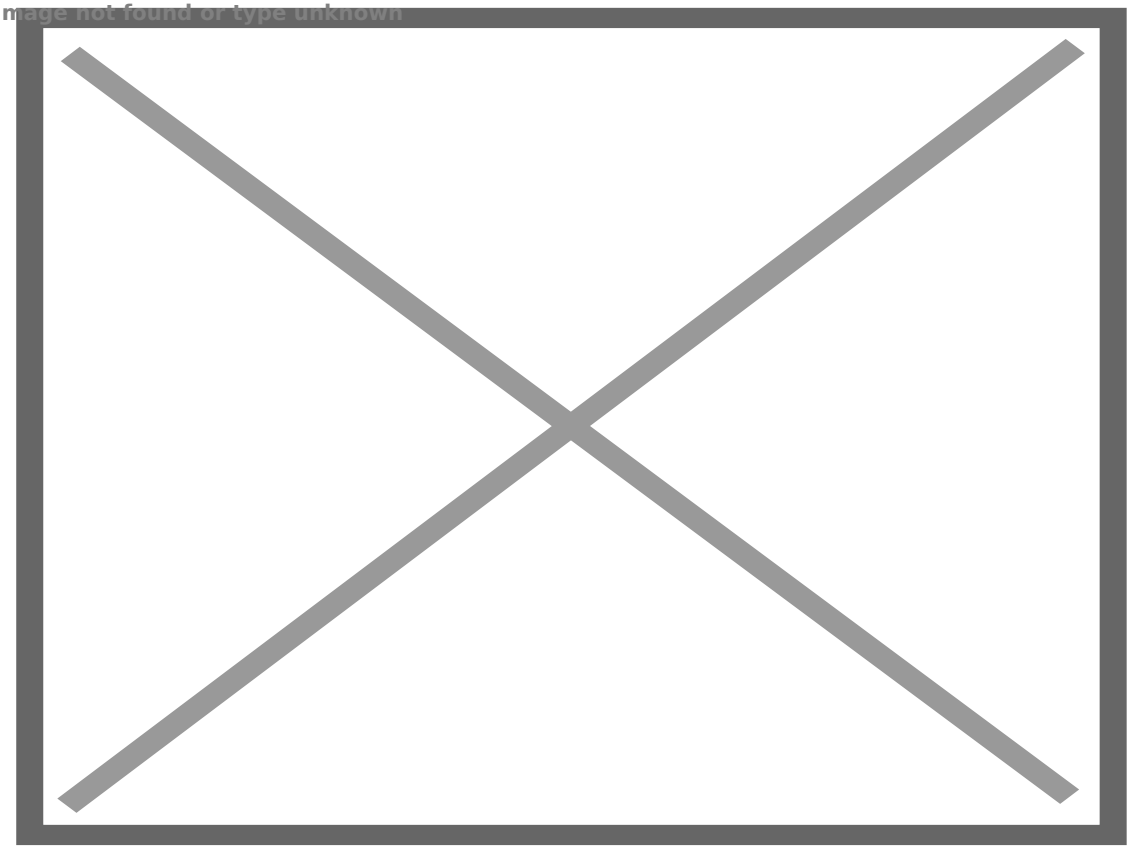
Không chỉ là cảnh báo

18:05 09/09/2016

Tác giả: Admin

Với xu hướng bùng nổ của các thiết bị thông minh có kết nối Internet hiện nay, cùng với sự phát triển mạnh mẽ của báo điện tử và các dịch vụ trực tuyến đi kèm thì nguy cơ về tấn công mạng đối với tất cả cơ quan, tổ chức ngày càng lớn, đặc biệt là các cơ quan báo chí sẽ là mục tiêu tấn công của tin tặc.

Image not found or type unknown



Ảnh minh họa. Nguồn: Internet

Nguy cơ hiện hữu

Hiện nay, các cơ quan báo chí phải đối mặt với nhiều vấn đề phức tạp từ những nguy cơ thường gặp trong tấn công an ninh mạng như làm gián đoạn thông tin; làm sai lệch thông tin, đánh cắp thông tin, phá huỷ thông tin, làm lộ thông tin.

Nguy cơ thứ nhất và cũng thường xảy ra nhất là các kênh thông tin trực tuyến của cơ quan báo chí sẽ bị gián đoạn thông tin, nó trực tiếp làm mất tính thời sự của báo chí, kéo theo đó là số lượng truy cập thông tin trực tuyến sụt giảm đồng nghĩa với việc doanh thu từ các dịch vụ cũng sụt giảm.

Nguy hiểm hơn, trong các thời điểm khủng hoảng (thiên tai, địch họa...), sự gián đoạn thông tin của các cơ quan báo chí chính trị đầu não có thể gây tổn hại đến an ninh quốc gia.

Mối hiểm họa thứ hai đến từ các tấn công chiếm quyền điều khiển máy chủ nội dung của tờ báo điện tử và làm sai lệch thông tin mà cơ quan báo chí đưa ra hoặc phát tán các thông tin sai sự thật, điều này dẫn đến sự sai lệch các thông tin nhạy cảm sẽ gây ra sự bất ổn và hoang mang cho xã hội và rất khó khăn để phục hồi lại nội dung gốc. Việc bị chiếm quyền điều khiển nội dung thì những thông tin mật, thông tin không chính thức của cơ quan hay thông tin cá nhân hoàn toàn có thể bị rò rỉ hoặc công bố trái phép. Hậu quả tất yếu của việc này là khủng hoảng, đặc biệt là những thông tin liên quan tới vấn đề quân sự, an ninh, hay ngoại giao.

