳ; xây dựng hệ thống quản lý tài khoản chặt chẽ kết hợp xác thực đa yếu tố; áp dụng các biện pháp mã hóa dữ liệu quan trọng và tách biệt môi trường xử lý dữ liệu nhạy cảm. Ngoài ra, việc triển khai đào tạo nhận thức an ninh mạng theo từng vai trò và phát triển các sản phẩm công nghệ nội địa cũng là các giải pháp cốt lõi. Hợp tác quốc tế và đầu tư vào công nghệ bảo mật tiên tiến được nhấn mạnh để đối phó với các thách thức ngày càng phức tạp trong không gian mạng, góp phần xây dựng một môi trường mạng bền vững và an toàn.

Từ khóa: An toán thông tin, chuyển đổi số, an ninh mạng,…

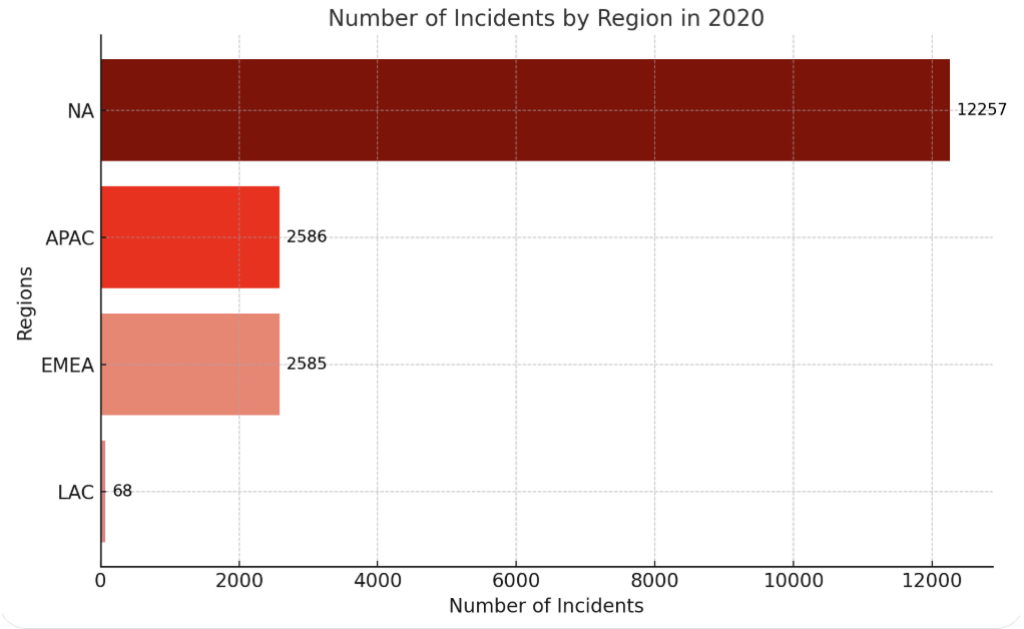
1. Tổng quan về an toàn thông tin

1.1. Tình hình thế giới

a. Thực trạng hiện tại

Tình hình an ninh mạng toàn cầu trong năm 2020 đã trở nên nghiêm trọng hơn bao giờ hết, với sự gia tăng đáng kể của các cuộc tấn công mạng trong bối cảnh đại dịch COVID-19. Việc chuyển đổi số mạnh mẽ, cùng sự gia tăng của làm việc và học tập từ xa, đã tạo điều kiện thuận lợi cho tin tặc nhắm vào các mục tiêu quan trọng như bệnh viện, trường học, và cơ sở hạ tầng thiết yếu. Báo cáo ghi nhận hơn 2.953 vụ vi phạm dữ liệu trong ba quý đầu năm, với tổng cộng 36 tỷ dữ liệu bị rò rỉ, tăng 51% so với cùng kỳ năm trước. Các loại malware phổ biến nhất gồm password dumper, trojan và ransomware, tập trung khai thác thông tin cá nhân và tài chính.

