TẠP CHÍ
Nghiên cứu Con Người
Journal of Human Studies
ISSN 2815 - 5777
Số 1(130) 2024

- Nghiên cứu chuẩn mực con người trong thời kì mới
- Một số vấn đề lí luận về tri thức bản địa trong thích ứng với biến đổi khí hậu
- Một số vấn đề lí luận nghiên cứu hòa nhập số
- Xâm phạm an ninh mạng - Một số hành vi phổ biến và gợi ý giải pháp xây dựng, phát triển năng lực quản lí sự cố an ninh mạng

VIỆN NGHIÊN CỨU CON NGƯỜI
VIỆN HÀN LÂM KHOA HỌC XÃ HỘI VIỆT NAM

Nghiên cứu Con người

NĂM THỨ HAI MƯƠI HAI - TẠP CHÍ RA 2 THÁNG MỘT KỲ

Số 1(130) 2024

MỤC LỤC

XÂM PHẠM AN NINH MẠNG - MỘT SỐ HÀNH VI PHỔ BIẾN VÀ GỢI Ý GIẢI PHÁP XÂY DỰNG, PHÁT TRIỂN NĂNG LỰC QUẢN LÍ SỰ CỐ AN NINH MẠNG[1]

PHẠM HƯƠNG TRÀ(*)
LÊ NGUYỄN PHƯƠNG THẢO(**)

Tóm tắt: Cuộc Cách mạng công nghiệp 4.0 đã mang lại những lợi ích vô cùng quan trọng, đồng thời đặt ra nhiều thách thức lớn đối với an ninh trật tự quốc tế. An ninh mạng, trong bối cảnh này, đã trở thành một vấn đề toàn cầu quan trọng. Nhận diện các hành vi xâm phạm an ninh mạng như lợi dụng dữ liệu cá nhân, tấn công mạng, và vô hiệu hóa chức năng của hệ thống ngày càng trở nên cấp thiết; đồng thời cần xây dựng và phát triển năng lực quản lí sự cố an ninh mạng quốc gia, hướng đến mục tiêu đảm bảo an ninh mạng và phát triển bền vững cho hệ thống thông tin trong môi trường số đang ngày càng phát triển và phức tạp.

Từ khóa*: an ninh mạng, tội phạm mạng, nhận diện hành vi.*

Abstract: The Fourth Industrial Revolution has brought about immensely significant benefits while simultaneously posing substantial challenges to international security. In this context, cybersecurity has become a crucial global issue. The identification of cybersecurity breach behaviors, such as the exploitation of personal data, cyber attacks, and the disablement of system functions, has become increasingly urgent. Simultaneously, there is a pressing need to build and develop national cybersecurity incident management capabilities, aiming to ensure the cybersecurity and sustainable development of information systems in an ever-growing and complex digital environment.

Keywords*: cybersecurity, cybercrime, cybersecurity, behavior identification.*

Ngày nhận bài: 10/01/2024; ngày gửi phản biện: 11/01/2024; ngày duyệt đăng bài: 16/02/2024.

1. Giới thiệu: Xâm phạm an ninh mạng - vấn nạn mang tính toàn cầu

Cuộc Cách mạng công nghiệp 4.0 hiện đang tiến triển với tốc độ nhanh chóng, đồng thời đi kèm với sự phát triển mạnh mẽ của không gian mạng. Đặc biệt, với xu hướng công nghệ toàn cầu, khi mọi hoạt động được số hóa, không gian mạng ngày càng trở nên quan trọng và mở rộng. Sự kết hợp giữa các hệ thống và thực thể ảo đang thay đổi cách con người làm việc và tạo ra sản phẩm, từ đó tạo ra "cuộc cách mạng 4.0" về tổ chức sản xuất,

(*) Học viện Báo chí và Tuyên truyền.
(**) Đại học Khoa học Huế.

[1] Bài viết trong khuôn khổ Đề tài cấp Nhà nước KX04.32/21-25: *Vấn đề an ninh phi truyền thống, trọng tâm là an ninh mạng trong nền an ninh quốc gia* thuộc Chương trình khoa học xã hội trọng điểm cấp Quốc gia giai đoạn 2021 - 2025 "Nghiên cứu khoa học lí luận chính trị giai đoạn 2021 - 2025".

chuỗi giá trị, phát triển kinh tế và xã hội. Bên cạnh những lợi ích to lớn không thể phủ nhận, ưu điểm của kết nối toàn cầu với đặc thù không biên giới cũng mang lại nhiều thách thức lớn cho an ninh trật tự của các quốc gia trên thế giới. Điều này đặc biệt đúng ở các nước phát triển và có nền công nghệ tiên tiến, khiến cho an ninh mạng trở thành một vấn đề cấp thiết. Tội phạm mạng gây thiệt hại ước tính khoảng 600 tỉ USD hàng năm, tương đương 0,8% GDP toàn cầu. Riêng khu vực Đông Á, thiệt hại ước tính khoảng 12 - 200 tỉ USD, tương đương 0,53% - 0,89% GDP của khu vực. Mức thiệt hại 642 triệu đô la Mĩ, tương đương 0,26% GDP của Việt Nam, chưa phải là cao so với khu vực và thế giới, nhưng vẫn là mức đáng kinh ngạc (Thông tấn xã Việt Nam, 2018).

