CHUYÊN ĐỀ SỐ 28 (THÁNG 9/2023)

PHỔ BIẾN KIẾN THỨC

TÀI LIỆU THAM KHẢO CỦA LIÊN HIỆP CÁC HỘI KHOA HỌC VÀ KỸ THUẬT VIỆT NAM

CHỦ QUYỀN QUỐC GIA TRÊN KHÔNG GIAN MẠNG

TRONG SỐ NÀY

CONTENTS 09 / 2023

GÓC CHUYÊN GIA

Bảo đảm an toàn, an ninh trên không gian mạng cho tổ chức, doanh nghiệp và người dân *(T.5)*

CẦM TAY CHỈ VIỆC

Cách sử dụng mạng xã hội hiệu quả và thông minh cho học sinh *(T.11)*

HỎI ĐÁP KHOA HỌC

Vì sao phải có chính sách bảo đảm an toàn thông tin mạng? *(T.16)*

TIN TỨC SỰ KIỆN

Triển khai chống lừa đảo trực tuyến trên TikTok *(T.23)*

CHỊU TRÁCH NHIỆM XUẤT BẢN:

LÊ THANH TÙNG

Trưởng ban Truyền thông và Phổ biến kiến thức, Liên hiệp các Hội Khoa học & Kỹ thuật Việt Nam

BAN BIÊN TẬP:

PHẠM THỊ BÍCH HỒNG

NGUYỄN MINH THUẬN

NGUYỄN MẠNH HÀ

ĐỖ THỊ CẨM LINH

THIẾT KẾ

NGUYỄN QUỐC THÁI

NGUYỄN TƯỜNG HUY

CHUYÊN ĐỀ PHỔ BIẾN KIẾN THỨC SỐ 28 (THÁNG 09/2023)

Mọi thông tin phản hồi về nội dung xin liên hệ Ban Truyền thông và Phổ biến kiến thức

- **Địa chỉ: Lô D20, ngõ 19 Duy Tân, phường Dịch Vọng Hậu, quận Cầu Giấy, Hà Nội**
- **Điện thoại: (024)3.9438108**
- **Email: bichhongvusta@gmail.com; thuanminhanh@gmail.com**

Bảo vệ chủ quyền quốc gia trên không gian mạng

Chủ quyền quốc gia trên không gian mạng là một phần quan trọng của chủ quyền quốc gia. Bảo vệ chủ quyền quốc gia trên không gian mạng là bảo vệ hệ thống thông tin, các dữ liệu, tài nguyên số, đảm bảo tính toàn vẹn, bí mật, sẵn sàng của thông tin. Bên cạnh tự chủ về công nghệ, nâng cao năng lực của các lực lượng chuyên trách, phát huy vai trò của toàn dân thực hiện đồng bộ những giải pháp mới có thể bảo đảm an ninh quốc gia trên không gian mạng để phát triển đất nước trong thời gian tới.

Chiến lược bảo vệ chủ quyền quốc gia trên không gian mạng

Thượng tướng, PGS, TS Nguyễn Văn Thành, Phó chủ tịch chuyên trách Hội đồng Lý luận Trung ương cho rằng: "Cũng giống như chủ quyền lãnh thổ, các quốc gia có quyền tối cao, tuyệt đối, hoàn toàn và riêng biệt đối với phạm vi không gian mạng thuộc quyền kiểm soát của mình, tức là có chủ quyền quốc gia trên không gian mạng. Việc xác định chủ quyền quốc gia trên không gian mạng cần căn cứ vào phạm vi không gian mạng mà một quốc gia được quyền kiểm soát, chi phối trên cơ sở chủ quyền, lợi ích quốc gia và luật pháp quốc tế.

Thực chất, việc quốc gia xác lập chủ quyền không gian mạng là xác lập quyền quản lý, kiểm soát đối với cơ sở hạ tầng không gian mạng và thông tin được tạo ra, lưu trữ, xử lý và truyền tải trên đó, được thực hiện thông qua xác lập chủ quyền, quyền tài phán theo luật pháp quốc tế đối với cơ sở hạ tầng mạng thuộc sở hữu cả ở trong và ngoài lãnh thổ quốc gia; đồng thời mã hóa thông tin số truyền tải trên không gian mạng toàn cầu".

Thời gian qua, một số đối tượng phản động, cực đoan và tội phạm có tổ chức đã lợi dụng thành tựu của khoa học - công nghệ để tấn công cá nhân, quốc gia trên chính "vùng lãnh thổ mới" này.

Tại Việt Nam, từ năm 2018, Luật An ninh mạng được ban hành, trong đó xác định "An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân" và "Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát". Trước nguy cơ đe dọa chủ quyền quốc gia trên không gian mạng và bảo đảm an ninh mạng, Bộ Chính trị đã ban hành Nghị quyết số 29-NQ/TW, ngày 25/7/2018 về "Chiến lược bảo vệ Tổ quốc trên không gian mạng"; Nghị quyết số 30-NQ/TW, ngày 25/7/2018 về "Chiến lược An ninh mạng quốc gia"... Các văn kiện nêu trên thể hiện rõ quan điểm của Đảng, Nhà nước ta về nhiệm vụ bảo vệ Tổ quốc trên không gian mạng, xác định bảo vệ an ninh mạng là nhiệm vụ trọng yếu, thường xuyên của toàn Đảng, toàn quân, toàn dân và cả hệ thống chính trị.

Bảo vệ an ninh mạng là cấu thành trọng yếu của hoạt động bảo vệ an ninh quốc gia. Các thông tin bịa đặt, xuyên tạc đường lối, chủ trương, chính sách của Đảng và Nhà nước, công kích chế độ, kích động, chia rẽ khối đại đoàn kết dân tộc,… cần phải được kiểm soát, ngăn chặn kịp thời. Các quốc gia, cá nhân, pháp nhân, tổ chức khác phải

tôn trọng thể chế, pháp luật quốc gia trên không gian mạng.

Việt Nam là một trong số 20 quốc gia có người sử dụng internet cao trên thế giới, với hơn 68 triệu tài khoản mạng xã hội Facebook, 70 triệu người sử dụng internet và 154 triệu thiết bị kết nối internet có tỷ lệ truy cập hằng ngày chiếm 94%. Tuy nhiên, Việt Nam cũng nằm trong danh sách các quốc gia bị ảnh hưởng nhiều bởi các thách thức an ninh mạng. Không gian mạng trở thành nơi mà một số đối tượng chống đối đang lợi dụng để thường xuyên đăng tải thông tin sai lệch, tin giả nhằm chống phá Đảng, Nhà nước Việt Nam, gây mất ổn định chính trị, xã hội, nhằm thực hiện âm mưu chiến lược "diễn biến hòa bình" để thúc đẩy "tự diễn biến", "tự chuyển hóa" trong nội bộ, kích động biểu tình, bạo loạn, móc nối trong ngoài và tập hợp lực lượng nhằm lật đổ chính quyền...

Sự phát triển mạnh mẽ của khoa học - công nghệ tạo ra thuận lợi, thời cơ cho đất nước ta đẩy nhanh tiến trình công nghiệp hóa, hiện đại hóa và hội nhập quốc tế, với những mục tiêu như xây dựng Chính phủ số, xã hội số và nền kinh tế số. Tuy nhiên bên cạnh thời cơ, những thách thức, mối đe dọa từ không gian mạng đối với chủ quyền, lợi ích quốc gia, an ninh quốc gia cũng không ngừng gia tăng. Trong giai đoạn 2010-2021, với việc sử dụng hơn 8.784 web, blog có tên miền nước ngoài, 381 web, blog có tên miền trong nước, các lực lượng chống đối đã phát tán hơn 60.000 bản tin, bài viết nhằm bôi nhọ lãnh đạo Đảng, Nhà nước, kích động biểu tình trên không gian mạng... nhưng đã bị lực lượng an ninh mạng của Việt Nam xử lý và ngăn chặn kịp thời. Ngoài ra, lực lượng chức năng của Việt Nam cũng đã phát hiện hơn 80% số vụ lộ bí mật nhà nước là qua hệ thống thông tin.

Một số giải pháp trong bảo vệ chủ quyền quốc gia trên không gian mạng

Giai đoạn tới, dự báo tình hình diễn biến trên không gian mạng diễn ra hết sức phức tạp. Do đó để chủ động ứng phó, tác chiến trong mọi tình huống nhằm bảo vệ chủ quyền quốc gia trên không gian mạng, bảo vệ an ninh mạng, lực lượng tác chiến trên không gian mạng, lực lượng an ninh mạng và phòng, chống tội phạm công nghệ cao.

Một là cần tiếp tục triển khai, thực hiện có hiệu quả Nghị quyết, Chỉ thị của Đảng về bảo vệ Tổ quốc trên không gian mạng và An ninh mạng quốc gia, trọng tâm là Nghị quyết số 29-NQ/TW và Nghị quyết số 30-NQ/TW của Bộ Chính trị.

Hai là, hoàn thiện khung khổ luật pháp quốc gia, ban hành cơ chế, chính sách phù hợp với các quy định quốc tế nhằm nâng cao hiệu lực, hiệu quả công tác quản lý nhà nước về an toàn thông tin, an ninh mạng, sẵn sàng ứng phó với các thách thức an ninh mạng, đặc biệt là tội phạm sử dụng công nghệ cao nhằm bảo vệ tốt hơn quyền, lợi ích hợp pháp của các tổ chức và cá nhân.

Ba là, xác định rõ vai trò, tầm quan trọng của chiến tranh thông tin, chiến tranh mạng từ đó tiếp tục tăng cường đầu tư cơ sở hạ tầng kỹ thuật, phát triển nguồn nhân lực trong đảm bảo an toàn thông tin, an ninh mạng, đặc biệt là các lực lượng vũ trang để thực hiện tốt nhiệm vụ đảm bảo an ninh mạng, đấu tranh phòng, chống tội phạm trên không gian mạng.

Bốn là, tổ chức tuyên truyền, tập huấn, vận động, thuyết phục người sử dụng mạng tuân thủ pháp luật, văn hóa, đạo đức, quan hệ và ứng xử xã hội trên không gian mạng. Nâng cao nhận thức và năng lực tự bảo vệ của các tổ chức, cá nhân khi tham gia vào các hoạt động trên mạng.

Năm là, tăng cường công tác quản lý nhà nước các dịch vụ trên không gian mạng, nâng cao sự phối hợp giữa các bộ, ban, ngành để phát huy sức mạnh tổng hợp của toàn hệ thống chính trị và toàn xã hội.

Không gian mạng được coi như vùng "lãnh thổ đặc biệt" của quốc gia, chứa đựng lợi ích quốc gia, dân tộc. Do đó, chủ quyền trên không gian mạng là một phần không thể tách rời của chủ quyền quốc gia và bảo đảm chủ quyền quốc gia trên không gian mạng cũng chính là bảo vệ chủ quyền quốc gia, dân tộc.

