ỦY BAN NHÂN DÂN TỈNH LÀO CAI	CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM Độc lập - Tự do - Hạnh phúc
Số: 1829/QĐ-UBND	*Lào Cai, ngày 19 tháng 08 năm 2022*

QUYẾT ĐỊNH
Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống Thư điện tử công vụ tỉnh Lào Cai

CHỦ TỊCH ỦY BAN NHÂN DÂN TỈNH LÀO CAI

Căn cứ Luật Tổ chức chính quyền địa phương ngày 19/6/2015; Luật sửa đổi, bổ sung một số điều của Luật Tổ chức Chính phủ và Luật Tổ chức chính quyền địa phương ngày 22/11/2019;

Căn cứ Luật An toàn thông tin mạng ngày 19/11/2015;

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

Căn cứ Thông tư số 03/2017/TT-BTTTT ngày 24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của 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;

Theo đề nghị của Giám đốc Sở Thông tin và Truyền thông tại Tờ trình số 50/TTr-STTTT ngày 13/5/2022.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt cấp độ an toàn hệ thống thông tin đối với Hệ thống thư điện tử công vụ tỉnh Lào Cai, cụ thể như sau:

1. Thông tin chung

a) Tên hệ thống thông tin: Hệ thống thư điện tử công vụ tỉnh Lào Cai.

b) Đơn vị vận hành hệ thống thông tin: Trung tâm Công nghệ thông tin và Truyền thông Lào Cai.

c) Địa chỉ: Đại lộ Trần Hưng Đạo, phường Nam Cường, thành phố Lào Cai, tỉnh Lào Cai.

2. Cấp độ an toàn hệ thống thông tin: Cấp độ 3.

3. Phương án bảo đảm an toàn thông tin trong thiết kế kỹ thuật và vận hành hệ thống thư điện tử công vụ tương ứng với cấp độ 3, phù hợp với quy định tại 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 số 85/2016/NĐ-

CP và với Tiêu chuẩn quốc gia TCVN 11930:2017 về công nghệ thông tin - các kỹ thuật an toàn - yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

(Có phương án đảm bảo an toàn thông tin kèm theo)

Điều 2. Tổ chức thực hiện

1. Trung tâm Công nghệ thông tin và Truyền thông Lào Cai chịu trách nhiệm bảo đảm an toàn thông tin cho Hệ thống thư điện tử công vụ tỉnh Lào Cai theo các quy định tại Điều 22 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.

2. Sở Thông tin và Truyền thông chủ trì, phối hợp với các cơ quan liên quan chịu trách nhiệm kiểm tra, giám sát việc bảo đảm an toàn hệ thống thông tin cho Hệ thống thư điện tử công vụ tỉnh Lào Cai theo quy định.

Điều 3. Quyết định này có hiệu lực kể từ ngày ký ban hành.

Chánh Văn phòng UBND tỉnh, Giám đốc Sở Thông tin và Truyền thông, Thủ trưởng các sở, ban, ngành thuộc UBND tỉnh, Chủ tịch UBND các huyện, thị xã, thành phố và các cơ quan, đơn vị liên quan căn cứ Quyết định thi hành./.

Nơi nhận:
- Như Điều 3 (QĐ);
- TT UBND tỉnh;
- CVP, PCVP2;
- Cổng TTĐT tỉnh;
- Lưu: VT, TH1, TCHC, KSTT, VX1.

CHỦ TỊCH

ỦY BAN NHÂN DÂN TỈNH LÀO CAI

Trịnh Xuân Trường

PHƯƠNG ÁN ĐẢM BẢO AN TOÀN HỆ THỐNG THÔNG TIN HỆ THỐNG THƯ ĐIỆN TỬ CÔNG VỤ TỈNH LÀO CAI

(Kèm theo Quyết định số /QĐ-UBND ngày / /2022 của Chủ tịch UBND tỉnh Lào Cai)

1. Bảo đảm an toàn mạng

a) Thiết kế hệ thống

- Hệ thống ứng dụng được thiết kế tách biệt với các hệ thống dịch vụ khác. Việc phân các vùng chức năng được thực hiện trên Firewall Fortigate 600E.