Trong thực tế, hầu hết các cuộc tấn công mạng được thực hiện thông qua việc sử dụng một hoặc nhiều công cụ phần mềm được xây dựng bởi kẻ tấn công, hoặc được lấy từ các nguồn khác nhau với mục đích phá hoại, làm thất thoát hoặc chiếm đoạt tài sản một cách bất hợp pháp. Các hành vi này không chỉ gây tổn thất về dữ liệu mà còn ảnh hưởng đến quyền riêng tư cá nhân và thậm chí có thể để lại hậu quả nặng nề cho an ninh quốc gia. Quy mô và mức độ nguy hiểm của các cuộc tấn công mạng đang gia tăng, tạo ra những thách thức mới đòi hỏi sự phối hợp trong các lĩnh vực kĩ thuật, pháp luật và xã hội để ứng phó và xử lí kịp thời. Nhiều quốc gia trên thế giới liên tục ghi nhận các cuộc tấn công, xâm nhập vào hệ thống máy tính của các cơ quan chính phủ, tổ chức chính trị, các ngành công nghiệp, các đơn vị kinh tế tiên phong và các tổ chức truyền thông, các hãng hàng không lớn, các tổ chức y tế và giáo dục. Ở Mĩ, các vụ tấn công nổi bật bao gồm xâm nhập vào hệ thống thư điện tử của Bộ Ngoại giao, máy tính của Nhà Trắng, và cơ quan quản lí nhân sự Chính phủ Mĩ. Nhiều nhóm hacker đã sử dụng mã độc để đánh cắp dữ liệu và thu thập thông tin tình báo quan trọng về các khía cạnh chính trị, kinh tế và quân sự.

Nghiên cứu này tập trung vào việc phân tích, nhận diện các hành vi xâm phạm an ninh mạng phổ biến và đề xuất các giải pháp xây dựng, phát triển năng lực quản lí sự cố an ninh mạng, mở ra những triển vọng trong việc xây dựng cơ sở hạ tầng an ninh mạng toàn cầu và tăng cường sự hợp tác quốc tế để đối phó với thách thức ngày càng phức tạp này.

2. Cơ sở lí thuyết

Tác giả Ross J. Anderson trong cuốn sách *Security Engineering: A Guide to Building Dependable Distributed Systems* (Kĩ thuật bảo mật: Hướng dẫn xây dựng hệ thống phân tán đáng tin cậy) đã định nghĩa xâm phạm an ninh mạng (cybersecurity breach): "Sự việc hệ thống mạng bị tấn công và bị chiếm đoạt, thất thoát thông tin hoặc chức năng của nó bị ảnh hưởng một cách bất hợp pháp" (Ross J. Anderson, 2008). Những nguy cơ này không chỉ xuất phát từ cá nhân hay tổ chức tội phạm mạng, mà còn từ các quốc gia hoặc tổ chức có mục tiêu thù địch. Hệ thống pháp luật và kĩ thuật phòng ngừa ngày càng trở nên quan trọng, cần phải đồng bộ và linh hoạt để ứng phó với những thách thức đa dạng và ngày càng phức tạp.

Hai tác giả Richard A. Clarke, Robert Knake cho rằng đây là: "Hành động có chủ đích nhằm vào hệ thống máy tính, mạng, hoặc dữ liệu để gây hại hoặc thu thập thông tin

một cách trái pháp luật". Trong định nghĩa này, "hành động có chủ đích" đặt ra khía cạnh quan trọng của sự cố, kết quả của một kế hoạch có chủ đích. Hành động này không chỉ hướng đến việc gây thiệt hại về mặt kĩ thuật mà còn liên quan đến mục đích thu thập thông tin quan trọng, có thể làm thay đổi tình hình quốc gia, kinh tế, hay thậm chí là an ninh quốc gia (Richard A. Clarke, Robert Knake, 2010).

Như vậy, bất kì hành vi nào được thực hiện có chủ đích sử dụng phương tiện không gian mạng ảnh hưởng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân và quốc gia hoặc sự ổn định chính trị, xã hội, chẳng hạn như chỉ trích chính trị hoặc phát ngôn chống lại các phán quyết đều được xem là xâm phạm an ninh mạng.

Tại Diễn đàn Kinh tế thế giới 2018 (World Economic Forum, 2018), các nhà lãnh đạo toàn cầu bày tỏ lo ngại về xu hướng ngày càng gia tăng của các cuộc tấn công mạng nhằm vào cơ sở hạ tầng quan trọng và các lĩnh vực công nghiệp chiến lược, với lí do lo ngại về trường hợp xấu nhất có thể dẫn đến sự đổ vỡ của các hệ thống giữ cho các xã hội hoạt động. Các hành vi xâm phạm an ninh mạng phổ biến:

Thứ nhất, tấn công trực tiếp. Các cuộc tấn công trực tiếp thường được sử dụng ở giai đoạn đầu để truy cập nội bộ. Một phương pháp tấn công cổ điển là phát hiện tên người dùng và mật khẩu. Phương pháp này đơn giản, dễ thực hiện và không yêu cầu bất kì điều kiện đặc biệt nào để bắt đầu. Những kẻ tấn công có thể dựa vào thông tin mà chúng biết, chẳng hạn như tên người dùng, ngày sinh, địa chỉ, số nhà, v.v. để đoán mật khẩu dựa trên các quy trình tự động nhằm dò mật khẩu. Trong một số trường hợp, tỉ lệ thành công của phương pháp này có thể cao tới 30%. Phương pháp khai thác lỗ hổng trong các ứng dụng và bản thân hệ điều hành đã được sử dụng kể từ những cuộc tấn công đầu tiên và vẫn tiếp tục chiếm được quyền truy cập. Trong một số trường hợp, phương pháp này cho phép kẻ tấn công có được đặc quyền của quản trị viên hệ thống.

