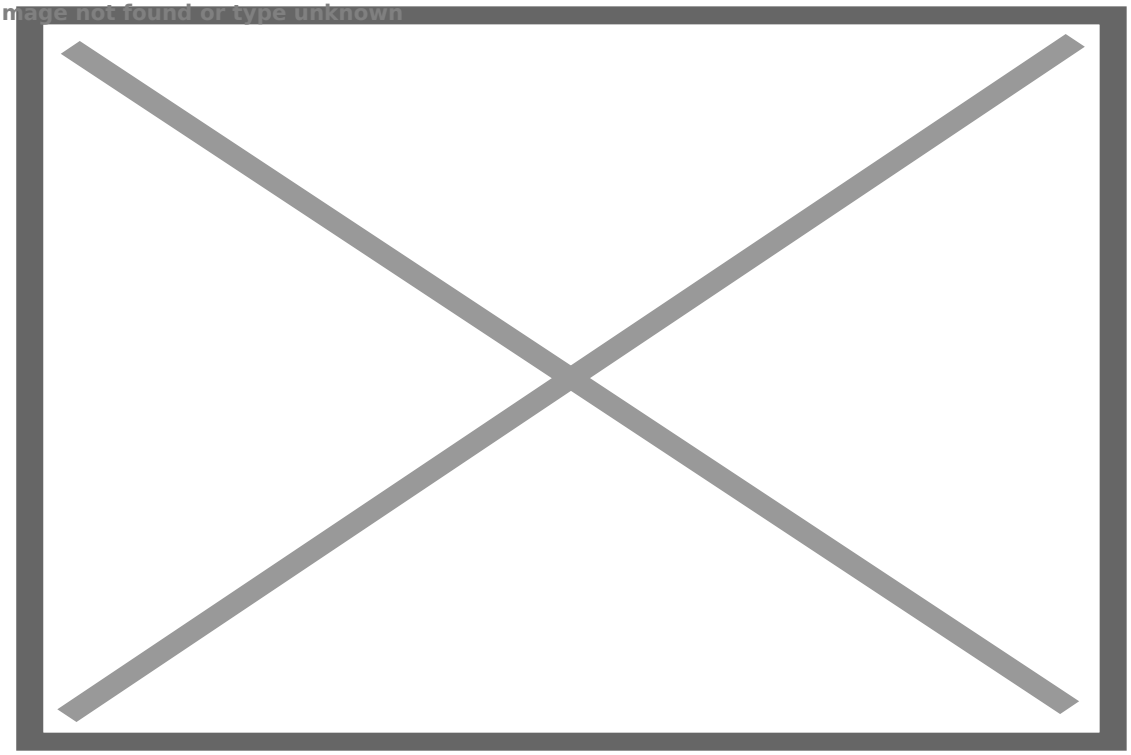
Vấn đề an toàn thông tin cho các cơ quan báo chí

17:19 30/08/2016

Tác giả: Admin

Sự cố hệ thống mạng thông tin của Vietnam Airlines bị tin tặc tấn công là hồi chuông cảnh tỉnh cho các cơ quan báo chí, đặc biệt là báo điện tử đang sở hữu nhiều dữ liệu thông tin quan trọng, trong bối cảnh công tác bảo đảm an toàn, an ninh thông tin mạng hiện nay còn nhiều bất cập



Ảnh minh họa. Nguồn: Internet

Sự cố hệ thống mạng thông tin của Tổng công ty Hàng không Quốc gia (Vietnam Airlines) bị tin tặc tấn công là hồi chuông cảnh tỉnh cho các cơ quan báo chí, đặc biệt là báo điện tử đang sở hữu nhiều dữ liệu thông tin quan trọng, trong bối cảnh công tác bảo đảm an toàn, an ninh thông tin mạng hiện nay còn nhiều bất cập cả về hạ tầng, nguồn nhân lực và nhận thức.

“Lỗ hổng” an ninh, bảo mật

Không phải ngẫu nhiên, Eugene Kaspersky, đồng sáng lập và là Giám đốc điều hành của Hãng sản xuất và phân phối phần mềm bảo mật của Nga Kasperspy Lab đã đánh giá: Những năm 90 của thế kỷ XX là thập kỷ của những kẻ phá hoại trên mạng; những năm đầu thế kỷ XXI là thập kỷ của tội

phạm mạng và giờ đây là kỷ nguyên mới của chiến tranh không gian ảo và khủng bố không gian mạng. Theo báo cáo toàn cầu mới nhất từ Kaspersky Lab, Việt Nam đứng thứ 3 trên thế giới về sự nguy hiểm tiềm ẩn khi lướt web với 35% số người dùng đã bị tấn công.

