NÂNG CAO NHẬN THỨC VỀ AN NINH MẠNG ĐỐI VỚI THUYỀN VIÊN VIỆT NAM

RAISING AWARENESS ON CYBER SECURITY FOR VIETNAMESE SEAFARERS

ĐÀO QUANG DÂN
Khoa Hàng hải, Trường Đại học Hàng hải Việt Nam
Email liên hệ: daoquangdan@vimaru.edu.vn

Tóm tắt

Tàu biển thương mại ngày càng được trang bị rất nhiều thiết bị, hệ thống tự động hóa, công nghệ thông tin hiện đại dựa trên máy tính và internet. Điều này cũng đồng nghĩa với việc luôn có các mối đe dọa tấn công mạng, mà hậu quả có thể ảnh hưởng nghiêm trọng đến ngành hàng hải.

Thuyền viên Việt Nam được trang bị khá hạn chế kiến thức về an ninh mạng. Nhiều thuyền viên vẫn chưa nhận thức đầy đủ về các mối nguy hiểm và hậu quả cùng các cách thức tấn công mạng nhằm vào tàu biển để có các biện pháp phòng tránh hiệu quả. Ngay cả trong nội dung những chương trình huấn luyện an ninh cho thuyền viên (có cấp chứng chỉ), cũng chưa đề cập đến vấn đề an ninh mạng và an ninh mạng đối với tàu biển.

Với mục đích nâng cao nhận thức về an ninh mạng đối với thuyền viên Việt Nam, bài báo nêu lên các cách thức đang được sử dụng để tấn công mạng cũng như làm nổi bật đối tượng yếu nhất chính là thuyền viên và đề xuất các giải pháp nhằm loại bỏ, giảm thiểu các mối đe dọa hoặc tránh phạm lỗi của một cuộc tấn công mạng.

Từ khóa: *An ninh hàng hải; Các mối đe dọa đối với hàng hải; An ninh mạng đối với tàu biển.*

Abstract

Commercial ships are increasingly equipped with a lot of equipment, automation systems, modern information technology based on computers and the internet. This also means that there are always cyberattacks, which can have a serious impact on the maritime industry.

Vietnamese seafarers have limited knowledge of cyber security. Many seafarers are still not fully aware of the dangers and consequences, as well as the types of cyber attacks against ships to take effective preventive measures. Even in the content of security training programs for crews (with certification), did not mention the issue of cyber security and network security for ships.

With purpose to raise the awareness of cybersecurity for Vietnamese seafarers, the article highlights the ways in which cyber attacks are used as well as highlighting the weakest target seafarers and proposing solutions on how to eliminate, minimize threats or to avoid falling foul of an attack cyber.

Keywords: *Maritime Security; Maritime threats; Cyber Security on the ships.*

1. Đặt vấn đề

Vận tải hàng hải đóng vai trò hết sức quan trọng đối với nền kinh tế thế giới. Hơn 80% lượng hàng hóa trên thế giới tính theo thể tích và hơn 70% giá trị của chúng được vận chuyển bằng đường biển. Trong vận tải hàng hải, tàu biển là phương tiện chính và đóng vai trò chủ chốt. Những con tàu ngày càng sử dụng nhiều hơn các trang thiết bị, các hệ thống tự động hóa và công nghệ thông tin hiện đại. Các hệ thống này chủ yếu được kết nối với internet và hệ thống thông tin liên lạc từ xa. Các thiết bị và hệ thống lắp đặt trên tàu được thiết kế và vận hành bằng cách sử dụng máy tính và kết nối Internet và như vậy sẽ làm cho chúng dễ bị tấn công mạng. Đặc biệt, trong những trường hợp khi con tàu đang trong vùng ven biển hoặc ở gần bến cảng mà chúng bị tấn công mạng thì hậu quả có thể ảnh hưởng nghiêm trọng đến cả một khu vực rộng lớn.

