SỞ KHOA HỌC VÀ CÔNG NGHỆ HẢI PHÒNG

EBOOK

BÌNH DÂN HỌC VỤ SỐ

SỐ 5/2026

CHUYÊN ĐỀ

CHUYÊN ĐỀ AN NINH MẠNG

MỤC LỤC

I. KIẾN THỨC, KỸ NĂNG SỐ CƠ BẢN

II. TRAO ĐỔI THẢO LUẬN

III. HỎI ĐÁP

GIỚI THIỆU CHUNG VỀ LUẬT AN NINH MẠNG 2025

Ngày 10/12/2025, tại kỳ họp thứ 10, Quốc hội khóa XV đã chính thức thông qua Luật An ninh mạng số 116/2025/QH15. Luật có hiệu lực thi hành từ ngày 01/7/2026. Việc ban hành Luật nhằm hoàn thiện cơ sở pháp lý trong công tác bảo vệ an ninh mạng, bảo đảm trật tự an toàn xã hội, đồng thời bảo vệ quyền và lợi ích hợp pháp của cơ quan, tổ chức và cá nhân trên không gian mạng.

Kỳ họp Quốc hội biểu quyết thông qua Luật An ninh mạng.

Luật An ninh mạng 2025 gồm 08 chương, 45 điều quy định toàn diện về hoạt động bảo vệ an ninh mạng, trách nhiệm của cơ quan, tổ chức, doanh nghiệp và cá nhân trong việc sử dụng không gian mạng an toàn, đúng pháp luật, cụ thể:

- Chương I gồm 07 điều, quy định các vấn đề chung, như: phạm vi điều chỉnh và đối tượng áp dụng; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; các biện pháp bảo vệ an ninh mạng; hợp tác quốc tế và các hành vi bị nghiêm cấm.

- Chương II gồm 05 điều, quy định về bảo vệ an ninh mạng đối với hệ thống thông tin, như: phân loại cấp độ hệ thống thông tin; hệ thống thông tin quan trọng về an ninh quốc gia; nhiệm vụ, biện pháp và trách nhiệm bảo vệ đối với từng loại hệ thống; kiểm tra an ninh mạng đối với hệ thống thông tin không thuộc danh mục hệ thống thông tin quan trọng về an ninh quốc gia.

- Chương III gồm 10 điều, quy định chi tiết về các thông tin và hành vi xâm phạm an ninh quốc gia, trật tự an toàn xã hội; phòng ngừa, xử lý thông tin vi phạm; bảo vệ bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân; phòng chống xâm hại trẻ em; phòng chống phần mềm độc hại, tấn công mạng, khủng bố mạng; xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng và ngăn chặn xung đột thông tin.

- Chương IV gồm 4 điều, quy định về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước; bảo vệ cơ sở hạ tầng không gian mạng quốc gia; bảo đảm an ninh thông tin mạng và bảo đảm an ninh dữ liệu.

- Chương V, gồm 03 điều, quy định về tiêu chuẩn, quy chuẩn kỹ thuật; danh mục sản phẩm, dịch vụ an ninh mạng và điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng.

- Chương VI, gồm 09 điều, quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực; tuyển chọn, đào tạo, giáo dục, bồi dưỡng kiến thức; phổ biến kiến thức; nghiên cứu phát triển; nâng cao năng lực tự chủ và kinh phí bảo vệ an ninh mạng.

- Chương VII gồm 04 điều, quy định trách nhiệm của cơ quan, tổ chức, cá nhân về an ninh mạng.

- Chương VIII gồm 03 điều, quy định về các điều khoản thi hành.

Một trong những nội dung nổi bật của Luật An ninh mạng 2025 là tăng cường các biện pháp bảo vệ dữ liệu cá nhân và xử lý nghiêm các hành vi lợi dụng không gian mạng để thực hiện hành vi vi phạm pháp luật như lừa đảo trực tuyến, phát tán thông tin giả mạo, xúc phạm danh dự nhân phẩm người khác, tổ chức đánh bạc, chiếm đoạt tài sản hoặc chống phá Nhà nước. Luật cũng quy định rõ trách nhiệm phối hợp của các doanh nghiệp cung cấp dịch vụ trên không gian mạng trong việc ngăn chặn, gỡ bỏ thông tin vi phạm theo yêu cầu của cơ quan có thẩm quyền.

Bên cạnh đó, Luật An ninh mạng 2025 còn chú trọng nâng cao ý thức, trách nhiệm của người sử dụng internet. Mỗi cá nhân cần sử dụng mạng xã hội văn minh, tuân thủ pháp luật, không chia sẻ thông tin sai sự thật, chủ động bảo vệ tài khoản và dữ liệu cá nhân nhằm hạn chế nguy cơ bị lừa đảo hoặc đánh cắp thông tin.

Việc Quốc hội thông qua Luật An ninh mạng số 116/2025/QH15 có ý nghĩa quan trọng trong quá trình xây dựng môi trường số an toàn, lành mạnh và hiện đại. Luật không chỉ góp phần bảo vệ an ninh quốc gia mà còn tạo điều kiện thuận lợi cho phát triển kinh tế số, xã hội số và công dân số trong giai đoạn mới. Mỗi cơ quan, tổ chức và người dân cần tích cực tìm hiểu, chấp hành nghiêm các quy định của luật để cùng xây dựng không gian mạng an toàn, văn minh và phát triển bền vững./.

Đức Anh

NHỮNG ĐIỂM MỚI CỦA LUẬT AN NINH MẠNG NĂM 2025

Luật An ninh mạng năm 2025 được Quốc hội khóa XV thông qua có nhiều nội dung sửa đổi, bổ sung quan trọng so với Luật An ninh mạng năm 2018. Đây được xem là bước hoàn thiện quan trọng trong hệ thống pháp luật Việt Nam về bảo vệ chủ quyền số quốc gia, đồng thời tạo hành lang pháp lý thống nhất, đồng bộ cho hoạt động quản lý nhà nước trên không gian mạng.

Thứ nhất, hoàn thiện và thống nhất hệ thống pháp luật về an ninh mạng: Một trong những điểm mới nổi bật của Luật An ninh mạng năm 2025 là việc hợp nhất Luật An toàn thông tin mạng năm 2015 và Luật An ninh mạng năm 2018 nhằm xây dựng một khuôn khổ pháp lý thống nhất, đồng bộ. Luật mới đã khắc phục tình trạng phân tán, chồng chéo bằng việc sử dụng thống nhất thuật ngữ "an ninh mạng" trong toàn bộ hệ thống pháp luật; Luật quy định Chính phủ thống nhất quản lý nhà nước về an ninh mạng; Bộ Công an là cơ quan đầu mối chịu trách nhiệm chính trong công tác quản lý, xây dựng chính sách, xử lý sự cố và bảo vệ an ninh mạng quốc gia.

Thứ hai, tăng cường quản lý nhà nước đối với không gian mạng: Luật An ninh mạng năm 2025 khẳng định nguyên tắc bảo vệ an ninh mạng phải đặt dưới sự quản lý thống nhất của Nhà nước. Đồng thời, Luật đã định nghĩa rõ "không gian mạng quốc gia" là phần không gian mạng thuộc chủ quyền, quyền tài phán và quyền kiểm soát của Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam. Điểm mới quan trọng là Nhà nước được trao thêm nhiều quyền hạn nhằm bảo vệ chủ quyền số quốc gia như: yêu cầu doanh nghiệp trong và ngoài nước cung cấp thông tin phục vụ điều tra; yêu cầu ngăn chặn, gỡ bỏ thông tin vi phạm pháp luật; kiểm tra, đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng. Điều này tạo cơ sở pháp lý vững chắc để kiểm soát hiệu quả các hoạt động trên không gian mạng.

Thứ ba, mở rộng và cụ thể hóa các hành vi bị nghiêm cấm: Không chỉ dừng lại ở các hành vi đơn giản như tấn công hệ thống thông tin, phát tán mã độc, Luật mới còn bao quát các hành vi mới phát sinh như phát tán thông tin giả, lừa đảo trực tuyến, xâm phạm dữ liệu cá nhân, lợi dụng mạng xã hội để gây mất trật tự xã hội. Việc quy định rõ ràng, cụ thể các hành vi này giúp cơ quan chức năng có cơ sở pháp lý vững chắc để xử lý nghiêm các vi phạm.

Thứ tư, tăng cường trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng: Luật An ninh mạng năm 2025 quy định cụ thể hơn trách nhiệm của doanh nghiệp, đặc biệt là các doanh nghiệp cung cấp dịch vụ xuyên biên giới.

Luật An ninh mạng 2025, vì một không gian mạng an toàn, lành mạnh.

Thứ năm, tăng cường bảo vệ dữ liệu cá nhân và dữ liệu quốc gia: Theo quy định mới, việc thu thập và xử lý dữ liệu cá nhân phải bảo đảm minh bạch, đúng mục đích và có sự đồng ý của chủ thể dữ liệu. Người dân có quyền yêu cầu doanh nghiệp cung cấp thông tin về phạm vi sử dụng, thời gian lưu trữ và mục đích xử lý dữ liệu của mình. Luật cũng yêu cầu các doanh nghiệp phải xây dựng hệ thống bảo mật dữ liệu, áp dụng biện pháp kỹ thuật phòng chống rò rỉ thông tin và thông báo kịp thời cho cơ quan chức năng khi xảy ra sự cố mất an toàn dữ liệu. Đặc biệt, Luật đã bổ sung khái niệm "dữ liệu quan trọng của quốc gia", bao gồm dữ liệu liên quan đến quốc phòng, an ninh, tài chính, ngân hàng, điện lực, viễn thông, giao thông và các cơ sở dữ liệu quốc gia. Việc bảo vệ nhóm dữ liệu này được đặt ở mức ưu tiên cao nhất nhằm bảo đảm an ninh quốc gia trong kỷ nguyên số.

Thứ sáu, thúc đẩy tự chủ quốc gia về an ninh mạng: Nhà nước khuyến khích phát triển các sản phẩm, dịch vụ và công nghệ an ninh mạng do Việt Nam nghiên cứu, sản xuất; Nhà nước ưu tiên đầu tư cho các trung tâm dữ liệu lớn, khu công nghiệp an ninh mạng và các cơ sở nghiên cứu, thử nghiệm công nghệ số. Quy định này thể hiện quyết tâm xây dựng ngành công nghiệp an ninh mạng Việt Nam hiện đại, giảm phụ thuộc vào công nghệ nước ngoài và bảo đảm chủ quyền số quốc gia trong dài hạn.

Thứ bảy, quy định bảo vệ nhóm yếu thế trên không gian mạng: Một điểm mới mang tính nhân văn sâu sắc của Luật An ninh mạng năm 2025 là việc thiết lập cơ chế bảo vệ các nhóm yếu thế như trẻ em, người cao tuổi và người hạn chế nhận thức trên không gian mạng.

Theo đó, doanh nghiệp cung cấp dịch vụ mạng phải có biện pháp lọc, cảnh báo và hạn chế nội dung độc hại đối với trẻ em; xây dựng công cụ kiểm soát của cha mẹ; không được thu thập dữ liệu trẻ em khi chưa có sự đồng ý của người giám hộ.

Bảo bệ trẻ em trên không gian mạng.

Luật cũng tăng cường xử lý nghiêm các hành vi dụ dỗ, lừa đảo, xâm hại trẻ em trên mạng; nghiêm cấm việc phát tán hình ảnh, thông tin cá nhân của trẻ em hoặc người không đủ năng lực nhận thức mà chưa được phép. Bên cạnh đó, Luật còn nhấn mạnh trách nhiệm của gia đình, nhà trường và xã hội trong việc giáo dục kỹ năng an toàn số, xây dựng môi trường mạng lành mạnh và nhân văn.

Thứ tám, tăng cường hợp tác quốc tế về an ninh mạng: Cụ thể, Việt Nam sẽ tăng cường hợp tác với các quốc gia và tổ chức quốc tế trong các hoạt động như: Chia sẻ thông tin và cảnh báo sớm; Hỗ trợ điều tra, truy vết tội phạm mạng; Trao đổi chứng cứ điện tử; Đào tạo nguồn nhân lực và chuyển giao công nghệ; Tương trợ tư pháp và dẫn độ tội phạm mạng. Đồng thời, Luật cũng nội luật hóa nhiều nội dung của Công ước Liên Hợp Quốc về chống tội phạm mạng, góp phần nâng cao vị thế và trách nhiệm của Việt Nam trong hợp tác quốc tế về an ninh mạng.

