UBND TỈNH QUẢNG NGÃI
SỞ GIÁO DỤC VÀ ĐÀO TẠO
Số: 228 /SGDĐT-VP
V/v tiếp tục công tác đảm bảo an toàn, an ninh mạng dịp Tết Nguyên đán Giáp Thìn năm 2024 trong ngành giáo dục và đào tạo

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Quảng Ngãi, ngày 26 tháng 01 năm 2024

Kính gửi:
- Phòng Giáo dục và Đào tạo huyện, thị xã, thành phố;
- Trung tâm GDNN - GDTX huyện, thị xã;
- Đơn vị trực thuộc Sở GDĐT.

Trong thời gian gần đây một số trang website bị tấn công, các website có tên miền .gov.vn và .edu.vn đã bị hacker (tin tặc) tấn công kiểu mới, biến thành các trang quảng cáo cho những trang web cờ bạc *(cá độ bóng đá, lô, đề, đánh bài ăn tiền,...)*, để tăng thứ hạng trên google tin tặc nhờ liên kết từ nhiều website của cơ quan nhà nước (tên miền chính phủ .gov.vn hoặc tên miền giáo dục .edu.vn), vì Google ưu tiên tìm kiếm các website có tên miền .gov.vn nên tin tặc cài cắm vào các trang này. Để phòng, chống đảm bảo an toàn thông tin cho các cơ sở giáo dục, Giám đốc Sở Giáo dục và Đào tạo yêu cầu thủ trưởng các đơn vị giáo dục, theo dõi, chỉ đạo bộ phận phụ trách an toàn thông tin một số nội dung sau:

1. Cách nhận biết và phòng chống

website .gov.vn và .edu.vn khi bị tấn công deface kiểu mới, thông thường, các mục tiêu của tấn công deface thường là các tệp tin web mặc định như index.php, index.html, home.html, default.html,... Trong trường hợp này, chỉ cần xử lý các tệp tin này là website có thể hoạt động trở lại bình thường. Đối với những trường hợp khó phát hiện hơn, khi tin tặc không thay đổi nội dung ở các trang web, việc phát hiện sự xâm nhập hệ thống có thể phức tạp hơn.

Để phòng chống các cuộc tấn công thay đổi giao diện, cần quét mã nguồn website, thiết lập giới hạn truy cập, chọn plugin cẩn thận, cài đặt quét website tự động. Chủ sở hữu, quản trị viên website có thể tự kiểm tra các phần mềm độc hại trên website của mình; quét mã nguồn là cách hiệu quả để ngăn chặn tấn công deface.

Ngoài ra, hạn chế số lượng tài khoản admin, hạn chế người dùng tài khoản admin và giới hạn quyền truy cập cho từng tài khoản để giảm nguy cơ tấn công. Đồng thời, lựa chọn plugin và ứng dụng một cách cẩn thận, chỉ sử dụng những cái thực sự cần thiết và thường xuyên kiểm tra, gỡ bỏ các plugin không sử dụng. Đặc biệt, tuyệt đối tránh sử dụng các plugin có tính phí đã bị phá mã bảo vệ và chia sẻ miễn phí (cracked).

2. Khắc phục hậu quả

Có 6 cách chính để khắc phục hậu quả của một cuộc tấn công thay đổi giao diện web. Đó là khắc phục tạm thời, rà soát và xử lý, phân tích và xử lý

thành phần độc hại, xác định và vá lỗ hổng, điều tra nguồn tấn công và đưa website hoạt động lại bình thường.

Cụ thể, ngay khi phát hiện website bị tấn công, cần đổi mật khẩu đăng nhập đủ mạnh *(chữ hoa, chữ thường, chữ số, ký tự đặc biệt, độ dài trên 8 ký tự)* và thông báo tạm thời bảo trì. Sau đó, so sánh các tệp tin với bản sao lưu, sử dụng các câu lệnh như "# dif -qr" hoặc "#md5sum" để xác định tệp tin bị thay đổi.

Tiếp đó, phân tích hành vi của mã độc, khoanh vùng và theo dõi kết nối đến máy chủ (server), sau đó loại bỏ mã độc. Phối hợp với các bộ phận chuyên môn để vá lỗ hổng, cập nhật phiên bản mới cho mã nguồn và các module, plugin.

Khi điều tra nguồn tấn công, tìm thông tin server điều khiển và địa chỉ thực hiện tấn công, phối hợp với cơ quan chức năng để điều tra. Cuối cùng, khôi phục hoạt động website sau khi xử lý xong hậu quả của đợt tấn công.

Tài khoản, mật khẩu đăng nhập phải giao cho cá nhân có trách nhiệm, nếu thay đổi vị trí công tác thì phải bàn giao, người tiếp nhận mới phải thay đổi mật khẩu và chịu trách nhiệm quản lý; không lưu mật khẩu trên các trình duyệt web; không nên sử dụng wifi công cộng để đăng nhập (khuyến cáo dùng 3G, 4G); đối với các tài khoản có chức năng xác thực 2 lớp thì phải cài đặt xác thực 2 lớp.

3. Tiếp tục thực hiện Công văn số 2985/SGDĐT-VP ngày 29/12/2023 của Sở Giáo dục và Đào tạo về việc tăng cường công tác đảm bảo an toàn, an ninh thông tin mạng trong thời gian nghỉ Tết Dương lịch 2024 và Tết Nguyên đán Giáp Thìn trong ngành giáo dục; Công văn số 116/STTTT-BCVT&CNTT ngày 17/01/2024 của Sở Thông tin và Truyền thông về việc tăng cường công tác bảo đảm an toàn, an ninh mạng trong thời gian Tết Nguyên đán Giáp Thìn 2024.

Trong trường hợp cần hỗ trợ xử lý, ứng cứu và khắc phục sự cố đề nghị liên hệ Ông Nguyễn Đức Huân, Phó Chánh văn phòng, Sở Giáo dục và Đào tạo, Điện thoại/Zalo: 0914121856; Email: ndhuan@quangngai.edu.vn ; Ông Trần Văn Thuận, Chuyên viên Văn phòng, Sở Giáo dục và Đào tạo, Điện thoại/Zalo: 0862575279; Email: tvthuan@quangngai.edu.vn

Đề nghị các đơn vị quan tâm triển khai thực hiện, nếu phát sinh vấn đề báo cáo về Văn phòng Sở Giáo dục và Đào tạo để theo dõi, tổng hợp, tham mưu chỉ đạo./.

Nơi nhận:
- Như trên;
- Lãnh đạo Sở GDĐT;
- Các phòng thuộc Sở GDĐT;
- Lưu: VT, VPndh.

GIÁM ĐỐC

Ký bởi: SỞ GIÁO DỤC VÀ ĐÀO TẠO
Thời gian ký: 26/01/2024 15:25:22

CỘNG HÒA X.H.C.N VIỆT NAM
SỞ GIÁO DỤC VÀ ĐÀO TẠO
TỈNH QUẢNG NGÃI

Nguyễn Ngọc Thái