UBND TỈNH HÀ TĨNH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1016 /KH-STTTT

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

Hà Tĩnh, ngày 08 tháng 11 năm 2019.

Ký bởi: Sở Thông tin và Truyền thông
Email: sott_tt@hatinh

KẾ HOẠCH
Triển khai rà quét lỗ hổng bảo mật Cổng, Trang thông tin điện tử của các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh năm 2019

Thực hiện Quyết định số 1354/QĐ-UBND ngày 13/05/2019 của UBND tỉnh về việc phân bổ kinh phí ứng dụng Công nghệ thông tin (CNTT) phục vụ quản lý Nhà nước năm 2019, trong đó nội dung bổ sung trang thiết bị máy chủ và triển khai phần mềm rà quét lỗ hổng bảo mật Cổng, Trang thông tin điện tử (TTĐT) của các cơ quan nhà nước trên địa bàn tỉnh, Sở Thông tin và Truyền thông xây dựng kế hoạch triển khai như sau:

I. CĂN CỨ PHÁP LÝ

- Luật an toàn thông tin mạng số 86/2015/QH13;

- Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ;

- Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng chính phủ về việc nâng cao năng lực phòng, chống phần mềm độc hại;

- Chỉ thị số 14/CT-TTg ngày 07/6/2019 của Thủ tướng Chính phủ về việc tăng cường bảo đảm an toàn, an ninh mạng nhằm cải thiện chỉ số xếp hạng của Việt Nam;

- Chỉ thị số 15/CT-TTg ngày 17/6/2014 của Thủ tướng Chính phủ về tăng cường công tác đảm bảo an ninh và an toàn thông tin mạng trong tình hình mới;

- Quyết định số 05/2017/QĐ-TTg ngày 16/3/2017 của Thủ tướng chính phủ về Ban hành quy định về hệ thống phương án ứng cứu khẩn cấp bảo đảm an toàn thông tin mạng quốc gia;

- Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về bảo đảm an toàn hệ thống thông tin theo cấp độ.

- Thông tư số 121/2018/TT-BTC ngày 12/12/2018 của Bộ Tài chính, Quy định về việc lập dự toán, quản lý, sử dụng và quyết toán kinh phí để thực hiện công tác ứng cứu sự cố, bảo đảm an toàn thông tin mạng.

- Quyết định số 2859/QĐ-UBND ngày 16/9/2013 của UBND tỉnh ban hành Quy chế đảm bảo an toàn thông tin trong quản lý, vận hành và khai thác các hệ thống thông tin của các cơ quan nhà nước trên địa ban tỉnh;

- Chỉ thị số 13/CT-UBND ngày 13/8/2019 của UBND tỉnh về việc tăng

cường bảo đảm an toàn thong tin mạng trong các cơ quan nhà nước trên địa bàn tỉnh Hà Tĩnh;

- Công văn số 4163/UBND-KGVX$_1$ ngày 13/7/2018 của UBND tỉnh về việc thực hiện Chỉ thị số 14/CT-TTg ngày 25/5/2018 của Thủ tướng Chính phủ;

- Kế hoạch số 256/KH-UBND ngày 03/8/2018 về kế hoạch Bảo đảm an toàn thông tin mạng trong hoạt động của cơ quan nhà nước tỉnh Hà Tĩnh giai đoạn 2018-2020;

- Quyết định số 1354/QĐ-UBND ngày 13/05/2019 của UBND tỉnh về việc phân bổ kinh phí ứng dụng CNTT phục vụ quản lý Nhà nước năm 2019.

II. MỤC TIÊU

- Nâng cao năng lực bảo đảm an toàn, an ninh thông tin cho cho tổ thường trực thực hiện nhiệm vụ là đơn vị chuyên trách kỹ thuật ứng cứu sự cố an toàn thông tin mạng trên địa bàn tỉnh;

- Rà soát lỗ hổng, bảo mật Cổng/Trang TTĐT các cơ quan, đơn vị tăng cường công tác bảo mật, tránh lộ lọt thông tin, ngăn chặn tấn công Cổng/Trang TTĐT tại các cơ quan, đơn vị.

- Nâng cao nhận thức và trách nhiệm của các cấp, các ngành và các tổ chức, cá nhân đối với công tác đảm bảo an ninh và an toàn thông tin mạng trên địa bàn tỉnh.

III. NỘI DUNG KẾ HOẠCH

1. Mua sắm thiết bị máy chủ

Mua sắm thêm một máy chủ để triển khai phần mềm rà quét và các phần mềm liên quan đến công tác An toàn thông tin mạng, hỗ trợ xử lý sự cố tại các cơ quan, đơn vị.

Mục đích sử dụng: Cài đặt và triển khai phần mềm rà quét lỗ hổng bảo mật các Cổng/trang thông tin điện tử, phần mềm CSDL chuyên ngành.

Đơn vị sử dụng: Trung tâm Công nghệ thông tin và Truyền thông (Đơn vị Chuyên trách kỹ thuật về an toàn thông tin mạng của tỉnh).