Điển hình, nền tảng ForceNet - hoạt động dưới dạng mạng xã hội, giúp các quân nhân và nhân viên quốc phòng liên lạc với gia đình của Bộ Quốc phòng Australia bị tấn công trực tiếp bằng mã độc tống tiền. Đây cũng là địa chỉ chia sẻ thông tin về các sự kiện cộng đồng, cơ hội việc làm, cũng như liên hệ với các dịch vụ hỗ trợ dành cho người dân. Hoặc trường hợp công ty bảo hiểm y tế lớn nhất của Australia là Medibank xác nhận tin tặc đã truy cập dữ liệu của ít nhất 4 triệu khách hàng đăng kí mua bảo hiểm của công ty, bao gồm cả dữ liệu về sức khỏe cá nhân và số tài khoản ngân hàng.

Thứ hai, nghe trộm. Các ứng dụng và chương trình trên hệ thống có thể cung cấp thông tin như tên người dùng, mật khẩu và dữ liệu bí mật nếu bị kẻ tấn công theo dõi. Các nỗ lực ghi lại dữ liệu này được thực hiện ngay lập tức khi kẻ xâm nhập có được quyền truy cập vào hệ thống. Những thông tin này cũng có thể dễ dàng lấy được trên internet. Hiện nay, trên lãnh thổ Việt Nam, ở nhiều địa điểm trên địa bàn thành phố Hồ Chí Minh, tỉnh Lâm Đồng, Sơn La, v.v., Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (Bộ Công an) đã bắt giữ nhiều đối tượng trong đường dây mua bán các phần mềm nghe lén trên điện thoại di động, phần mềm gián điệp. Phần mềm này khi được

cài đặt vào điện thoại di động có thể đánh cắp thông tin cá nhân như: tài khoản ngân hàng, tài khoản Email, Viber, Zalo, Facebook; các giao dịch internet banking có thể bị kiểm soát mà chủ thể không hề hay biết. Ngoài ra, phần mềm này còn ghi âm bí mật nội dung cuộc đàm thoại nghe, gọi. Đáng lo ngại, toàn bộ thông tin, dữ liệu của các máy điện thoại bị cài đặt phần mềm nghe lén này được chuyển đến máy chủ lưu trữ tại nước ngoài.

Thứ ba, giả mạo địa chỉ. Những kẻ tấn công có thể vượt qua bảo mật bằng cách chèn một địa chỉ an toàn (thông thường là địa chỉ của một mạng hoặc một máy được coi là an toàn đối với mạng bên trong) vào các gói IP của chúng. Chúng sử dụng thủ thuật này để giả dạng một địa chỉ an toàn và gửi các gói IP giả vào mạng nội bộ. Ví dụ, năm 2021, báo Công an nhân dân **(**CAND) phát hiện một trang web không có tên miền cụ thể, được truy cập thông qua hai dải địa chỉ IP: http://167.179.86.xxx và http://45.63.124.xxx có giao diện và nội dung giả mạo Báo điện tử CAND (N. Thắng, 2021). Khi người dùng bị dụ dỗ truy cập vào IP giả mạo trên và click vào bất cứ nội dung nào trên trang web thì sẽ bị nhóm tội phạm mạng đánh cắp thông tin sau đó đe dọa "phong tỏa" toàn bộ tài khoản ngân hàng cũng như nhiều thông tin cá nhân quan trọng khác nhằm mục đích lừa đảo, chiếm đoạt tài sản. Đây là mối đe dọa an ninh đối với cá nhân, doanh nghiệp, các đơn vị, tổ chức và quốc gia.

Thứ tư, vô hiệu hóa các chức năng của hệ thống. Đây là một cuộc tấn công vô hiệu hóa hệ thống, ngăn cản thực hiện chức năng đã thiết kế. Loại tấn công này không thể ngăn chặn được vì phương tiện bị tấn công cũng là phương tiện hoạt động trên mạng và truy cập thông tin. Một ví dụ tại Trung tâm Giam giữ Metropolitan ở bang New Mexico, tin tặc đã xâm nhập hệ thống máy tính khiến toàn bộ hệ thống nhà tù bị ngắt kết nối, camera an ninh và cơ chế đóng mở cửa tự động bị vô hiệu hóa. Hình thức tấn công mạng bằng mã độc đòi tiền chuộc đang ngày càng phổ biến ở Mĩ[2]. Với hình thức tấn công này, tin tặc tìm cách đưa mã độc xâm nhập hệ thống mạng của một công ty, tổ chức hoặc doanh nghiệp để mã hóa các thông tin dữ liệu trong đó, sau đó chúng đòi một khoản tiền chuộc để mở khóa các thông tin.