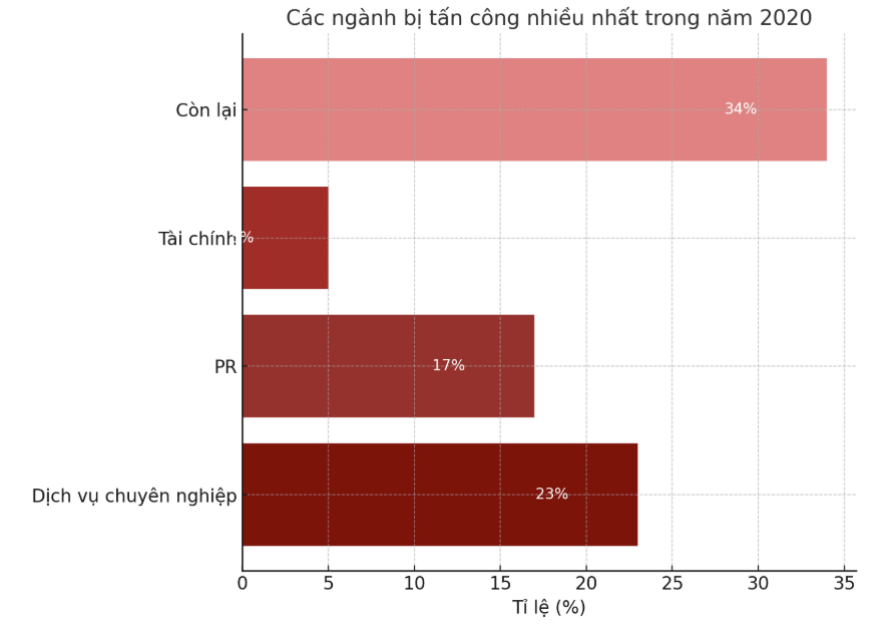
Bắc Mỹ là khu vực bị ảnh hưởng nghiêm trọng nhất, với hơn 12.257 sự cố, trong khi các ngành bị tấn công nhiều nhất bao gồm công nghệ thông tin, dịch vụ chuyên nghiệp và tài chính.



Nguồn: Vina Aspire (2020)

b. Dự báo tương lai

Trong tương lai, an ninh mạng toàn cầu sẽ tiếp tục đối mặt với các thách thức ngày càng lớn, đặc biệt khi công nghệ 5G và IoT được triển khai rộng rãi, mở ra các lỗ hổng bảo mật mới. Các thiết bị IoT, thường thiếu các lớp bảo vệ mạnh mẽ, sẽ trở thành mục tiêu chính trong các thành phố thông minh và hệ thống hạ tầng công cộng. Bên cạnh đó, việc sử dụng điện toán đám mây dự kiến sẽ tăng, nhưng cũng kèm theo nguy cơ tấn công chuỗi cung ứng và xâm nhập hệ thống qua các cấu hình sai. Xu hướng làm việc từ xa sau đại dịch sẽ tiếp tục đặt ra rủi ro từ các mạng gia đình không an toàn. Trong khi đó, sự phổ biến của tiền mã hóa sẽ tạo thêm không gian hoạt động cho các giao dịch bất hợp pháp. Để đối phó, các quốc gia cần tăng cường đầu tư vào công nghệ bảo mật tiên tiến, nâng cao nhận thức cộng đồng và đẩy mạnh hợp tác quốc tế nhằm xây dựng một không gian mạng an toàn và bền vững.

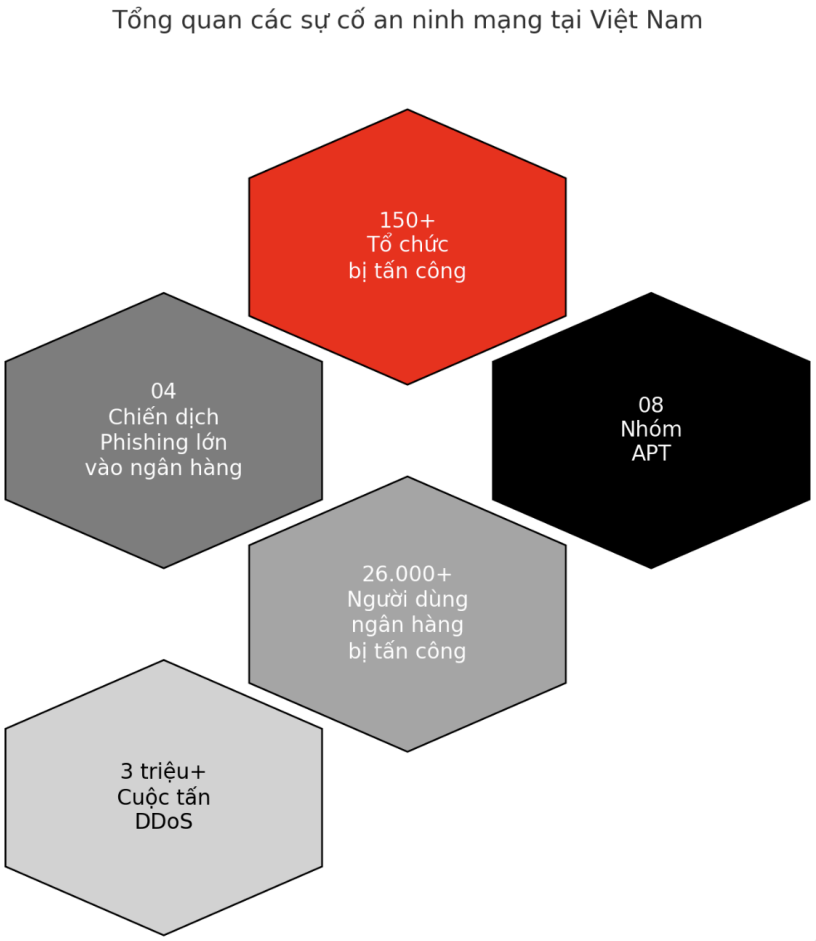


Nguồn: Vina Aspire (2020)