- Mỗi vùng được chia vào các VLAN riêng, bao gồm:

+ Vùng máy chủ, dữ liệu (APP);

+ Vùng DMZ;

+ Vùng quản trị MNGT;

+ Để truy cập được vào hệ thống dịch vụ cần thông qua hệ thống VPN.

- Phương án thiết kế bảo đảm các yêu cầu sau:

+ Hệ thống có phương án quản lý truy cập, quản trị từ xa an toàn thông qua VPN. Để truy cập quản trị và truy cập từ xa đến hệ thống ứng dụng cần truy cập thông qua VPN của tỉnh.

+ Các server và thiết bị như Switch, Firewall trong hệ thống đều có một cặp chạy chế độ dự phòng cho nhau.

+ Firewall Fortigate 600E, Fortimail 200F có khả năng phòng chống tấn công từ chối dịch vụ.

+ Toàn bộ hệ thống được triển khai giám sát tập trung bằng hệ thống SOC.

+ Thực hiện việc sao lưu dự phòng tập trung tại Trung tâm mạng trên thiết bị chuyên dụng SAN/NAS và ổ cứng di động.

+ Hệ thống triển khai giải pháp quản lý và phòng chống mã độc trên máy chủ bằng giải pháp Kaspersky Endpoint tập trung.

+ Có 4 đường truyền riêng biệt của VNPT và Viettel triển khai cho hệ thống được kết nối qua hệ thống cân bằng tải chuyên dụng.

+ Thực hiện phân quyền và quản lý tài khoản theo chính sách của Trung tâm mạng.

b) Kiểm soát truy cập từ bên ngoài mạng

- Hệ thống được triển khai trên vùng mạng riêng biệt. Để truy cập được từ bên ngoài đến hệ thống cần kết nối qua hệ thống VPN. Thời gian chờ (timeout) thiết lập là 30 phút trên mỗi phiên kết nối.

- Hệ thống chặn tất cả truy cập từ bên ngoài mạng Internet, chỉ mở các IP mà Trung tâm mạng cung cấp.

- Thiết lập giới hạn số lần kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng trên thiết bị Firewall Fortigate 600E.

c) Kiểm soát truy cập từ bên trong mạng

Không truy cập được vào hệ thống máy chủ nội bộ. Hệ thống dich vụ chỉ được truy cập từ phía Trung tâm mạng. Không cho phép các máy chủ truy cập ra các mạng bên ngoài.

d) Nhật ký hệ thống

Có thiết lập đầy đủ các chức năng ghi nhật lý hệ thống trên các thiết bị Firewall và các Server. Nhật ký của hệ thống được lưu trữ riêng. Hệ thống được lưu trữ 03 tháng.

đ) Phòng chống xâm nhập

- Sử dụng tính năng phòng chống xâm nhập trên Firewall Fortigate 600E. Trên thiết bị Firewall có thiết lập chức năng (license) IDS, IPS (phòng chống xâm nhập). Thiết lập chế độ cập nhập tự động trên thiết bị Firewall.

- Áp dụng các công nghệ dựa theo cơ sở dữ liệu về thông tin nhận diện (Signature), Heuristic và phân tích hành vi trên Firewall Fortimail 200F.

e) Phòng chống phần mềm độc hại trên môi trường mạng

- Sử dụng tính năng IDS & IPS trên Firewall Fortigate 600E. Thiết lập chế độ cập nhập tự động trên thiết bị Firewall.

- Sử dụng giải pháp phòng chống phần mềm độc hại của Kaspersky Endpoint. Thiết lập chế độ tự động cập nhập cơ sở dữ liệu tập trung trên giải pháp Kaspersky.

g) Bảo vệ thiết bị hệ thống

- Thực hiện định kỳ hàng tháng rà soát các điểm yếu, các sự kiện về an ninh, thông tin từ nhà cung cấp để cập nhập xử lý điểm yếu an toàn thông tin của thiết bị hệ thống.