Theo dữ liệu điều tra của các cơ quan an ninh mạng, phần lớn các cuộc tấn công mạng trên tàu được vô tình kích hoạt bởi thuyền viên, khi họ có thể là đã mở các file đính kèm email giả hoặc siêu liên kết hoặc sử dụng phương tiện di động đã bị nhiễm virus độc hại phá hoại. Theo báo cáo khảo sát vào năm 2018, có đến 92% thuyền viên xác nhận rằng việc truy cập internet có ảnh hưởng mạnh mẽ đến họ và họ thường xuyên thực hiện việc này [1]. Trong khi đó, thuyền viên Việt Nam chưa được trang bị đầy

TẠP CHÍ ISSN: 1859-316X
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

đủ kiến thức về an ninh mạng một cách chính thống. Minh chứng cho điều này đó là, nội dung kiến thức thuyền viên được trang bị trong các khóa học có cấp chứng chỉ về an ninh dựa trên bộ luật quốc tế về an ninh tàu và bến cảng (ISPS) cũng không đề cập đến an ninh mạng. Có rất nhiều thuyền viên cho rằng với sự phức tạp của các hệ thống trên tàu thì các cuộc tấn công mạng khó có thể xảy ra.

2. Phân tích an ninh mạng trong các văn bản pháp luật quốc tế

Với vị trí và vai trò của mình Tổ chức Hàng hải Quốc tế (IMO) đã ban hành nhiều văn bản pháp luật liên quan đến an ninh, an toàn trong lĩnh vực hàng hải.

2.1. Công ước về an toàn sinh mạng trên biển (SOLAS) và những bộ luật, hướng dẫn liên quan

Điều 1 trong chương XI-2 của công ước SOLAS, ngay trong phần định nghĩa "sự cố an ninh bất thường" đã không bao gồm những rủi ro và nguy hiểm mạng.

Bộ luật quốc tế chính, đặc thù nhất về an ninh đối với tàu biển là bộ luật ISPS. Nội dung chi tiết nhất của bộ luật liên quan đến an ninh tàu biển được thể hiện cụ thể trong các mục A/8.4, B/8 và B/15 của bộ luật là các quy định về thiết lập và duy trì kế hoạch an ninh đối với một con tàu. Tuy nhiên, cũng giống như SOLAS, đó là, ISPS chỉ cung cấp kế hoạch an ninh chống lại các mối đe dọa vật lý như cướp biển.

Vào tháng 6 năm 2016 tổ chức IMO đã phê duyệt và ban hành văn bản MSC.1/Circ. 1526 "Hướng dẫn tạm thời về Quản lý rủi ro mạng hàng hải" trong phiên họp thứ 96 của Ủy ban An toàn Hàng hải. Đến tháng 7 năm 2017 IMO đã ban hành văn bản MSC-FAL.1/Circ.3, 2017 "Hướng dẫn về quản lý rủi ro không gian mạng hàng hải", thay thế cho MSC.1/Circ. 1526. Các văn bản này chủ yếu cung cấp các khuyến nghị mức cao cho sự quản lý rủi ro không gian mạng cùng các yếu tố hỗ trợ việc quản lý rủi ro mạng. Các văn bản này cùng các hướng dẫn của một số tổ chức hàng hải lớn trên thế giới như Hiệp hội hàng hải Quốc tế và Baltic (BIMCO), Cơ quan Vận tải biển quốc tế (ICS) tập trung vào hướng dẫn xây dựng quy trình quản lý rủi ro mạng hàng hải cho các công ty và các nhà khai thác tàu gồm 5 bước, nhận diện; phòng ngừa; phát hiện; ứng phó và khôi phục.

Ngoài các bộ luật và hướng dẫn trên còn có Nghị quyết MSC.428(98) về "Quản rủi ro mạng hàng hải trong hệ thống quản lý an toàn" của IMO. Nghị quyết MSC.428(98) khuyến khích các quốc gia mà tàu mang cờ buộc các công ty đối xử với quản lý an ninh mạng ở cấp độ công ty thông qua hệ thống quản lý an toàn (SMS) theo yêu cầu của bộ luật quản lý an toàn quốc tế (ISM).