Thứ năm, tấn công vào yếu tố con người. Kẻ xâm nhập có thể giả danh người dùng và liên hệ với quản trị viên hệ thống để yêu cầu thay đổi mật khẩu, thay đổi quyền truy cập hệ thống của họ hoặc thậm chí thực hiện thay đổi cấu hình của hệ thống. Với kiểu tấn công này không một thiết bị nào có thể ngăn chặn một cách hữu hiệu, và chỉ có một cách giáo dục người sử dụng mạng nội bộ về những yêu cầu bảo mật để đề cao cảnh giác với những hiện tượng đáng nghi.

3. Phương pháp nghiên cứu

Nghiên cứu được tiếp cận bằng phương pháp định tính, cụ thể như sau:

Nghiên cứu các tài liệu như sách, tạp chí liên quan đến các vấn đề: an ninh mạng, tội phạm mạng, xâm phạm an ninh mạng, từ đó nhằm nhận diện rõ hơn hành vi xâm phạm

[2] https://baolangson.vn/tin-tac-vo-hieu-hoa-he-thong-an-ninh-tai-nha-tu-o-my-de-doi-tien-chuoc-1474609.html.

an ninh mạng không chỉ giới hạn trong việc đánh cắp thông tin quan trọng mà còn mở rộng ra các hoạt động đa dạng như tấn công mạng, lừa đảo điện tử và truy cập trái phép vào hệ thống. Các hành vi này không chỉ gây tổn thất về dữ liệu mà còn ảnh hưởng đến quyền riêng tư cá nhân và thậm chí có thể để lại hậu quả nặng nề cho an ninh quốc gia.

Ngoài ra, nghiên cứu cũng phân tích các trường hợp xâm phạm an ninh mạng diễn ra trong thực tế được thực hiện bởi các tổ chức tội phạm trong nước và quốc tế, từ đó đề xuất các giải pháp xây dựng, phát triển năng lực quản lí sự cố an ninh mạng.

4. Kết quả và thảo luận

Hiện nay, Việt Nam đã triển khai nhiều chính sách và chiến lược nhằm thúc đẩy ứng dụng và phát triển công nghệ thông tin, nhằm hỗ trợ sự phát triển kinh tế - xã hội và đảm bảo quốc phòng, an ninh. Cơ sở hạ tầng viễn thông, công nghệ thông tin được xây dựng khá đồng bộ; hầu hết các ngành đang số hóa cơ sở dữ liệu và ứng dụng công nghệ thông tin để tối ưu hóa quản lí và giảm thiểu thủ tục hành chính. Song song đó, kinh tế số đang phát triển mạnh mẽ và trở thành một yếu tố quan trọng của nền kinh tế. Nhiều mô hình kinh doanh và dịch vụ mới, mang tầm quốc gia đã xuất hiện, dựa trên nền tảng công nghệ số và internet. Việc tham gia tích cực vào Cuộc Cách mạng công nghiệp 4.0 và quá trình chuyển đổi số quốc gia tạo ra cơ hội cho phát triển kinh tế - xã hội và đồng thời giải quyết một cách hiệu quả những thách thức liên quan đến an ninh quốc gia và trật tự an toàn xã hội.

Việc nhìn nhận đúng đắn đối với nguy cơ và thách thức từ không gian mạng là quan trọng để chủ động bảo vệ quyền lợi hợp pháp khi tham gia vào không gian số và xã hội số. Trong bối cảnh công nghệ thông tin phát triển nhanh chóng, tình hình an ninh mạng của Việt Nam sẽ tiếp tục chịu ảnh hưởng của nhiều yếu tố, với sự gia tăng của tội phạm mạng và hoạt động xâm phạm trên mọi lĩnh vực, chủ yếu tập trung vào các hoạt động hack, xâm nhập, và thu thập thông tin tình báo. Các cuộc tấn công mạng ngày càng trở nên phức tạp, đặc biệt là với sự xuất hiện của các hình thức tội phạm nhà nước mới:

Thứ nhất, tấn công mạng gây sự cố vào các hệ thống thông tin. Theo Trung tâm Giám sát an toàn không gian mạng quốc gia, số cuộc tấn công mạng gây sự cố vào các hệ thống thông tin trong nước tháng 9/2022 tăng đến 19,9% so với cùng kì năm 2021. Cũng trong quý III/2022, Trung tâm đã ghi nhận, cảnh báo và hướng dẫn xử lí 2.878 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin Việt Nam, tăng 15,5% so với quý III/2021 (Minh Sơn, 2022). Những kẻ tấn công ngày càng tinh vi, bằng chứng là thông tin về các vi phạm bảo mật và các loại tấn công được công khai trên internet. Chưa kể những kẻ tấn công không chuyên nghiệp, hay những người có trình độ chuyên môn cao khi đọc những thông tin này chỉ cần hiểu biết một chút về lập trình cũng có thể trở thành hacker. Chính vì lí do này mà số lượng các cuộc tấn công an ninh mạng tiếp tục gia tăng, nhiều phương thức tấn công mới và không thể kiểm soát được xuất hiện theo sự phát triển của xã hội. Theo Báo cáo Chỉ số An ninh mạng toàn cầu năm 2017 của Liên minh Viễn thông Quốc tế (ITU), chỉ một nửa số quốc gia trên thế giới hiện có