- Các thiết bị khi không được sử dụng đều được xóa bỏ toàn bộ thông tin về cấu hình, dữ liệu và cài đặt lại.

2. Bảo đảm an toàn máy chủ

a) Xác thực:

- Thiết lập chính sách xác thực trên máy chủ bằng cơ chế Username / Password. Thực hiện thiết lập cấu hình các máy chủ để đảm bảo mật khẩu an toàn theo chính sách quản lý của Trung tâm mạng:

+ Yêu cầu thay đổi mật khẩu mặc định;

+ Quy tắc đặt mật khẩu gồm các thành phần thường, hoa, chữ số, ký tự đặc biệt;

+ Đăng nhập hệ thống sai 5 lần trong khoảng thời gian nhất định với một tài khoản nhất định tài khoản đó sẽ bị khóa;

+ Thời gian yêu cầu mật khẩu 30 ngày.

b) Kiểm soát truy cập

- Đã thiết lập các truy cập quản trị máy chủ từ xa chỉ được thực hiện thông qua hệ thống VPN. Thiết lập thời gian chờ (timeout = 300 phút), nếu không có thao tác từ người dùng thì hệ máy chủ sẽ đóng phiên kết nối.

- Quản trị thông qua Remote desktop. Không cho phép quản trị trực tiếp từ bên ngoài. Phân quyền truy cập cho các tài khoản qua hệ thống VPN của Trung tâm mạng.

c) Nhật ký hệ thống

Thiết lập ghi cấu hình log mặc định trên các máy chủ bao gồm:

+ Nhật ký truy cập;

+ Nhật ký về các sự kiện;

+ Nhật ký kết nối;

+ Nhật ký về thay đổi cấu hình;

+ Nhật ký cài đặt.

d) Phòng chống xâm nhập

- Các thiết bị máy chủ được cài đặt hệ điều hành mới. Đã rà soát và loại bỏ các tài khoản mặc định của máy chủ.

- Tất cả các máy chủ đều sử dụng tường lửa và phần mềm Kapersky Enpoint để cấm các truy cập trái phép tới máy chủ.

- Thực hiện định kỳ hàng tháng rà soát các điểm yếu, các sự kiện về an ninh, thông tin từ nhà cung cấp để cập nhập xử lý điểm yếu an toàn thông tin của máy chủ hệ thống.

đ) Phòng chống phần mềm độc hại

- Tất cả các máy chủ đều được cài đặt phần mềm phòng chống mã độc Kaspersky Endpoint.

- Không cho phép phương tiện lưu trữ di động kết nối tới máy chủ trong quá trình hoạt động.

- Các phần mềm trước khi cài đặt được kiểm tra bởi phòng Tích hợp hệ thống.

e) Xử lý máy chủ khi chuyển giao

- Khi chuyển giao hệ thống toàn bộ dữ liệu sẽ được xóa sạch thông tin, xóa cấu hình RAID, thay đổi thứ tự ổ cứng của máy chủ.

- Thực hiện GHOST máy chủ trước khi xóa. Luôn có 1 bản backup máy chủ dự phòng tránh trướng hợp cần khôi phục lại máy chủ sau khi xóa.

3. Bảo đảm an toàn ứng dụng

a) Xác thực

- Không sử dụng tài khoản, mật khẩu mặc định để đăng nhập ứng dụng. Khi khởi tạo tài khoản ứng dụng có gửi thông báo cho người sử dụng về việc đổi mật khẩu mới và đảm bảo tính bí mật của tài khoản người sử dụng.

- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự trong cấu hình hệ thống. Thiết lập thời gian yêu cầu thay đổi mật khẩu.