1.2. Tình hình Việt Nam

a. Thực trạng tại Việt Nam

Tình hình an ninh mạng tại Việt Nam đang đối mặt với nhiều thách thức nghiêm trọng, đòi hỏi các biện pháp ứng phó mạnh mẽ và toàn diện. Trong năm qua, hệ thống giám sát an ninh mạng đã ghi nhận hơn 3 triệu cuộc tấn công từ chối dịch vụ (DDoS), nhắm vào các tổ chức và hệ thống quan trọng trên cả nước. Theo thống kê, có 156 tổ chức và 306 website thuộc các tổ chức chính phủ bị ảnh hưởng, trong đó các chiến dịch phishing đã gây tác động lớn đến ngành ngân hàng với hơn 26.000 người dùng bị ảnh hưởng. Các số liệu này phản ánh mức độ nguy hiểm và sự phức tạp ngày càng gia tăng của các mối đe dọa mạng.



Nguồn: Vina Aspire (2020)

Để ứng phó với thực trạng này, Việt Nam đã xây dựng và triển khai nhiều giải pháp chiến lược nhằm tăng cường an toàn thông tin. Một trong những sáng kiến quan trọng là Hệ thống đánh giá, kiểm định an toàn thông tin theo tiêu chuẩn quốc tế, được phát triển bởi Cục An toàn thông tin. Dự án này được thiết kế để kiểm định 300-500 phiên bản sản phẩm an toàn thông tin trong giai đoạn 2021-2025, góp phần tối ưu hóa thời gian đánh giá và giảm chi phí cho các doanh nghiệp nội địa. Nhờ đó, năng lực kiểm soát và bảo vệ an toàn thông tin tại Việt Nam đã được cải thiện đáng kể.

Bên cạnh đó, hệ sinh thái các sản phẩm an toàn an ninh mạng (ATANM) nội địa đã đạt được nhiều thành tựu đáng kể. Hiện tại, Việt Nam đã làm chủ 90% các sản phẩm ATANM phục vụ các cơ quan Đảng và Nhà nước, với mục tiêu đạt 100% vào đầu năm 2021. Đây không chỉ là dấu mốc quan trọng trong việc khẳng định năng lực công nghệ mà còn thể hiện quyết tâm của Việt Nam trong việc bảo vệ chủ quyền mạng và xây dựng một không gian mạng an toàn, bền vững.

Mặc dù đạt được nhiều tiến bộ, các thách thức liên quan đến an ninh mạng vẫn còn tồn tại, đặc biệt là các cuộc tấn công có tổ chức từ các nhóm tin tặc chuyên nghiệp. Do đó, việc nâng cao nhận thức cộng đồng, đẩy mạnh hợp tác quốc tế, và phát triển các sản phẩm công nghệ "Make in Vietnam" tiếp tục là những ưu tiên quan trọng. Những nỗ lực này không chỉ giúp tăng cường năng lực ứng phó mà còn thúc đẩy sự phát triển của ngành an ninh mạng Việt Nam trong bối cảnh toàn cầu hóa và Cách mạng Công nghiệp 4.0.

b. Dự báo xu hướng an ninh mạng tại Việt Nam

Xu hướng an ninh mạng tại Việt Nam được dự báo sẽ đối mặt với nhiều thách thức lớn trong tương lai gần. Sự phát triển và thương mại hóa 5G bởi các tập đoàn lớn như Viettel, MobiFone, và VNPT mang lại nhiều cơ hội nhưng đồng thời cũng tạo ra các nguy cơ bảo mật mới, đặc biệt đối với các thiết bị liên lạc không dây. Bên cạnh đó, việc chuyển đổi sang sử dụng dịch vụ đám mây ngày càng phổ biến tại các doanh nghiệp, dù mang lại nhiều tiện ích và sự an toàn, nhưng các lỗi cấu hình hoặc lơ là trong thiết kế có thể gây ảnh hưởng nghiêm trọng đến an ninh mạng dựa trên nền tảng cloud. Đồng thời, các hành vi sử dụng phần mềm lậu vẫn là mối lo ngại lớn, đòi hỏi cần tăng cường kiểm soát, rà soát và xử phạt để giảm thiểu các nguy cơ tiềm ẩn. Ngoài ra, các hoạt động lừa đảo thông qua mạng xã hội và đánh cắp thông tin cá nhân cũng đang gia tăng nhanh chóng với mức độ ngày càng tinh vi, tạo ra nhu cầu cấp thiết trong việc nâng cao nhận thức cộng đồng và ứng dụng các biện pháp bảo mật tiên tiến[1].