CÁT TƯỜNG (GHI)

Bảo đảm an toàn, an ninh trên không gian mạng cho tổ chức, doanh nghiệp và người dân

Cùng với sự phát triển của khoa học, kỹ thuật và công nghệ, sự bùng nổ của internet, quá trình chuyển đổi số đang diễn ra mạnh mẽ tại Việt Nam đã tạo nên sự thay đổi đồng bộ về nhận thức và hành vi của cả cộng đồng.

Không thể phủ nhận những lợi ích to lớn mà chuyển đổi số đem lại cho xã hội hiện đại, tuy nhiên nguy cơ mất an toàn, an ninh thông tin cũng đang đặt ra nhiều thách thức, đòi hỏi công tác bảo đảm an toàn, an ninh trên không gian mạng cho tổ chức, doanh nghiệp và người dân trong quá trình chuyển đổi số cần được đặc biệt chú trọng.

Song để thực hiện được nhiệm vụ này, bên cạnh các lực lượng chuyên trách về an toàn thông tin, còn cần sự vào cuộc của các bộ, ngành, địa phương, doanh nghiệp, người dân... với việc thay đổi nhận thức, cách làm để cùng gìn giữ môi trường mạng an toàn, lành mạnh.

An toàn thông tin không đồng tốc với chuyển đổi số

Theo Bộ Thông tin và Truyền thông, trung bình mỗi người Việt Nam hoạt động trực tuyến khoảng 7-8 tiếng. Thời gian này càng gia tăng thì nguy cơ mất an ninh thông tin mạng lại càng cao hơn. Nhất là trong bối cảnh tình hình an ninh thông tin ở Việt Nam đã và đang có những diễn biến phức tạp, tiềm ẩn nhiều rủi ro và nguy cơ đối với an ninh con người, an ninh quốc gia và trật tự an toàn xã hội.Gần 1.300GB dữ liệu chứa hàng tỷ thông tin của tổ chức, doanh nghiệp, người dân được mua bán trái phép.

Còn khảo sát năm 2022 của Hiệp hội An toàn thông tin Việt Nam tại 135 tổ chức, doanh nghiệp trong nước cho thấy, cứ 4 tổ chức, doanh nghiệp có 1 đơn vị từng bị gián đoạn hệ thống, dịch vụ do tấn công mạng. Cục An toàn thông tin (Bộ Thông tin và Truyền thông) cho biết, trong 11 tháng năm 2022, Cục đã ghi nhận, cảnh báo và hướng dẫn xử lý 11.213 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam, tăng 44,2% so với cùng kỳ năm 2021; 2.063 website vi phạm (trong đó có 1.255 website lừa đảo) bị ngăn chặn. Tuy nhiên, vẫn còn nhiều cơ quan, tổ chức, doanh nghiệp chưa quan tâm xử lý các vấn đề liên quan đến an toàn thông tin; mới chỉ có 54,8% hệ thống thông tin đã phê duyệt hồ sơ bảo đảm an toàn thông tin theo cấp độ.

Lý giải về thực trạng bảo đảm an toàn thông tin hiện nay, Phó Giám đốc Công ty An ninh mạng Viettel Lê Quang Hà cho rằng, quá trình chuyển đổi số diễn ra nhanh chóng, song an toàn thông tin cho chuyển đổi số lại chưa theo kịp. Sự không đồng tốc này nằm ở 3 vấn đề: Nhận thức và cách làm; nguồn lực cho chuyển đổi số còn hạn chế; công nghệ an toàn thông tin không theo kịp.

Thay đổi nhận thức, tạo ra sản phẩm an toàn thông tin

Về giải pháp, ông Lê Quang Hà đề xuất, việc chuyển đổi số phải gắn với chiến lược về an toàn thông tin, từ đó thay đổi nhận thức và cách làm. Nói cách khác, trước hết phải chuyển đổi số trong chính lĩnh vực an toàn thông tin; tổ chức lực lượng an toàn thông tin

Ông Lê Quang Hà, Phó Giám đốc Công ty An ninh mạng Viettel

Ông Trần Đăng Khoa, Phó Cục trưởng phụ trách Cục An toàn thông tin

trong lực lượng chuyển đổi số, đưa an toàn thông tin vào sản phẩm, dịch vụ chuyển đổi số.

Từ góc độ doanh nghiệp công nghệ, Phó Giám đốc công nghệ Công ty Hệ thống thông tin FPT (Tập đoàn FPT) Đào Gia Hạnh chia sẻ, những năm gần đây, FPT đầu tư rất nhiều cho nghiên cứu và phát triển, đồng thời tập trung đào tạo nhân lực an toàn thông tin. "Các giải pháp bảo mật của FPT bảo vệ toàn diện tài sản số của tổ chức, doanh nghiệp, cá nhân tham gia giao dịch, dịch vụ trên môi trường số", ông Đào Gia Hạnh nói.

Tương tự, Tổng Giám đốc Công ty TNHH An ninh an toàn CMC Hà Thế Phương cho hay, các doanh nghiệp công nghệ trong nước hoàn toàn có khả năng tạo ra các sản phẩm, dịch vụ an toàn thông tin mạng chất lượng cao.

Mong muốn chung tay nâng cao nhận thức an toàn thông tin cho người dùng internet tại Việt Nam, ông Shash Hegde, chuyên gia an toàn thông tin cao cấp, khối dịch vụ khách hàng công của Google châu Á - Thái Bình Dương, cho biết Google bắt đầu từ những sáng kiến ở từng quốc gia để nâng cao nhận thức cho người dùng internet.

Theo Phó Cục trưởng phụ trách Cục An toàn thông tin Trần Đăng Khoa, năm 2023 được Bộ Thông tin và Truyền thông xác định là năm kỷ cương, tuân thủ quy định về an toàn thông tin. Theo đó, Bộ sẽ trình Thủ tướng Chính phủ ban hành chỉ thị về tuân thủ quy định pháp luật và tăng cường bảo đảm hệ thống thông tin theo cấp độ. Đặc biệt, từ ngày 1-1-2024, các hệ thống thông tin không đáp ứng đầy đủ quy định của pháp luật về an toàn sẽ phải dừng vận hành. "Năm 2023 lấy chủ đề dữ liệu số, với một số nhiệm vụ trọng tâm là tổ chức bảo vệ dữ liệu, nâng cao nhận thức, liên minh tuyên truyền và tổ chức chiến dịch tuyên truyền", ông Trần Đăng Khoa thông tin.

Thứ trưởng Bộ Thông tin và Truyền thông Nguyễn Huy Dũng nhận định, vấn đề gốc, cốt lõi nhất là làm sao để người dân có thể chủ động bảo vệ mình trên không gian mạng. Vì vậy, nhiệm vụ quan trọng là cần nâng cao nhận thức và trang bị kỹ năng an toàn thông tin cho đông đảo người dân. Và để đông đảo người dân ý thức, quan tâm đến vấn đề này thì hoạt động tuyên truyền cần phải đáp ứng tốt nhất. Việc liên minh tuyên truyền nâng cao nhận thức, kỹ năng bảo đảm an toàn thông tin cho người dân trên không gian mạng được Bộ Thông tin và Truyền thông chủ trì thành lập vừa qua là để thực hiện mục tiêu này.

Khẳng định không lực lượng đơn lẻ nào có thể làm hết việc "quản" khối lượng công việc khổng lồ trên không gian mạng, song Thứ trưởng Bộ Thông tin và Truyền thông cho rằng, đã đến lúc cần thay đổi nhận thức để hiểu việc bảo đảm an toàn không gian mạng là trách nhiệm phải chủ động vào cuộc của tất cả bộ, ngành, địa phương, theo nguyên tắc "thực sao ảo vậy". Nghĩa là cơ quan quản lý lĩnh vực nào trong đời thực thì cũng có trách nhiệm quản lý nội dung đó trên không gian mạng.

Bảo đảm an toàn, an ninh trên không gian mạng cho tổ chức, doanh nghiệp và người dân không chỉ là trách nhiệm của Nhà nước, của các cơ quan chức năng mà còn là nghĩa vụ, trách nhiệm của mỗi công dân vì đó cũng là cách để chúng ta tự bảo vệ lợi ích của chính mình.

TRUNG KIÊN *(GHI)*

Không gian mạng và bảo vệ an ninh quốc gia trên không gian mạng

Bảo vệ an ninh quốc gia trên không gian mạng được xác định là trách nhiệm của toàn Đảng, toàn dân, toàn quân, c ác cấp, các ngành. Trong bối cảnh Cách mạng công nghiệp lần thứ tư, cần phải tăng cường hơn nữa bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm an ninh quốc gia trên không gian mạng.

Hiện nay, trên thế giới vẫn chưa có khái niệm thống nhất về không gian mạng. Quan điểm của Mỹ đề cập trong Chỉ thị số 54 về An ninh quốc gia và Chỉ thị số 23, năm 2008, về An ninh nội địa của Tổng thống Mỹ cho rằng, không gian mạng là mạng lưới kết nối các cơ sở hạ tầng bao gồm internet, các mạng viễn thông, các hệ thống máy tính, các hệ thống xử lý và điều khiển trong ngành công nghiệp trọng yếu; không gian mạng được dùng để mô tả một môi trường ảo, trong đó diễn ra việc trao đổi thông tin và tương tác giữa con người với nhau, không bị giới hạn bởi không gian và thời gian. Bộ Quốc phòng Nhật Bản xác định không gian mạng là không gian ảo, bao gồm cả internet, trong đó thông tin được trao đổi bằng công nghệ thông tin và viễn thông; không gian mạng là "trường", trong đó các hoạt động tình báo, tấn công và phòng thủ được tiến hành như "trường" trên bộ, trên biển, trên không và trong không gian.

Trung Quốc coi không gian mạng là chiến trường thứ năm và là mặt trận tình báo mới. Trong phát biểu tại hội nghị thành lập Tiểu tổ Lãnh đạo an ninh mạng và thông tin hóa Trung ương ở Bắc Kinh, ngày 27/2/2014, Tổng Bí thư, Chủ tịch nước Tập Cận Bình cho rằng, internet và an ninh thông tin đã trở thành thách thức mới đối với Trung Quốc vì cả hai đều gắn liền với an ninh quốc gia và ổn định xã hội.

Luật An ninh mạng được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam thông qua ngày 12/6/2018 khẳng định, không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian. Không gian mạng quốc gia là không gian mạng do Chính phủ xác lập, quản lý và kiểm soát.