Những điểm mới của Luật không chỉ tập trung vào đấu tranh phòng, chống tội phạm mạng mà còn chú trọng bảo vệ dữ liệu cá nhân, phát triển công nghiệp an ninh mạng trong nước, bảo vệ nhóm yếu thế và thúc đẩy hợp tác quốc tế. Qua đó, Luật góp phần xây dựng môi trường mạng an toàn, lành mạnh, tạo nền tảng vững chắc cho phát triển kinh tế số, xã hội số và hội nhập quốc tế trong thời kỳ chuyển đổi số toàn diện./.

Phẳng Châu

CÁC HÀNH VI BỊ NGHIÊM CẤM THEO QUY ĐỊNH CỦA LUẬT AN NINH MẠNG

Để bảo đảm môi trường mạng an toàn, lành mạnh, Luật An ninh mạng đã quy định rõ các hành vi bị nghiêm cấm, nhằm ngăn chặn và xử lý kịp thời những vi phạm, bao gồm:

Thứ nhất là, Đăng tải, phát tán thông tin có nội dung sau trên không gian mạng:

- Tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm: tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân; chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước; xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc;

- Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

- Bịa đặt, vu khống, thông tin sai sự thật, xâm phạm nhân phẩm, danh dự, uy tín của người khác hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

Các hành vi bị nghiêm cấm trong Luật An ninh mạng.

- Sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động bình thường của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá trị khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, kinh doanh theo phương thức đa cấp, chứng khoán.

Thứ hai là, thực hiện hành vi sau trên không gian mạng:

- Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

- Kích động, kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân; kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự;

- Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh; chiếm đoạt, mua bán, thu giữ, cố ý làm lộ bí mật cá nhân, bí mật gia đình và đời sống riêng tư gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân; cố ý nghe lén, ghi âm, ghi hình trái phép các cuộc đàm thoại trên không gian mạng; tiết lộ thông tin về sản phẩm mật mã dân sự, thông tin về khách hàng sử dụng hợp pháp sản phẩm mật mã dân sự; sử dụng, kinh doanh các sản phẩm mật mã dân sự không rõ nguồn gốc;

- Hoạt động mại dâm, tệ nạn xã hội, mua bán người, các bộ phận cơ thể người; tuyên truyền văn hóa phẩm dâm ô, đồi trụy; kích động, cổ xúy bạo lực, lối sống trụy lạc, lệch chuẩn, phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

- Lừa đảo chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng Internet; trộm cắp cước viễn thông quốc tế trên nền Internet; tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cấm theo quy định của pháp luật; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

- Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng, tài sản mã hóa, tài sản số của người khác; phát hành, cung cấp, sử dụng trái phép các phương tiện thanh toán; giả mạo giấy tờ của cơ quan, tổ chức;

- Sử dụng trí tuệ nhân tạo hoặc công nghệ mới để giả mạo video, hình ảnh, giọng nói của người khác trái quy định của pháp luật; tạo lập, đăng tải, phát tán thông tin trái quy định;

- Thu thập, sử dụng, phát tán, trao đổi, chuyển nhượng, kinh doanh trái pháp luật thông tin, dữ liệu cá nhân của người khác;

- Hướng dẫn, xúi giục, lôi kéo, kích động người khác phạm tội hoặc thực hiện hành vi vi phạm pháp luật;

- Thực hiện hành vi khác trên không gian mạng bằng việc sử dụng công nghệ thông tin, phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

Tuyên truyền Luật An ninh mạng 2025.

Thứ ba là, thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng, tội phạm sử dụng công nghệ cao; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin.

Thứ tư là, sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoặc phát tán thư rác, tin nhắn rác, cuộc gọi rác, chương trình tin học gây hại đến hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử.

Thứ năm là, xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

Thứ sáu là, Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

Thứ bảy là, lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi...

Việc tuân thủ các quy định về những hành vi bị nghiêm cấm trong Luật An ninh mạng là trách nhiệm của mỗi người khi sử dụng internet. Qua đó, góp phần xây dựng không gian mạng an toàn, văn minh và bảo vệ lợi ích chung của xã hội./.

Minh Thảo

TRÁCH NHIỆM CỦA CƠ QUAN, TỔ CHỨC, CÁ NHÂN SỬ DỤNG KHÔNG GIAN MẠNG

Trong thời đại công nghệ số, không gian mạng đã trở thành môi trường quan trọng phục vụ học tập, làm việc và giao tiếp của mọi cá nhân, tổ chức. Tuy nhiên, cùng với những tiện ích đó là yêu cầu ngày càng cao về trách nhiệm khi tham gia và sử dụng không gian mạng. Luật An ninh mạng đã quy định rõ trách nhiệm của cơ quan, tổ chức và cá nhân nhằm bảo đảm việc sử dụng internet đúng pháp luật, an toàn và lành mạnh, gồm:

- Tuân thủ quy định của pháp luật về an ninh mạng.

Luật An ninh mạng quy định trách nhiệm của cá nhân, tổ chức.

- Có trách nhiệm bảo mật thông tin đăng ký, mở, quản lý, sử dụng tài khoản số của mình. Trường hợp sử dụng tài khoản số để thực hiện hành vi vi phạm pháp luật, tùy theo tính chất, mức độ của hành vi vi phạm, chủ tài khoản số, người sử dụng tài khoản số bị xử lý kỷ luật, xử phạt vị phạm hành chính hoặc bị trụy cứu trách nhiệm hình sự nếu gây thiệt hại đến lợi ích của Nhà nước, quyền và lợi ích hợp pháp của tổ chức, cá nhân thì phải bồi thường thiệt hại theo quy định pháp luật.

- Kịp thời cung cấp thông tin liên quan đến bảo vệ an ninh mạng, nguy cơ đe dọa an ninh mạng, hành vi xâm phạm an ninh mạng cho cơ quan có thẩm quyền, lực lượng bảo vệ an ninh mạng.

- Thực hiện yêu cầu và hướng dẫn của cơ quan có thẩm quyền trong bảo vệ an ninh mạng; giúp đỡ, tạo điều kiện cho cơ quan, tổ chức và người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

Thực hiện nghiêm túc trách nhiệm khi sử dụng không gian mạng theo Luật An ninh mạng không chỉ giúp bảo vệ quyền và lợi ích hợp pháp của mỗi cá nhân, tổ chức mà còn góp phần xây dựng môi trường mạng an toàn, văn minh. Qua đó, nâng cao ý thức pháp luật và chung tay giữ gìn an ninh quốc gia trong thời đại số./.

Thu Thảo

TRÁCH NHIỆM CỦA DOANH NGHIỆP KINH DOANH SẢN PHẨM, DỊCH VỤ AN NINH MẠNG

Các doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng không chỉ cung cấp giải pháp kỹ thuật nhằm phòng chống nguy cơ tấn công mạng mà còn góp phần bảo vệ an ninh quốc gia, trật tự an toàn xã hội. Vì vậy, pháp luật đã quy định rõ trách nhiệm của các doanh nghiệp trong quá trình hoạt động nhằm bảo đảm việc kinh doanh đúng quy định, an toàn và hiệu quả.

- Thực hiện đúng giấy phép kinh doanh sản phẩm, dịch vụ an ninh mạng; tuân thủ quy định của pháp luật về an ninh mạng và quy định khác của pháp luật có liên quan;

- Bảo đảm về chất lượng sản phẩm, dịch vụ an ninh mạng đúng với tiêu chuẩn công bố áp dụng, quy chuẩn kỹ thuật tương ứng theo quy định của pháp luật về chất lượng sản phẩm, hàng hóa, pháp luật về tiêu chuẩn và quy chuẩn kỹ thuật trước khi lưu thông trên thị trường;

- Lập, lưu giữ và bảo mật thông tin của khách hàng, quản lý hồ sơ, tài liệu về giải pháp kỹ thuật, công nghệ của sản phẩm, hoạt động cung cấp dịch vụ theo quy định của pháp luật;

- Từ chối cung cấp sản phẩm, dịch vụ an ninh mạng khi phát hiện tổ chức, cá nhân vi phạm pháp luật về sử dụng sản phẩm, dịch vụ an ninh mạng, vi phạm cam kết đã thỏa thuận về sử dụng sản phẩm, dịch vụ do doanh nghiệp cung cấp;

- Phối hợp, tạo điều kiện, thực hiện yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện các biện pháp bảo vệ an ninh mạng.

Việc thực hiện đầy đủ trách nhiệm của doanh nghiệp kinh doanh sản phẩm, dịch vụ an ninh mạng có ý nghĩa quan trọng trong công tác bảo vệ hệ thống thông tin và xây dựng môi trường mạng an toàn, lành mạnh. Mỗi doanh nghiệp cần nâng cao ý thức chấp hành pháp luật, tăng cường trách nhiệm trong hoạt động kinh doanh để góp phần bảo đảm an ninh mạng quốc gia trong thời kỳ chuyển đổi số hiện nay./.

Hải Anh

CÁC BIỆN PHÁP ĐỂ QUẢN LÝ VÀ GIẢM THIỂU CÁC MỐI ĐE DỌA AN NINH MẠNG TRONG DOANH NGHIỆP

Việc thực hiện các biện pháp về an ninh mạng có thể giúp các tổ chức, doanh nghiệp giảm thiểu rủi ro và hạn chế tác động tiềm tàng của các cuộc tấn công mạng. Dưới đây là một số chiến lược và biện pháp hiệu quả nhất mà các doanh nghiệp có thể áp dụng để giảm thiểu các mối đe dọa an ninh mạng.

Thường xuyên cập nhật và vá lỗi phần mềm: Tội phạm mạng thường khai thác các lỗ hổng đã biết trong phần mềm lỗi thời để truy cập trái phép vào hệ thống. Bằng cách giữ cho phần mềm luôn được cập nhật và áp dụng các bản vá bảo mật ngay khi chúng được phát hành, các doanh nghiệp có thể khắc phục những lỗ hổng này và giảm nguy cơ bị khai thác.

Áp dụng các biện pháp kiểm soát truy cập mạnh mẽ: Các doanh nghiệp nên thực thi nguyên tắc quyền hạn tối thiểu, đảm bảo rằng người dùng chỉ có quyền truy cập vào các hệ thống và dữ liệu cần thiết cho vai trò của họ. Việc triển khai xác thực đa yếu tố (MFA) bổ sung thêm một lớp bảo mật bằng cách yêu cầu người dùng cung cấp nhiều hình thức xác minh trước khi được cấp quyền truy cập. Ngoài ra, việc thường xuyên xem xét và cập nhật quyền truy cập có thể giúp ngăn chặn truy cập trái phép và giảm nguy cơ bị tấn công từ nội bộ.

Tiến hành kiểm tra và đánh giá an ninh định kỳ: Các cuộc kiểm tra này nên bao gồm việc xem xét kỹ lưỡng các chính sách, thực tiễn và cơ sở hạ tầng an ninh mạng của tổ chức. Đánh giá lỗ hổng, kiểm thử xâm nhập và đánh giá rủi ro có thể giúp doanh nghiệp xác định các điểm yếu trong hệ thống an ninh của mình và ưu tiên các nỗ lực khắc phục. Giám sát liên tục mạng lưới và hệ thống cũng rất quan trọng để phát hiện và ứng phó với các mối đe dọa tiềm tàng trong thời gian thực.

Đào tạo nhân viên về nhận thức an ninh mạng: Các doanh nghiệp nên thường xuyên tổ chức các khóa đào tạo nâng cao nhận thức về an ninh mạng để giáo dục nhân viên về các mối đe dọa phổ biến, chẳng hạn như lừa đảo trực tuyến (phishing), tấn công phi kỹ thuật (social engineering) và mã độc tống tiền (ransomware).

Chương trình đào tạo cũng nên bao gồm các biện pháp tốt nhất để đảm bảo an toàn trực tuyến, chẳng hạn như nhận biết email đáng ngờ, sử dụng mật khẩu mạnh và tránh các trang web nguy hiểm.

Triển khai mã hóa dữ liệu: Các doanh nghiệp nên triển khai các giao thức mã hóa mạnh mẽ cho tất cả dữ liệu nhạy cảm, bao gồm thông tin khách hàng, hồ sơ tài chính và dữ liệu kinh doanh độc quyền.

Xây dựng kế hoạch ứng phó sự cố: Kế hoạch nên nêu rõ các bước cần thực hiện trong trường hợp bị tấn công mạng, bao gồm các thủ tục ngăn chặn, loại bỏ, phục hồi và liên lạc.