chiến lược an ninh mạng hoặc đang trong quá trình phát triển chiến lược này. Cụ thể, khoảng 38% quốc gia trên toàn thế giới đã công bố chiến lược an ninh mạng. Trong số này, chỉ 11% có chiến lược an ninh mạng độc lập và chuyên dụng. Ngoài ra, 12% quốc gia đang phát triển chiến lược. Báo cáo này cho biết hơn 40 văn bản quy phạm pháp luật đã được hơn 23 quốc gia trên thế giới ban hành chỉ trong vòng 6 năm qua. Tất cả đều liên quan đến an ninh mạng (Global Cybersecurity Index, 2017).

Thứ hai, nguy cơ lớn nhất của xâm hại an ninh mạng là xuất hiện các luận điệu xuyên tạc đường lối, chủ trương, quan điểm của Đảng, chính sách, pháp luật của Nhà nước; âm mưu, thủ đoạn thổi phồng những sơ hở, yếu kém của Đảng, Nhà nước ta nhằm kích động tâm lí bất mãn, chống đối, chia rẽ nội bộ Đảng, chia rẽ khối đại đoàn kết toàn dân tộc. Các thế lực thù địch truyền tải thông điệp giả mạo, thay đổi nội dung trực tuyến và tạo ra thông tin độc hại nhằm gây nhầm lẫn và tranh cãi. Những hành động này nếu không được kiểm soát và ngăn chặn kịp thời sẽ ảnh hưởng đến sự ổn định chính trị và an ninh quốc gia. Thực tế này gắn liền với yêu cầu của Ban Chỉ đạo 35 các cấp, xác định công tác tuyên truyền, ngoài kênh truyền thông chính thống, các cấp, ngành, địa phương phải chú trọng mạng xã hội, tận dụng ưu thế của mạng xã hội để tuyên truyền các ngành, đoàn thể, cán bộ, đảng viên và nhân dân nâng cao cảnh giác, chủ động phòng ngừa, đấu tranh chống âm mưu, hoạt động diễn biến hòa bình của các thế lực thù địch; xác định rõ trách nhiệm của mình trong việc bảo vệ Đảng, bảo vệ chế độ xã hội chủ nghĩa, giữ vững quan điểm, lập trường, tin tưởng vào sự lãnh đạo của Đảng, nâng cao tinh thần cảnh giác cách mạng, đoàn kết thống nhất ý chí và hành động nhằm bảo vệ tốt an ninh chính trị, trật tự xã hội.

Thứ ba, dữ liệu cá nhân bị thu thập trở thành công cụ cho lừa đảo trực tuyến. Dữ liệu cá nhân là một thành quả của quá trình phát triển khoa học công nghệ và triển khai máy tính cá nhân vào cuộc sống hàng ngày. Theo thời gian, mô hình kinh doanh dựa trên dữ liệu, đặc biệt là dữ liệu cá nhân, đã trở nên ngày càng phổ biến do lợi ích kinh tế mà nó mang lại. Quá trình xử lí dữ liệu cá nhân không chỉ tạo ra giá trị kinh tế mà còn đồng thời mở ra những rủi ro đối với an ninh và quyền riêng tư. Những thông tin cá nhân (tên, địa chỉ, thông tin tài khoản ngân hàng) khi rơi vào tay những kẻ xâm hại, có thể được sử dụng để thực hiện các hành động gian lận, lừa đảo hoặc thậm chí là đe dọa an ninh cá nhân. Nguyên nhân của tình trạng này bao gồm sự thiếu ý thức bảo vệ dữ liệu cá nhân từ phía người sử dụng, việc công khai thông tin mà không cân nhắc và lỗ hổng trong quá trình chuyển giao, lưu trữ và trao đổi dữ liệu. Nhiều doanh nghiệp chủ động thu thập thông tin cá nhân của khách hàng để hình thành kho dữ liệu cá nhân, sử dụng trong các hoạt động kinh doanh và buôn bán, nhưng không tuân theo các quy định, không có sự kiểm soát và xử lí hợp lí từ pháp luật.

Thứ tư, vấn đề về bảo vệ an ninh thông tin bí mật nhà nước, an ninh quốc gia liên quan đến mọi mặt của đời sống xã hội. Từ năm 2001, Việt Nam đã ghi nhận hơn 840 vụ lộ bí mật nhà nước, chủ yếu liên quan đến lĩnh vực thông tin, truyền thông, báo chí,