Trên không gian mạng, Việt Nam có hệ thống thông tin quan trọng về an ninh quốc gia. Hệ thống này gồm hệ thống thông tin quân sự, an ninh, ngoại giao, cơ yếu; hệ thống thông tin lưu trữ, xử lý thông tin thuộc bí mật nhà nước; hệ thống thông tin phục vụ lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; hệ thống thông tin phục vụ bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái; hệ thống thông tin phục vụ bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; hệ thống thông tin quan trọng phục vụ hoạt động của cơ quan, tổ chức ở Trung ương; hệ thống thông tin quốc gia

thuộc lĩnh vực năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí; hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

Từ khái niệm bảo vệ an ninh quốc gia được đề cập trong Luật An ninh quốc gia Việt Nam năm 2004 có thể hiểu, bảo vệ an ninh quốc gia trên không gian mạng là phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại các hoạt động xâm phạm an ninh quốc gia trên không gian mạng. Thực tế cho thấy, không gian mạng quốc gia Việt Nam chứa đựng những yếu tố hết sức quan trọng, nếu bị xâm hại sẽ ảnh hưởng nghiêm trọng tới lợi ích, an ninh quốc gia. Hiện nay, các thế lực thù địch, phản động trong và ngoài nước vẫn không từ bỏ âm mưu, hoạt động chống phá Việt Nam. Chúng luôn lợi dụng thành tựu khoa học - kỹ thuật và không gian mạng vào các hoạt động chống phá với các thủ đoạn ngày càng tinh vi, nguy hiểm. Trong bối cảnh đó, yêu cầu bảo vệ an ninh quốc gia trên không gian mạng đặt ra trong tình hình hiện nay là hết sức cấp thiết. Chính vì vậy, Nghị quyết số 51-NQ/TW, ngày 5/9/2019, của Bộ Chính trị, về "Chiến lược bảo vệ an ninh quốc gia" xác định, cần phải tăng cường bảo vệ an toàn, an ninh mạng các hệ thống thông tin quan trọng quốc gia và các hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, phát hiện và đấu tranh ngăn chặn các hoạt động xâm phạm an ninh quốc gia trên không gian mạng; khắc phục điểm yếu, lỗ hổng bảo mật, nguy cơ mất an toàn, an ninh mạng, an ninh thông tin.

Bảo vệ an ninh quốc gia trên không gian mạng được xác định là trách nhiệm của toàn Đảng, toàn dân, toàn quân ta. Do đó, để triển khai công tác này, phải phát huy được sức mạnh dân tộc kết hợp với sức mạnh thời đại; đồng thời, xác định đây là cuộc đấu tranh của toàn dân, dưới sự lãnh đạo của Đảng, là nhiệm vụ trọng yếu của cuộc đấu tranh bảo vệ an ninh quốc gia, giữ gìn trật tự, an toàn xã hội, là trách nhiệm của cả hệ thống chính trị, trong đó, lực lượng công an giữ vai trò nòng cốt, lực lượng an ninh mạng và cảnh sát phòng, chống tội phạm công nghệ cao có trách nhiệm trực tiếp thực hiện nhiệm vụ bảo vệ chủ quyền, lợi ích quốc gia trên không gian mạng. Đây là quan điểm, tư tưởng cơ bản, xuyên suốt của Đảng, quyết định thắng lợi cuộc đấu tranh bảo vệ an ninh, chủ quyền quốc gia trên không gian mạng. Các nguyên tắc cần quán triệt trong bảo vệ an ninh quốc gia trên không gian mạng bao gồm: Tuân thủ Hiến pháp, pháp luật, bảo đảm lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân; đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước, huy động sức mạnh tổng hợp của hệ thống chính trị và toàn dân tộc; lực lượng chuyên trách bảo vệ an ninh quốc gia trên không gian mạng làm nòng cốt. Kết hợp chặt chẽ giữa nhiệm vụ bảo vệ an ninh quốc gia với nhiệm vụ xây dựng, phát triển kinh tế, văn hóa, xã hội. Chủ động phòng ngừa, đấu tranh làm thất bại mọi âm mưu và hoạt động xâm phạm an ninh quốc gia trên không gian mạng.

Bảo vệ an ninh quốc gia trên không gian mạng là bảo vệ chế độ chính trị và Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ Việt Nam trên không gian mạng; bảo vệ an ninh về tư tưởng và văn hóa, khối đại đoàn kết toàn dân tộc, quyền lợi và lợi ích hợp pháp của các cơ quan, tổ chức, cá nhân trên không gian mạng; bảo vệ an ninh trong các lĩnh vực kinh tế, quốc phòng, đối ngoại và các lợi ích khác của quốc gia trên không gian mạng; bảo vệ bí mật nhà nước và các mục tiêu quan trọng về an ninh quốc gia trên không gian mạng; phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại và loại trừ các hoạt động xâm phạm an ninh quốc gia, nguy cơ đe dọa an ninh quốc gia trên không gian mạng.

NGUYỄN QUỲNH (GHI)

Bảo vệ an ninh quốc gia trên không gian mạng

Hiện nay, không gian mạng được hình thành từ sự kết hợp của những công nghệ đột phá, như: Internet kết nối vạn vật, máy tính lượng tử, điện toán đám mây, dữ liệu lớn, truy cập nhanh… đã làm cho thế giới kết nối nhau, tương tác đa chiều, không còn khoảng cách biên giới và con người gần gũi nhau hơn. Việc bảo vệ an ninh quốc gia trên không gian mạng hiện nay rất cần thiết.

Việt Nam là một trong những quốc gia có tốc độ phát triển internet cao nhất thế giới và đứng đầu ASEAN về số lượng tên miền quốc gia… Không gian mạng và đi liền với nó là các thiết bị thông minh ngày càng phổ biến, đã làm cho xã hội thông tin và kinh tế tri thức của ta ngày càng phát triển.

Với việc Đảng và Nhà nước chủ trương đẩy mạnh phát triển Chính phủ điện tử, đã làm giảm thiểu các thủ tục hành chính, nâng cao hiệu quả quản lý nhà nước, tạo nhiều thuận lợi cho người dân và các doanh nghiệp truy cập thông tin. Cùng với đó, nhiều địa phương đang nỗ lực xây dựng thành phố thông minh, đã tạo ra môi trường sống tốt hơn, nâng cao hiệu quả phát triển kinh tế, xã hội và tăng cường quốc phòng, an ninh.

Không gian mạng cũng đang bị các thế lực xấu lợi dụng, làm nảy sinh nhiều nguy cơ, thách thức đối với đất nước. Đó là: Các cuộc tấn công mạng với quy mô ngày càng lớn, tính chất ngày càng nghiêm trọng; các hành vi chiếm đoạt tài sản thông qua các hoạt động thương mại điện tử; sử dụng các dịch vụ Internet, viễn thông, mạng xã hội để lừa đảo; tổ chức đánh bạc và đánh bạc xuyên quốc gia, tống tiền, phát tán văn hóa phẩm đồi trụy, kinh doanh trái phép các loại tiền điện tử… Đặc biệt, lợi dụng khả năng đưa tin nhanh, đa chiều và rộng khắp trên không gian mạng, một số tổ chức, cá nhân trong và ngoài nước cấu kết với nhau, tập trung chống phá nền tảng tư tưởng, thể chế chính trị đất nước rất quyết liệt. Trên các địa chỉ: VOA, BBC, RFI, "Dân luận" và một số trang facebook,… họ xuyên tạc, phủ nhận chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh, Cương lĩnh, đường lối của Đảng, chính sách, pháp luật của Nhà nước.

Thực tiễn cách mạng nước ta chứng minh chân lý: Nhờ kiên định và vận dụng sáng tạo chủ nghĩa Mác - Lênin, tư tưởng Hồ Chí Minh mà Đảng Cộng sản Việt Nam đã lãnh đạo toàn dân tộc đoàn kết một lòng, chiến thắng mọi kẻ thù, giành được thắng lợi vẻ vang trong các cuộc kháng chiến bảo vệ Tổ quốc cũng như trong sự nghiệp đổi mới, xây dựng đất nước hiện nay. Trong tiến trình công nghiệp hóa, hiện đại hóa, nhất là trong đẩy mạnh thực hiện cách mạng công nghiệp lần thứ 4, các thế lực thù địch càng ra sức chống phá ta trên không gian mạng. Bởi vậy, chúng ta cần tích cực đấu tranh phản bác mọi luận điệu xuyên tạc, bảo vệ các giá trị chân chính của dân tộc và thời đại, bảo vệ sự nghiệp đổi mới, xây dựng, bảo vệ Tổ quốc xã hội chủ nghĩa. Trong cuộc đấu tranh này, cần huy động được sức mạnh tổng hợp của mọi lực lượng, nhất là của cán bộ, đảng viên; lực lượng quân đội, công an, trí thức, thanh niên…

Đồng thời, phát huy vai trò của các cơ quan nghiên cứu, cơ quan báo chí, truyền thông, đấu tranh vạch trần các luận điệu xuyên tạc của chúng; làm rõ cơ sở khoa học, cơ sở thực tiễn của đường lối đổi mới, nhiệm vụ công tác quân sự, quốc phòng của Đảng và những thành tựu to lớn mà nhân dân ta đạt được trong phát triển kinh tế, xã hội, tăng cường quốc phòng, an ninh đất nước.

Cần khẳng định rằng, Luật An ninh mạng là phù hợp với Hiến pháp Việt Nam và các điều ước quốc tế mà Việt Nam là thành viên. Tổ chức thực hiện tốt Luật này sẽ bảo vệ được lợi ích của Nhân dân, an ninh chính trị, trật tự, an toàn xã hội và chủ quyền của quốc gia, góp phần quan trọng vào việc đấu tranh ngăn chặn, loại trừ các nhân tố phá hoại trên không gian mạng.

NGÔ VÂN

Nâng cao ý thức, trách nhiệm để xây dựng không gian mạng lành mạnh

Sử dụng không gian mạng là nhu cầu không thể thiếu của mỗi chúng ta hiện nay và trở thành xu hướng của thời đại. Vai trò to lớn của không gian mạng đối với sự phát triển của xã hội loài người là không thể phủ nhận.

Trên không gian mạng mà trực tiếp là truyền thông mạng là công cụ đắc lực của các thế lực thù địch, các tổ chức phản động để thúc đẩy "tự diễn biến", "tự chuyển hóa" trong lòng xã hội Việt Nam. Vì vậy, để xây dựng "không gian mạng lành mạnh", mỗi người dân cần làm tốt một số nội dung sau:

Một là, mỗi cá nhân cần nghiên cứu, hiểu rõ ý nghĩa, giá trị, nội dung của Luật An ninh mạng, quyền lợi, nghĩa vụ, trách nhiệm và những hành vi bị cấm khi tham gia hoạt động trên không gian mạng.