Việc có một kế hoạch ứng phó sự cố rõ ràng cho phép các doanh nghiệp phản ứng nhanh chóng và hiệu quả trước các vi phạm an ninh, giảm thiểu thiệt hại và thời gian ngừng hoạt động. Thường xuyên kiểm tra và cập nhật kế hoạch ứng phó sự cố đảm bảo rằng kế hoạch vẫn hiệu quả khi bối cảnh mối đe dọa thay đổi.

Sao lưu dữ liệu thường xuyên: Các doanh nghiệp nên triển khai các quy trình sao lưu tự động để thường xuyên lưu trữ bản sao dữ liệu quan trọng tại các địa điểm an toàn, ngoài trụ sở chính.

Cảnh báo lừa đảo từ các cuộc gọi giả danh.

Ngoài ra, việc kiểm tra bản sao lưu định kỳ rất quan trọng để đảm bảo dữ liệu có thể được khôi phục nhanh chóng và hiệu quả trong trường hợp xảy ra thảm họa. Có các bản sao lưu đáng tin cậy có thể giảm thiểu đáng kể tác động của một cuộc tấn công mạng và đẩy nhanh quá trình phục hồi.

Sử dụng các công cụ phát hiện mối đe dọa nâng cao: Các doanh nghiệp nên xem xét triển khai các công cụ phát hiện mối đe dọa tiên tiến, chẳng hạn như hệ thống phát hiện xâm nhập (IDS), giải pháp phát hiện và phản hồi điểm cuối (EDR) và nền tảng quản lý thông tin và sự kiện bảo mật (SIEM) .

Truy cập từ xa an toàn: Các doanh nghiệp nên triển khai các giải pháp truy cập từ xa an toàn với mã hóa mạnh và xác thực đa yếu tố.

Ngoài ra, cần tăng cường bảo mật điểm cuối cho các thiết bị từ xa để bảo vệ chống lại các mối đe dọa như phần mềm độc hại và truy cập trái phép. Việc giám sát và kiểm tra thường xuyên hoạt động truy cập từ xa có thể giúp xác định và giải quyết các vấn đề bảo mật tiềm ẩn trước khi chúng trở nên nghiêm trọng.

Phát triển văn hóa an ninh mạng: Bao gồm việc tích hợp an ninh mạng vào mọi khía cạnh của hoạt động kinh doanh, từ việc ra quyết định của ban lãnh đạo đến các hoạt động hàng ngày. Ban lãnh đạo nên ưu tiên an ninh mạng, phân bổ nguồn lực phù hợp và truyền đạt tầm quan trọng của an ninh cho tất cả nhân viên.

Khuyến khích giao tiếp cởi mở về các vấn đề an ninh mạng và liên tục củng cố các thực tiễn tốt nhất có thể giúp tạo ra một môi trường chú trọng an ninh, chủ động giải quyết các mối đe dọa./.

Ngọc Huyền

TRÁCH NHIỆM CỦA DOANH NGHIỆP CUNG CẤP DỊCH VỤ TRÊN KHÔNG GIAN MẠNG

Các doanh nghiệp cung cấp dịch vụ trên không gian mạng cần thực hiện đầy đủ trách nhiệm của mình nhằm bảo đảm an ninh mạng, bảo vệ quyền lợi người dùng và góp phần xây dựng môi trường mạng an toàn, lành mạnh.

Theo Điều 41 Luật An ninh mạng 2025, doanh nghiệp cung cấp dịch vụ trên không gian mạng có trách nhiệm sau:

- Tuân thủ quy định của pháp luật về an ninh mạng.

- Cảnh báo khả năng mất an ninh mạng trong việc sử dụng dịch vụ trên không gian mạng do mình cung cấp và hướng dẫn biện pháp phòng ngừa đối với người sử dụng dịch vụ; xây dựng phương án ứng cứu khẩn cấp bảo đảm an ninh mạng để chủ động xử lý điểm yếu, rủi ro và sự cố an ninh mạng.

- Khi xảy ra sự cố an ninh mạng, ngay lập tức triển khai phương án ứng cứu khẩn cấp bảo đảm an ninh mạng, đồng thời báo cáo ngay với lực lượng chuyên trách bảo vệ an ninh mạng theo quy định của Luật này.

- Áp dụng các biện pháp, giải pháp kỹ thuật để bảo đảm an ninh mạng cho hoạt động xử lý dữ liệu, xử lý dữ liệu cá nhân theo quy định của Luật này, pháp luật về dữ liệu, pháp luật về bảo vệ dữ liệu cá nhân và quy định khác của pháp luật có liên quan.

- Có trách nhiệm định danh địa chỉ IP của tổ chức, cá nhân sử dụng dịch vụ internet; cung cấp thông tin định danh địa chỉ IP cho lực lượng chuyên trách bảo vệ an ninh mạng để thực hiện biện pháp bảo vệ an ninh mạng.

- Phối hợp thực hiện theo hướng dẫn của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an để thiết lập hệ thống kết nối, đấu nối đường truyền kỹ thuật, truyền tải dữ liệu và đáp ứng các điều kiện cần thiết khác để triển khai các giải pháp, biện pháp bảo vệ an ninh mạng khi có yêu cầu để phục vụ điều tra, xác minh, xử lý hành vi vi phạm pháp luật về an ninh mạng...

Việc thực hiện đúng trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng không chỉ giúp bảo vệ người sử dụng mà còn góp phần giữ vững an ninh, trật tự xã hội trong thời đại số. Đây là yêu cầu cần thiết để xây dựng môi trường mạng minh bạch, an toàn và phát triển bền vững./.

Lê Tuấn

TRÁCH NHIỆM CỦA DOANH NGHIỆP TRONG NƯỚC VÀ NƯỚC NGOÀI KHI CUNG CẤP DỊCH VỤ TRÊN KHÔNG GIAN MẠNG TẠI VIỆT NAM

Khi Luật An ninh mạng 2025 chính thức có hiệu lực, các doanh nghiệp trong và ngoài nước cung cấp dịch vụ trên Internet sẽ phải thực hiện nhiều yêu cầu chặt chẽ hơn về quản lý dữ liệu, bảo mật thông tin và phối hợp với cơ quan chức năng. Điều này đòi hỏi doanh nghiệp phải chủ động rà soát, nâng cao trách nhiệm và tuân thủ đúng quy định pháp luật trong hoạt động trên không gian mạng.

Căn cứ khoản 2 Điều 25 Luật An ninh mạng 2025 quy định những điều doanh nghiệp cần lưu ý, như sau:

- Xác thực thông tin khi người dùng đăng ký tài khoản số; bảo mật thông tin, tài khoản người dùng; cung cấp thông tin người dùng cho lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong thời hạn 24 giờ kể từ khi có yêu cầu bằng văn bản, thư điện tử, điện thoại hoặc hình thức khác đã được xác nhận; trường hợp khẩn cấp đe dọa an ninh quốc gia, tính mạng con người, thời hạn cung cấp thông tin là 03 giờ;

- Ngăn chặn, xóa bỏ thông tin, gỡ bỏ dịch vụ, ứng dụng có nội dung vi phạm theo yêu cầu của lực lượng chuyên trách bảo vệ an ninh mạng thuộc Bộ Công an trong thời hạn 24 giờ; trường hợp khẩn cấp, thời hạn thực hiện là 06 giờ; đồng thời lưu nhật ký hệ thống phục vụ xác minh, điều tra, xử lý vi phạm;

- Không cung cấp hoặc ngừng cung cấp dịch vụ đối với tổ chức, cá nhân đăng tải thông tin có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; phá hoại chính sách đoàn kết, chính sách kinh tế - xã hội nước Cộng hòa xã hội chủ nghĩa Việt Nam; xâm phạm quyền, lợi ích hợp pháp của tổ chức, cá nhân.

- Lưu trữ thông tin cá nhân người sử dụng dịch vụ và dữ liệu do người sử dụng tạo ra, gồm: tên tài khoản, thời gian sử dụng, thông tin thanh toán, địa chỉ IP và các dữ liệu liên quan khác trong thời gian theo quy định của pháp luật sau khi người dùng kết thúc việc sử dụng dịch vụ.

Việc nắm rõ và thực hiện đầy đủ các quy định của Luật An ninh mạng 2025 không chỉ giúp doanh nghiệp hạn chế rủi ro pháp lý mà còn góp phần xây dựng môi trường Internet an toàn, minh bạch và ổn định. Đây cũng là điều kiện quan trọng để doanh nghiệp phát triển bền vững trong thời đại số./.

Hà Anh

AN NINH MẠNG
TRỤ CỘT MỚI CỦA AN NINH QUỐC GIA TRONG KỶ NGUYÊN SỐ

Trong thế giới siêu kết nối hiện nay, an ninh mạng đã trở thành trụ cột quan trọng của khả năng phục hồi, ổn định kinh tế, chủ quyền và an ninh quốc gia.

Sự gia tăng các cuộc tấn công mạng tinh vi hơn, cùng với căng thẳng địa chính trị ngày càng leo thang, đang đòi hỏi một sự thay đổi căn bản trong chiến lược: An ninh mạng phải được xem là thành phần cốt lõi của cả phòng thủ quốc gia lẫn ổn định toàn cầu.

Các mối đe dọa từ tấn công mạng ngày càng phức tạp và biến động khó lường

Công nghệ, đặc biệt là trí tuệ nhân tạo tạo sinh (GenAI), đang phát triển với tốc độ chóng mặt, không chỉ tăng cường khả năng phòng thủ mà còn trao cho tin tặc công cụ mạnh mẽ để tự động hóa và mở rộng quy mô tấn công.

GenAI giúp kẻ tấn công lan truyền thông tin sai lệch nhanh hơn, tạo ra các chiến dịch lừa đảo và giả mạo hình ảnh, giọng nói tinh vi hơn, đồng thời thiết kế mã độc có khả năng thích ứng để né tránh các biện pháp phòng vệ truyền thống.

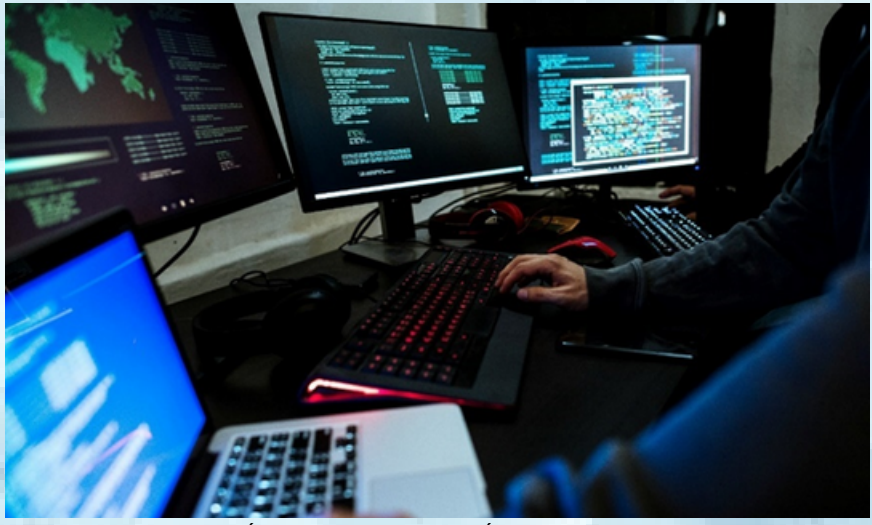
Trong khi đó, lực lượng phòng thủ phải đối mặt với nhiều áp lực: Yêu cầu pháp lý khắt khe hơn, chuỗi cung ứng dễ tổn thương và tình trạng thiếu hụt nhân lực trầm trọng.

Hiện thế giới thiếu từ 2,8 đến 4,8 triệu chuyên gia an ninh mạng và 70% tổ chức thừa nhận khoảng trống này khiến họ dễ bị tấn công hơn. Căng thẳng địa chính trị càng khiến tình hình thêm nghiêm trọng.

Hàng loạt vụ tấn công trong thời gian gần đây đã cho thấy mức độ nguy hiểm và phá hoại của tội phạm mạng đối với hạ tầng trọng yếu và an toàn công cộng.

Nhiều bệnh viện, sân bay, hệ thống điện, nước trên các châu lục đã phải tạm ngừng hoạt động, hủy chuyến bay hoặc trì hoãn chăm sóc y tế khẩn cấp vì bị tấn công mạng. Những sự cố này cho thấy tính mong manh của các hệ thống nền tảng cho xã hội hiện đại, từ giao thông, y tế đến năng lượng và tài chính.