xuất bản, và quan hệ quốc tế. Các thông tin sai lệch về điều kiện tài chính, sự bỏ trốn của một số cán bộ cấp cao và giám đốc ngân hàng ảnh hưởng đến sự ổn định của các tổ chức tài chính và tín dụng, có thể tạo ra tác động lan tỏa đến toàn bộ nền kinh tế. Tính đến tháng 2/2022, tổng dân số của Việt Nam là 98,56 triệu người, tăng từ 97,96 triệu người vào năm 2021. Trong số đó, có 77,93 triệu người dùng internet tương ứng tỉ lệ thâm nhập là 73,2%, tăng 4,9% so với cùng kì năm 2021. Facebook dẫn đầu với 93,8% người dùng hoạt động hàng tháng, Zalo đứng thứ hai với 91,3%. Tiếp theo là Facebook Messenger, TikTok, Instagram, Twitter (Thảo Nguyên, 2022). Những thách thức về an ninh mạng, quyền riêng tư và bảo mật thông tin luôn được báo động cao. Thông tin từ Bộ Công an cũng cho biết, Việt Nam đứng trong top 10 quốc gia bị tấn công mạng và lây nhiễm phần mềm độc hại nguy hiểm, thứ 7 về số nạn nhân bị tấn công mạng và thứ 2 trên thế giới bị lây nhiễm mã độc đào tiền ảo nhiều nhất[3]. Do đó, việc giải thích công khai và nguồn thông tin rõ ràng trở nên vô cùng quan trọng. Đặc biệt, khi tương tác với chính quyền và các tổ chức, quan điểm chủ động phổ biến thông tin chính xác là điều bắt buộc để đảm bảo sự minh bạch và tin cậy trong quá trình quản lí và thực hiện giao dịch.

Một nghiên cứu của Hiệp hội An toàn Thông tin Việt Nam (VNISA - Vietnam Information Security Association), vào năm 2012 đã phát hiện ra 3.697 lỗi trong 100 website có tên miền .gov.vn (trang web của Chính phủ Việt Nam). Trong số này, 489 lỗi được coi là mức cao, 396 lỗi được coi là mạnh và 2.812 lỗi được coi là trung bình hoặc yếu. 80% website được khảo sát không có biện pháp bảo mật tối thiểu. Năm 2015, hơn 10.000 website/cổng thông tin điện tử có tên miền .vn bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc (tăng 68% so với năm 2014), trong đó 224 trang do cơ quan nhà nước quản lí (so với năm 2014 giảm 11%) (Trung Hiền, Hồng Sơn, 2016). Năm 2016, tin tặc đã tấn công và làm tê liệt trung tâm điều hành hàng không tại sân bay Tân Sơn Nhất và Nội Bài trong nhiều giờ, gây thiệt hại lớn về kinh tế và gây phẫn nộ dư luận. Nhiều hành khách hốt hoảng khi thấy màn hình thông tin chuyến bay của Vietnam Airlines có sự thay đổi đột ngột. Nhóm tin tặc, sau khi chiếm quyền kiểm soát trang web của Vietnam Airlines đã phổ biến thông tin sai lệch về vấn đề Biển Đông, xúc phạm Việt Nam và Philippines, đồng thời nói rõ: "Đây là cảnh báo của nhóm hacker Trung Quốc 1937CN". Điều đáng chú ý, một tin tặc nổi tiếng tại Việt Nam xâm nhập trang web của Vietnam Airlines và trộm cắp thông tin của 411.000 hành khách. Đây là một trong những vụ tấn công hệ thống thông tin sân bay lớn nhất mà Vietnam Airlines từng phải đối mặt tính đến thời điểm hiện tại. Sự cố đã được khắc phục vào 17h45 cùng ngày sau những nỗ lực hỗ trợ khẩn cấp từ các chuyên gia an ninh mạng (Nhóm phóng viên báo VnExpress, 2020).

Dựa vào khảo sát của Cục An toàn thông tin và Hiệp hội An toàn thông tin Việt Nam (VNISA), một trong những yếu tố quan trọng đó là các cơ quan và tổ chức của Việt Nam

[3] https://baotintuc.vn/thoi-su/dam-bao-an-toan-an-ninh-thong-tin-cac-linh-vuc-trong-yeu-quoc-gia-20220617171356363.htm

nhận thức không đồng đều về an toàn thông tin. Báo cáo đánh giá cho biết xếp hạng bảo đảm an toàn thông tin mạng năm 2018, cụ thể: tỉ lệ cơ sở có khả năng ghi nhận các cuộc tấn công mạng đạt 25,3%, trong khi tỉ lệ cơ sở có hệ thống giám sát an toàn thông tin mạng chỉ 9,2%. Đối với quy trình vận hành tiêu chuẩn để ứng phó với sự cố, chỉ có 35,7% cơ sở được đánh giá là đã thiết lập. Điểm đáng lưu ý nhất là có tới 51,82% cơ sở tự đánh giá rằng an toàn thông tin chưa nhận được sự quan tâm đúng mức, và gần 30% cơ sở cho rằng lãnh đạo chưa quan tâm đến vấn đề này. Đối mặt với thực tế nêu trên, Bộ Thông tin và Truyền thông cam kết thực hiện các cảnh báo đều đặn về an toàn và an ninh mạng. Mỗi khi có thông báo liên quan đến an toàn hoặc bảo mật, doanh nghiệp, cơ quan và tổ chức đều bị bắt buộc phải tập trung theo dõi. Bất tuân trong việc đối phó với những thông báo này có thể dẫn đến những hậu quả nghiêm trọng, ảnh hưởng đến danh tiếng và tài chính của họ. Các cơ quan, tổ chức và doanh nghiệp cũng được khuyến khích tham gia vào Mạng lưới ứng phó sự cố quốc gia để chia sẻ và tiếp nhận thông tin liên quan đến các sự cố về an ninh mạng và hỗ trợ xử lí khi cần thiết (D. Bùi, 2019).