Nhà báo Hoàng Anh Vinh,

Phó Tổng Biên tập Báo Hải Quan:

Khi tin tặc tấn công vào mạng của cơ quan báo chí sẽ để lại hậu quả hết sức trầm trọng và nguy hại, do báo chí là cơ quan truyền thông, có tham gia định hướng và phản biện dư luận xã hội. Đối với các cơ quan báo chí, khi bị tấn công mạng, nhẹ thì ảnh hưởng đến tốc độ truy cập hoặc đình trệ hệ thống (tấn công Ddos như từng xảy ra với Vietnamnet); nặng thì bị xóa hết cơ sở dữ liệu và thay đổi nội dung xấu lên trên trang chủ. Điều này không chỉ ảnh hưởng đến khả năng phục hồi dữ liệu mà còn ảnh hưởng đến uy tín và niềm tin của bạn đọc đối với tờ báo đó. Về ảnh hưởng đến xã hội, như tôi đã đề cập ở trên về vai trò của báo chí, việc bị tấn công, thay đổi bằng nội dung xấu sẽ khiến dữ luận hiểu sai về thông tin truyền thông và sai lệch trong định hướng dư luận xã hội.

- *Hà Vân (ghi)*

Kasperspy Lab cho biết, Việt Nam đứng số 1 thế giới về tỷ lệ lây nhiễm mã độc qua thiết bị lưu trữ ngoài (USB, thẻ nhớ, ổ cứng di động) với tỷ lệ 70,83% máy tính bị lây nhiễm; 39,95% người dùng phải đối mặt với mã độc bắt nguồn từ không gian mạng.

Thống kê trong năm 2015, có hơn 10.000 trang (hoặc cổng) thông tin điện tử có tên miền .vn bị tấn công, chiếm quyền điều khiển, thay đổi giao diện, cài mã độc (tăng 68% so với năm 2014), trong đó có 224 trang thuộc quản lý của các cơ quan Nhà nước. Những số liệu đó cho thấy, mối đe dọa từ tội phạm mạng ngày càng lớn, trong khi nhiều tổ chức cá nhân vẫn chưa thực sự quan tâm sử dụng các biện pháp bảo đảm an toàn thông tin một cách hiệu quả.

Bên cạnh việc khai thác các lỗ hổng bảo mật trên các hệ điều hành và hệ thống mạng để tấn công xâm nhập, nguy hiểm hơn, tin tặc còn sử dụng chính các tài liệu, văn bản lưu hành nội bộ ở các cơ quan báo chí mà chúng đã đánh cắp được để đăng tải thông tin trên các trang mạng phản động làm mồi phát tán mã độc, xâm nhập hệ thống mạng của các cơ quan khác của Việt Nam.

Có nhiều cách tin tặc có thể tấn công các trang báo điện tử như thông qua các lỗi trên ứng dụng web, lỗi trên máy chủ hoặc thực hiện các cuộc tấn công đến những người quản lý trang web vì thông thường các báo sẽ có nhiều biên tập viên cùng tham gia quản trị. Các nhà quản trị, biên tập viên cần hết sức lưu ý khi nhận được email, các dữ liệu đính kèm (thường là file.doc) hay đường

dẫn đang nghi ngờ.

Cũng theo các chuyên gia an ninh mạng của Bkav, các cơ quan báo chí là loại đối tượng đặc biệt nhạy cảm. Nếu bị hacker tấn công mạng, chỉnh sửa nội dung tuyên truyền định hướng, đường lối, chính sách thì hậu quả sẽ rất nghiêm trọng. Nhưng hiện mới có một số ít cơ quan báo chí quan tâm tới việc đầu tư an toàn an ninh thông tin. Trừ một số cơ quan báo chí có hạ tầng kỹ thuật tốt, còn đa phần không có hạ tầng kỹ thuật, phải đi thuê hạ tầng, nhân lực chuyên trách về an toàn an ninh cũng không có, nên an toàn thông tin vẫn là thách thức rất lớn.