2. Kinh nghiệm các quốc gia

2.1. Hoa kỳ

Hoa Kỳ, với sự phát triển sớm về internet, đã nhanh chóng trở thành mục tiêu của các tội phạm công nghệ cao gây thiệt hại nghiêm trọng. Theo FBI, năm 2020, các hoạt động tội phạm mạng đã làm tổn thất khoảng 402 tỷ USD trong ngành công nghệ thông tin, chủ yếu bởi các nhóm tổ chức chuyên trộm cắp thông tin cá nhân, tín dụng và tạo lập mạng botnet. Trước thực trạng này, các nhà lập pháp Hoa Kỳ đã ban hành những đạo luật chuyên biệt nhằm ứng phó kịp thời và hiệu quả với các mối đe dọa từ không gian mạng[2].

---

[1] Vina Aspire. (2020). Báo cáo tổng kết an ninh mạng 2020 và dự báo 2021

[2] Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023

Đạo luật Lạm dụng và Gian lận Máy tính (CFAA) được Quốc hội Hoa Kỳ thông qua năm 1986 để bổ sung các quy định còn thiếu sót trong việc xử lý gian lận máy tính. CFAA tập trung vào bảo vệ dữ liệu tài chính, thông tin mật và tín dụng thuộc Chính phủ cũng như các tổ chức tài chính, đồng thời đưa ra hình phạt nghiêm khắc cho các hành vi truy cập trái phép hoặc vượt quá thẩm quyền nhằm chiếm đoạt dữ liệu. Qua nhiều lần sửa đổi, CFAA đã mở rộng phạm vi và nâng cao hiệu quả trong việc xử lý các hành vi gian lận, trở thành công cụ pháp lý quan trọng trong bảo vệ an ninh mạng.

Việc thực thi CFAA được giao cho Bộ Tư pháp, Cục Điều tra Liên bang (FBI), và Cơ quan Mật vụ, với phạm vi áp dụng trên toàn lãnh thổ Hoa Kỳ. Đạo luật cũng cho phép các cá nhân bị thiệt hại khởi kiện dân sự để yêu cầu bồi thường. Các mức án phạt dao động từ 1 năm đến 20 năm tù, tùy theo mức độ nghiêm trọng của hành vi, cùng với việc tịch thu các tài sản liên quan đến tội phạm. Tuy nhiên, một số bất cập của CFAA đã được chỉ ra, như định nghĩa mơ hồ về công nghệ, dẫn đến nguy cơ hình sự hóa những vi phạm nhỏ trong thỏa thuận dịch vụ trực tuyến, gây tranh cãi về tính công bằng trong áp dụng pháp luật.

Ngoài CFAA, các quy định trong Luật Hình sự Hoa Kỳ cũng được sử dụng để xử lý các hành vi tội phạm công nghệ cao như truy cập dữ liệu trái phép, trộm danh tính, và gian lận qua truyền thông. Những trường hợp nghiêm trọng liên quan đến khủng bố hoặc buôn bán ma túy có thể bị áp dụng các án phạt trên 5 năm tù. Đồng thời, các tòa án Hoa Kỳ cũng yêu cầu bồi thường toàn bộ thiệt hại cho nạn nhân trong các vụ trộm danh tính, góp phần giảm thiểu tác động của tội phạm mạng đối với cá nhân và tổ chức.

2.2. Trung Quốc

Với dân số lớn nhất thế giới, Trung Quốc đã khẳng định vị thế của mình là cộng đồng trực tuyến lớn nhất toàn cầu với 802 triệu người dùng internet vào năm 2018[3]. Tuy nhiên, cùng với sự phát triển mạnh mẽ này, Trung Quốc cũng trở thành tâm điểm của các cuộc tấn công mạng, đặc biệt là từ phần mềm độc hại và nhiều hình thức tội phạm mạng khác. Trước tình hình đó, chính phủ nước này đã thực hiện các biện pháp mạnh mẽ nhằm kiểm soát và ngăn chặn hiệu quả các mối đe dọa từ không gian mạng[4].

Luật An ninh mạng (Luật ANM), được ban hành vào ngày 7/11/2016 và chính thức có hiệu lực từ ngày 1/6/2017, là một bước đi quan trọng trong việc củng cố nền tảng pháp lý của Trung Quốc về an ninh mạng[5]. Luật gồm 79 điều chia thành 7 chương, với mục tiêu

[3] Trung tâm Thông tin Internet Trung Quốc (CNNIC).
[4] Symantec. (2021). Symantec security summary - December 2021.
[5] The National People's Congress of the People's Republic of China. (2021). Data Security Law of the People's Republic of China.

chính là bảo vệ chủ quyền mạng, đảm bảo an toàn thông tin cá nhân, và quản lý cơ sở hạ tầng thông tin quan trọng. Các quy định trong luật nhấn mạnh vai trò lãnh đạo và kiểm soát của nhà nước, đồng thời đặt ra các yêu cầu khắt khe đối với các nhà cung cấp dịch vụ internet trong việc thực hiện trách nhiệm bảo mật và bảo vệ dữ liệu[6].