Theo đó, Luật An ninh mạng nhằm bảo vệ người dùng hợp pháp trên không gian mạng; phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống Nhà nước, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, kích động biểu tình, phá rối của các thế lực phản động. Phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các đợt tấn công mạng, khủng bố mạng và phòng, chống nguy cơ chiến tranh mạng.

Luật An ninh mạng quy định rõ những hành vi bị cấm như: sử dụng không gian mạng để tuyên truyền chống Nhà nước; tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước; xuyên tạc lịch sử...). Những quy định này không xâm phạm đến quyền con

người, không cản trở tự do ngôn luận, không tạo rào cản, không cản trở hoạt động bình thường, đúng luật của các tổ chức, cá nhân như những thông tin trên mạng xã hội, blog, web phản động tuyên truyền, xuyên tạc trong thời gian vừa qua. Thực hiện đúng Luật, nghĩa là bảo vệ chính mình, người thân và gia đình, đồng thời, góp phần bảo vệ an ninh mạng quốc gia.

Hai là, tự trau dồi kỹ năng nhận diện âm mưu, thủ đoạn gây nguy cơ mất an ninh mạng, nhất là âm mưu, thủ đoạn "diễn biến hòa bình", bạo loạn lật đổ của các thế lực thù địch. Nhận diện được các tổ chức chống đối hoạt động trên không gian mạng như Việt Tân, Chính phủ quốc gia Việt Nam lâm thời...; các thủ đoạn tạo vỏ bọc "xã hội dân sự", "diễn đàn dân chủ",... để chống phá; các website giả mạo, các trang mạng có nhiều nội dung thông tin xấu, độc.

Ba là, nâng cao ý thức phòng tránh, tự vệ khi tham gia mạng xã hội. Nghiên cứu kỹ trước khi like hoặc chia sẻ các file, các bài viết hoặc các đường link; cảnh giác với trang web lạ (web đen), E-mail chưa rõ danh tính và đường dẫn đáng nghi ngờ; tuyệt đối không a dua, hiếu kỳ, hoặc tham tiền bạc cùng với những lời kích động, xúi giục của các đối tượng xấu. Kịp thời cung cấp thông tin, thực hiện yêu cầu và hướng dẫn của cơ quan nhà nước có thẩm quyền, người có trách nhiệm.

Bốn là, cần biết cách tận dụng, sử dụng mạng xã hội một cách đúng đắn và hiệu quả, biến mạng xã hội thành một phương tiện, một kênh hữu ích để mở mang kiến thức, cùng nhau xây dựng môi trường văn hóa mạng xã hội lành mạnh, tránh bị các thông tin ảo chi phối tác động, góp phần phòng chống, ngăn chặn những tư tưởng, quan điểm sai trái, thù địch một cách có hiệu quả.

Năm là, phổ biến, tuyên truyền trong gia đình, người thân, bạn bè và Nhân dân nơi cư trú các quy định của Luật An ninh mạng để mọi người nắm, hiểu và không thực hiện các hành vi vi phạm liên quan đến an ninh mạng, góp phần xây dựng "không gian mạng lành mạnh từ cơ sở".

THÁI BẢO

Cách sử dụng mạng xã hội hiệu quả và thông minh cho học sinh

Không gian mạng chứa đựng kho kiến thức khổng lồ, song nếu không biết khai thác và sử dụng mạng Internet đúng cách sẽ tiềm ẩn nhiều nguy hại khó lường. Do đó, để có thể sử dụng mạng Internet an toàn, hiệu quả trong học tập, học sinh cần được trang bị phương pháp học tập với máy tính và mạng Internet.

Không thể phủ nhận rằng mạng xã hội mang lại rất nhiều lợi ích cho người dùng. Mạng xã hội cho phép các con kết nối, chia sẻ cùng nhau ngay cả khi không đến lớp. Con có thể liên lạc với bạn để chia sẻ tài liệu, trao đổi học tập hay giúp nhau giải đáp thắc mắc ở lớp.

Bên cạnh đó, rất nhiều tài liệu học tập bổ ích được chia sẻ trên mạng xã hội. Đây sẽ là nguồn tài nguyên to lớn để phục vụ việc học tập và nghiên cứu của học sinh. Tuy nhiên điều này rất dễ phản tác dụng vì trẻ con thường thích khám phá và tò mò, điều bố mẹ cấm đôi khi lại là điều kích thích khiến con lén dùng mạng xã hội. Thay vì cấm cản, bố mẹ có thể hướng dẫn con sử dụng mạng xã hội an toàn, hiệu quả, có văn hóa như:

Bảo mật thông tin cá nhân: Những thông tin như tên thật, tuổi, trường lớp, địa chỉ nhà, ảnh cá nhân hay các loại mật khẩu là những thông tin cá nhân, cần được bảo mật, không nên chia sẻ những thông tin này trên mạng. Bố mẹ cũng nên hướng dẫn con bảo mật tài khoản 2 lớp để tránh bị lấy cắp tài khoản phục vụ cho những mục đích xấu.

Suy nghĩ kỹ trước khi chia sẻ bất cứ điều gì: Mạng xã hội vẫn luôn là con dao hai lưỡi, vì vậy trước khi bình luận, chia sẻ hay đăng tải bất cứ thông tin gì con cần phải tìm hiểu và suy nghĩ kỹ. Vì những bài đăng trên mạng sẽ có nhiều người xem, có thể con sẽ bị người khác soi mói, đánh giá, bình luận tiêu cực khiến con thấy buồn hay lo sợ.

Bên cạnh đó, thông tin được đăng tải trên mạng xã hội không phải lúc nào cũng đúng. Có rất nhiều tin sai sự thật, tin kích động chống phá nhà nước,… được lan truyền trên mạng. Nếu không tìm hiểu kỹ thì con có thể chia sẻ, tin tưởng vào các nguồn tin sai trái, ảnh hưởng đến nhận thức, tiếp tay cho kẻ xấu lan truyền tin giả.

Các con có thể nhờ sự giúp đỡ từ bố mẹ để xem thông tin mình định chia sẻ có đúng sự thật không, có phù hợp để chia sẻ không.

Ứng xử văn minh trên mạng: Nhiều trẻ nghĩ rằng mạng xã hội là ảo, con có làm gì thì cũng không ảnh hưởng đến bản thân và người khác. Tuy nhiên, mạng cũng là một xã hội thu nhỏ, tất cả những điều con làm trên mạng đều có thể ảnh hưởng đến bản thân con và mọi người.

Vì vậy hãy sử dụng mạng xã hội một cách văn minh, không hùa theo cộng đồng mạng để chửi rủa, miệt thị người khác. Nếu có điều gì buồn bực hay bất đồng quan điểm với bạn bè, người thân, con hãy chọn cách nói chuyện trực tiếp để cùng nhau đưa ra cách giải quyết phù hợp. Mạng xã hội là ảo nhưng nỗi đau là thật, đừng để một dòng chữ trong lúc không suy nghĩ làm ảnh hưởng đến cuộc đời của một con người.

☞ Nhận biết các dạng lừa đảo qua mạng: Hiện này có rất nhiều dạng lừa đảo qua mạng. Kẻ xấu có thể tạo một tài khoản ảo, kết bạn và trò chuyện với con để lấy lòng tin sau đó dò hỏi những thông tin của con. Chúng có thể đóng vai một người bạn, muốn con cung cấp thông tin để gửi quà. Tuy nhiên các con luôn nhớ nguyên tắc "không chia sẻ thông tin cá nhân", đặc biệt là chia sẻ trên mạng xã hội để không trở thành nạn nhân của lừa đảo. Bên cạnh đó, con cũng cần cẩn thận với các trò chơi trúng thưởng, không nên nhấn vào đường link lạ để tránh bị mất tài khoản hay bị đánh cắp thông tin.

Nếu có người yêu cầu các con gửi ảnh cá nhân, đặc biệt là ảnh nhạy cảm, hãy từ chối ngay và nói với bố mẹ. Đây cũng là một dạng lạm dụng cần được đề phòng và tránh xa.

Giới hạn thời gian sử dụng mạng xã hội: Bố mẹ nên thống nhất và giới hạn thời gian sử dụng mạng xã hội cho con. Con chỉ nên sử dụng khi có điều cần trao đổi với bạn bè, thầy cô. Hoặc con có thể sử dụng mạng xã hội để giải trí sau khi đã hoàn thành các việc cần thiết.

Với các bạn còn nhỏ, bố mẹ nên giới hạn mục đích sử dụng của con, việc dùng mạng xã hội chỉ để liên lạc, trao đổi học tập với bạn và thầy cô dưới sự giám sát của bố mẹ.

Bố mẹ cũng nên dành nhiều thời gian bên con, hạn chế dùng mạng xã hội trước mặt con để đảm bảo sự thống nhất trong việc giáo dục và làm gương cho con.

THẾ ANH

Vai trò đảm bảo an ninh mạng đối với hệ thống thông tin trọng yếu quốc gia

Hiện nay, các chiến dịch tấn công mạng, gián điệp mạng, khủng bố mạng trên quy mô lớn nhằm vào hệ thống thông tin trọng yếu của các quốc gia liên tục diễn ra, gây ra những hậu quả khôn lường. Chính vì vậy, bảo đảm an ninh mạng đang là ưu tiên hàng đầu được thể hiện rõ trong các quan điểm, chiến lược và hành động cụ thể của các quốc gia.

Những năm qua, Đảng, Nhà nước ta đã có nhiều chủ trương đẩy mạnh ứng dụng, phát triển công nghệ thông tin phục vụ nhiệm vụ phát triển kinh tế - xã hội, bảo đảm quốc phòng, an ninh và đã đạt được nhiều thành tựu rất quan trọng. Nhiều chính sách, pháp luật được ban hành nhằm thúc đẩy ứng dụng công nghệ thông tin phát triển kinh tế - xã hội, đồng thời bảo đảm an ninh mạng, như Luật An ninh mạng, Luật An toàn thông tin mạng, Luật Bảo vệ bí mật nhà nước (BMNN) và các văn bản hướng dẫn thi hành… Thông qua việc ban hành các văn bản chính sách, pháp luật, nước ta đã chính thức xác định và thừa nhận tầm quan trọng của các hệ thống thông tin trọng yếu quốc gia hay được gọi là hệ thống thông tin quan trọng về an ninh quốc gia. Theo đó, hệ thống thông tin quan trọng về an ninh quốc gia là hệ thống thông tin khi bị sự cố, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt, tấn công hoặc phá hoại sẽ xâm phạm nghiêm trọng an ninh mạng.