5. Kết luận

An toàn thông tin mạng được coi là một trụ cột quan trọng, xâm nhập sâu vào cơ sở hạ tầng thông tin của đất nước, đặt ra những yêu cầu cao về việc xây dựng niềm tin và đảm bảo sự phát triển bền vững trong kỉ nguyên số, thực hiện thành công chuyển đổi số quốc gia. Quá trình ứng cứu sự cố an toàn thông tin mạng đã được nhận định là một hoạt động then chốt và cấp thiết. Đây là một bước quan trọng để giúp các cơ quan, doanh nghiệp và tổ chức giảm thiểu thiệt hại, thậm chí là khi đối mặt với các sự cố nghiêm trọng nhất. Một số giải pháp xây dựng và phát triển năng lực quản lí sự cố an ninh mạng quốc gia:

Một là, mỗi tổ chức, đơn vị lập kế hoạch xây dựng Đội phản ứng sự cố bảo vệ máy tính (CSIRT - Computer Security Incident Response Team). Bước quan trọng trong việc đảm bảo an ninh mạng quốc gia là việc xây dựng và tăng cường chất lượng của CSIRT. CSIRT cần được thiết kế với sự linh hoạt cao, có đội ngũ chuyên gia có kiến thức đa ngành và sở hữu khả năng đối phó linh hoạt với các mức độ sự cố từ những vấn đề đơn giản đến những thách thức phức tạp. Để đảm bảo hiệu suất của CSIRT quốc gia, cần thực hiện các bài kiểm tra mô phỏng sự cố, giúp đánh giá và đảm bảo khả năng phản ứng, tạo cơ hội để nâng cao kĩ năng và hiệu suất của nhóm trong các tình huống thực tế. Việc này giúp CSIRT quốc gia chuẩn bị tốt hơn cho các tình huống khẩn cấp và đảm bảo khả năng đối phó với mọi biến động của môi trường an ninh mạng.

Hai là, tăng cường hợp tác liên ngành và quốc tế. Mục tiêu của việc này là chia sẻ thông tin và xây dựng cơ sở hạ tầng an toàn thông tin chung. Tham gia vào các hợp tác quốc tế là một phương tiện quan trọng để chia sẻ thông điệp nhất quán và chuẩn hóa quy trình quản lí sự cố an ninh mạng. Điều này giúp xây dựng một cộng đồng an ninh mạng toàn cầu, tạo ra một môi trường đồng thuận về chuẩn mực an ninh mạng và quản lí

sự cố. Thêm vào đó, việc học hỏi từ các quốc gia có kinh nghiệm trong lĩnh vực an ninh mạng là quan trọng để nâng cao hiệu quả và sức mạnh của các biện pháp phòng ngừa và ứng phó với sự cố an ninh mạng.

Ba là, nâng cao năng lực phân tích thông tin. Để nâng cao khả năng quản lí sự cố an ninh mạng, việc phát triển và duy trì năng lực phân tích thông tin là bước quan trọng, nhằm nhanh chóng xác định nguyên nhân và mối đe dọa trong trường hợp sự cố. Đối với mục tiêu này, sử dụng trí tuệ nhân tạo (AI) và machine learning (ML) là quan trọng. Quá trình này không chỉ tăng cường khả năng dự đoán mối đe dọa mà còn giúp phân loại chúng một cách hiệu quả. Sự kết hợp giữa công nghệ AI và ML mang lại khả năng tự động hóa việc phân tích dữ liệu lớn và phức tạp, giúp hệ thống nhanh chóng nhận diện các biểu hiện của sự cố và cung cấp thông tin chính xác và chi tiết về nguồn gốc và tính chất của mối đe dọa.

Bốn là, đào tạo và nâng cao kĩ năng nhân sự. Quá trình đầu tư vào chương trình đào tạo và phát triển kĩ năng cho nhân viên CSIRT cực kì quan trọng để đảm bảo hiệu suất công tác. Chương trình đào tạo cần bao gồm việc cập nhật kiến thức về các kĩ thuật mới và mối đe dọa đang phát triển trong lĩnh vực an ninh mạng. Điều này bao gồm việc đảm bảo rằng nhân viên CSIRT không chỉ nắm vững những công nghệ hiện đại nhất mà còn hiểu rõ về các xu hướng mới và biến động trong môi trường an ninh mạng.

Năm là, tăng cường hoạt động tuyên truyền nhằm nâng cao nhận thức của cộng đồng về việc bảo vệ dữ liệu cá nhân trong môi trường mạng. Để đạt được mục tiêu này, mỗi cá nhân nên tự nâng cao ý thức và kiến thức của mình để bảo vệ thông tin cá nhân, tránh tự ý chia sẻ thông tin cá nhân và hình ảnh trên mạng, cũng như không tùy tiện truy cập hoặc chia sẻ các đường link và thông tin mà chưa được kiểm chứng và đảm bảo về tính an toàn. Mỗi gia đình cần thực hiện biện pháp giám sát để đảm bảo an toàn cho trẻ em khi tiếp cận môi trường mạng, ngăn chặn các rủi ro rò rỉ dữ liệu cá nhân. Biện pháp này cũng giúp xây dựng một môi trường an toàn và bảo mật trong gia đình, góp phần giảm thiểu nguy cơ xâm phạm dữ liệu cá nhân và các sự cố liên quan trên môi trường mạng.