2.2. Công ước quốc tế về Tiêu chuẩn huấn luyện, cấp chứng chỉ và trực ca cho thuyền viên (STCW 78/2010)

Không chỉ phần A-VI/ 5 của Công ước STCW mô tả trình độ của một sĩ quan an ninh tàu biển, mà phần A-VI/ 6 của STCW cũng yêu cầu thuyền viên tàu biển phải được đào tạo, huấn luyện làm quen về an ninh, những người chịu trách nhiệm về an ninh của con tàu phải được đào tạo nâng cao nhận thức về an ninh. Tuy nhiên, trong các chương trình đào tạo, huấn luyện liên quan đến an ninh của STCW như chương trình huấn luyện 3.19 (model course 3.19) cho sĩ quan an ninh tàu biển, chương trình huấn luyện 3.20 (model course 3.20) cho sĩ quan an ninh công ty, model course 3.26 đào tạo an ninh cho những thuyền viên được chỉ định đảm nhiệm nhiệm vụ an ninh của tàu, chương trình 3.27 đào tạo, huấn luyện nhận thức an ninh cho tất cả thuyền viên, đều không chứa bất kỳ nội dung nào về an ninh mạng, mà chỉ cung cấp đào tạo về an ninh vật lý, điển hình nhất là cướp biển.

Tất cả các văn bản pháp luật của IMO cũng như rất nhiều hướng dẫn về an ninh, huấn luyện và đào tạo an ninh của các tổ chức hàng hải quốc tế lớn, uy tín cũng mới chỉ tập trung vào:

- Đề cập kế hoạch an ninh chống lại các mối đe dọa vật lý như cướp biển;
- Đào tạo, huấn luyện thuyền viên chống lại các mối đe dọa vật lý như cướp biển;
- Xây dựng quy trình quản lý rủi ro an ninh mạng.

Theo đúng quy định trong phần A-VI/6 của STCW thì thuyền viên phải được huấn luyện an ninh mạng đối với tàu biển ngay ở mức độ làm quen về an ninh. Trong khi đó, mặc dù được huấn luyện và cấp chứng chỉ về an ninh, nhưng thuyền viên không được trang bị một cách chính thống về an ninh mạng, mà đây lại là một trong những đòi hỏi hết sức cần thiết trong tình hình hiện nay. Có nhiều thuyền viên vẫn chưa thể hiểu được hậu quả mà một cuộc tấn công mạng gây ra.

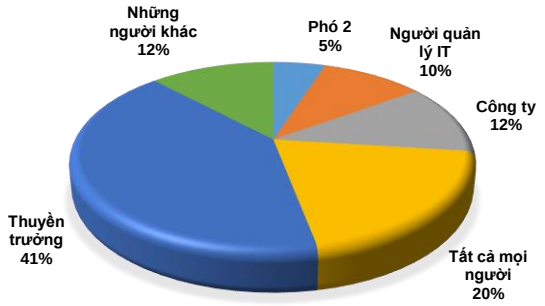
3. Tấn công mạng vào tàu biển thông qua mối liên kết yếu nhất chính là thuyền viên

Các con tàu ngày càng trở nên tối tân hơn và có kết nối nhiều hơn. Liên lạc của tàu, ngày nay, mang

nhiều dữ liệu và nhanh hơn bao giờ hết. Các thiết bị, hệ thống được trang bị trên tàu rất hiện đại lại càng ngày càng dễ bị tấn công xâm nhập, can thiệp. Thuyền viên trên tàu được luân chuyển thường xuyên, điều đó có nghĩa thuyền viên thường xuyên sử dụng các hệ thống mà họ không quen thuộc. Điều này làm tăng cơ hội lỗi do thuyền viên gây ra [3]. Trong khi thuyền viên liên tục tương tác với các hệ thống trên bờ và trên tàu, yếu tố con người vẫn sẽ đóng một vai trò quan trọng trong phần lớn các sự cố an ninh mạng.