Hệ thống thông tin quan trọng về an ninh quốc gia được xác định trong các lĩnh vực bao gồm: quân sự, an ninh, ngoại giao, cơ yếu; lưu trữ, xử lý thông tin thuộc BMNN; lưu giữ, bảo quản hiện vật, tài liệu có giá trị đặc biệt quan trọng; bảo quản vật liệu, chất đặc biệt nguy hiểm đối với con người, môi trường sinh thái; bảo quản, chế tạo, quản lý cơ sở vật chất đặc biệt quan trọng khác liên quan đến an ninh quốc gia; hoạt động của cơ quan, tổ chức ở trung ương; năng lượng, tài chính, ngân hàng, viễn thông, giao thông vận tải, tài nguyên và môi trường, hóa chất, y tế, văn hóa, báo chí; hệ thống điều khiển và giám sát tự động tại công trình quan trọng liên quan đến an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia.

QUỲNH ANH

"An toàn, an ninh mạng là trụ cột quan trọng thúc đẩy chuyển đổi số"

Nhấn mạnh tầm quan trọng của việc đảm bảo an toàn, an ninh mạng, Phó trưởng ban Kinh tế Trung ương Nguyễn Đức Hiển cho rằng, an toàn an ninh mạng là 1 trụ cột, 1 nội dung quan trọng để tạo niềm tin số, thúc đẩy chuyển đổi số.

Nhận định trên được ông Nguyễn Đức Hiển, Phó Trưởng ban Kinh tế Trung ương đưa ra trong phát biểu tại hội nghị bàn tròn cấp cao Lãnh đạo CNTT và An toàn thông tin năm 2022, được Cục An toàn thông tin - Bộ TT&TT, Công ty An ninh mạng Viettel (Viettel Cyber Security) và IEC Group phối hợp tổ chức chiều ngày 21/9 tại TP.HCM.

Với chủ đề "Tối ưu nguồn lực - Tăng cường hiệu quả đầu tư an toàn thông tin trong kỷ nguyên số", các đơn vị tổ chức sự kiện hướng tới mục tiêu tăng cường năng lực tổ chức ứng phó, phát hiện sớm các nguy cơ và bảo vệ các hệ thống thông tin trong các lĩnh vực quan trọng.

Theo Phó Trưởng ban Kinh tế Trung ương Nguyễn Đức Hiển, trong xu thế phát triển, có 3 quá trình chuyển đổi quan trọng, đó là chuyển đổi số, chuyển đổi xanh và chuyển đổi lao động, từ chưa có kỹ năng hay kỹ năng thấp sang có kỹ năng, trình độ cao hơn.

Ở góc độ doanh nghiệp, ông Robert Trọng Trần, Phó Tổng giám đốc Dịch vụ Tư vấn, Lãnh đạo mảng rủi ro công nghệ và an ninh mạng của EY Việt Nam cho biết, theo khảo sát, 81% các lãnh đạo trên toàn cầu phản hồi đại dịch Covid-19 đã bắt buộc các doanh nghiệp phải bỏ qua các quy trình an toàn bảo mật cần thiết, trong khi các cuộc tấn công mạng đang diễn ra nhiều hơn theo phản hồi từ 77% số người tham gia khảo sát. "Đây cũng là lý do vì sao EY luôn nhấn mạnh rằng chuyển đổi số phải được thúc đẩy bởi an ninh mạng. Việc có 1 chiến lược an ninh mạng rõ ràng sẽ cho phép các tổ chức tiến nhanh và tự tin trong môi trường đầy nguy cơ và thách thức như hiện nay", ông Robert Trọng Trần nói.

Trong quá trình chuyển đổi số, vấn đề rất quan trọng chính là bảo đảm an toàn, an ninh mạng. "Khi thực hiện chuyển đổi số, an toàn, an ninh mạng là 1 trụ cột, 1 nội dung rất quan trọng để tạo niềm tin số, thúc đẩy quá trình chuyển đổi số. Nếu không bảo đảm được an toàn, an ninh mạng thì quá trình chuyển đổi số cũng không thể thu được thành công như mong muốn", ông Nguyễn Đức Hiển chia sẻ quan điểm.

Khẳng định quan điểm an ninh mạng phải luôn song hành cùng chuyển đổi số, đại diện Viettel Cyber Security cho rằng, cần xác định và ưu tiên đưa nguồn lực an toàn thông tin vào cùng với lực lượng chuyển đổi số; phát triển hệ sinh thái sản phẩm theo định hướng tích hợp đồng bộ trên 1 nền tảng quản trị duy nhất; đồng thời đồng bộ mô hình đầu tư các dự án chuyển đổi số với các dự án bảo đảm an toàn thông tin cũng như tăng cường năng lực phòng thủ bằng công nghệ.

Bên cạnh đó, đại diện Viettel Cyber Security cũng đưa ra khuyến nghị về việc xây dựng mô hình chuyển đổi số cân bằng, vững chắc và an toàn giữa 3 bên gồm chủ đầu tư, đối tác chuyển đổi số và đối tác an toàn thông tin.

LÊ HIẾU

Một số phương pháp bảo mật API hiệu quả cho doanh nghiệp

Ngày nay, trong quy trình xem xét, đánh giá và phân bổ nguồn lực của các doanh nghiệp, bảo mật dữ liệu vẫn được coi là ưu tiên hàng đầu. Tuy nhiên, nhiều doanh nghiệp vẫn phải đối mặt với nhiều hơn những mối đe dọa từ các sự cố an ninh mạng mà họ lường trước.

API là một phần cơ bản của các mẫu phần mềm hiện đại như kiến trúc microservice (các dịch vụ độc lập), cho phép các ứng dụng phần mềm tương tác với nhau. Bảo mật API là quá trình bảo vệ API khỏi các cuộc tấn công. Do các API được sử dụng rất phổ biến và cho phép truy cập vào các chức năng cũng như dữ liệu nhạy cảm của phần mềm, nên API đang trở thành mục tiêu chính của những kẻ tấn công. Vì vậy, các doanh nghiệp cần phải thường xuyên kiểm tra các API để xác định và xử lý các lỗ hổng bằng những biện pháp bảo mật tốt nhất.

Bằng cách thực hành các nguyên tắc cơ bản phù hợp, các tổ chức/doanh nghiệp có thể sử dụng tích hợp API và các công nghệ tương tự để giữ an toàn cho hệ thống của họ trước nhiều hình thức tấn công ngày càng tinh vi. Dưới đây là một số phương pháp giúp các doanh nghiệp bảo mật API hiệu quả:

Đánh giá các quy trình hoạt động và cơ sở hạ tầng của tổ chức

Với việc sử dụng ngày càng nhiều các API và microservice được kết nối trên nhiều cài đặt tại chỗ và đám mây khác nhau, việc tìm ra các điểm yếu trở nên khó khăn, do đó các doanh nghiệp cần phải đánh giá và xem xét thường xuyên những yếu tố sau:

API hướng tới khách hàng: Bằng cách tận dụng các API, các công ty có thể chia sẻ thông tin với khách hàng mà không cần phải cho họ truy cập vào cơ sở dữ liệu hoặc hệ thống cơ bản của mình. Các doanh nghiệp có thể giới hạn những gì khách hàng có thể truy cập, chỉ tiết lộ các phân đoạn dữ liệu cụ thể. Việc sử dụng API để chỉ hiển thị một phần cơ sở dữ liệu và đảm bảo rằng người dùng không thể truy

cập toàn bộ hệ thống, nhưng dữ liệu được tiết lộ vẫn phải được bảo vệ.

API nội bộ: Các nhóm CNTT phải đảm bảo rằng họ đồng bộ hóa các dịch vụ thông qua API để chỉ cung cấp quyền truy cập cần thiết, thay vì cho phép mọi người trong mọi bộ phận truy cập vào nhiều loại dịch vụ, điều này có thể gây khó khăn đối với vấn đề quản trị.

Vì vậy điều quan trọng nhất là doanh nghiệp cần tạo một hệ thống các chính sách và tiêu chuẩn phối hợp với các nhóm tuân thủ và bảo mật nội bộ. Một số doanh nghiệp cũng có thể xem xét các nghĩa vụ pháp lý và đảm bảo các biện pháp bảo mật được cập nhật và tuân thủ.

Đánh giá rủi ro API của tổ chức

Để bảo mật API cần thực hiện đánh giá rủi ro cho tất cả các API hiện tại của tổ chức/doanh nghiệp. Thiết lập các biện pháp để đảm bảo chúng đáp ứng các chính sách bảo mật và không dễ bị tấn công trước các rủi ro đã biết.

Đánh giá rủi ro phải xác định tất cả các hệ thống và dữ liệu bị ảnh hưởng nếu API bị xâm phạm, sau đó vạch ra kế hoạch xử lý và các biện pháp kiểm soát cần thiết để giảm mọi rủi ro xuống mức có thể chấp nhận được.

Đảm bảo rằng người dùng chỉ có thể truy cập dữ liệu thích hợp

Các phòng, ban và người dùng trong một doanh nghiệp yêu cầu các mức độ truy cập khác nhau vào hệ thống và dữ liệu của tổ chức và quyền truy cập này nên được cấp theo vị trí, công việc.

Yêu cầu xác thực đa yếu tố

Thông tin đăng nhập liên quan đến tên người dùng và mật khẩu không còn đủ để đảm bảo an toàn, do đó cần bắt buộc sử dụng các tiêu chuẩn như xác thực hai yếu tố (2FA) hoặc xác thực an toàn bằng OAuth (một cách xác thực mở). Để đạt được mục tiêu này, hãy đảm bảo hệ thống của doanh nghiệp có thể xác thực người dùng bằng OAuth 2.0 với điểm cuối là nhà cung cấp danh tính.

Lưu giữ khóa API cẩn thận

Các doanh nghiệp cần ghi lại tất cả các API trong sổ đăng ký để xác định các đặc điểm như tên, mục đích, tải trọng, cách sử dụng, quyền truy cập, ngày hoạt động, ngày ngừng hoạt động và chủ sở hữu. Ghi chi tiết thông tin cần thiết như ai, cái gì và khi nào sẽ giúp đáp ứng các yêu cầu tuân thủ và kiểm toán, cũng như hỗ trợ phân tích trong trường hợp xảy ra sự cố bảo mật.

Khóa API xác định và xác minh quyền truy cập cho ứng dụng hoặc trang web thực hiện lệnh gọi API. Chúng cũng có thể chặn hoặc điều tiết các cuộc gọi được thực hiện tới API và xác định các kiểu sử dụng.

TRẦN THANH TÙNG

Bảo vệ thông tin cá nhân trên không gian mạng

Theo thông tin từ Bộ Công an, trong 2 năm 2019 và 2020, dữ liệu cá nhân mua bán trái phép trên thị trường chợ đen lên tới gần 1.300 GB dữ liệu, chứa hàng tỷ thông tin về các cá nhân của nhiều tổ chức, doanh nghiệp trên cả nước. Những con số dữ liệu người dùng khổng lồ mà có lẽ, chính những người là nạn nhân cũng không hề hay biết rằng, thông tin của mình đang trở thành một món "hàng hóa" cho việc thu lợi bất chính của các đối tượng.