Ngoài việc trao quyền giám sát mạnh mẽ cho chính phủ, Luật ANM còn yêu cầu các nhà cung cấp mạng thực hiện các biện pháp nghiêm ngặt nhằm đảm bảo an ninh mạng. Những biện pháp này bao gồm xây dựng hệ thống quản lý nội bộ, lưu trữ nhật ký mạng trong ít nhất 6 tháng, và sao lưu dữ liệu quan trọng. Các doanh nghiệp và tổ chức liên quan cũng được yêu cầu tuân thủ luật pháp, đạo đức xã hội và thực hiện trách nhiệm bảo vệ an ninh mạng dưới sự giám sát của chính phủ và cộng đồng.

Hiệu quả của Luật ANM đã được thể hiện qua việc giảm thiểu đáng kể các vụ tấn công mạng tại Trung Quốc. Tuy nhiên, luật này cũng gặp phải nhiều chỉ trích, đặc biệt liên quan đến các quy định về quyền riêng tư và tự do trực tuyến. Các yêu cầu như đăng ký tên thật, lưu trữ dữ liệu trong nước hay giám sát chặt chẽ nội dung đã làm dấy lên lo ngại về xâm phạm quyền cá nhân và hạn chế tính tự do của mạng internet. Mặc dù vậy, những biện pháp này vẫn được đánh giá là cần thiết để đối phó với các mối đe dọa an ninh ngày càng phức tạp, đặt ra câu hỏi về sự cân bằng giữa bảo mật và tự do cá nhân trong không gian mạng[7].

2.3. Anh quốc

Vương quốc Anh, với vị thế là một trung tâm tài chính hàng đầu thế giới, đã trở thành mục tiêu quan trọng của các cuộc tấn công mạng. Để ứng phó với các thách thức này, một hành lang pháp lý chặt chẽ đã được thiết lập nhằm kiểm soát và xử lý hiệu quả các hành vi vi phạm trong không gian mạng. Sự phát triển của các quy định pháp lý này không chỉ thể hiện sự phản ứng nhanh nhạy của Anh Quốc mà còn trở thành hình mẫu cho nhiều quốc gia khác trên thế giới.

Đạo luật Lạm dụng Máy tính (Computer Misuse Act) năm 1990 được xem là nền tảng pháp lý đầu tiên tại Anh dành riêng để xử lý tội phạm công nghệ cao. Đạo luật này, với 18 điều chia thành 3 chương, đã quy định rõ các hành vi vi phạm như truy cập trái phép và phá hoại dữ liệu máy tính, đồng thời xác định thẩm quyền xử lý của các cơ quan chức năng. Các quy định cũng bao gồm hướng dẫn cụ thể về sự phối hợp giữa các khu vực thành viên như Scotland và Bắc Ireland trong việc phòng chống tội phạm mạng. Tính linh hoạt

[6] Beckett, N. (2017). A guide for businesses to China's first cyber security law.
[7] Điều 5 và 9 Luật an ninh mạng nước Cộng hòa nhân dân Trong Hoa.

và khả năng răn đe của đạo luật đã giúp Anh Quốc hạn chế đáng kể các hành vi vi phạm, đồng thời được nhiều quốc gia như Canada và Ireland học hỏi, áp dụng[8].

Sự phát triển không ngừng của công nghệ và tội phạm mạng đã thúc đẩy Anh Quốc sửa đổi và cập nhật Đạo luật Lạm dụng Máy tính vào năm 2015, tích hợp vào Đạo luật Tội phạm Nghiêm trọng (Serious Crime Act). Các sửa đổi bổ sung đã mở rộng phạm vi xử lý, bao gồm cả các hành vi cung cấp công cụ hỗ trợ tội phạm mạng mà không phụ thuộc vào mục đích ban đầu của người cung cấp. Đồng thời, quyền tài phán cũng được mở rộng, cho phép truy tố công dân Anh vi phạm pháp luật tại nước ngoài, qua đó nâng cao hiệu quả phòng chống tội phạm xuyên quốc gia.

Việc không ngừng cải tiến và cập nhật luật pháp đã giúp Anh Quốc duy trì một hệ thống pháp luật linh hoạt, phù hợp với bối cảnh phát triển của Cách mạng Công nghiệp 4.0. Các biện pháp này không chỉ đảm bảo một nền tảng vững chắc để đối phó với tội phạm mạng mà còn tạo ra sự cân bằng hợp lý giữa bảo vệ quyền riêng tư cá nhân và đảm bảo an ninh quốc gia. Qua đó, Anh Quốc tiếp tục khẳng định vai trò dẫn đầu trong lĩnh vực quản lý và phòng chống tội phạm công nghệ cao.