Lãnh đạo Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao nhận định rằng sự bùng nổ công nghệ với các thiết bị thông minh, trí tuệ nhân tạo (artificial intelligence - AI) sẽ làm gia tăng nguy cơ dữ liệu bị xâm phạm (Minh Sơn, 2021). Ngoài ra, người dùng phải đối mặt nhiều hơn với các thông tin xấu, độc hại và những chiêu thức lừa đảo, chiếm đoạt tài sản, đánh bạc, tiền ảo hay kinh doanh trái phép trên không gian mạng. Sự gia tăng về mức độ tinh vi của tội phạm sử dụng công nghệ cao ở Việt Nam đồng nghĩa với việc số lượng và phương thức tấn công ngày càng phức tạp, gây ra những hậu quả nghiêm trọng và lan rộng trên quy mô lớn. Do đó, để ứng phó hiệu quả với các thách thức an ninh mạng, các quốc gia, tổ chức quốc tế, tổ chức và công ty công nghệ cần thiết lập quan hệ hợp tác chặt chẽ trong lĩnh vực bảo đảm an ninh mạng ở cấp độ song phương và đa phương thông qua các cơ chế và khuôn khổ pháp lý để ngăn chặn tội phạm mạng.

Tài liệu tham khảo

1. D. Bùi. 2019. "Phải vào cuộc lập tức khi xảy ra sự cố an ninh mạng". (https://tapchitaichinh.vn/tai-chinh-phap-luat/phai-vao-cuoc-lap-tuc-khi-xay-ra-su-co-an-ninh-mang-315754.html).
2. Trung Hiền, Hồng Sơn. 2016. "Mất an toàn thông tin: Nguy cơ từ chính thiết bị "kè kè" bên người", (https://www.mic.gov.vn/atantt/Pages/TinTuc/132987/Mat-an-toan-thong-tin--Nguy-co-tuchinh-thiet-bi--ke-ke--ben-nguoi.html).
3. Global Cybersecurity Index (GCI). 2017. (https://www.itu.int/dms_pub/itu-d/opb/str/DSTR-GCI.01-2017-PDF-E.pdf).
4. Nhóm phóng viên báo VnExpress. 2020. "Sân bay Nội Bài, Tân Sơn Nhất bị tin tặc tấn công", (https://vnexpress.net/san-bay-noi-bai-tan-son-nhat-bi-tin-tac-tan-cong-3444469.html).
5. Thảo Nguyên. 2022. "Data Station #25 - Digital 2022: Số người dùng Việt quan ngại về an toàn dữ liệu giảm gần một nửa so với năm 2020", (https://www.brandsvietnam.com/congdong/topic/323902-Data-Station-25-Digital-2022-So-nguoi-dung-Viet-quan-ngai-ve-an-toan-du-lieu-giam-gan-1-nua-so-voi-nam-2020).
6. Minh Sơn. 2022. "Gần 1.000 cuộc tấn công mạng vào hệ thống thông tin trong nước", (https://www.vietnamplus.vn/gan-1000-cuoc-tan-cong-mang-vao-he-thong-thong-tin-trong-nuoc/821517.vnp).
7. Richard A. Clarke, Robert Knake. 2010. *Cyber War: The Next Threat to National Security and What to Do About It*. Ecco Publisher.
8. Ross J. Anderson. 2008. *Security Engineering: A Guide to Building Dependable Distributed Systems.* Wileyy. New Jersey.
9. Minh Sơn. 2021. "An ninh mạng Việt Nam trong năm 2021: Tấn công ngày càng tinh vi", (https://www.vietnamplus.vn/an-ninh-mang-viet-nam-trong-nam-2021-tan-cong-ngay-cang-tinh-vi/749427.vnp).
10. N. Thắng. 2021. "Trang web từ nước ngoài giả mạo Báo CAND để lừa đảo", (https://cand.com.vn/Phap-luat/Canh-bao-trang-web-gia-mao-Bao-CAND-de-lua-dao-i617622/).
11. Thông tấn xã Việt Nam. 2018. "Thế giới thiệt hại tới 600 tỷ USD mỗi năm do tấn công mạng", (https://www.vietnamplus.vn/the-gioi-thiet-hai-toi-600-ty-usd-moi-nam-do-tan-cong-mang/489235.vnp).
12. Thư viện pháp luật. 2018. "Luật An ninh mạng", (https://thuvienphapluat.vn/van-ban/Cong-nghe-thong-tin/Luat-an-ninh-mang-2018-351416.aspx).
13. World Economic Forum. 2018. "Insight Report: Regional Risks for Doing Business 2018", (https://www3.weforum.org/docs/WEF_Regional_Risks_Doing_Business_report_2018.pdf).