Chính người dùng cũng không thể tin được, đôi khi chỉ vì thói quen để lại thông tin khi được bên thứ ba yêu cầu mà chưa tìm hiểu rõ mục đích, cũng có thể là cơ sở cho nhiều thủ đoạn lừa đảo. Điển hình là tình trạng ngày càng xuất hiện tràn lan các cuộc gọi, tin nhắn rác, với nội dung chủ yếu là lời mời làm cộng tác viên, làm việc online, hay thông báo trúng thưởng,... Những chiêu trò núp bóng dưới vỏ bọc hấp dẫn đánh vào tâm lý người dùng, cùng thủ đoạn tinh vi của đối tượng lừa đảo, từ thiết kế giao diện web, đường link, mà thoạt nhìn qua rất dễ bị nhầm lẫn với các tổ chức uy tín. Từ đó, người dùng dễ dàng bị cuốn theo chiêu trò lừa đảo như: chuyển khoản đặt cọc nhận việc, cung cấp thông tin để nhận thưởng, hay truy cập vào các đường link độc hại, từ đó chiếm đoạt tài sản người dùng. Không ít trường hợp vì cả tin, vì hy vọng vào một phiếu quà tặng "từ trên trời rơi xuống" mà bị đánh cắp thông tin tài khoản ngân hàng, khiến số tiền trong tài khoản cũng "không cánh mà bay". Nguy hiểm hơn, không chỉ dừng lại ở việc chiếm đoạt tài sản, nhiều người dùng mạng còn trở thành nạn nhân của các vụ bôi nhọ, đe dọa, thậm chí là khủng bố hay mua bán người trên không gian mạng.

Để bảo vệ dữ liệu cá nhân trên không gian mạng, người dùng cần cảnh giác với các đường link giả mạo, các trang web có yêu cầu điền thông tin cá nhân, chỉ cung cấp các thông tin cá nhân cho các tổ chức tin cậy và thực sự cần, với những mục đích và những cam kết bảo mật thông tin rõ ràng. Bởi bảo vệ, giữ gìn thông cá nhân chính là tự bảo vệ mình trước các rủi ro trên môi trường mạng.

Đối với các tài khoản cá nhân, nên sử dụng mật khẩu mạnh, kết hợp bảo mật nhiều lớp. Hạn chế đăng nhập tài khoản trên các thiết bị công cộng, thiết bị lạ gay rò rỉ thông tin đăng nhập. Cùng với đó, nên cài đặt trình diệt virus phù hợp để tránh nhiễm mã độc, đe dọa đến việc bảo mật dữ liệu cá nhân được lưu trữ tại các thiết bị này.

Ngoài ra, khi nhận được những cuộc gọi, tin nhắn với những đề nghị, cảnh báo, đe dọa, người dùng cần cảnh giác, bình tĩnh xác minh thông tin, không vì lo sợ hay mất bình tĩnh mà vội vàng cung cấp các dữ liệu cá nhân, đặc biệt là các thông tin quan trọng liên quan đến nhân thân, tài khoản ngân hàng...

Đối với các doanh nghiệp, tổ chức, đặc biệt là những tổ chức có lưu trữ thông tin cá nhân người dùng, cần xác định việc bảo vệ dữ liệu cá nhân không chỉ là bảo vệ người dùng, khách hàng mà còn là bảo vệ tài sản quý giá cho doanh nghiệp. Đây là những cơ sở quan trọng để hướng đến xây dựng môi trường không gian mạng an toàn, nơi mà các dữ liệu cá nhân thực sự sẽ là của mỗi cá nhân.

NGÂN HÀ

CHÍNH SÁCH BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Hỏi: *Vì sao phải có chính sách bảo đảm an toàn thông tin mạng? (Anh Xuân Tuấn ở Quảng Nam)*

Trả lời: Công tác bảo đảm an toàn thông tin (ATTT) mạng gắn liền với công tác tuyên truyền, nâng cao nhận thức; đào tạo, phát triển nguồn nhân lực ATTT; các biện pháp quản lý, quy trình nghiệp vụ.

Hiện nay, trong ngành công nghệ thông tin, ba yếu tố chính: nhận thức, nhân lực, quy trình có ảnh hưởng trực tiếp đến công tác bảo đảm an toàn thông tin. Các yếu tố này đều gắn chặt với yếu tố con người.

Trong số các phương tiện kỹ thuật, mạng máy tính có vai trò đặc biệt. Nếu một mạng máy tính không áp dụng các biện pháp bảo vệ thì với một laptop, những kẻ khai thác bất hợp pháp dễ dàng đột nhập vào cơ sở dữ liệu của máy tính để lấy đi hoặc sửa đổi, bóp méo các tệp thông tin mà chúng quan tâm.

Trên phương diện quản lý nhà nước, kết quả giám sát an toàn mạng giúp tạo ra các báo cáo tổng hợp, thống kê về tình hình tấn công mạng. Việc giám sát an toàn mạng quốc gia là hết sức cấp bách, nhằm tạo ra môi trường để các cơ quan, tổ chức, doanh nghiệp có thể phối hợp, chia sẻ thông tin giám sát, cảnh báo nguy cơ mất ATTT.

THÁI BẢO

CÁC NHIỆM VỤ BẢO VỆ AN NINH QUỐC GIA

Hỏi: *Các nhiệm vụ bảo vệ an ninh quốc gia là gì? (Chị Như Ngọc ở Ba Vì, Hà Nội)*

Trả lời: Căn cứ vào điều 14 của Luật an ninh quốc gia năm 2004, nhiệm vụ bảo vệ an ninh bao gồm:

1. Bảo vệ chế độ chính trị và Nhà nước Cộng hoà xã hội chủ nghĩa Việt Nam, bảo vệ độc lập, chủ quyền, thống nhất, toàn vẹn lãnh thổ của Tổ quốc.

2. Bảo vệ an ninh về tư tưởng và văn hoá, khối đại đoàn kết toàn dân tộc, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

3. Bảo vệ an ninh trong các lĩnh vực kinh tế, quốc phòng, đối ngoại và các lợi ích khác của quốc gia.

4. Bảo vệ bí mật nhà nước và các mục tiêu quan trọng về an ninh quốc gia.

5. Phòng ngừa, phát hiện, ngăn chặn, đấu tranh làm thất bại và loại trừ các hoạt động xâm phạm an ninh quốc gia, nguy cơ đe doạ an ninh quốc gia.

CÁT TƯỜNG

CÁC NGUYÊN TẮC BẢO ĐẢM AN TOÀN THÔNG TIN MẠNG

Hỏi: *Không gian mạng là gì? Các nguyên tắc bảo đảm an toàn thông tin mạng?*
(Ông Nguyễn Mạnh ở Hưng Yên)

Trả lời: Theo khoản 3 Điều 2 Luật An ninh mạng 2018, không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

Nguyên tắc bảo đảm an toàn thông tin mạng: Căn cứ vào điều 4 của Luật an toàn thông tin mạng năm 2018 quy định như sau:

1. Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế - xã hội.

2. Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.

3. Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.

4. Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.

NGÔ VÂN

VÌ SAO AN NINH MẠNG CÓ VAI TRÒ QUAN TRỌNG TRONG NỀN AN NINH QUỐC GIA?

Hỏi: *Vì sao an ninh mạng có vai trò quan trọng trong nền an ninh quốc gia?*
(Chị Lan Hương ở Bắc Giang)

Trả lời: Tình hình quốc tế và trong nước ngày càng diễn biến phức tạp, sự phát triển như vũ bão của khoa học công nghệ hiện nay, việc đảm đảm an ninh quốc gia là yêu cầu tối thiết để đảm đảm hòa bình, phát triển đất nước.

Với việc xem không gian mạng là vùng 'lãnh thổ đặc biệt', bảo mật, an ninh mạng và an toàn thông tin sử dụng kỹ thuật mật mã sẽ ngày càng khẳng định vai trò to lớn trong bảo vệ chủ quyền, phát triển kinh tế, giữ vững ổn định chính trị - xã hội của các quốc gia".

Hoạt động tấn công mạng vào hệ thống thông tin trọng yếu của an ninh quốc gia nhằm phá hoại cơ sở dữ liệu, gây gián đoạn hoặc chiếm quyền điều khiển diễn ra thường xuyên hơn. Vấn đề an ninh mạng đang đòi hỏi phải tiếp tục được nhận diện, luận giải, phân tích những điểm mới về mặt lý luận và thực

tiễn, tìm kiếm những phương châm, kế sách, giải pháp từ góc độ mật mã, góc độ quản trị để phòng ngừa, ứng phó, giải quyết có hiệu quả các mối đe dọa an ninh phi truyền thống, trọng tâm là an ninh mạng trong nền an ninh quốc gia phù hợp với bối cảnh mới, điều kiện mới".

HỒNG LIÊN

KIỂM TRA AN NINH MẠNG ĐỐI VỚI HỆ THỐNG THÔNG TIN QUAN TRỌNG VỀ AN NINH QUỐC GIA

Hỏi: *Hiểu như nào về kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia? (Anh Nghĩa ở Tuyên Quang)*

Trả lời: Kiểm tra an ninh mạng là hoạt động xác định thực trạng an ninh mạng của hệ thống thông tin, cơ sở hạ tầng hệ thống thông tin hoặc thông tin được lưu trữ, xử lý, truyền đưa trong hệ thống thông tin nhằm phòng ngừa, phát hiện, xử lý nguy cơ đe dọa an ninh mạng và đưa ra các phương án, biện pháp bảo đảm hoạt động bình thường của hệ thống thông tin.

Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quan trọng về an ninh quốc gia, trừ hệ thống thông tin quân sự do Bộ Quốc phòng quản lý, hệ thống thông tin cơ yếu thuộc Ban Cơ yếu Chính phủ và sản phẩm mật mã do Ban Cơ yếu Chính phủ cung cấp để bảo vệ thông tin thuộc bí mật nhà nước. Lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Quốc phòng kiểm tra an ninh mạng đột xuất đối với hệ thống thông tin quân sự.

CÁT TƯỜNG

LUẬT AN NINH MẠNG CÓ LIÊN QUAN TỚI BỘ LUẬT HÌNH SỰ HAY CÁC VĂN BẢN LUẬT KHÁC KHÔNG?