2.4. Bài học kinh nghiệm cho Việt Nam

Kinh nghiệm từ Hoa Kỳ cho thấy việc xây dựng hành lang pháp lý chuyên biệt để xử lý tội phạm công nghệ cao cần được ưu tiên hàng đầu tại Việt Nam. Đạo luật CFAA của Hoa Kỳ, được ban hành năm 1986, đã thiết lập một nền tảng pháp lý nhằm bảo vệ dữ liệu mật, thông tin tài chính và tín dụng. Hệ thống này không chỉ đưa ra các quy định rõ ràng về hành vi truy cập trái phép mà còn bổ sung khung hình phạt nghiêm khắc cho các hành vi gian lận máy tính. Qua đó, hiệu quả trong việc truy tố và xử lý tội phạm đã được cải thiện đáng kể. Tại Việt Nam, một hệ thống tương tự cần được xây dựng nhằm nâng cao năng lực đối phó với các loại hình tội phạm mạng đang ngày càng gia tăng về mức độ phức tạp.

Vai trò quản lý mạnh mẽ của nhà nước trong kiểm soát không gian mạng được thể hiện rõ qua kinh nghiệm từ Trung Quốc. Với việc Luật An ninh mạng được ban hành vào năm 2016, trách nhiệm bảo mật đã được phân bổ chặt chẽ cho các nhà cung cấp dịch vụ internet, đồng thời các biện pháp giám sát dữ liệu và cơ sở hạ tầng thông tin quan trọng cũng được triển khai toàn diện. Tuy nhiên, những quy định này đã làm dấy lên tranh cãi về việc xâm phạm quyền riêng tư và hạn chế tự do trực tuyến. Đối với Việt Nam, các biện pháp quản lý cần được áp dụng một cách linh hoạt hơn, vừa đảm bảo an ninh mạng vừa tạo điều kiện cho không gian số phát triển bền vững.

---

[8] Parliament of the United Kingdom. (1990). Computer Misuse Act 1990.

Từ kinh nghiệm của Vương quốc Anh, việc cập nhật và điều chỉnh luật pháp để phù hợp với sự phát triển của công nghệ cần được ưu tiên. Việc sửa đổi Đạo luật Lạm dụng Máy tính và tích hợp vào Đạo luật Tội phạm Nghiêm trọng đã mở rộng đáng kể phạm vi xử lý, đặc biệt là các hành vi phạm tội xuyên biên giới. Các biện pháp này đã cho phép chính phủ Anh đối phó hiệu quả hơn với các mối đe dọa mới trong không gian mạng. Tại Việt Nam, luật pháp hiện hành cần được sửa đổi và bổ sung để không chỉ theo kịp các xu hướng công nghệ mới mà còn đáp ứng được yêu cầu của một môi trường mạng toàn cầu hóa.

Hợp tác quốc tế đã được chứng minh là một giải pháp hiệu quả trong việc phòng chống tội phạm công nghệ cao ở các quốc gia như Hoa Kỳ, Trung Quốc và Vương quốc Anh. Việc chia sẻ dữ liệu, phối hợp điều tra, và tham gia các thỏa thuận quốc tế đã giúp các quốc gia này tăng cường khả năng ứng phó với các mối đe dọa mạng xuyên quốc gia. Tại Việt Nam, việc tham gia tích cực vào các sáng kiến hợp tác quốc tế không chỉ giúp tăng cường năng lực nội địa mà còn nâng cao vị thế quốc gia trên trường quốc tế trong lĩnh vực an ninh mạng.

Đầu tư vào công nghệ và đào tạo nhân lực đã được xem là yếu tố quan trọng trong việc nâng cao năng lực xử lý tội phạm công nghệ cao. Tại các quốc gia như Hoa Kỳ và Trung Quốc, các chương trình đào tạo chuyên sâu và hệ thống công nghệ tiên tiến đã được triển khai để tăng cường khả năng phát hiện và ngăn chặn tội phạm. Tại Việt Nam, các chương trình tương tự cần được thực hiện, với trọng tâm là xây dựng đội ngũ chuyên gia có trình độ cao và ứng dụng các công nghệ hiện đại để bảo vệ không gian mạng một cách hiệu quả.

Việc áp dụng các bài học quốc tế vào bối cảnh Việt Nam sẽ góp phần quan trọng trong việc xây dựng một hệ thống quản lý an ninh mạng toàn diện. Các biện pháp như hoàn thiện pháp luật, tăng cường vai trò quản lý, thúc đẩy hợp tác quốc tế và đầu tư vào công nghệ cần được triển khai đồng bộ, nhằm đảm bảo không gian mạng an toàn và hỗ trợ sự phát triển bền vững của nền kinh tế số quốc gia.

3. Các giải pháp tăng cường an ninh mạng cho Việt Nam

- Đầu tư vào hạ tầng viễn thông và công nghệ thông tin

Cần tập trung đầu tư xây dựng các trung tâm dữ liệu (Data Center) có quy mô lớn, hiện đại, đáp ứng tiêu chuẩn quốc tế. Những trung tâm này đóng vai trò quan trọng trong việc xây dựng một nền tảng công nghệ bền vững, giúp giảm thiểu các lỗ

hổng liên quan đến dữ liệu, đồng thời đảm bảo sự ổn định cho các hoạt động quản lý và bảo mật thông tin trên phạm vi toàn diện.