Trong lĩnh vực y tế, Tổ chức Y tế Thế giới (WHO) cảnh báo rằng, sự phát triển của công nghệ, bao gồm cả tấn công mạng, đã "định nghĩa lại bức tranh mối đe dọa sinh học", khi tin tặc có thể truy cập dữ liệu nghiên cứu nhạy cảm, phá hoại hệ thống bảo mật phòng thí nghiệm hoặc thực hiện hành vi gián điệp, phá hoại và đánh cắp dữ liệu.



Các mối đe dọa do các cuộc tấn công mạng gây ra rất phức tạp và luôn biến động. Nguồn: World Economic Forum.

Theo Báo cáo Triển vọng An ninh mạng Toàn cầu 2025, 72% lãnh đạo cho biết, rủi ro mạng đã tăng trong năm qua và gần 60% cho rằng căng thẳng địa chính trị đang tác động trực tiếp đến chiến lược an ninh mạng của họ. 1/3 CEO coi gián điệp mạng và đánh cắp tài sản trí tuệ là mối quan ngại hàng đầu, trong khi 45% khác lo ngại nguy cơ tấn công gây gián đoạn hoạt động kinh doanh.

"Con dao hai lưỡi" mang tên GenAI

GenAI là một công cụ vừa mang đến cơ hội, vừa tiềm ẩn rủi ro lớn. Trong khi tội phạm mạng đang tận dụng AI để triển khai các chiến dịch tấn công tinh vi hơn, công nghệ này cũng mang lại cho lực lượng phòng thủ những công cụ mạnh mẽ như phát hiện bất thường theo thời gian thực, tự động hóa phản ứng trước sự cố và mô phỏng các kịch bản tấn công phức tạp để nâng cao khả năng phục hồi.

Tuy nhiên, lợi ích này không được phân bổ đồng đều. Các tập đoàn lớn và quốc gia phát triển có khả năng đầu tư vào hệ thống phòng thủ dựa trên AI, trong khi doanh nghiệp nhỏ và các cơ quan công vẫn bị ràng buộc bởi hạ tầng cũ và thiếu nhân lực chuyên môn.

Khoảng cách này đang tạo ra sự bất cân bằng trong khả năng ứng phó toàn cầu, khiến nhiều khu vực trở thành "điểm yếu" trong mạng lưới phòng thủ chung.

Một số quốc gia đang nỗ lực thu hẹp khoảng cách đó và Các Tiểu vương quốc Ả Rập Thống nhất (UAE) là ví dụ tiêu biểu. UAE nhận thấy rằng, khả năng phục hồi không chỉ là vấn đề kỹ thuật, mà còn là vấn đề xã hội, đòi hỏi sự nhận thức và tham gia của toàn dân.

Đầu năm 2025, UAE công bố Chiến lược An ninh mạng Quốc gia 2025-2031 với năm trụ cột: Quản trị, bảo vệ, đổi mới, phát triển năng lực và hợp tác. Đồng thời, UAE phối hợp cùng Hội đồng Tawazun và Tập đoàn Lockheed Martin thành lập Trung tâm Xuất sắc về An ninh mạng (Cybersecurity Centre of Excellence) nhằm nâng cao năng lực trong nước và tiếp cận chuẩn mực quốc tế. UAE còn tiên phong triển khai mô hình hợp tác "Nhà nước - Doanh nghiệp - Người dân", đưa giáo dục an ninh mạng vào trường học, tổ chức diễn tập mạng quốc gia và thúc đẩy hợp tác công - tư toàn diện.

Đưa an ninh mạng vào trọng tâm quản trị quốc gia

Việc xem an ninh mạng như một phần của an ninh quốc gia không chỉ là thay đổi về ngôn từ mà đòi hỏi một sự tái tư duy toàn diện về quản trị, chính sách và đầu tư.

Các quốc gia cần lồng ghép giám sát rủi ro mạng ở cấp hội đồng quản trị trong mọi lĩnh vực trọng yếu, bảo đảm ngân sách ổn định và lâu dài để đầu tư vào hạ tầng, nhân lực và đổi mới công nghệ, đồng thời thường xuyên tiến hành diễn tập mô phỏng tấn công quy mô quốc gia nhằm đánh giá khả năng sẵn sàng và phản ứng trong các tình huống khẩn cấp.

Cùng với đó, việc tăng cường chia sẻ thông tin tình báo xuyên biên giới và phối hợp ứng phó khủng hoảng là yếu tố then chốt để ngăn chặn các sự cố cục bộ lan rộng thành khủng hoảng toàn cầu. Đây là sự chuyển mình tất yếu trong tư duy an ninh quốc gia, khi năng lực phục hồi số trở thành nền tảng của sức mạnh kinh tế và ổn định địa chính trị.

An ninh mạng đang bước vào giai đoạn phức tạp chưa từng có, nơi các biện pháp phòng thủ truyền thống không còn đủ mạnh. Dù phòng thủ tập thể không phải là giải pháp vạn năng, nó có thể giảm thiểu tác động của các cuộc tấn công và củng cố ổn định toàn cầu. Diễn đàn Kinh tế Thế giới (WEF), thông qua Trung tâm An ninh mạng (Centre for Cybersecurity) đóng vai trò cầu nối giữa khu vực công và tư để tăng cường niềm tin và xây dựng các khung hành động cụ thể.

Sáng kiến Partnership against Cybercrime của WEF quy tụ hơn 40 tổ chức quốc tế nhằm chia sẻ thông tin và triệt phá các mạng lưới tội phạm mạng toàn cầu, trong khi Cybercrime Atlas (nền tảng hợp tác tình báo) đã lập bản đồ hàng nghìn hoạt động tội phạm mạng, hỗ trợ cơ quan thực thi pháp luật và doanh nghiệp tháo dỡ hạ tầng tội phạm số.

Không gian mạng giờ đây là tuyến đầu của phòng thủ quốc gia và là mặt trận mới của cạnh tranh địa chính trị. Việc tích hợp an ninh mạng vào chiến lược quốc gia, cơ cấu quản trị thể chế và chính sách đối ngoại sẽ giúp các quốc gia dẫn đầu và phát triển bền vững trong kỷ nguyên số./.

Tạp chí Khoa học và Công nghệ

AN NINH MẠNG: BẮT ĐẦU TỪ XÂY DỰNG LỰC LƯỢNG CHẤT LƯỢNG CAO

Hiện nay, an ninh mạng không chỉ là vấn đề kỹ thuật mà đã trở thành một "mặt trận" bảo vệ chủ quyền, dữ liệu và hạ tầng của quốc gia. Điều này đòi hỏi phải có một lực lượng an ninh mạng đủ mạnh về số lượng và chất lượng.

Cần xây dựng 'hệ sinh thái giữ người' cho lĩnh vực an ninh mạng - Ảnh: VGP

"Khoảng trống" đáng lo ngại trong lĩnh vực an ninh mạng

Theo Hiệp hội An ninh mạng Quốc gia, nước ta nằm trong nhóm quốc gia có nguy cơ cao bị tấn công mạng. Thống kê của Hiệp hội này cho thấy, năm 2024 có hơn 659.000 vụ tấn công mạng xảy ra. Khoảng 46,15% cơ quan và doanh nghiệp trong nước bị tấn công mạng ít nhất một lần. Năm 2025, nước ta ghi nhận khoảng 552.000 cuộc tấn công mạng, giảm 19,4% về số lượng nhưng rủi ro tăng cao với 52,3% tổ chức bị thiệt hại. Trong đó, dữ liệu trở thành mục tiêu chính, tin tặc chuyển sang chiến lược "tấn công kép" là vừa đánh cắp, vừa tống tiền.

Nhìn tổng thể, nhận thức về an ninh mạng tại các cơ quan, tổ chức, doanh nghiệp hiện nay đã có những chuyển biến tích cực. Tuy nhiên, mức độ đầu tư về nhân lực và giải pháp kỹ thuật vẫn chưa tương xứng với tốc độ cũng như sự tinh vi của các cuộc tấn công mạng.

Đặc biệt, khoảng trống đáng lo ngại nhất là các doanh nghiệp tại Việt Nam đang thiếu hụt trầm trọng về nhân sự đảm bảo an toàn an ninh mạng. Gần một nửa số cơ quan, doanh nghiệp, tương đương 47,72% vẫn đang thiếu nhân sự an ninh mạng.

Từ góc độ chuyên gia an ninh mạng, ông Vũ Ngọc Sơn, Trưởng ban Công nghệ, Hiệp hội An ninh mạng quốc gia cho biết, con người luôn là mắt xích yếu nhất nếu nhắc đến bảo mật, dù ở bất kỳ hệ thống công nghệ thông tin nào.

Tuy nhiên, Việt Nam dự kiến thiếu hơn 700.000 nhân sự chuyên trách về an ninh mạng thời gian tới. Đặc biệt, chất lượng đào tạo kỹ sư chưa đáp ứng nhu cầu, khi chỉ 10% sinh viên tốt nghiệp đáp ứng đủ năng lực.

Nguyên nhân thiếu nguồn nhân lực được chỉ ra là do các trường đào tạo chưa theo kịp nhu cầu thực tiễn; số lượng trường đào tạo chuyên sâu còn ít; thiếu chương trình thực hành - kỹ năng xử lý tình huống thực tế.

Đặc biệt, hiện tượng chảy máu chất xám cũng là nguyên nhân khiến nhân lực lĩnh vực này thiếu hụt. Điều đáng nói là nhiều chuyên gia giỏi chuyển sang làm việc từ xa cho các công ty nước ngoài do mức lương, chế độ đãi ngộ của các cơ quan/doanh nghiệp trong nước chưa đủ hấp dẫn; người làm an ninh mạng thiếu cơ hội thăng tiến và phát triển năng lực chuyên sâu, thiếu cọ xát thực tế.

Cần xây dựng "hệ sinh thái giữ người" cho lĩnh vực an ninh mạng

Hệ quả của sự thiếu hụt này dẫn đến gia tăng số lượng và mức độ nghiêm trọng của các vụ tấn công mạng; phản ứng với sự cố chưa nhanh, thiếu hiệu quả; doanh nghiệp và cơ quan nhà nước gặp khó khăn trong vận hành số.

Cụ thể, theo một số số liệu ghi nhận từ quốc tế, năm 2025, thiệt hại do tội phạm mạng, tội phạm sử dụng công nghệ cao, tin tặc gây ra trên thế giới khoảng 10.000 tỷ USD, như Đức bị thiệt hại 1,6% GDP; Hà Lan thiệt hại 1,5% GDP; Hoa Kỳ thiệt hại 0,64% GDP; Singapore thiệt hại 0,41% GDP; Malaysia thiệt hại 0,18% GDP. Việt Nam cũng bị thiệt hại 0,13% GDP.

Trước thực tế này đòi hỏi mỗi quốc gia phải phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng.

Ở nước ta, Luật An ninh mạng chính thức có hiệu lực từ 1/7/2026, được đánh giá là dấu mốc quan trọng trong hoàn thiện khuôn khổ pháp lý cho quản lý an ninh mạng, góp phần bảo vệ chủ quyền số, trật tự an toàn xã hội và lợi ích của người dân, doanh nghiệp trong môi trường mạng.

Hiện nay, Bộ Công an đang xây dựng các văn bản Nghị định hướng dẫn triển khai Luật Luật An ninh mạng. Trong đó, có dự thảo Nghị định quy định về lực lượng bảo vệ an ninh mạng, nhấn mạnh nhiệm vụ phát triển nguồn nhân lực chất lượng cao.

Dự thảo này xác định rõ lực lượng bảo vệ an ninh mạng gồm ba cấu phần: lực lượng chuyên trách, lực lượng thường trực và lực lượng dự bị. Trong đó, lực lượng chuyên trách là nòng cốt, lực lượng thường trực được bố trí tại các bộ, ngành, địa phương, cơ quan, tổ chức, doanh nghiệp theo tính chất hệ thống thông tin; lực lượng dự bị là các tổ chức, cá nhân có thể được huy động khi cần tăng cường nguồn lực.

Cách tiếp cận này cho thấy vấn đề bảo vệ an ninh mạng không còn là nhiệm vụ của một nhóm kỹ thuật, mà phải là một "thế trận" gồm cả lực lượng tại chỗ, lực lượng cơ động và có thể huy động trí tuệ toàn xã hội khi cần.

Điều đáng nói, dự thảo còn đưa ra chính sách thu hút, trọng dụng, đãi ngộ, hỗ trợ điều kiện làm việc, đào tạo và phát triển nguồn nhân lực chất lượng cao trong lĩnh vực an ninh mạng phù hợp với yêu cầu chuyên môn, tính chất nhiệm vụ và mức độ rủi ro, đặc thù nghề nghiệp.