Hỏi: *Luật An ninh mạng có liên quan tới Bộ luật Hình sự hay các văn bản luật khác không? (Anh Văn Toàn – Nghệ An)*

Trả lời: : Khi được ban hành, Luật An ninh mạng có tính thống nhất cao với hệ thống pháp luật hiện hành của Việt Nam, bởi không gian mạng đã bao phủ toàn bộ các lĩnh vực của đời sống xã hội. Luật An ninh mạng có phản ánh trực tiếp hoặc gián tiếp một số nội dung theo 29 điều của Bộ luật Hình sự; có liên quan tới các quy định về bảo vệ quyền con người trong Hiến pháp, Bộ luật Hình sự, Bộ luật Dân sự và các văn bản khác có liên quan; đồng thời liên quan chặt chẽ tới Luật Xử lý vi phạm hành chính và các văn bản hướng dẫn thi hành.

HỒNG CHUYÊN

LUẬT AN NINH MẠNG CÓ KIỂM SOÁT, LÀM LỘ THÔNG TIN CÁ NHÂN CỦA NGƯỜI SỬ DỤNG KHÔNG?

Hỏi: *Luật An ninh mạng có kiểm soát, làm lộ thông tin cá nhân của người sử dụng không? (Bà Ngọc Thảo – Hà Nội)*

Trả lời: Luật An ninh mạng được ban hành không kiểm soát và làm lộ thông tin của công dân. Luật quy định chỉ khi phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng, Luật An ninh mạng mới yêu cầu doanh nghiệp cung cấp thông tin cá nhân có liên quan tới hành vi vi phạm pháp luật đó. Lực lượng chuyên trách bảo vệ an ninh mạng chỉ được phép tiếp cận thông tin cá nhân của người sử dụng có hoạt động vi phạm pháp luật, với trình tự, thủ tục nghiêm ngặt (bằng văn bản), được các cấp có thẩm quyền phê duyệt.

Các quy định trong Bộ luật Tố tụng Hình sự và các văn bản có liên quan đã quy định rõ về việc quản lý, sử dụng thông tin được cung cấp để phục vụ điều tra, xử lý các hành vi vi phạm pháp luật. Các cơ quan chức năng, doanh nghiệp và tổ chức, cá nhân có liên quan phải có trách nhiệm bảo vệ bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng.

Các hành vi như chiếm đoạt, mua bán, thu giữ, cố ý làm lộ, xóa, làm hư hỏng, thất lạc, thay đổi, đưa lên

không gian mạng những thông tin thuộc bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư của người khác mà chưa được phép của người sử dụng hoặc trái quy định của pháp luật sẽ bị xử lý.

Lực lượng chuyên trách bảo vệ an ninh mạng nếu lạm dụng, làm lộ thông tin cá nhân của người sử dụng sẽ bị xử lý theo quy định của pháp luật.

HOÀNG TOÀN

BẢO VỆ AN NINH MẠNG ĐƯỢC HIỂU NHƯ THẾ NÀO?

Hỏi: *Bảo vệ an ninh mạng được hiểu như thế nào? (Ông Ngọc Tiến – Bắc Giang)*

Trả lời: Theo Điều 2 Luật An ninh mạng 2018 quy định như sau:

- An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

- Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

...

Theo đó, bảo vệ an ninh mạng được hiểu là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng.

THÁI CHÂN

BẢO VỆ AN NINH MẠNG ĐƯỢC HIỂU NHƯ THẾ NÀO?

Hỏi: ***Những trường hợp nào được xem là tình huống nguy hiểm về an ninh mạng?***
(Chị Ngọc Mai – Thanh Hóa)

Trả lời: Căn cứ vào khoản 1 Điều 21 Luật An ninh mạng 2018 quy định như sau:

Phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng

1. Tình huống nguy hiểm về an ninh mạng bao gồm:

a) Xuất hiện thông tin kích động trên không gian mạng có nguy cơ xảy ra bạo loạn, phá rối an ninh, khủng bố;

b) Tấn công vào hệ thống thông tin quan trọng về an ninh quốc gia;

c) Tấn công nhiều hệ thống thông tin trên quy mô lớn, cường độ cao;

d) Tấn công mạng nhằm phá hủy công trình quan trọng về an ninh quốc gia, mục tiêu quan trọng về an ninh quốc gia;

đ) Tấn công mạng xâm phạm nghiêm trọng chủ quyền, lợi ích, an ninh quốc gia; gây tổn hại đặc biệt

nghiêm trọng trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Theo đó, 5 trường hợp nêu trên được xem là những tình huống nguy hiểm về an ninh mạng.

NGUYỄN NAM

CÁC BIỆN PHÁP NÀO ĐƯỢC ÁP DỤNG ĐỂ XỬ LÝ TÌNH HUỐNG NGUY HIỂM VỀ AN NINH MẠNG?

Hỏi: ***Những biện pháp nào được áp dụng để xử lý tình huống nguy hiểm về an ninh mạng?***
(Anh Văn Ninh – Hà Nam)

Trả lời: Căn cứ vào khoản 3 Điều 21 Luật An ninh mạng 2018 quy định về các biện pháp xử lý tình huống nguy hiểm về an ninh mạng như sau:

- Triển khai ngay phương án phòng ngừa, ứng phó khẩn cấp về an ninh mạng, ngăn chặn, loại trừ hoặc giảm nhẹ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

- Thông báo đến cơ quan, tổ chức, cá nhân có liên quan;

- Thu thập thông tin liên quan; theo dõi, giám sát liên tục đối với tình huống nguy hiểm về an ninh mạng;

- Phân tích, đánh giá thông tin, dự báo khả năng, phạm vi ảnh hưởng và mức độ thiệt hại do tình huống nguy hiểm về an ninh mạng gây ra;

- Ngừng cung cấp thông tin mạng tại khu vực cụ thể hoặc ngắt cổng kết nối mạng quốc tế;

- Bố trí lực lượng, phương tiện ngăn chặn, loại bỏ tình huống nguy hiểm về an ninh mạng;

- Biện pháp khác theo quy định của Luật An ninh quốc gia.

HIẾU LÊ

BẢO VỆ AN NINH MẠNG ĐỐI VỚI CƠ SỞ HẠ TẦNG KHÔNG GIAN MẠNG QUỐC GIA, CỔNG KẾT NỐI MẠNG QUỐC TẾ ĐƯỢC THỰC HIỆN NHƯ THẾ NÀO?

Hỏi: ***Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế được thực hiện như thế nào? (Anh Thiện Phước – TP Hồ Chí Minh)***

Trả lời: TTại Điều 25 của Luật An ninh mạng năm 2018 quy định:

1, Bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế phải bảo đảm kết hợp chặt chẽ giữa yêu cầu bảo vệ an ninh mạng với yêu cầu phát triển kinh tế - xã hội; khuyến khích cổng kết nối quốc tế đặt trên lãnh thổ Việt Nam; khuyến khích tổ chức, cá nhân tham gia đầu tư xây dựng cơ sở hạ tầng không gian mạng quốc gia.

2. Cơ quan, tổ chức, cá nhân quản lý, khai thác cơ sở hạ tầng không gian mạng quốc gia, cổng kết nối mạng quốc tế có trách nhiệm sau đây:

a) Bảo vệ an ninh mạng thuộc quyền quản lý; chịu sự quản lý, thanh tra, kiểm tra và thực hiện các yêu cầu về bảo vệ an ninh mạng của cơ quan nhà nước có thẩm quyền;

b) Tạo điều kiện, thực hiện các biện pháp kỹ thuật, nghiệp vụ cần thiết để cơ quan nhà nước có thẩm quyền thực hiện nhiệm vụ bảo vệ an ninh mạng khi có đề nghị.

HOÀNG ANH

TRẺ EM CÓ ĐƯỢC BẢO VỆ TRÊN KHÔNG GIAN MẠNG KHÔNG?

Hỏi: ***Trẻ em có được bảo vệ trên không gian mạng không? (Ngô Thái Hương – Đà Nẵng)***

Trả lời: Theo quy định tại Điều 29 Luật An ninh mạng năm 2018 quy định về bảo vệ trẻ em trên không gian mạng như sau:

Trẻ em có quyền được bảo vệ, tiếp cận thông tin, tham gia hoạt động xã hội, vui chơi, giải trí, giữ bí mật cá nhân, đời sống riêng tư và các quyền khác khi tham gia trên không gian mạng.

Chủ quản hệ thống thông tin, doanh nghiệp cung cấp dịch vụ trên mạng viễn thông, mạng Internet, các dịch vụ gia tăng trên không gian mạng có trách nhiệm kiểm soát nội dung thông tin trên hệ thống thông tin hoặc trên dịch vụ do doanh nghiệp cung cấp để không gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; ngăn chặn việc chia sẻ và xóa bỏ thông tin có nội dung gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em; kịp thời thông báo, phối hợp với lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để xử lý.

Cơ quan, tổ chức, cá nhân tham gia hoạt động trên không gian mạng có trách nhiệm phối hợp với cơ quan có thẩm quyền trong bảo đảm quyền của trẻ em trên không gian mạng, ngăn chặn thông tin có nội dung gây nguy hại cho trẻ em theo quy định của Luật này và pháp luật về trẻ em.

Cơ quan, tổ chức, cha mẹ, giáo viên, người chăm sóc trẻ em và cá nhân khác liên quan có trách nhiệm bảo đảm quyền của trẻ em, bảo vệ trẻ em khi tham gia không gian mạng theo quy định của pháp luật về trẻ em.

Lực lượng chuyên trách bảo vệ an ninh mạng và các cơ quan chức năng có trách nhiệm áp dụng biện pháp để phòng ngừa, phát hiện, ngăn chặn, xử lý nghiêm hành vi sử dụng không gian mạng gây nguy hại cho trẻ em, xâm phạm đến trẻ em, quyền trẻ em.

XUÂN TRƯỜNG

NHÂN SỰ PHỤ TRÁCH VỀ VẬN HÀNH, QUẢN TRỊ HỆ THỐNG VÀ BẢO VỆ AN NINH MẠNG PHẢI CÓ TRÌNH ĐỘ CHUYÊN MÔN NHƯ THẾ NÀO?

Hỏi: ***Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin có phải không? (Anh Hoàng Hải – sinh viên công nghệ thông tin)***

Trả lời: Theo Điều 9 Nghị định số 53/2022/NĐ-CP ngày 15 tháng 8 năm 2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng quy định về điều kiện về nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng như sau:

1. Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng.

2. Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin; có cam kết bảo mật thông tin liên quan đến hệ thống thông tin quan trọng về an ninh quốc gia trong quá trình làm việc và sau khi nghỉ việc.

3. Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị, bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Như vậy, căn cứ quy định nêu trên, nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng phải có trình độ chuyên môn về an ninh mạng, an toàn thông tin mạng, công nghệ thông tin.