An toàn thông tin là vấn đề sống còn

Tại cuộc họp báo thường kỳ của Chính phủ chiều 3/8, Bộ trưởng Bộ Thông tin &Truyền thông Trương Minh Tuấn cho biết, tấn công mạng là nguy cơ trên toàn cầu và có thể xảy ra bất cứ lúc nào. Bộ trưởng Trương Minh Tuấn cũng nhấn mạnh biện pháp ngăn chặn chính là phải chủ động bảo mật cho hệ thống mạng thông tin của mình, đồng thời khuyến cáo cộng đồng mạng cần bình tĩnh, tránh những khiêu khích có thể là nguy cơ dẫn đến “chiến tranh” mạng.

Nhà báo Nguyễn Ngọc Hưng,

Biên tập viên Báo Quân Đội Nhân Dân

Theo quy định hiện nay, Tổng biên tập của báo là người chịu trách nhiệm về nội dung, nhưng không dễ để chứng minh thông tin sai trên báo mạng của mình là do tin tặc gây ra. Thông tin sai lệch do tin tặc gây ra nếu không bị phát hiện thì sẽ gây tác động rất lớn tới bạn đọc và toàn xã hội, gây tâm lý hoang mang rất lớn cho xã hội. Bên cạnh những biện pháp nghiệp vụ nhằm phát hiện và xử lý tin tặc tấn công các cơ quan báo chí, cơ quan quản lý có thể cử các chuyên gia tới hướng dẫn hoặc giúp các cơ quan báo chí kiểm tra, đưa ra những gợi ý nhằm tăng cường an ninh mạng. Cơ quan quản lý cũng có thể đưa ra những cảnh báo kịp thời hoặc vào cuộc hỗ trợ khi các cơ quan báo chí bị tấn công mạng.

- Hà Vân (ghi)

Các chuyên gia an ninh mạng cũng cảnh báo, hiện nay, các cuộc tấn công thường “ăn theo” các sự kiện chính trị và có diễn biến ngày càng phức tạp. Việc giải quyết không ổn thỏa quan hệ chính trị, ngoại giao giữa các quốc gia cũng dễ gây nguy cơ chiến tranh mạng, trong đó các cơ quan báo chí là mục tiêu hàng đầu của các nhóm tin tặc nước ngoài.

Phòng hơn... chống!

Để tăng cường an ninh, sẵn sàng ứng phó với các tình huống an ninh mạng có thể xảy ra, các cơ quan báo chí nên rà soát lại hệ thống, kiểm tra định kỳ để tránh việc bị khai thác các lỗi bảo mật. Người quản trị nên có quy trình kiểm tra đánh giá website trước khi đưa vào sử dụng. Khi tiến hành thiết kế trang web, các kỹ sư phải phân tích, lường trước được tất cả các tình huống có thể xảy ra để tránh tồn tại “lỗ hổng” bảo mật. Thêm vào đó, các cơ quan tổ chức nên tiến hành đào tạo, củng cố, tăng cường kiến thức về an toàn thông tin cho cán bộ phóng viên, biên tập viên. Bên cạnh đó, các đơn vị báo chí cần thiết lập chính sách bắt buộc thay đổi mật khẩu hàng tháng, không lưu mật khẩu các máy chủ trên máy tính.

Bên cạnh đó, các cơ quan báo chí cần chủ động xây dựng kế hoạch và đầu tư kinh phí cho hệ thống từ quy trình, công nghệ đến nâng cao trình độ nguồn nhân lực; chủ động đầu tư hạ tầng riêng, làm chủ công nghệ, không quá lệ thuộc hoàn toàn vào đơn vị thuê ngoài đối với vấn đề an ninh mạng.

Mặt khác, cơ quan quản lý Nhà nước về lĩnh vực này cần có sự hỗ trợ tích cực về chuyên môn, tránh để xảy ra những "lỗ hổng" để bọn tội phạm lợi dụng. Nhưng trước khi có sự hỗ trợ này, các cơ quan báo chí cần phải liên tục cập nhật và sử dụng các công cụ bảo đảm an ninh, bảo vệ hệ thống mạng của chính mình, nhất là phải xây dựng được quy trình, quy định chặt chẽ đối với từng đối tượng sử dụng mạng. Về lâu dài, vấn đề bảo đảm an ninh mạng cần có sự vào cuộc quyết liệt từ phía cơ quan quản lý Nhà nước để hoàn thiện hệ thống luật pháp về lĩnh vực này.

Ngọc Quang

Link bài viết: https://nguoilambao.vn/public/van-de-an-toan-thong-tin-cho-cac-co-quan-bao-chi