Trong Hội nghị thượng đỉnh vận tải hàng hải tại trường đại học kỹ thuật Đan Mạch, trưởng phòng Điều tiết Công nghệ Hàng hải của BIMCO đã đề cập "80% các sự cố an ninh mạng có thể được ngăn chặn nếu người dùng đơn lẻ đã có thể nhận ra mối đe dọa". Giáo dục và nâng cao nhận thức của con người là bước tiến lớn đầu tiên cần thực hiện để tăng cường an toàn và an ninh. Điều cực kỳ quan trọng là giáo dục đội ngũ thuyền viên để nâng cao nhận thức về các lỗ hổng phát sinh từ lỗi của con người.

Theo kết quả khảo sát đối với thuyền viên do Roger Adamson, giám đốc điều hành của Futurenautics Maritime thực hiện từ năm 2012 đến 2018 với hơn 6.000 thuyền viên, cho thấy rằng, chỉ có 15% thuyền viên đã trải qua một hình thức đào tạo về an ninh mạng; 20% cảm thấy rằng đào tạo về an ninh mạng bị thiếu trên tàu; 60% mong muốn được đào tạo thêm về khả năng phục hồi và quản lý an ninh mạng; 49% thừa nhận rằng họ không biết về chính sách an ninh mạng của công ty. Cuộc khảo sát cũng cho thấy 47% thuyền viên đã đi trên một con tàu có trở thành mục tiêu tấn công mạng [2].



Hình 1. Kết quả khảo sát về người chịu trách nhiệm đối với an ninh mạng trên tàu *[2]*

Ngoài những cuộc tấn công mạng lớn, có chủ đích, các hệ thống và dữ liệu không gian mạng của tàu có xu hướng bị xâm phạm do nhầm lẫn bởi thuyền viên trên tàu hoặc các nhân viên trên bờ.

4. Các phương thức tấn công mạng

Cách thức được sử dụng phổ biến trong các cuộc tấn công mạng đối với tàu biển thương mại, đó là sử dụng các công cụ và kỹ thuật ứng dụng tin học sau đây:

+ *Malware*: Là phần mềm độc hại. Nó chính là các đoạn chương trình máy tính được viết ra nhằm chiếm quyền truy cập hoặc gây thiệt hại cho máy tính, máy chủ hoặc mạng. Mục đích của Malware là đánh cắp tài nguyên từ máy tính và khai thác các thiếu sót hoặc các sự cố đã biết của mạng. Phần mềm độc hại có thể là virus, trojan horse, ransomware, spyware và worms.

- *Virus*: Đây là một chương trình máy tính có thể tự tạo ra rất nhiều bản sao giống nó và lây lan sang các máy tính được kết nối khác bằng cách tự gắn vào các chương trình hoặc tài liệu hợp pháp và chương trình này sẽ tự động chạy khi thuyền viên chạy một trong những chương trình đó.

- *Trojan horse*: Nó được ẩn trong những phần mềm tưởng như vô hại. Nó tạo ra một môi trường giao tiếp giả mạo, nơi thuyền viên nghĩ rằng đó là môi trường giao tiếp thực tế, khi đó nó sẽ đánh cắp mật khẩu giao dịch của thuyền viên, truy cập vào máy tính của thuyền viên và kiểm soát nó. Cuối cùng tiến hành đánh cắp thông tin, dữ liệu từ máy tính bị nhiễm cũng như các Trojans truy cập từ xa được thiết kế để cho kẻ tấn công toàn quyền kiểm soát máy tính.

- *Ransomware*: Là một loại phần mềm độc hại nhằm tống tiền người dùng bằng cách xâm nhập vào máy tính và thao túng dữ liệu của nạn nhân bằng cách mã hóa các dữ liệu trong máy tính của người dùng và giữ nó làm con tin, buộc người dùng phải trả tiền chuộc để lấy lại tập tin của họ.

- *Spyware*: Loại phần mềm độc hại, được thiết kế để ẩn trên máy tính và giám sát mọi hành động của người dùng. Nó có thể theo dõi web hoạt động, truy cập E-mail và thậm chí đánh cắp tên người dùng và mật khẩu.

- *Worms*: Là một chương trình máy tính độc hại có thể sửa đổi, xóa các tập tin và thậm chí gắn thêm phần mềm độc hại vào máy tính. Mục tiêu chính của *worms* là tạo ra càng nhiều bản sao của nó có thể lây lan từ máy tính này sang máy tính khác càng tốt. Một *worm* có thể tự sao chép mà không cần bất kỳ sự tương tác nào của con người và không nhất thiết phải gắn vào chương trình.