2. Cài đặt phần mềm bản quyền rà quét lỗ hổng bảo mật

- Tên phần mềm: **IBM Security AppScan Standard.**

- Cơ chế rà quét:

Quét ứng dụng web: Định cấu hình AppScan để tự động khám phá và kiểm tra ứng dụng web; Rà quét cấu trúc phần mềm; rà quét các dòng code được viết bởi con người tìm ra lỗi trong các dòng lệnh.

Quét các dịch vụ web: Sử dụng trình duyệt hoặc công cụ dịch vụ web của công cụ kiểm tra bên thứ ba khác để khám phá dịch vụ web của bạn theo cách thủ công (và sau đó để AppScan tự động kiểm tra nó).

Quét bằng ứng dụng khách bên ngoài: Sử dụng thiết bị di động, trình duyệt hoặc ứng dụng khách khác để khám phá ứng dụng hoặc dịch vụ của bạn theo cách thủ công và sau đó để phần mềm AppScan tự động kiểm tra.

- Đơn vị thực hiện: Trung tâm Công nghệ Thông tin và Truyền thông.

3. Triển khai phần mềm rà quét lỗ hổng bảo mật Cổng/Trang thông tin điện tử cho các cơ quan, đơn vị trên địa bàn tỉnh.

*** Công tác rà quét, đánh giá lỗ hổng các phần mềm, Cổng/Trang thông tin điện tử.**

Nội dung: Rà quét tổng thể phần mềm, Cổng/Trang TTĐT, rà quét tất cả các trang con thuộc phần mềm, Cổng/Trang TTĐT, sắp xếp ưu tiên mức độ lỗ hổng theo các mức độ nguy hiểm.

- Giải pháp thực hiện:

+ Xây dựng kịch bản đánh giá, rà quét.

+ Định cấu hình AppScan để kiểm tra ứng dụng web; Rà quét cấu trúc phần mềm; rà quét các dòng code được lập trình để tìm ra lỗ hổng trong các dòng lệnh.

+ Rà soát an toàn mã nguồn tập trung vào việc tìm kiếm các lỗ hổng về: xác thực (Authentication), Phân quyền (Authrization), cấu hình (Configuration), Quản lý phiên (Session Management), ghi nhật ký (Logging), Kiểm tra dữ liệu (Data validation), Xử lý lỗi và ngoài lệ (Error/Excaption handling), Mã hóa (Encryption), Business logic.

+ Rà quét các lỗi về bảo mật dạng **SQL injection; Buffer overflow;** Uncontrolled Format String; **Zero-Day Exploits**; **Cross Site Scripting (XSS); Cross-Site Request Forgery (CSRF)…**

*** Phân tích chi tiết các lỗ hổng**

- Nội dung: Phân tích chi tiết các lỗ hổng, điểm yếu, nguy cơ phát hiện được.

- Giải pháp thực hiện: Thông qua công tác rà quét, tổng hợp lỗ hổng của phần mềm, quá trình phân tích chi tiết của lỗ hổng, điểm yếu, câu lệnh bị lỗi.

- Sắp xếp ưu tiên mức độ lỗ hổng, lỗi theo các mức độ nguy hiểm

*** Xây dựng báo cáo kết quả rà quét lần 1**

- Báo cáo kết quả kiểm tra đánh giá ATTT bao gồm các nội dung:

- Mô tả chi tiết các lỗi gặp phải.
- Phân loại mức độ nghiêm trọng các lỗi phát hiện.
- Bằng chứng các lỗi.
- Khuyến nghị khắc phục các lỗ hổng được phát hiện

Cảnh báo tới các đơn vị, yêu cầu các đơn vị phối hợp với các chuyên gia, các nhà viết phần mềm, phát triển Cổng/ Trang TTĐT của các đơn vị để thực hiện khắc phục các lỗ hổng, lỗi đã được phát hiện, có thời hạn báo cáo kết quả khắc phục lỗi của các đơn vị.

*** Công tác rà quét, kiểm tra khắc phục lỗ hổng các phần mềm, Cổng/Trang thông tin điện tử của các đơn vị.**

Nội dung: Rà quét lần 2, kiểm tra việc khắc phục của các Cổng/Trang TTĐT của các đơn vị đã được cảnh báo.

Rà quét tổng thể phần mềm, Cổng/Trang TTĐT, rà quét tất cả các trang con thuộc phần mềm.

- Giải pháp thực hiện:

+ Định cấu hình AppScan để khám phá và kiểm tra ứng dụng web; Rà quét cấu trúc phần mềm; rà quét các dòng code được viết bởi con người tìm ra lỗi trong các dòng lệnh, tìm các lỗi phát sinh sau quá trình sửa lỗi của các đơn vị.