- Xây dựng hệ thống pháp luật về quản lý và lưu trữ dữ liệu

Xây dựng khung pháp luật yêu cầu các doanh nghiệp khai thác dữ liệu người dùng đặt máy chủ tại Việt Nam để tăng cường kiểm soát thông tin cá nhân và bảo vệ dữ liệu quốc gia. Chính sách này cũng đảm bảo sự tuân thủ nghiêm ngặt của doanh nghiệp đối với các quy định an ninh mạng và bảo mật dữ liệu.

- Thành lập doanh nghiệp giám sát độc lập

Đề xuất thành lập hoặc hợp tác với các doanh nghiệp thứ ba chuyên trách giám sát các hoạt động quản lý, bảo mật và khai thác thông tin người dùng. Những doanh nghiệp này sẽ đảm bảo các quy trình đều tuân thủ pháp luật và các tiêu chuẩn bảo mật, giảm thiểu rủi ro lạm dụng thông tin.

- Tăng cường quản lý doanh nghiệp nền tảng và xuyên quốc gia

Các công ty nền tảng công nghệ, đặc biệt là những doanh nghiệp vận hành xuyên quốc gia như (Netflix, các nền tảng từ Thái Dương,…), cần thực hiện nghiêm túc các quy định quốc gia về bảo mật và quản lý thông tin. Chính phủ cần có cơ chế giám sát chặt chẽ để đảm bảo sự tuân thủ này.

- Hợp tác với các công ty công nghệ uy tín

Hợp tác với các doanh nghiệp công nghệ cao, uy tín trong lĩnh vực viễn thông và công nghệ thông tin thông qua các hợp đồng có ràng buộc để đảm bảo an toàn thông, từ hạ tầng lõi đến các thiết bị cuối trong hệ thống.

- Tăng cường kiểm thực thông tin và xác thực dữ liệu

Trong các giao dịch kinh tế và thương mại, cần tăng cường quy trình xác thực dữ liệu người dùng. Điều này không chỉ giảm thiểu rủi ro từ các thông tin giả mạo mà còn củng cố niềm tin của người tiêu dùng vào hệ thống giao dịch trực tuyến.

- Quản lý tài sản phần cứng

Quản lý tài sản phần cứng là nền tảng để bảo vệ an toàn thông tin mạng, bao gồm việc lập danh mục và theo dõi trạng thái của tất cả các thiết bị phần cứng. Các tài sản cần được nhận diện chi tiết theo thông tin như địa chỉ IP tĩnh, địa chỉ MAC, số serial, và vị trí lắp đặt trong hệ thống. Điều này không chỉ giúp kiểm soát hiệu

quả mà còn hỗ trợ trong việc ứng phó kịp thời khi xảy ra sự cố. Đồng thời, các thiết bị không được quản lý hoặc kết nối trái phép cần bị rà soát định kỳ và xử lý ngay lập tức bằng cách loại bỏ hoặc cách ly khỏi hệ thống mạng. Để đảm bảo bảo mật, tất cả các thiết bị phải được kiểm tra an ninh trước khi đưa vào sử dụng và phải được giao trách nhiệm cụ thể cho cá nhân hoặc bộ phận quản lý. Quy trình này đòi hỏi cập nhật danh sách ít nhất hai lần mỗi năm nhằm duy trì tính chính xác và đồng bộ với hệ thống quản lý an ninh.

- Quản lý tài sản phần mềm

Tài sản phần mềm cần được quản lý dựa trên danh sách các ứng dụng đã được phê duyệt, bao gồm thông tin về mục đích sử dụng, phiên bản, bản quyền, và trạng thái hỗ trợ kỹ thuật. Việc kiểm soát này giúp hạn chế việc sử dụng phần mềm trái phép, đồng thời giảm thiểu nguy cơ phát sinh các lỗ hổng bảo mật từ các ứng dụng không được kiểm tra. Hơn nữa, các phần mềm trái phép nhưng cần thiết phải được đưa vào danh sách ngoại lệ kèm theo các biện pháp kiểm soát nghiêm ngặt. Để duy trì an toàn hệ thống, tổ chức cần định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng, đồng thời kiểm soát việc cài đặt hoặc gỡ bỏ phần mềm một cách có hệ thống. Quy trình này cũng cần triển khai các công cụ giám sát hoạt động của phần mềm để đảm bảo mọi thay đổi đều nằm trong phạm vi cho phép.

- Quản lý tài sản thông tin

Quản lý tài sản thông tin yêu cầu tổ chức phải xác định rõ mức độ nhạy cảm của dữ liệu, từ đó áp dụng các biện pháp phù hợp cho từng loại thông tin. Ví dụ, tài liệu công khai không cần yêu cầu bảo mật, nhưng dữ liệu nội bộ hoặc thông tin bí mật nhà nước cần có các biện pháp mã hóa và kiểm soát truy cập nghiêm ngặt. Tổ chức cần xây dựng và duy trì một quy trình đầy đủ về phát hiện, phân loại, xử lý, lưu trữ, và tiêu hủy thông tin, trong đó có việc giám sát quyền truy cập và đảm bảo dữ liệu được tách biệt giữa các môi trường xử lý. Ngoài ra, việc tài liệu hóa luồng dữ liệu và kiểm tra định kỳ quyền truy cập là yếu tố không thể thiếu để bảo vệ an ninh thông tin trong dài hạn.