Với những người trực tiếp thực hiện nhiệm vụ ở vị trí trọng yếu, trực chiến 24/7, ứng cứu sự cố nghiêm trọng hoặc làm các nhiệm vụ có yêu cầu bảo mật đặc biệt, Dự thảo đang đề xuất cơ chế thưởng theo kết quả và các hỗ trợ đặc thù khác.

Dự thảo cũng đề xuất cả một "hệ sinh thái giữ người" gồm điều kiện làm việc, chăm sóc sức khỏe, nhà ở, đào tạo, phát triển nguồn nhân lực, hỗ trợ chuyên gia trong và ngoài nước, hỗ trợ học bổng trong nước và nước ngoài, cơ chế bug bounty (chương trình săn tìm mối đe dọa nhận tiền thưởng), diễn tập phối hợp công - tư, hỗ trợ nghiên cứu, thử nghiệ m và đổi mới sáng tạo.

Những đề xuất này được kỳ vọng sẽ thu hút được nguồn nhân tài thực sự đủ chất trong lĩnh vực an ninh mạng - một lĩnh vực đặc biệt, gắn với chủ quyền số, an ninh dữ liệu, bí mật công nghệ và sức chống chịu của quốc gia trong thời đại số./.

Báo điện tử Chính phủ

NHỮNG YÊU CẦU ĐẶT RA ĐỂ NÂNG CAO NĂNG LỰC HOẠT ĐỘNG CỦA LỰC LƯỢNG BẢO VỆ AN NINH MẠNG QUỐC GIA

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ trên toàn cầu, không gian mạng đã trở thành môi trường quan trọng gắn liền với mọi lĩnh vực của đời sống xã hội, từ kinh tế, chính trị, quốc phòng đến an ninh quốc gia. Bên cạnh những lợi ích to lớn mà công nghệ số mang lại, các nguy cơ, thách thức về an ninh mạng ngày càng gia tăng với tính chất phức tạp, tinh vi và khó kiểm soát. Các hoạt động tấn công mạng, đánh cắp dữ liệu, phát tán thông tin xấu độc, xâm phạm chủ quyền quốc gia trên không gian mạng đang đặt ra yêu cầu cấp thiết phải xây dựng lực lượng bảo vệ an ninh mạng quốc gia đủ mạnh, chuyên nghiệp và hiện đại. Vì vậy, theo Quyết định số 515/QĐ-TTg ngày 30 tháng 3 năm 2026, Đề án "Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia" có ý nghĩa đặc biệt quan trọng nhằm đáp ứng yêu cầu bảo vệ an ninh quốc gia trong tình hình mới. Để triển khai hiệu quả Đề án này, cần xác định rõ những yêu cầu đặt ra đối với công tác tổ chức, đào tạo, trang bị kỹ thuật, hoàn thiện cơ chế phối hợp và nâng cao chất lượng nguồn nhân lực trong lĩnh vực an ninh mạng.

Xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại

Mục tiêu của Đề án là nâng cao năng lực tổng thể, xây dựng lực lượng bảo vệ an ninh mạng tinh nhuệ, hiện đại, nhằm chủ động phòng ngừa, sẵn sàng ứng phó hiệu quả với mọi nguy cơ, thách thức trên không gian mạng, bảo vệ vững chắc an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng.

Đến năm 2030, Việt Nam nằm trong nhóm 15 quốc gia dẫn đầu thế giới theo Chỉ số An ninh mạng toàn cầu (ITU-GCI); hình thành và phát triển Trung tâm Đào tạo khu vực về phòng, chống tội phạm mạng và an ninh mạng tại Việt Nam để nâng cao vị thế và năng lực dẫn dắt trong khu vực; Phấn đấu đến năm 2030, Việt Nam có ít nhất 10.000 chuyên gia an ninh mạng chuyên sâu, trong đó 20% đạt trình độ quốc tế; 100% lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng, lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, UBND cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước có chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng do cơ quan có thẩm quyền cấp; được cập nhật kiến thức an ninh mạng ít nhất 1 lần/năm; 90% người sử dụng Internet có cơ hội tiếp cận hoạt động nâng cao nhận thức, kỹ năng và công cụ bảo đảm an ninh mạng; nghiên cứu, phát triển, từng bước làm chủ công nghệ chiến lược về an ninh mạng; Phát triển hệ sinh thái sản phẩm, dịch vụ an ninh mạng do Việt Nam làm chủ công nghệ.

Nhà nước lựa chọn tối thiểu 2 tổ chức, doanh nghiệp làm chủ công nghệ cho mỗi loại sản phẩm, dịch vụ an ninh mạng trọng điểm, nền tảng để tập trung nguồn lực thúc đẩy; 70% các ban, bộ, ngành, địa phương và các hệ thống thông tin quan trọng quốc gia sử dụng sản phẩm công nghệ chiến lược "Make in Vietnam"; 100% các sản phẩm, dịch vụ an ninh mạng phải được kiểm định, đánh giá trước khi đưa vào sử dụng, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội và đời sống nhân dân...

Nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia.

Tầm nhìn đến năm 2045, Việt Nam thuộc nhóm quốc gia dẫn đầu khu vực châu Á - Thái Bình Dương về an ninh mạng

Cũng theo Đề án, đến năm 2045, Việt Nam thuộc nhóm quốc gia dẫn đầu khu vực châu Á - Thái Bình Dương về an ninh mạng, có năng lực mạnh trong phòng thủ, tấn công trấn áp tội phạm mạng và các thế lực thù địch, bảo vệ vững chắc chủ quyền số, bảo vệ cho mọi hoạt động của Nhà nước, doanh nghiệp và người dân trên không gian mạng. Công nghiệp an ninh mạng trở thành ngành kinh tế - kỹ thuật mũi nhọn, có 3 doanh nghiệp an ninh mạng Việt Nam nằm trong nhóm 50 doanh nghiệp dẫn đầu toàn cầu về cung cấp giải pháp an ninh mạng, xuất khẩu sản phẩm, dịch vụ, công nghệ ra thị trường thế giới.

Để đạt được các mục tiêu trên, Đề án đã đưa ra một số nhiệm vụ, giải pháp trọng tâm cần thực hiện như:

Một là, hoàn thiện thể chế, xây dựng và triển khai các cơ chế, chính sách đặc thù: Rà soát, cập nhật, hoàn thiện các văn bản quy phạm pháp luật, văn bản hướng dẫn công tác bảo đảm an ninh mạng bảo đảm đồng bộ, thống nhất, hiệu quả giữa các lực lượng, đáp ứng yêu cầu quản lý, bảo vệ không gian mạng trong bối cảnh phát triển nhanh chóng của các công nghệ mới; Xây dựng, ban hành các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật đối với các sản phẩm, dịch vụ an ninh mạng, bảo mật thông tin, thiết lập cơ chế hợp chuẩn, hợp quy, đánh giá sự phù hợp, tổ chức đánh giá, công bố sản phẩm đáp ứng các tiêu chuẩn, quy chuẩn đã ban hành, áp dụng trước hết đối với hạ tầng thông tin quan trọng quốc gia, hệ thống thông tin của các cơ quan trong hệ thống chính trị có ảnh hưởng trực tiếp đến an ninh quốc gia, trật tự xã hội

và đời sống nhân dân; Xây dựng khung quản lý rủi ro an ninh mạng quốc gia, chuyển đổi từ quản lý kỹ thuật thuần túy sang quản trị rủi ro toàn diện, dựa trên các tiêu chuẩn quốc tế nhằm tăng tính chủ động của các cơ quan, tổ chức trong việc phân bổ nguồn lực, giảm thiểu tổn thất từ các cuộc tấn công...

Hai là, tổ chức lực lượng an ninh mạng: Củng cố, kiện toàn Ban Chỉ đạo An ninh mạng Quốc gia và các tiểu ban tại các bộ, ngành, địa phương; Củng cố, kiện toàn cơ quan chuyên trách về an ninh mạng tại Bộ Công an, Bộ Quốc phòng, hướng dẫn các bộ, ngành, UBND cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia tổ chức lực lượng bảo vệ an ninh mạng; Xây dựng mạng lưới liên kết các chuyên gia an ninh mạng trong nước và nước ngoài tham gia hỗ trợ công tác bảo đảm an ninh mạng; Mở rộng Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia; hình thành đội ngũ chuyên gia an ninh mạng có năng lực chuyên sâu về các công nghệ trọng yếu (AI, mật mã kháng lượng tử, blockchain...) đạt đẳng cấp thế giới...

Ba là, đào tạo, phát triển nguồn nhân lực an ninh mạng chất lượng cao: Xây dựng, ban hành tiêu chuẩn chức danh, vị trí việc làm, khung kiến thức, kỹ năng chuyên sâu về an ninh mạng; quy định về đào tạo, sát hạch, cấp chứng nhận đáp ứng yêu cầu kiến thức, kỹ năng chuyên sâu về an ninh mạng cho lực lượng bảo vệ an ninh mạng, cán bộ trực tiếp quản trị vận hành hệ thống thông tin cấp độ 3, cấp độ 4, cấp độ 5, trong cơ quan, tổ chức, doanh nghiệp Nhà nước. Xây dựng, ban hành và định kỳ cập nhật các chương trình khung, tài liệu, giáo trình đào tạo tập huấn về bảo vệ an ninh mạng; chuẩn hóa hoạt động đào tạo, tập huấn đáp ứng yêu cầu về chuẩn kỹ năng và kiến thức về an ninh mạng tương ứng với từng cấp độ năng lực.

Hàng năm, trên cơ sở khảo sát nhu cầu thực tiễn, tổ chức các khóa đào tạo, tập huấn ngắn hạn theo hình thức tập trung, trực tuyến hoặc kết hợp cho các cơ quan của Đảng, Nhà nước, Mặt trận Tổ quốc Việt Nam (gồm các tổ chức chính trị - xã hội) từ Trung ương đến cấp xã và lực lượng vũ trang để cập nhật kiến thức, huấn luyện chuyên sâu kiến thức, kỹ năng an ninh mạng.

Phát triển nhân lực an ninh mạng quốc gia, kết nối nhà trường/viện nghiên cứu (sinh viên, giảng viên, nghiên cứu viên), doanh nghiệp và cơ quan nhà nước trong lĩnh vực an ninh mạng, thúc đẩy liên kết công - tư và bồi dưỡng thế hệ chuyên gia an ninh mạng mới.

Bốn là, nghiên cứu phát triển, nâng cao năng lực tự chủ công nghệ, làm chủ công nghệ lõi trong lĩnh vực an ninh mạng: Rà soát, xây dựng, công bố danh mục công nghệ, danh mục sản phẩm, dịch vụ an ninh mạng cốt lõi quốc gia ưu tiên làm chủ, tự chủ; Thúc đẩy cơ chế để cơ quan nhà nước đặt hàng doanh nghiệp phát triển các sản phẩm về an ninh mạng; ưu tiên thí điểm, thử nghiệm các sản phẩm do Việt Nam làm chủ công nghệ;

- Triển khai các giải pháp hỗ trợ các doanh nghiệp vừa và nhỏ bảo đảm an ninh mạng thông qua các gói hỗ trợ đào tạo, tư vấn, cung cấp giải pháp an ninh mạng nội địa. Đồng thời, thúc đẩy phát triển các trung tâm đo kiểm an ninh mạng đủ năng lực thực hiện thử nghiệm, đánh giá sự phù hợp tiêu chuẩn, quy chuẩn đối với sản phẩm, dịch vụ an ninh mạng trong nước và quốc tế..

Trong bối cảnh phát triển mới tại Việt Nam, vấn đề bảo đảm an ninh mạng, an toàn thông tin ngày càng quan trọng.

Năm là, nâng cao uy tín quốc gia và tăng cường hợp tác quốc tế: Tăng cường hợp tác song phương với các quốc gia tiên tiến về an ninh mạng, các tổ chức lớn thông qua các hoạt động chia sẻ thông tin, hỗ trợ kỹ thuật, và đào tạo nhân lực, ưu tiên mở rộng hợp tác với các đối tác như Hoa Kỳ, Liên minh châu Âu, Nhật Bản, Hàn Quốc, Ấn Độ, Israel, Trung Quốc, Anh, Pháp, Đức...

Chủ động tham gia các tổ chức như: ITU, FIRST, APCERT, GFCE, ISO, IEC... đề xuất sáng kiến, chia sẻ thông tin, tài liệu, phối hợp tổ chức các hoạt động, sự kiện quốc tế để nâng cao hình ảnh, vị thế quốc gia, tranh cử các vị trí lãnh đạo hoặc điều phối trong các nhóm công tác chuyên môn. Thiết lập các tổ chức, diễn đàn quốc tế do Việt Nam dẫn dắt về an ninh mạng.