TẠP CHÍ ISSN: 1859-316X
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

+ *Social engineering*: Đây là một cách được những kẻ tấn công có trình độ sử dụng nhằm thao túng các thuyền viên, phá vỡ quy trình an ninh, thông thường những kiểu tấn công này thông qua tương tác qua phương tiện truyền thông xã hội. Điển hình cho kiểu tấn công này có thể là giả mạo thông báo từ công ty hoặc sử dụng các cách buộc thuyền viên phải phản hồi ngay lập tức do tình huống khẩn cấp. Khi thuyền viên nhấp vào liên kết đó có thể đã kích hoạt phần mềm độc hại.

+ *Phishing*: Bằng cách gửi E-mail đến một số lượng lớn các mục tiêu tiềm năng yêu cầu cung cấp các thông tin cá nhân nhạy cảm như yêu cầu cho biết tên thuyền viên, mật khẩu, số PIN hoặc làm cho nạn nhân truy cập một trang web giả bằng cách sử dụng siêu liên kết được cung cấp. Phishing, được thiết kế để đánh lừa thuyền viên và yêu cầu dữ liệu bí mật các thông tin đó.

+ *Water holing*: Phát triển các web giả mạo dựa trên sở thích của thuyền viên đối với một trang web chính hãng để khai thác các thuyền viên truy cập và có quyền truy cập vào dữ liệu của họ.

+ *Port Scanning*: Là một phần mềm ứng dụng sẽ sử dụng để trao đổi liên lạc qua hệ điều hành máy chủ và qua Internet. Một cuộc tấn công port scanning xảy ra khi kẻ tấn công gửi các gói dữ liệu đến một máy tính, thay đổi port (Port là giao thức bit 16 đứng đầu của mỗi tập tin trong giao thức TCP, UDP hay còn gọi là cánh cổng quy định các tập dữ liệu riêng biệt. Nó là một dạng thuật toán được định sẵn mà mỗi máy tính cần phải đăng ký mới có thể nhận và xuất tập tin được khi chúng ta đăng ký các loại port trên hệ thống máy tính của chúng ta sẽ giúp cho các tập tin được truy cập, được đưa vào đúng với địa chỉ port khớp với đầu bit tập tin đó) đích. Mục tiêu chính của cuộc tấn công đó là kiểm tra những port nào người dùng đã mở kết nối đến.

+ *Built-in software weaknesses*: Các lỗ hổng liên quan đến thiếu sót kiểm soát quyền truy cập vào hệ thống của tàu hoặc do lỗi của thuyền viên chưa kiểm tra kỹ trước khi chuyển dữ liệu nhận trên mạng vào cơ sở dữ liệu.

+ *Third party contribution*: Các nhà cung cấp thiết bị và những kỹ thuật viên dịch vụ có quyền truy cập vào hệ thống của công ty, tàu. Họ có thể để lại các lỗ hổng dễ bị tấn công mà công ty và tàu không biết.

+ *Brute force*: Một cuộc tấn công bằng cách thử rất nhiều mật khẩu với hy vọng cuối cùng sẽ đoán được mật khẩu chính xác. Kẻ tấn công kiểm tra một cách có hệ thống tất cả các mật khẩu có thể cho đến khi tìm thấy mật khẩu chính xác.

+ *Denial of service (DDoS):* Từ chối cung cấp dịch vụ được thiết kế để ngăn người dùng hợp pháp và được ủy quyền truy cập thông tin, thường là bằng cách làm ngập mạng đích với lưu lượng truy cập liên tục từ các nguồn khác nhau. Một cuộc tấn công DDoS nhằm mục đích phá vỡ hoạt động bình thường trên một máy chủ hoặc một mạng cụ thể.

+ *Spear-phishing*: Giống như Phishing, nhưng mục tiêu là các cá nhân, với Email cá nhân, chứa phần mềm độc hại hoặc đường kết nối với các phần mềm độc hại.