THANH THIỆN

CÁCH NHẬN BIẾT NHỮNG RỦI RO TRÊN KHÔNG GIAN MẠNG

Hỏi: ***Làm thế nào để nhận biết những rủi ro trên không gian mạng (Chị Khánh Tình – Nam Định)***

Trả lời: : Theo Thượng tá Nguyễn Tuyên, Trưởng phòng An toàn thông tin, Bộ Tư lệnh 86 cho biết: Trên không gian mạng, các rủi ro mất an toàn dữ liệu thông tin rất đa dạng, phức tạp. Tin tặc luôn cố gắng tìm kiếm các kẽ hở để tấn công xâm nhập, đánh cắp thông tin, dữ liệu. Việc nhận diện rủi ro chủ yếu dựa vào sự cảnh giác, kinh nghiệm và kiến thức về an toàn thông tin, an ninh mạng.

Do vậy, người dân nên chủ động tham khảo, tự tìm hiểu, tự học hỏi hoặc nghe các chương trình về nâng cao hiểu biết an toàn thông tin, an ninh mạng trên phương tiện thông tin đại chúng. Đồng thời, cần nâng cao ý thức cảnh giác trước các thủ đoạn lừa đảo tinh vi trên không gian mạng.

Các cơ quan, đơn vị, tổ chức, doanh nghiệp cần phải thường xuyên tổ chức các đợt kiểm tra đánh giá trên môi trường mạng để nâng cao nhận thức, ý thức

cảnh giác về an toàn thông tin, an ninh mạng tới cán bộ, công nhân viên. Một biện pháp kiểm tra khá hiệu quả đó là sử dụng hình thức câu hỏi trắc nghiệm hoặc hệ thống mô phỏng các hành động lừa đảo của tin tặc trên mạng tương tác với người dùng.

THÁI BẢO

TRIỂN KHAI CHỐNG LỪA ĐẢO TRỰC TUYẾN TRÊN TIKTOK

Vừa qua, TikTok Việt Nam phối hợp Cục An toàn thông tin (Bộ Thông tin Truyền thông) triển khai chiến dịch chống lừa đảo trực tuyến.

Thông qua hình thức truyền thông bằng các video ngắn, chiến dịch này cung cấp thông tin, kỹ năng cũng như bảo vệ người dùng mạng xã hội trước các hình thức lừa đảo tinh vi trên mạng.

Ông Nguyễn Phú Lương, đại diện Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin, chia sẻ: "Chúng tôi đặt mục tiêu trang bị cho mọi công dân số khả năng tự định vị bẫy lừa đảo, bảo vệ bản thân và gia đình trước những thủ đoạn tinh xảo của tội phạm mạng. Với sự phối hợp cùng các thành viên Liên minh tuyên truyền nâng cao nhận thức an toàn thông tin, trong đó có TikTok, nhằm tạo ra các hoạt động tuyên truyền đa dạng trong chiến dịch chống lừa đảo trực tuyến (#LuaDaoTrucTuyen), tiếp cận đến nhiều người dân hơn và thành công tuyên truyền, nâng cao cảnh giác của người dân đối với các hành vi lừa đảo trên mạng".

NGÔ VÂN

NGÀY HỘI TOÀN DÂN BẢO VỆ AN NINH TỔ QUỐC NĂM 2023

Ngày hội toàn dân bảo vệ an ninh Tổ quốc năm 2023 được tổ chức trong thời gian từ ngày 7/7 đến ngày 19/8, bảo đảm thiết thực, ý nghĩa sâu sắc và hướng về cơ sở.

Việc tổ chức Ngày hội tiếp tục thực hiện Kết luận số 44-KL/TW ngày 22/1/2019 của Ban Bí thư về việc tiếp tục đẩy mạnh thực hiện Chỉ thị số 09-CT/TW của Ban Bí thư khóa XI về tăng cường sự lãnh đạo của Đảng đối với phong trào toàn dân bảo vệ an ninh Tổ quốc trong tình hình mới; Quyết định số 521/QĐ-TTg ngày 13/6/2005 của Thủ tướng Chính phủ về "Ngày hội toàn dân bảo vệ an ninh Tổ quốc"…

Ngày hội nhằm giáo dục truyền thống yêu nước, lòng tự hào dân tộc, nâng cao ý thức, trách nhiệm của cán bộ, đảng viên và các tầng lớp nhân dân trong sự nghiệp bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội và xây dựng lực lượng công an nhân dân thực sự trong sạch, vững mạnh, chính quy, tinh nhuệ, hiện đại, đáp ứng yêu cầu, nhiệm vụ trong tình hình mới.

CÁT TƯỜNG

KỸ NĂNG CƠ BẢN ĐỂ BẢO ĐẢM AN TOÀN THÔNG TIN CÁ NHÂN

Theo thông tin từ Bộ Công an, lừa đảo trực tuyến đang có xu hướng gia tăng tại Việt Nam, các cuộc tấn công mạng có xu hướng tập trung chủ yếu vào con người thay vì máy móc, thiết bị. Mới đây, cơ quan chức năng khuyến cáo 3 kỹ năng cơ bản để bảo đảm an toàn thông tin cá nhân.

Người dân hạn chế chia sẻ thông tin cá nhân của mình trên mạng, trừ khi chắc chắn thông tin được sử dụng có kiểm soát; chỉ cung cấp thông tin cá nhân cho cá nhân và tổ chức tin tưởng.

Người dân sử dụng mật khẩu an toàn để bảo vệ tài khoản của mình trên mạng. Mật khẩu nên dài hơn 8 ký tự và bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt. Nên đổi mật khẩu thường xuyên và không nên sử dụng mật khẩu giống nhau cho nhiều tài khoản.

Người dân chủ động tìm hiểu về các phương thức bảo mật thông tin, cập nhật những tin tức mới nhất về các mối đe dọa bảo mật và học cách phòng ngừa chúng. Sử dụng các công cụ bảo mật như phần mềm chống virus và phần mềm chống đánh cắp thông tin để bảo vệ tài khoản của mình trên mạng.

TRÚC THI

ĐẠI HỘI THÀNH LẬP HIỆP HỘI AN NINH MẠNG QUỐC GIA

Chiều ngày 8/9, tại trụ sở Bộ Công an, Hiệp hội An ninh mạng quốc gia là trang trọng tổ chức Đại hội Đại biểu toàn quốc lần thứ nhất nhiệm kỳ 2023-2028.

Theo đó, Hiệp hội là tổ chức xã hội – nghề nghiệp của công dân và tổ chức Việt Nam, hoạt động trong lĩnh vực an ninh mạng tự nguyện thành lập nhằm bảo vệ quyền, lợi ích hợp pháp của hội viên, hỗ trợ nhau hoạt động có hiệu quả, đoàn kết bảo đảm an ninh mạng theo định hướng, chiến lược về an ninh mạng của Đảng, Nhà nước góp phần bảo vệ Tổ quốc và thúc đẩy phát triển kinh tế - xã hội của đất nước.

Đại hội đã thông qua Chương trình, phương hướng hoạt động của Hiệp hội, nhiệm kỳ 2023 – 2028, Điều lệ của Hiệp hội và Đề án tổ chức nhân sự của Hiệp hội nhiệm kỳ I.

Đại hội cũng đã bầu ra Ban Chấp hành, Ban Kiểm tra, Ban Thường vụ Hiệp hội, một số chức danh lãnh đạo và thông qua Nghị quyết Đại hội lần thức nhất với sự nhất trí cao của toàn thể hội viên.

VĂN TUỆ

ĐẢM AN TOÀN, AN NINH MẠNG QUỐC GIA CÓ HIỆU QUẢ TRONG THỜI GIAN TỚI

Để thực hiện công tác bảo đảm an toàn, an ninh mạng quốc gia có hiệu quả trong thời gian tới, Thủ tướng Chính phủ Phạm Minh Chính, Trưởng Ban Chỉ đạo An toàn, an ninh mạng quốc gia yêu cầu Ban Chỉ đạo cần thống nhất một số nhiệm vụ trọng tâm.

Nhiệm vụ bảo vệ an toàn, an ninh mạng cho Đảng, Nhà nước, cho nhân dân, cho doanh nghiệp là một trong những nhiệm vụ chính trị quan trọng trong điều kiện, bối cảnh hiện nay.

Phải huy động sức mạnh tổng hợp của cả hệ thống chính trị, của người dân và doanh nghiệp, trong đó có các lực lượng chức năng làm nòng cốt.

Phải thực hiện công việc này một cách thường xuyên, liên tục, cả về nâng cao nhận thức, cả về ý thức trách nhiệm, cả về tổ chức thực hiện một cách hiệu lực, hiệu quả, đầu tư thỏa đáng các hạ tầng thiết yếu.

Xây dựng các cơ chế chính sách đặc thù, đặc biệt trong thu hút nguồn lực, cơ sở vật chất, hạ tầng và đẩy mạnh hợp tác công tư.

Tự chủ, tự lực, tự cường trong bảo vệ an toàn, an ninh, chủ quyền trên không gian mạng.

NGỌC LINH

ĐA DẠNG HÌNH THỨC LỪA ĐẢO DIỄN RA TRÊN KHÔNG GIAN MẠNG VIỆT NAM

Lừa đảo trực tuyến là vấn đề đã và đang nhận được nhiều sự quan tâm của toàn xã hội. Các đối tượng xấu lợi dụng bối cảnh bùng nổ công nghệ thông tin để thực hiện nhiều vụ lừa đảo trực tuyến, chiếm đoạt tài sản có giá trị cao.

Trong đó, có 3 nhóm lừa đảo chính (giả mạo thương hiệu, chiếm đoạt tài khoản và các hình thức kết hợp khác) với rất nhiều hình thức lừa đảo đang diễn ra trên không gian mạng Việt Nam như: Lừa đảo "combo du lịch giá rẻ"; Lừa đảo cuộc gọi video Deepfake, Deepvoice; Lừa đảo "khóa SIM" vì chưa chuẩn hóa thuê bao; Giả mạo biên lai chuyển tiền thành công; Giả danh giáo viên/nhân viên y tế báo người thân đang cấp cứu; Chiêu trò lừa đảo tuyển người mẫu nhí; Thủ đoạn giả danh các công ty tài chính, ngân hàng; Cài cắm ứng dụng, link quảng cáo cờ bạc, cá độ, tín dụng đen

Các hình thức lừa đảo trên không gian mạng được kẻ lừa đảo thực hiện bằng nhiều hình thức khác nhau và ngày càng tinh vi, trong đó nhắm vào nhiều nhóm đối tượng, bao gồm: Người cao tuổi, trẻ em, sinh viên, đối tượng công nhân, nhân viên văn phòng… Mỗi nhóm đối tượng ở độ tuổi khác nhau, kẻ lừa đảo thực hiện những hình thức dẫn dụ khác nhau, mục tiêu chung là lấy lòng tin, đánh cắp thông tin người dùng, sau đó chiếm đoạt tài sản.

NGỌC HOÀI