Tham gia hoạt động của Liên hợp quốc, ASEAN, APEC... để xây dựng và thúc đẩy các chuẩn mực, quy tắc ứng xử toàn cầu về an ninh mạng. Tích cực thúc đẩy các nước ký và phê chuẩn Công ước Liên hợp quốc về chống tội phạm mạng sớm đưa Công ước có hiệu lực thực thi.

Thu hút nguồn lực từ nước ngoài và các đối tác quốc tế cho hoạt động nghiên cứu, ứng dụng, đổi mới sáng tạo, khởi nghiệp, chuyển giao công nghệ về bảo đảm an ninh mạng và đưa chuyên gia, tổ chức trong nước tham gia các hoạt động toàn cầu, các hội nghị như: RSAC Conference, Black Hat, DEFCON, CyberTech, Hack in the Box...; khuyến khích doanh nghiệp, viện nghiên cứu đạt các chứng nhận, giải thưởng quốc tế về an ninh mạng.

Để nâng cao năng lực hoạt động của lực lượng bảo vệ an ninh mạng quốc gia, cần chú trọng đồng bộ nhiều yếu tố như hoàn thiện cơ chế, chính sách pháp luật; đầu tư trang thiết bị, công nghệ hiện đại; nâng cao trình độ chuyên môn, bản lĩnh chính trị cho lực lượng thực thi nhiệm vụ; đồng thời tăng cường phối hợp giữa các cơ quan, tổ chức và doanh nghiệp. Đây là yêu cầu cấp thiết nhằm bảo đảm an ninh quốc gia, giữ vững trật tự an toàn xã hội và bảo vệ chủ quyền trên không gian mạng trong tình hình mới./.

Ngọc Anh

BẢO ĐẢM AN NINH MẠNG TRONG KỶ NGUYÊN AI: YÊU CẦU CẤP THIẾT TỪ THỰC TIỄN PHÁT TRIỂN

Trong bối cảnh trí tuệ nhân tạo phát triển mạnh mẽ, trở thành động lực cốt lõi của nền kinh tế số, vấn đề bảo đảm an ninh mạng đang nổi lên như một yêu cầu cấp thiết, mang tính nền tảng đối với sự phát triển bền vững của mỗi quốc gia.

Tìm giải pháp cho vấn đề an ninh mạng và AI

Thực tiễn cho thấy, AI không chỉ thúc đẩy đổi mới sáng tạo, tối ưu hóa vận hành mà còn làm thay đổi sâu sắc cấu trúc của không gian mạng. Khi dữ liệu ngày càng được kết nối, chia sẻ và xử lý ở quy mô lớn, các rủi ro an ninh mạng cũng gia tăng cả về mức độ lẫn tính chất, đòi hỏi những cách tiếp cận mới trong quản trị và bảo vệ hệ thống.

Tại Việt Nam, hành lang pháp lý liên quan đến an ninh mạng và trí tuệ nhân tạo đang từng bước được hoàn thiện với Luật An ninh mạng, chiến lược quốc gia về AI đến năm 2030 cùng các định hướng quản lý mới. Những chính sách này nhấn mạnh yêu cầu bảo đảm an toàn, minh bạch và trách nhiệm giải trình trong toàn bộ vòng đời công nghệ, đặc biệt khi AI ngày càng trở thành một phần quan trọng của hạ tầng số quốc gia.

Từ góc độ quản lý lĩnh vực tài chính, ông Phạm Tiến Dũng, Phó Thống đốc Ngân hàng Nhà nước nhận định trí tuệ nhân tạo (AI) không chỉ là động lực thúc đẩy đổi mới, nâng cao hiệu quả hoạt động mà còn đang làm thay đổi sâu sắc phương thức quản lý và vận hành của các tổ chức. Theo ông, trong lĩnh vực tài chính ngân hàng, AI đang được nghiên cứu và ứng dụng ở nhiều khâu như đánh giá tín dụng, chấm điểm khách hàng, phát hiện gian lận, tự động hóa quy trình và nâng cao chất lượng dịch vụ. Qua đó, góp phần nâng cao hiệu quả hoạt động của hệ thống, đồng thời mở rộng khả năng tiếp cận dịch vụ tài chính cho người dân và doanh nghiệp.

Tuy nhiên, đi cùng với cơ hội là những rủi ro ngày càng rõ nét. Ông Phạm Tiến Dũng cho rằng, các công cụ AI ngày càng dễ tiếp cận có thể bị lợi dụng để tạo ra các hình thức tấn công tinh vi, giả mạo và thao túng thông tin, khiến môi trường an ninh mạng trở nên phức tạp và khó kiểm soát hơn.

Không chỉ vậy, chính các hệ thống AI cũng có thể trở thành mục tiêu tấn công, làm gia tăng nguy cơ rò rỉ dữ liệu, sai lệch thông tin hoặc đưa ra các quyết định thiếu chính xác nếu không được kiểm soát chặt chẽ. Những phương thức bảo đảm an ninh truyền thống đang dần bộc lộ hạn chế trước các mối đe dọa mới. Điều này đòi hỏi một cách tiếp cận song hành: Vừa thiết kế, phát triển AI theo hướng an toàn, có kiểm soát, vừa tận dụng chính AI như một công cụ để nâng cao năng lực phòng thủ an ninh mạng.

Bài toán an ninh mạng toàn cầu

Từ góc nhìn quốc tế, bà Ruma Balasubramanian, Chủ tịch khu vực châu Á-Thái Bình Dương và Nhật Bản của Công ty Check Point Software Technologies cho rằng AI đang tái định hình cả đổi mới kinh doanh lẫn các rủi ro an ninh mạng, đặt ra yêu cầu cấp thiết đối với việc xây dựng các chiến lược bảo mật tiên tiến, thích ứng. Những phương thức bảo đảm an ninh truyền thống đang dần bộc lộ hạn chế trước các mối đe dọa mới. Điều này đòi hỏi một cách tiếp cận song hành: Vừa thiết kế, phát triển AI theo hướng an toàn, có kiểm soát, vừa tận dụng chính AI như một công cụ để nâng cao năng lực phòng thủ an ninh mạng.

Trước thực tế đó, yêu cầu đặt ra là phải thay đổi cách tiếp cận trong phát triển và ứng dụng AI. Theo ông Phạm Tiến Dũng, việc triển khai các hệ thống AI cần dựa trên đánh giá mức độ rủi ro và tác động. Những hệ thống có ảnh hưởng trực tiếp đến thị trường cần được giám sát nghiêm ngặt, có cơ chế kiểm soát và can thiệp kịp thời. Đối với các hệ thống hỗ trợ ra quyết định, cần bảo đảm độ chính xác, tính minh bạch và khả năng giải trình nhằm bảo vệ quyền lợi của khách hàng. Trong khi đó, các ứng dụng AI phục vụ phát hiện và phòng chống gian lận cần được phát triển theo hướng vừa nâng cao hiệu quả, vừa bảo đảm an toàn, bảo mật thông tin.

Ông Ngô Tuấn Anh Chủ tịch SafeGate giới thiệu bộ sản phẩm, giải pháp an ninh mạng phục vụ hạ tầng an ninh tin cậy của SafeGate tại Hội nghị "Phát triển các giải pháp an ninh mạng chiến lược".

Việc xây dựng một hệ sinh thái AI an toàn cần được triển khai một cách toàn diện, từ quản trị dữ liệu, quản trị rủi ro đến bảo đảm an ninh trong suốt quá trình thiết kế, phát triển và vận hành hệ thống. Đồng thời, theo các chuyên gia, cần tăng cường sự phối hợp giữa cơ quan quản lý nhà nước, cộng đồng doanh nghiệp và các tổ chức chuyên môn nhằm hoàn thiện chính sách, cơ chế quản trị và tiêu chuẩn kỹ thuật, tiệm cận với các chuẩn mực quốc tế.

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, Việt Nam đang đứng trước cơ hội lớn để bứt phá. Tuy nhiên, để tận dụng hiệu quả cơ hội này, việc xây dựng một nền tảng an ninh mạng vững chắc, nơi đổi mới sáng tạo đi đôi với an toàn và kiểm soát rủi ro, sẽ là điều kiện tiên quyết, bảo đảm cho sự phát triển nhanh và bền vững trong kỷ nguyên số./.

Báo Nhân dân

AN NINH MẠNG - YÊU CẦU CẤP THIẾT TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ

Trong bối cảnh cuộc cách mạng công nghiệp 4.0 và quá trình chuyển đổi số diễn ra mạnh mẽ trên mọi lĩnh vực, không gian mạng đã trở thành môi trường quan trọng gắn liền với đời sống kinh tế, chính trị, văn hóa và xã hội. Tuy nhiên, cùng với những lợi ích to lớn là sự gia tăng của các nguy cơ mất an toàn thông tin, tấn công mạng và lộ lọt dữ liệu. Vì vậy, bảo đảm an ninh mạng đang trở thành yêu cầu cấp thiết nhằm bảo vệ chủ quyền số quốc gia, giữ vững ổn định xã hội và thúc đẩy phát triển bền vững trong thời đại số.

Chuyển đổi số và những nguy cơ đối với an ninh mạng

Chuyển đổi số là quá trình ứng dụng công nghệ số nhằm thay đổi toàn diện phương thức quản lý, vận hành và cung cấp dịch vụ của cơ quan, tổ chức, doanh nghiệp. Hiện nay, nhiều lĩnh vực như tài chính, ngân hàng, giáo dục, y tế, giao thông, thương mại điện tử... đều đang đẩy mạnh ứng dụng trí tuệ nhân tạo (AI), dữ liệu lớn (Big Data), điện toán đám mây (Cloud Computing), Internet vạn vật (IoT) và các nền tảng số hiện đại. Tuy nhiên, khi mọi hoạt động ngày càng phụ thuộc vào môi trường mạng thì nguy cơ mất an toàn thông tin cũng gia tăng nhanh chóng. Các đối tượng tội phạm công nghệ cao lợi dụng không gian mạng để thực hiện nhiều hành vi vi phạm pháp luật như xâm nhập trái phép hệ thống thông tin, đánh cắp dữ liệu cá nhân, lừa đảo chiếm đoạt tài sản, phát tán thông tin sai sự thật và tấn công vào cơ sở dữ liệu quan trọng của cơ quan, doanh nghiệp.

Quang cảnh Hội nghị Tuyên truyền nâng cao nhận thức cộng đồng về phòng, chống tội phạm tại phường Hải An, thành phố Hải Phòng.

Đặc biệt, sự phát triển của trí tuệ nhân tạo đã khiến các hình thức tấn công mạng trở nên tinh vi hơn. Công nghệ deepfake (công nghệ sử dụng trí tuệ nhân tạo (AI) và học sâu (deep learning) để tạo ra các sản phẩm truyền thông giả mạo (hình ảnh, video, âm thanh) nhưng giống thật đến mức khó phân biệt) có thể giả mạo hình ảnh, giọng nói của cá nhân nhằm thực hiện hành vi lừa đảo hoặc phát tán thông tin xấu độc. Các email giả mạo, website giả mạo ngân hàng hay cơ quan nhà nước được thiết kế ngày càng giống thật khiến người dùng khó nhận biết.

Bên cạnh đó, mã độc tống tiền (ransomware) tiếp tục là mối đe dọa nghiêm trọng khi nhiều hệ thống bị mã hóa dữ liệu, gây đình trệ hoạt động và thiệt hại lớn về kinh tế.

Ngoài ra, các thiết bị IoT như camera giám sát, thiết bị điện tử thông minh hay hệ thống điều khiển tự động cũng tiềm ẩn nguy cơ bị tấn công nếu không được bảo mật chặt chẽ. Khi số lượng thiết bị kết nối Internet ngày càng tăng, nguy cơ lộ lọt dữ liệu và mất quyền kiểm soát hệ thống cũng ngày càng lớn.

Vai trò của an ninh mạng trong bối cảnh chuyển đổi số

An ninh mạng không chỉ là vấn đề kỹ thuật mà còn liên quan trực tiếp đến ổn định chính trị, phát triển kinh tế và bảo đảm trật tự an toàn xã hội. Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, việc bảo đảm an ninh mạng có vai trò đặc biệt quan trọng.

Trước hết, an ninh mạng giúp bảo vệ dữ liệu cá nhân và quyền riêng tư của người dân. Hiện nay, phần lớn hoạt động giao dịch, thanh toán, lưu trữ thông tin đều được thực hiện trên môi trường số. Nếu dữ liệu cá nhân bị đánh cắp hoặc sử dụng trái phép sẽ gây ảnh hưởng nghiêm trọng đến quyền lợi của người dân cũng như uy tín của các tổ chức cung cấp dịch vụ.