+ *Subverting the supply chain:* Tấn công một công ty hoặc tàu bằng cách thỏa thuận cung cấp thiết bị, phần mềm hoặc dịch vụ hỗ trợ cho công ty hoặc tàu. Kiểu tấn công này cực kỳ phổ biến trong ngành hàng hải.

5. Hậu quả bị tấn công mạng do nhận thức chưa đầy đủ của thuyền viên về an ninh mạng

Hậu quả của các cuộc tấn công mạng do nhận thức chưa đầy đủ của thuyền viên về an ninh mạng phụ thuộc vào bản chất của từng cuộc tấn công cũng như sự phức tạp của các kịch bản và vị trí vai trò quan trọng của các mục tiêu bị tấn công trên tàu. Dưới đây là một số hậu quả:

- Hậu quả đầu tiên dễ xảy ra và dễ nhận biết nhất, đó là, làm gián đoạn các hoạt động bình thường diễn ra trên tàu, do các thiết bị bị hỏng không hoạt động được vì bị nhiễm virus từ những thiết bị cá nhân của thuyền viên kết nối vào mạng hoặc các hệ thống, thiết bị trên tàu.

- Chậm chễ trong việc giao hàng; mất hàng hóa; có thể làm gián đoạn các hoạt động của cảng. Hiện nay, việc lập sơ đồ hàng hóa cho một số loại tàu như tàu container được thực hiện bởi những người chuyên lập sơ đồ hàng hóa tại công ty hoặc tại các cảng. Việc trao đổi dữ liệu giữa tàu và người lập sơ đồ hàng hóa được tiến hành qua mạng dưới dạng các file điện tử. Nguy cơ rất cao những dữ liệu và sơ đồ này rơi vào tay tội phạm mạng do sự bất cẩn, sơ xuất của thuyền viên, đặc biệt là đại phó. Vào tháng 8 năm 2011, tin tặc đã xâm nhập vào sơ đồ hàng hóa một số tàu của công ty Iran Shipping Line. Tin tặc đã thay đổi số lượng hàng hóa, ngày giao hàng, địa điểm giao hàng,… do vậy một số container chứa hàng đã bị mất. Và hậu quả lớn hơn, đó là, rất có thể sẽ tái diễn vụ tấn công mạng xảy ra tại cảng Antwerp của Bỉ trong hai năm, từ 2011 đến 2013 các băng đảng ma túy đã kiểm

soát hoàn toàn và vận chuyển số lượng container chứa ma túy và súng đến và đi tại cảng này.

- Mắc cạn và có thể gây ô nhiễm và thảm họa ô nhiễm; gây hư hỏng hoặc thiệt hại cho cấu trúc tàu, các trang thiết bị trên tàu do tàu bị đâm va; gây thương tích về mặt thể xác hoặc lấy đi mạng sống của thuyền viên trên tàu,… do nhiễu, lỗi hoặc gián đoạn bất kỳ hệ thống thiết yếu nào phục vụ cho công tác dẫn tàu an toàn và xác định vị trí tàu. Các thiết bị trên buồng lái như radar, hệ thống định vị toàn cầu (GPS), hệ thống hiển thị và thông tin hải đồ điện tử *(ECDIS*),… được kết nối với nhau qua các giao thức Ethernet. Trong khi đó, ECDIS là hệ thống hầu như không được cài đặt phần mềm diệt virus. Vào ngày 17/1/2013, tàu chiến của Hải quân Hoa Kỳ đã bị mắc cạn vào một rặng san hô Tubbataha giữa biển Sulu của Philippines do lỗi của ECDIS. Vào năm 2017, một thuyền viên trên chiếc tàu dầu trọng tải 80.000DWT, đã mang theo một chiếc USB có nhiễm virus để cập nhật hải đồ cho hệ thống ECDIS, hàng loạt thiết bị hàng hải trên tàu đã bị nhiễm virus và con tàu đã bị hoãn thời gian khởi hành, đồng thời một cuộc điều tra đã được tiến hành [4]. Nhưng, đó là trường hợp may mắn vì nếu con tàu dầu này khởi hành và bị mắc cạn do virus từ chiếc USB thì rất có thể sẽ gây ra thảm họa về môi trường. Nghiên cứu và thực nghiệm đã cho thấy, virus có thể loại bỏ các mục tiêu radar khỏi màn hình mà radar vẫn hoạt động bình thường. Đây là một điều thực sự đáng sợ.