+ Rà soát an toàn mã nguồn tập trung vào việc tìm kiếm các lỗ hổng về: xác thực (Authentication), Phân quyền (Authrization), cấu hình (Configuration), Quản lý phiên (Session Management), ghi nhật ký (Logging), Kiểm tra dữ liệu (Data validation), Xử lý lỗi và ngoài lệ (Error/Excaption handling), Mã hóa (Encryption), Business logic; Các lỗi đã được cảnh báo qua lần rà quét thứ nhất.

+ Rà quét các lỗi về bảo mật dạng **SQL injection; Buffer overflow;** Uncontrolled Format String; **Zero-Day Exploits**; **Cross Site Scripting (XSS); Cross-Site Request Forgery (CSRF)…**

*** Xây dựng báo cáo kết quả rà quét lần 2**

+ Báo cáo kết quả kiểm tra đánh giá sau khi các đơn vị đã triển khai sửa lỗi, bao gồm các nội dung:

- Mô tả chi tiết các lỗi gặp phải.
- Phân loại mức độ nghiêm trọng các lỗi phát hiện.
- Bằng chứng các lỗi.
- Đánh giá mức độ khắc phục, sửa lỗi của các đơn vị.

+ Tổng hợp kết quả, thông báo về các đơn vị.

- Đơn vị thực hiện: Trung tâm Công nghệ Thông tin và Truyền thông.

- Đơn vị phối hợp: Phòng Công nghệ thông tin.

3. Thời gian, tiến độ thực hiện trong năm 2019

- Thời gian: Triển khai thực hiện trong quý IV năm 2019

- Tiến độ:

Tổ chức rà quét cho 13 đơn vị đã xây dựng mới hoặc nâng cấp Cổng TTĐT năm 2018 - 2019:

1	Sở Y tế	http://soyte.hatinh.gov.vn/
2	Sở Tài chính.	http://sotaichinh.hatinh.gov.vn/
3	Sở GTVT	http://sogtvt.hatinh.gov.vn/
4	Sở Nội vụ.	http://sonoivu.hatinh.gov.vn
5	Sở Tư Pháp	http://tuphap.hatinh.gov.vn
6	Sở LĐ TBXH	http://ldtbxh.hatinh.gov.vn/
7	Sở NNPTNT	http://sonongnghiep.hatinh.gov.vn/

8	UBND huyện Thạch Hà.	http://thachha.hatinh.gov.vn/
9	UBND TX Hồng Lĩnh	http://honglinh.hatinh.gov.vn
10	UBND huyện Đức Thọ	http://ductho.hatinh.gov.vn/
11	UBND huyện Lộc Hà	http://locha.hatinh.gov.vn/
12	UBND huyện Can Lộc	http://canloc.hatinh.gov.vn/
13	UBND huyện Hương Sơn	http://huongson.hatinh.gov.vn

III. KINH PHÍ

Nguồn kinh phí kinh phí ứng dụng CNTT phục vụ quản lý Nhà nước năm 2019 tại quyết định số 1354/QĐ-UBND ngày 13/5/2019 của UBND tỉnh.

1. Chi phí mua sắm Máy chủ: 89.400.000 Đ

2. Chi phí rà quét, đánh giá lỗ hổng (13 đơn vị): 210.600.000 Đ

3. Tổng Cộng (1+2): 300.000.000 Đ

Bằng chữ: Ba trăm triệu đồng chẵn.

(Có Thẩm định giá kèm theo).

IV. TỔ CHỨC THỰC HIỆN

1. Trung tâm Công nghệ thông tin và Truyền thông

- Chủ trì triển khai thực hiện kế hoạch, đồng thời phối hợp, hướng dẫn các đơn vị trong việc triển khai các nội dung, hạng mục theo kế hoạch đề ra.

- Phối hợp với Văn phòng sở hoàn thiện hồ sơ thanh quyết toán kinh phí và báo cáo kết quả về Sở theo quy định hiện hành.

2. Phòng Công nghệ thông tin

Đôn đốc, hướng dẫn và giám sát Trung tâm CNTT và Truyền thông triển khai thực hiện kế hoạch.

3. Văn phòng Sở

Phối hợp với Trung tâm CNTT và Truyền thông kiểm tra, thẩm định dự toán, thanh quyết toán và giám sát quá trình triển khai kế hoạch.

4. Đề nghị các sở, ban, ngành; UBND các huyện, thành phố, thị xã

Phối hợp với Phòng Công nghệ thông tin, Trung tâm CNTT và Truyền thông triển khai các nội dung rà quét đã được phân công tại kế hoạch./.

Nơi nhận:
- UBND tỉnh (để b/c);
- Các sở, ban, ngành, cấp tỉnh;
- UBND các huyện, TX, TP;
- Lãnh đạo Sở;
- Đội Ứng cứu sự cố ATTT mạng tỉnh;
- P.CNTT, VP Sở, TTCNTT;
- Lưu: VT, $CNTT_2$, $TTCNTT_2$.

KT. GIÁM ĐỐC
PHÓ GIÁM ĐỐC

(Đã ký)

Bùi Đắc Thế