- Cấu hình an toàn cho thiết bị và phần mềm

Cấu hình an toàn giúp hạn chế các rủi ro xâm nhập từ bên ngoài thông qua việc thiết lập các quy định và quy trình bảo mật cụ thể. Các biện pháp cơ bản bao

gồm khóa tự động sau một khoảng thời gian không hoạt động, vô hiệu hóa các tính năng không cần thiết, và thiết lập cấu hình mạng an toàn. Tất cả các thiết bị và phần mềm cần được duy trì cấu hình bảo mật phù hợp với các giao thức kết nối an toàn và phải được rà soát, cập nhật định kỳ để phù hợp với các yêu cầu bảo mật mới nhất. Bên cạnh đó, tổ chức cần áp dụng các giải pháp kỹ thuật như tường lửa và mã hóa dữ liệu để bảo vệ hệ thống trước các nguy cơ tiềm tàng.

- Quản lý tài khoản và quyền truy cập

Việc quản lý tài khoản người dùng và quyền truy cập là một yếu tố quan trọng để đảm bảo chỉ những cá nhân có thẩm quyền mới được truy cập vào dữ liệu và tài nguyên của tổ chức. Tài khoản cần được phân loại rõ ràng thành các loại như tài khoản người dùng, quản trị và dịch vụ, với danh sách chi tiết bao gồm trạng thái, quyền hạn, và người quản lý. Đồng thời, tổ chức cần áp dụng mật khẩu mạnh và cơ chế xác thực đa yếu tố đối với các tài khoản quan trọng. Việc rà soát tài khoản không hoạt động và vô hiệu hóa ngay khi có thay đổi nhân sự là cần thiết để ngăn chặn rủi ro từ việc lạm dụng tài khoản.

- Quản lý lỗ hổng bảo mật

Để bảo vệ hệ thống trước các lỗ hổng bảo mật, tổ chức cần xây dựng quy trình phát hiện, đánh giá và xử lý lỗ hổng thường xuyên. Rà soát định kỳ giúp phát hiện sớm các điểm yếu trong phần cứng và phần mềm, từ đó triển khai các biện pháp khắc phục kịp thời. Bên cạnh đó, việc chia sẻ thông tin về các lỗ hổng với cơ quan chức năng và đối tác liên quan cũng giúp cải thiện hiệu quả trong việc giảm thiểu nguy cơ. Quy trình này cần được đánh giá và cập nhật định kỳ để luôn đảm bảo phù hợp với tình hình thực tế và các thay đổi trong công nghệ.

- Giám sát và bảo vệ an ninh mạng

Hệ thống giám sát an ninh mạng cần được triển khai toàn diện để phát hiện và ứng phó với các sự cố. Tổ chức nên sử dụng các công cụ quản lý sự kiện an ninh mạng tập trung, tích hợp các giải pháp như tường lửa, IDS/IPS, và công cụ lọc gói tin để ngăn chặn xâm nhập trái phép. Hơn nữa, cần thiết lập các cấu hình kiểm soát truy cập tại các cổng kết nối mạng, thu thập nhật ký lưu lượng để phân tích và cảnh báo kịp thời. Mỗi sự cố cần được đánh giá và xử lý ngay, đi kèm với việc diễn tập định kỳ để nâng cao năng lực ứng phó.

- Nâng cao nhận thức và đào tạo kỹ năng an ninh mạng

Đào tạo nâng cao nhận thức an ninh mạng là hoạt động bắt buộc để xây dựng văn hóa bảo mật trong tổ chức. Các chương trình đào tạo cần được thiết kế phù hợp với vai trò của từng cá nhân, bao gồm cả việc nhận diện các nguy cơ như lừa đảo, tấn công phi kỹ thuật, và cách ứng phó. Ngoài ra, lực lượng chuyên biệt bảo vệ an ninh mạng cần được thành lập và huấn luyện với các kỹ năng chuyên sâu nhằm sẵn sàng ứng phó với các sự cố nghiêm trọng

Tài liệu tham khảo:

Beckett, N. (2017). *A guide for businesses to China's first cyber security law*.

Parliament of the United Kingdom. (1990). *Computer Misuse Act 1990*.

Symantec. (2021). *Symantec security summary - December 2021*.

The National People's Congress of the People's Republic of China. (2021). *Data Security Law of the People's Republic of China*.

Trung tâm Thông tin Internet Trung Quốc (CNNIC).

Vina Aspire. (2020). *Báo cáo tổng kết an ninh mạng 2020 và dự báo 2021*.

Annual amount of monetary damage caused by reported cybercrime in the United States from 2001 to 2023.