6. Đề xuất các giải pháp nâng cao nhận thức đối với thuyền viên về an ninh mạng

Nhằm bảo đảm an toàn và an ninh cho con tàu, cho công ty, cho môi trường hàng hải và cho chính bản thân thuyền viên, tác giả xin đề xuất một số giải pháp nhằm nâng cao nhận thức đối với thuyền viên Việt Nam về an ninh mạng.

Phân cấp và kiểm soát sự truy cập vào các hệ thống, máy tính trên tàu: Quy định và tuân thủ sự phân cấp cấp độ truy cập vào các hệ thống, thiết bị đối với từng chức danh trên tàu tương ứng với tầm quan trọng của dữ liệu, thông tin cũng như các trang thiết bị. Việc sử dụng các ổ đĩa cá nhân, USB, CD, v.v để kết nối với mạng trên tàu cần phải báo cáo, đồng thời phải kiểm tra tính an toàn của các thiết bị này và chỉ khi được phép của cấp có thẩm quyền mới được truy cập. Đối với những người không phải là thành viên của tàu như người của cảng, của công ty, đại lý hay thanh tra viên,… nếu có yêu cầu cần sử dụng máy tính hoặc máy in, thì cung cấp cho họ một máy tính, máy in độc lập, không được kết nối với mạng, cũng như không kết nối với các thiết bị của tàu.

Giữ mật khẩu của mỗi cá nhân một cách cẩn trọng: Rò rỉ mật khẩu là một trong những lỗ hổng phổ biến nhất đối với thuyền viên. Hầu hết thuyền viên có thói quen sử dụng cùng một mật khẩu trên tất cả các ứng dụng và tất cả các trang web cho thuận tiện. Nhưng điều này lại rất rủi ro. Cần sử dụng các mật khẩu khác nhau cho các trang web và các ứng dụng khác nhau. Để bảo mật tốt hơn, mật khẩu nên kết hợp cả chữ hoa và chữ thường cùng các ký tự đặc biệt và số. Tuyệt đối không nên chia sẻ mật khẩu hoặc bất kỳ thông tin nhạy cảm với bất cứ ai.

E-mail: Tránh mở bất kỳ liên kết hoặc file đính kèm nào từ các email đáng ngờ, đặc biệt nếu đang mở chúng trên hệ thống hoặc mạng của tàu. Trường hợp nghi ngờ về tính xác thực của email, hãy đánh dấu chúng và sau đó mở chúng ở trên một mạng được bảo mật, không kết nối với bất kỳ hệ thống hoặc mạng nào của tàu. Nếu bị Phishing nên báo cho những người có thẩm quyền biết.

Cần cẩn trọng khi sử dụng các wifi miễn phí. Khi tàu đến những cảng (địa điểm) mới, thuyền viên thường tìm kiếm các điểm có wifi miễn phí. Thông thường các điểm có wifi miễn phí là những địa điểm công cộng, đông người và rất dễ phát sinh và có nhiều hoạt động gian lận mạng (hack).

Duyệt các trang web. Nên tránh duyệt web nhấp vào các liên kết đáng ngờ.

Tránh trở thành nạn nhân của các tin nhắn (SMS). Sử dụng tin nhắn là phương thức ưa thích của các tin tặc để lấy thông tin cá nhân từ thuyền viên. Vì thuyền viên thường có thói quen sử dụng các thẻ SIM khác nhau để có được tốc độ gọi và dữ liệu tốt nhất, khi đó tin tặc sẽ gửi SMS lừa đảo kèm theo liên kết để nhận được các ưu đãi rẻ nhất về các cuộc gọi và gói dữ liệu. Khi liên kết được kích hoạt, nó sẽ tải phần mềm độc hại vào điện thoại.