Báo cáo viên trực tiếp trao đổi, giải đáp nhiều câu hỏi, tình huống thực tiễn do người dân đặt ra tại Hội nghị Tuyên truyền nâng cao nhận thức cộng đồng về phòng, chống tội phạm tại phường Hải An, thành phố Hải Phòng.

Bên cạnh đó, an ninh mạng góp phần bảo vệ hệ thống thông tin trọng yếu của quốc gia. Các lĩnh vực như ngân hàng, điện lực, y tế, giao thông hay quốc phòng đều sử dụng hệ thống công nghệ thông tin để quản lý và vận hành. Một cuộc tấn công mạng nghiêm trọng có thể làm gián đoạn hoạt động của các hệ thống này, gây thiệt hại lớn về kinh tế và ảnh hưởng trực tiếp đến đời sống xã hội.

Đối với doanh nghiệp, bảo đảm an ninh mạng giúp duy trì hoạt động ổn định, bảo vệ bí mật kinh doanh và nâng cao niềm tin của khách hàng. Trong môi trường cạnh tranh hiện nay, dữ liệu được xem là tài sản quan trọng của doanh nghiệp. Nếu bị lộ lọt thông tin hoặc bị tấn công mạng, doanh nghiệp không chỉ chịu tổn thất tài chính mà còn ảnh hưởng đến uy tín và thương hiệu.

Ngoài ra, an ninh mạng còn là yếu tố quan trọng thúc đẩy quá trình chuyển đổi số bền vững. Một môi trường mạng an toàn sẽ tạo điều kiện để người dân, doanh nghiệp yên tâm sử dụng các dịch vụ số, từ đó thúc đẩy phát triển kinh tế số và xã hội số.

Một số giải pháp nâng cao hiệu quả bảo đảm an ninh mạng

Trước những mối đe dọa ngày càng phức tạp, công tác bảo đảm an ninh mạng đã và đang được các quốc gia, tổ chức và doanh nghiệp đặc biệt quan tâm. Nhiều giải pháp bảo mật hiện đại được nghiên cứu, triển khai nhằm nâng cao khả năng phòng ngừa, phát hiện và ứng phó với các sự cố an ninh mạng.

Thứ nhất, cần tiếp tục hoàn thiện hệ thống pháp luật và cơ chế quản lý về an ninh mạng. Nhà nước cần xây dựng các quy định phù hợp với thực tiễn phát triển công nghệ, tăng cường công tác thanh tra, kiểm tra và xử lý nghiêm các hành vi vi phạm pháp luật trên không gian mạng.

Thứ hai, đẩy mạnh đầu tư hạ tầng công nghệ và các giải pháp bảo mật hiện đại. Các cơ quan, tổ chức, doanh nghiệp cần ứng dụng các công nghệ bảo mật tiên tiến như xác thực đa yếu tố, mã hóa dữ liệu, trí tuệ nhân tạo trong giám sát an ninh mạng và mô hình bảo mật "Zero Trust" nhằm nâng cao khả năng phòng chống tấn công mạng.

Thứ ba, nâng cao chất lượng nguồn nhân lực về an ninh mạng. Hiện nay, nhu cầu nhân lực trong lĩnh vực này ngày càng lớn trong khi số lượng chuyên gia có trình độ cao còn hạn chế. Vì vậy, cần tăng cường đào tạo, bồi dưỡng kỹ năng an ninh mạng cho đội ngũ cán bộ, công chức, người lao động và học sinh, sinh viên.

Thứ tư, đẩy mạnh công tác tuyên truyền, nâng cao nhận thức cho người dân về an toàn thông tin. Nhiều sự cố an ninh mạng xuất phát từ sự thiếu hiểu biết hoặc chủ quan của người dùng như sử dụng mật khẩu yếu, truy cập đường link độc hại hoặc chia sẻ thông tin cá nhân không an toàn. Do đó, mỗi cá nhân cần chủ động trang bị kiến thức, kỹ năng sử dụng Internet an toàn để tự bảo vệ mình trước các nguy cơ trên không gian mạng.

Cuối cùng, cần tăng cường hợp tác quốc tế trong phòng, chống tội phạm mạng. Tội phạm công nghệ cao thường hoạt động xuyên quốc gia với thủ đoạn tinh vi, do đó việc chia sẻ thông tin, kinh nghiệm và phối hợp điều tra giữa các quốc gia là rất cần thiết nhằm nâng cao hiệu quả đấu tranh phòng chống tội phạm trên không gian mạng.

An ninh mạng không chỉ là vấn đề kỹ thuật mà còn là nhiệm vụ quan trọng của cả hệ thống chính trị, cơ quan, tổ chức và mỗi cá nhân trong xã hội. Trong tiến trình chuyển đổi số hiện nay, việc nâng cao nhận thức, hoàn thiện hệ thống bảo mật và tăng cường năng lực bảo vệ không gian mạng là yếu tố then chốt để xây dựng môi trường số an toàn, lành mạnh và phát triển bền vững./.

Diệu Thu

DOANH NGHIỆP NÂNG CAO NĂNG LỰC AN NINH MẠNG ĐỂ PHÁT TRIỂN KINH TẾ SỐ AN TOÀN, TIN CẬY

Chính phủ vừa ban hành Quyết định số 433/QĐ-TTg ngày 16/3/2026 phê duyệt Đề án chuyển đổi số các doanh nghiệp nhỏ và vừa giai đoạn 2026-2030.

Theo đó, Quyết định đặt mục tiêu hỗ trợ ít nhất 500.000 doanh nghiệp nhỏ và vừa, trong đó 300.000 doanh nghiệp được ứng dụng công nghệ số, nền tảng số và trí tuệ nhân tạo.

Quyết định là bước đi chiến lược nhằm đưa chuyển đổi số vào chiều sâu nhưng cũng đặt ra yêu cầu cấp thiết về bảo đảm an ninh mạng cho doanh nghiệp nhỏ và vừa còn hạn chế về nguồn lực, nhân sự công nghệ và năng lực phòng thủ số

Bốn nhóm thách thức an ninh mạng

Số liệu từ Bộ Tài chính, doanh nghiệp nhỏ và vừa chiếm khoảng 97-98% tổng số doanh nghiệp trong nước; gần 1,1 triệu doanh nghiệp hoạt động tính đến hết năm 2025.

Các kỹ sư công nghệ tham gia diễn tập an ninh mạng lĩnh vực tài chính, ngân hàng. (Ảnh: Ngọc Bích/TTXVN).

Nghị quyết số 68-NQ/TW ngày 4/5/2025 của Bộ Chính trị về phát triển kinh tế tư nhân đánh giá với hơn 940 nghìn doanh nghiệp và hơn 5 triệu hộ kinh doanh đang hoạt động, doanh nghiệp nhỏ và vừa đóng góp khoảng 50% GDP, hơn 30% tổng thu ngân sách và sử dụng khoảng 82% tổng lao động trong nền kinh tế. Đây không chỉ là trụ cột kinh tế mà còn là lực lượng quyết định sự ổn định việc làm, sáng tạo và năng động trong nền kinh tế số.

Tuy nhiên, trong tiến trình chuyển đổi số quốc gia, doanh nghiệp nhỏ và vừa là nhóm dễ tổn thương trước các rủi ro an ninh mạng. Theo báo cáo của Hiệp hội An ninh mạng quốc gia, năm 2025 ghi nhận mức gia tăng đáng báo động của các cuộc tấn công mạng tại Việt Nam. Cụ thể, các hệ thống thông tin trên cả nước đã phải đối mặt với khoảng 552.000 cuộc tấn công, trong đó hơn 52,3% cơ quan, tổ chức và doanh nghiệp bị ảnh hưởng.

Dữ liệu và hoạt động của các tổ chức đã trở thành mục tiêu hàng đầu của tội phạm mạng. Các hình thức tấn công ngày càng tinh vi, đặc biệt với sự hỗ trợ của trí tuệ nhân tạo, công nghệ giả mạo (deepfake) và các kỹ thuật xâm nhập kéo dài. Doanh nghiệp nhỏ và vừa được xem là "mắt xích yếu" trong hệ thống phòng thủ an ninh mạng do hạn chế về nguồn lực tài chính, thiếu hụt nhân sự chuyên môn sâu và nhận thức chưa đầy đủ về tầm quan trọng của an ninh mạng toàn diện.

Ông Vũ Duy Hiền, Phó Tổng thư ký kiêm Chánh Văn phòng Hiệp hội An ninh mạng quốc gia nhận định, với doanh nghiệp nhỏ và vừa, một sự cố lừa đảo, rò rỉ dữ liệu, mã độc hay giả mạo thương hiệu không chỉ là vấn đề kỹ thuật, mà có thể tác động trực tiếp đến uy tín, khách hàng và sự tồn tại của doanh nghiệp. Thực tế cho thấy, nhiều doanh nghiệp nhỏ và vừa vẫn sử dụng phần mềm không rõ nguồn gốc, ứng dụng giả mạo hoặc công nghệ chưa được kiểm chứng. Đây chính là "cửa ngõ" phổ biến để tội phạm công nghệ cao xâm nhập, từ đó khai thác dữ liệu phục vụ mục đích lừa đảo.

Vì vậy, ông Vũ Duy Hiền cho rằng các doanh nghiệp nhỏ và vừa cần thống nhất nhận thức, an toàn, an ninh mạng không đứng ngoài chuyển đổi số mà là điều kiện nền tảng để chuyển đổi số diễn ra hiệu quả và bền vững.

Theo các chuyên gia, nhận thức và định hướng chiến lược của doanh nghiệp nhỏ và vừa đã cải thiện rõ rệt thể hiện qua việc ngày càng hiểu rõ tầm quan trọng của chuyển đổi số. Tuy nhiên, các rào cản vẫn còn lớn, bao gồm hạn chế về tài chính, công nghệ, nhân lực, hệ sinh thái hỗ trợ, cũng như khoảng cách giữa chính sách và thực thi.

Ông Nguyễn Hoa Cương, Phó Viện trưởng Viện Nghiên cứu Chính sách và Chiến lược (Ban Chính sách Chiến lược Trung ương) nêu rõ 4 nhóm thách thức lĩnh vực an ninh mạng đối với doanh nghiệp nhỏ và vừa. Đầu tiên là các mối đe dọa hiện hữu, khi số lượng thiết bị bị tấn công và nhiễm mã độc ngày càng gia tăng.

Thứ hai là các "cửa ngõ" tấn công trong chuỗi cung ứng. Doanh nghiệp không hoạt động độc lập mà liên kết với nhiều đối tác. Nếu một mắt xích trong chuỗi có bảo mật yếu, toàn bộ hệ thống có thể bị ảnh hưởng. Trong khi đó, doanh nghiệp nhỏ và vừa thường có mức độ đầu tư cho an ninh mạng thấp và chỉ phản ứng khi sự cố xảy ra.

Bên cạnh đó là hạn chế trong chiến lược dài hạn. Nhiều doanh nghiệp mới chỉ số hóa từng phần, chưa thực hiện chuyển đổi số toàn diện. Việc đồng thời vừa chuyển đổi số, vừa đảm bảo an ninh mạng là một thách thức lớn, đặc biệt với doanh nghiệp nhỏ và siêu nhỏ.

Ngoài ra, doanh nghiệp còn phụ thuộc nhiều vào các nền tảng số như mạng xã hội để kinh doanh. Khi thuật toán thay đổi, hoạt động kinh doanh cũng bị ảnh hưởng đáng kể.

Cuối cùng là rào cản về nguồn lực. Các hạn chế về tài chính, nhân lực và hạ tầng luôn là vấn đề cốt lõi. Đây là những thách thức mang tính nền tảng, nếu không được giải quyết, sẽ tiếp tục cản trở quá trình chuyển đổi số và nâng cao năng lực cạnh tranh của doanh nghiệp trong kỷ nguyên số.

Phó Giám đốc Sở Tư pháp Hoàng Anh Phong phát biểu khai mạc Hội nghị phổ biến Luật An ninh mạng và Luật Tương trợ tư pháp về dân sự năm 2025 tại thành phố Hải Phòng.

Hệ sinh thái số an toàn cho doanh nghiệp vừa và nhỏ

Bảo đảm an toàn số không chỉ là nhiệm vụ bảo vệ an ninh quốc gia, mà còn là bệ đỡ phòng vệ hữu ích giúp cộng đồng doanh nghiệp và xã hội an toàn và phát triển mạnh mẽ hơn. An toàn số cho doanh nghiệp nhỏ và vừa đòi hỏi sự phối hợp chặt chẽ giữa Nhà nước, tổ chức xã hội - nghề nghiệp, cơ quan chuyên môn, doanh nghiệp công nghệ, cơ quan báo chí và chính cộng đồng doanh nghiệp.