Nguy cơ mất an ninh mạng đối với các báo điện tử ở Việt Nam thường gặp là bị tấn công từ chối dịch vụ làm gián đoạn thông tin trực tuyến, bị chiếm quyền điều khiển máy chủ của tờ báo điện tử bị thay đổi sang một giao diện khác với một số thông điệp đặc trưng của kẻ tấn công.

Có rất nhiều nguyên nhân dẫn tới tấn công mạng đối với báo điện tử và xét về mặt kỹ thuật thì nguyên nhân có thể là lỗi cấu hình, phân quyền cho website, lỗi lập trình, lỗi nhiễm mã độc, lỗi hệ thống... Và thực tế khi gặp phải sự cố an ninh mạng, đa số các cơ quan báo chí đều bất ngờ và bị động vì chưa có quy trình hoạt động phòng ngừa và xử lý sự cố.

Các cơ quan báo chí là tổ chức cung cấp thông tin tới độc giả, khi bị tấn công sẽ không chỉ gây thiệt hại tới tòa soạn mà sẽ có hàng triệu độc giả bị ảnh hưởng. Thiệt hại đơn giản nhất là dịch vụ sẽ bị ngưng trệ khiến độc giả không thể truy cập vào trang báo điện tử, hoặc bị chuyển hướng đến các trang web độc hại có nội dung xấu.
Để tăng cường công tác bảo đảm an toàn thông tin cho các cơ quan báo chí, cần thực hiện những biện pháp rà soát bảo vệ trước những cuộc tấn công có thể xảy ra. Các cơ quan báo chí cũng cần áp dụng quy trình kiểm tra hệ thống thường xuyên, trang bị giải pháp cảnh báo về những mối nguy tiềm ẩn nhằm bảo đảm cho hoạt động thông suốt của hệ thống. Cần thường xuyên tổ chức diễn tập với kịch bản cụ thể về phương án ứng cứu sự cố an ninh mạng, giống như các cuộc diễn tập về cứu hỏa, phòng cháy chữa cháy định kỳ thường niên. - Ông Ngô Tuấn Anh, Phó Chủ tịch Phụ trách An ninh Mạng, Tập đoàn BKAV

Phòng ngừa và xử lý sự cố an ninh mạng

Năm 2015, Quốc hội đã thông qua Luật An toàn thông tin mạng. Trong tương lai, cùng với các nghị định và thông tư hướng dẫn của Chính phủ, luật này sẽ là cơ sở pháp lý quan trọng không chỉ để

bảo đảm an toàn thông tin mạng cho quốc gia mà còn cho mọi tổ chức trong đó có các cơ quan báo chí. Bên cạnh đó, Chính phủ cũng thể hiện quyết tâm tạo chuyển biến trong nâng cao nhận thức về an toàn thông tin mạng bằng nhiều quyết định quan trọng, và gần nhất chính là quyết định số 898/QĐ-TTg về việc Phê duyệt phương hướng, mục tiêu, nhiệm vụ bảo đảm an toàn thông tin mạng giai đoạn 2016 - 2020

Bên cạnh các văn bản pháp quy, Trung tâm ứng cứu khẩn cấp máy tính Việt Nam (VNCERT) trực thuộc Bộ Thông tin và Truyền thông sẽ thực hiện chức năng chính điều phối hoạt động ứng cứu sự cố máy tính trên toàn quốc cũng như cảnh báo kịp thời các vấn đề về an toàn mạng máy tính; là đầu mối hợp tác với tổ chức ứng cứu máy tính (CERT) nước ngoài cũng như thúc đẩy hình thành hệ thống các CERT trong các cơ quan, tổ chức và doanh nghiệp. Gần đây nhất, VNCERT đã đưa ra cảnh báo số 232 ngày 30/7/2016 với các chỉ dẫn rất cụ thể để tăng cường kiểm soát bảo đảm an toàn các hệ thống thông tin cho các cơ quan tổ chức. Ngoài việc theo dõi các cảnh báo từ VNCERT, khi xảy ra các sự cố tấn công mạng, các cơ quan báo chí có thể liên hệ trực tiếp với VNCERT để nhận được các hướng dẫn và hỗ trợ. Tuy nhiên, để đảm bảo phòng tránh và xử lý có hiệu quả các sự cố tấn công mạng trong thực tế, tất cả các giải pháp nêu trên chỉ hiệu quả khi các cơ quan nhận thức được tầm quan trọng của an toàn thông tin mạng.

Với tính chất đặc biệt quan trọng của báo chí, tiêu chí bảo đảm an toàn thông tin mạng cần phải được coi trọng trong tổng thể chiến lược của cơ quan báo chí để tránh những hậu quả đáng tiếc có thể xảy ra.

Cao Minh Thắng

Phó Viện trưởng Viện CNTT và Truyền thông CDIT (Học viện Công nghệ Bưu chính Viễn thông)

Link bài viết: https://nguoilambao.vn/khong-chi-la-canh-bao