Tránh sử dụng ổ đĩa không xác định, thiết bị ổ đĩa nhỏ (USB) được sử dụng để trao đổi thông tin giữa nhiều hệ thống. Nếu ai đó đưa cho chúng ta các thanh USB, hãy tránh sử dụng những thiết bị đó nếu không biết rõ về chúng. Mỗi thuyền viên nên dùng một ổ USB/đĩa cứng riêng cho riêng mình và một ổ đĩa khác cho các công việc, hoạt động khác.

Sử dụng phần mềm diệt vi-rút mới nhất: Cần cài đặt phần mềm diệt virus mới nhất vào máy tính nhằm phát hiện và loại bỏ các phần mềm, chương trình độc hại.

TẠP CHÍ ISSN: 1859-316X
KHOA HỌC CÔNG NGHỆ HÀNG HẢI
JOURNAL OF MARINE SCIENCE AND TECHNOLOGY

Sử dụng phần mềm có bản quyền: Việc thuyền viên sử dụng các phần mềm không có bản quyền được sao chép lậu là lí do chính khiến cho máy tính của họ dễ bị phơi nhiễm trước mã độc, virus tấn công dẫn đến các lỗi hỏng hóc, lây nhiễm sang các máy tính khác và thậm chí mất dữ liệu.

Các thiết bị cá nhân. Các thiết bị này thường được thuyền viên mang theo lên tàu và thường kết nối với rất nhiều mạng khác nhau. Nếu những thiết bị, máy tính này thiếu phần mềm bảo mật như phần mềm diệt virus thì rất có thể chúng đã chuyển rủi ro sang mạng của tàu mà chúng kết nối.

Cài đặt phần mềm. Khi cài đặt và bảo trì phần mềm trên phần cứng máy thì rất có thể phần cứng đã bị nhiễm hoặc phần mềm đã bị nhiễm độc hại. Cần cài đặt phần mềm tại các địa chỉ uy tín.

7. Kết luận

Hiểu biết là một khía cạnh vô cùng quan trọng trong việc làm giảm nguy cơ tấn công mạng. Các mối đe dọa tiềm tàng từ không gian mạng cần được hiểu rõ, để có được khả năng đối phó với những rủi ro có thể xảy ra và đưa ra cách thức xử lý tốt nhất khi tàu gặp nguy hiểm.

Mỗi tàu bất kể kích cỡ và chủng loại đều có khả năng bị tấn công mạng và các mối đe dọa tấn công mạng ngày càng tăng. Mọi thuyền viên cần phải nhận thức được các mối đe dọa mà họ có thể là tác nhân gây ra đối với con tàu của chính mình. Trong phạm vi bài báo, tác giả đề cập đến những cách thức tấn công mạng cùng các giải pháp đối với thuyền viên nhằm loại bỏ, giảm thiểu các mối đe dọa hoặc tránh phạm lỗi của một cuộc tấn công.

Trường hợp phát hiện một mối đe dọa hoặc một cuộc tấn công đang diễn ra và cần phải làm gì trong trường hợp xảy ra sự cố an ninh sẽ được tác giả trình bày trong các bài báo sau.

Lời cảm ơn

Bài báo là sản phẩm của đề tài nghiên cứu khoa học cấp Trường năm học 2019-2020: "*Nghiên cứu an ninh hàng hải trong không gian mạng"*, được hỗ trợ kinh phí bởi Trường Đại học Hàng hải Việt Nam.

TÀI LIỆU THAM KHẢO

[1] *Report, Economic Impact of Cybercrime-No Slowing Down*, February 2018.

[2] Futurenautics Research. *Crew Connectivity 2018 Survey Report*. page 36, 2018.

[3] Keith Martin Rory Hopcraft, *50,000 Ships worldwide are vulnerable to cyberattacks*, Independent, Jun. 2018.

[4] Chris Baraniuk. *How hackers are targeting the shipping industry*, 2017.

Ngày nhận bài: 06/3/2020
Ngày nhận bản sửa: 25/3/2020
Ngày duyệt đăng: 08/4/2020