Hiện thực hóa các mục tiêu trên, Hiệp hội An ninh mạng quốc gia phối hợp với các đơn vị liên quan phát động Sáng kiến hỗ trợ doanh nghiệp vừa và nhỏ, đánh dấu bước tiến mới trong việc kết nối cơ quan quản lý, hiệp hội nghề nghiệp, cơ quan báo chí và các đối tác trong nước, quốc tế cùng đồng hành với doanh nghiệp trên hành trình xây dựng môi trường số an toàn, tin cậy và có trách nhiệm.

Với vai trò dẫn dắt và kết nối then chốt trong việc kết nối các nguồn lực, Hiệp hội An ninh mạng quốc gia xác định trách nhiệm trở thành một điểm tựa chiến lược cho cộng đồng doanh nghiệp Việt Nam, nhất là doanh nghiệp nhỏ và vừa. Để kiến tạo một tương lai số thực sự an toàn, cần những hành động cụ thể, những kết nối thực chất, những tri thức thực chiến.

Hiệp hội An ninh mạng quốc gia cụ thể hóa vai trò qua 3 cam kết hành động trọng tâm là kết nối nguồn lực, xóa bỏ tối đa sự đơn độc của doanh nghiệp vừa và nhỏ; lan tỏa tri thức thực chiến, phổ biến các chính sách, biến kinh nghiệm thành sức mạnh; hỗ trợ thực thi và phản ứng nhanh khi gặp sự cố, ông nhận định.

Quang cảnh Hội nghị phổ biến Luật An ninh mạng và Luật Tương trợ tư pháp về dân sự năm 2025 tại thành phố Hải Phòng.

Ông Vũ Duy Hiền nhấn mạnh, không dừng lại ở những lời khuyên lý thuyết, Hiệp hội hướng tới sự hỗ trợ mang tính thực tế và chính xác như tư vấn đúng lúc, hướng dẫn đúng chỗ, đưa ra giải pháp phù hợp với năng lực tài chính và nhu cầu thực tế của doanh nghiệp nhỏ và vừa. Hiệp hội An ninh mạng quốc gia cam kết tiếp tục phát huy vai trò cầu nối, góp phần xây dựng một môi trường để doanh nghiệp không chỉ nhận được sự hỗ trợ, mà còn cùng chia sẻ tri thức, cảnh báo rủi ro, nâng cao sức chống chịu và phát triển bền vững trên không gian số.

Đối với doanh nghiệp, theo ông Nguyễn Hoa Cương cần thực hiện "vệ sinh mạng" (cyber hygiene). Nền tảng cơ bản bao gồm việc sử dụng phần mềm diệt virus, tường lửa, chính sách mật khẩu mạnh, mã hóa dữ liệu và xác thực nhiều lớp. Cùng với đó, áp dụng quy trình sao lưu 3-2-1.

Ông Nguyễn Hoa Cương lưu ý, doanh nghiệp cần lưu trữ ít nhất 3 bản sao dữ liệu, trên 2 loại phương tiện khác nhau và có 1 bản lưu trữ ngoại vi để đảm bảo an toàn trước các cuộc tấn công mã hóa dữ liệu. Ngoài ra, doanh nghiệp cần chuyển đổi sang hệ thống điện toán đám mây; sử dụng phần mềm có bản quyền, thay thế các phiên bản miễn phí hoặc không rõ nguồn gốc bằng phần mềm có giấy phép để giảm thiểu lỗ hổng bảo mật; khuyến khích áp dụng các khung tiêu chuẩn để chuẩn hóa công tác an toàn thông tin...

An toàn số không phải là đích đến mà là một hành trình bền bỉ liên tục. Với sự đồng hành của các cơ quan quản lý, các tổ chức nghề nghiệp...doanh nghiệp nhỏ và vừa sẽ từng bước nâng cao năng lực tự bảo vệ, thích ứng và phát triển bền vững trong kỷ nguyên số./.

TTXVN

LUẬT AN NINH MẠNG TĂNG CƯỜNG KIỂM SOÁT CHẶT CHẼ NỘI DUNG LIÊN QUAN ĐẾN TRÍ TUỆ NHÂN TẠO?

Trên không gian mạng, các rủi ro tiềm ẩn phát sinh từ trí tuệ nhân tạo (AI) là một thách thức không nhỏ đối với các nhà cung cấp sản phẩm, dịch vụ an ninh mạng. Luật ANM đã bước đầu có những bổ sung những quy định trước sự phát triển liên tục của công nghệ này. Theo đó, Luật nghiêm cấm các hành vi sử dụng AI để giả mạo các video, hình ảnh, giọng nói của người khác với mục đích trái pháp luật. Việc lần đầu tiên đưa quy định này vào luật cho thấy nỗ lực điều chỉnh kịp thời của pháp luật trước thực trạng không gian mạng ngày càng bị lợi dụng để lừa đảo và xâm phạm quyền riêng tư.

Tuy nhiên, trước sự phát triển nhanh chóng và tác động ngày càng sâu rộng của AI, các vấn đề pháp lý liên quan đến công nghệ này đòi hỏi một khuôn khổ điều chỉnh toàn diện và chuyên biệt hơn. Do đó, các quy định chi tiết về phát triển, triển khai và quản lý AI sẽ được điều chỉnh chi tiết trong một văn bản pháp luật độc lập, cụ thể là Luật Trí tuệ nhân tạo 2025 đã có hiệu lực từ ngày 01/03/2026./.

AN NINH MẠNG LÀ GÌ?

Tại khoản 1 Điều 2 Luật An ninh mạng 2025, An ninh mạng là sự ổn định, an ninh, an toàn của không gian mạng; bảo vệ hệ thống thông tin và bảo đảm thông tin, dữ liệu, 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./.

LUẬT AN NINH MẠNG CÓ NGĂN CẢN, XÂM PHẠM QUYỀN TỰ DO NGÔN LUẬN HAY KHÔNG?

Luật An ninh mạng không ngăn cản, xâm phạm quyền tự do ngôn luận của công dân. Các hoạt động liên lạc, trao đổi, đăng tải, chia sẻ thông tin, mua bán, kinh doanh, thương mại vẫn diễn ra bình thường trên không gian mạng, không hề bị ngăn cản, miễn là những hoạt động đó không vi phạm pháp luật Việt Nam. Công dân có thể làm bất cứ điều gì trên không gian mạng mà pháp luật không cấm. Ngược lại, Luật An ninh mạng bảo vệ cho các hoạt động tự do ngôn luận, quyền và lợi ích hợp pháp của tổ chức, cá nhân khi mua bán, kinh doanh, trao đổi, thương mại trên không gian mạng./.

LUẬT AN NINH MẠNG CÓ KIỂM SOÁT TOÀN BỘ THÔNG TIN CÁ NHÂN CỦA CÔNG DÂN HAY KHÔNG?

Luật An ninh mạng không kiểm soát toàn bộ thông tin cá nhân của công dân.

Chỉ khi phục vụ điều tra, xử lý hành vi vi phạm pháp luật về an ninh mạng thì Luật An ninh mạng mới yêu cầu doanh nghiệp cung cấp thông tin cá nhân có liên quan tới hành vi vi phạm 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./.

KHI BỊ TẤN CÔNG MẠNG, CÁ NHÂN HOẶC DOANH NGHIỆP NÊN LÀM GÌ?

Khi bị tấn công mạng, cá nhân hoặc doanh nghiệp nên thực hiện:

- Ngắt kết nối internet: Để ngăn chặn hacker tiếp tục xâm nhập.
- Thay đổi mật khẩu ngay lập tức.

Người dân có thể thay đổi mật khẩu máy tính khi bị tấn công mạng.

- Báo cáo sự cố cho cơ quan chức năng hoặc bộ phận IT.
- Kiểm tra hệ thống, cập nhật phần mềm bảo mật./.

CÁC LOẠI HÌNH TẤN CÔNG MẠNG PHỔ BIẾN HIỆN NAY LÀ GÌ? HẬU QUẢ CỦA TỪNG LOẠI TẤN CÔNG?

1. Tấn công bằng phần mềm độc hại (Malware):

+ Gồm virus, trojan, spyware, ransomware...

+ Hậu quả: Đánh cắp dữ liệu, mã hóa file đòi tiền chuộc, gián điệp thông tin.

2. Tấn công lừa đảo (Phishing):

+ Gửi email giả mạo ngân hàng, tổ chức lớn để dụ người dùng cung cấp thông tin cá nhân.

+ Hậu quả: Đánh cắp mật khẩu, thông tin thẻ tín dụng.

3. Tấn công từ chối dịch vụ (DDoS):

+ Kẻ tấn công dùng hàng loạt máy tính để gửi yêu cầu truy cập liên tục vào một website hoặc máy chủ, làm hệ thống quá tải và ngừng hoạt động.

+ Hậu quả: Làm tê liệt trang web, gây tổn thất kinh tế lớn.

4. Tấn công Man-in-the-Middle (MITM):

+ Kẻ tấn công chèn vào giữa cuộc trao đổi dữ liệu giữa hai bên để đánh cắp hoặc thay đổi thông tin.

+ Hậu quả: Nguy cơ mất tài khoản ngân hàng, dữ liệu cá nhân./.

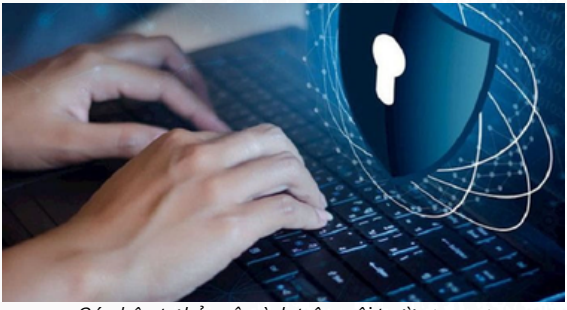
LÀM THẾ NÀO ĐỂ CÁ NHÂN TỰ BẢO VỆ MÌNH TRÊN MÔI TRƯỜNG MẠNG?

- Sử dụng mật khẩu mạnh: Ít nhất 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.

- Kích hoạt xác thực hai lớp (2FA): Giúp tăng cường bảo mật tài khoản ngân hàng, email, mạng xã hội.

- Không nhấp vào đường link lạ: Cẩn trọng với email hoặc tin nhắn yêu cầu nhập mật khẩu hoặc thông tin cá nhân.

- Cập nhật phần mềm và hệ điều hành: Đảm bảo thiết bị luôn chạy phiên bản mới nhất để tránh lỗ hổng bảo mật./.



Cá nhân tự bảo vệ mình trên môi trường mạng.

TẠI SAO AN NINH MẠNG LẠI QUAN TRỌNG?

An ninh mạng đóng vai trò quan trọng vì nhiều lý do, lý do rõ ràng nhất là bảo vệ dữ liệu nhạy cảm. Trong thế giới kỹ thuật số ngày nay, một lượng lớn dữ liệu cá nhân, tài chính và kinh doanh được lưu trữ trực tuyến. Các biện pháp an ninh mạng giúp bảo vệ dữ liệu này khỏi sự truy cập trái phép, đảm bảo tính bảo mật và toàn vẹn của dữ liệu.

Ngoài việc bảo vệ dữ liệu, an ninh mạng còn đóng vai trò thiết yếu trong việc duy trì hoạt động của cơ sở hạ tầng trọng yếu. Từ lưới điện đến hệ thống chăm sóc sức khỏe, nhiều dịch vụ thiết yếu dựa vào các hệ thống kỹ thuật số có thể bị gián đoạn bởi các cuộc tấn công mạng. Một hệ thống an ninh mạng vững chắc giúp bảo vệ các hệ thống này, đảm bảo chúng vẫn hoạt động ngay cả khi đối mặt với các mối đe dọa tiềm tàng.

Hơn nữa, các biện pháp an ninh mạng mạnh mẽ giúp xây dựng lòng tin. Đối với các doanh nghiệp, việc thể hiện cam kết về an ninh mạng có thể nâng cao danh tiếng và niềm tin của khách hàng, điều này đặc biệt quan trọng trong các ngành như tài chính, chăm sóc sức khỏe và thương mại điện tử. Ngược lại, việc thiếu an ninh mạng đầy đủ có thể dẫn đến các vụ vi phạm làm tổn hại danh tiếng, gây thiệt hại tài chính và thậm chí dẫn đến hậu quả pháp lý./.