- Hệ thống Firewall Fortimail 200F để tránh đăng nhập tự động. Cung cấp khả năng chống spam và chống phần mềm độc hại, email quảng cáo và phân loại email.

b) Kiểm soát truy cập

Hệ thống có thể thiết lập cho phép truy cập qua mạng an toàn, VPN trên thiết bị Firewall Fortigate 600E. Hệ thống cho phép giới hạn truy cập theo số lượng kết nối ở nhiều mức như ứng dụng, cơ sở dữ liệu. Sử dụng các tham số cấu hình để quy định số lượng kết nối đồng thời.

c) Nhật ký hệ thống

Nhật ký hệ thống được quản lý trên máy chủ ứng dụng và cơ sở dữ liệu. Có thiết lập việc ghi nhật ký ứng dụng gồm các thông tin:

- Thông tin truy cập được lưu trên máy chủ và cơ sở dữ liệu;

- Thông tin đăng nhập khi quản trị được lưu trên máy chủ và cơ sở dữ liệu;

- Thông tin lỗi được lưu trên máy chủ ứng dụng.

d) Bảo mật thông tin liên lạc:

Dữ liệu được truyền trên đường truyền số liệu chuyên dùng.

đ) An toàn ứng dụng và mã nguồn

- Giao diện thao tác có kiểm tra dữ liệu đầu vào do người dùng nhập. Dữ liệu trả về được kiểm tra trước khi hiển thị cho người dùng, các thông báo lỗi được tùy biến phù hợp với ngữ cảnh sử dụng.

- Mã nguồn được kiểm tra định kỳ đảm bảo an toàn trước các dạng tấn công phổ biến.

4. Bảo đảm an toàn dữ liệu

a) Nguyên vẹn dữ liệu

- Hệ quản trị CSDL cho phép tạo các vai trò quản trị đi kèm với mật khẩu quản trị đối với cơ sở dữ liệu. Muốn truy nhập trực tiếp vào cơ sở dữ liệu của hệ thống thông tin bằng các công cụ của hệ quản trị cơ sở dữ liệu không thông qua phần mềm phải có tên đăng nhập và mật khẩu của người quản trị cơ sở dữ liệu.

- Các thay đổi trong cơ sở dữ liệu được lưu ghi nhận và được lưu trự tại hệ thống log tập trung.

- Cơ sở dữ liệu được backup full vào cuối tuần.

b) Bảo mật dữ liệu

- Toàn bộ các dữ liệu quan trọng lưu trữ trong CSDL được mã hóa và phân quyền truy cập chặt chẽ.

- Hệ thống thực hiện phân quyền truy cập OS theo role người dùng; với dữ liệu hiển thị trên web được mã hóa một số trường thông tin quan trọng và phân quyền theo người dùng đăng nhập website.

c) *Sao lưu dự phòng*

Thực hiện backup các máy chủ sang thiết bị lưu trữ dữ liệu SAN/NAS và các ở cứng di động riêng biệt

5. Đảm bảo an toàn vật lý cho phòng hệ thống

- Vị trí phòng máy chủ phải được đặt ở trung tâm tòa nhà.

- Thiết lập hệ thống cổng điện tử để kiểm soát vào, ra phòng máy chủ.

- Thiết lập hệ thống camera giám sát, ghi lại thông tin vào ra phòng máy chủ. Dữ liệu nhật ký camera phải được lưu trữ tối thiểu 03 tháng.

- Có phương án kiểm soát các thiết bị, vật dụng được mang ra, vào phòng máy chủ.

- Thiết bị hệ thống phải được đặt trong phòng máy chủ và có tủ bảo vệ (tủ rack), được đặt cố định.

- Kết nối vật lý (cáp mạng, điện thoại,…) trong phòng phải được đi trên máng cáp; Thiết lập hệ thống báo động chống trộm tự động.

- Phòng máy chủ phải được thiết lập hệ thống chống sét. Các thiết bị, tủ kỹ thuật trong phòng máy chủ phải được nối đất.

- Phòng máy chủ phải lắp đặt hệ thống cảnh báo và chữa cháy tự động; Phòng máy chủ phải được xây dựng sử dụng các vật liệu chịu lửa.

- Có biện pháp ngăn không cho nước mưa thấm qua trần và tường vào phòng máy, tích tụ nước và di chuyển nước tích tụ trong phòng máy.

- Có hệ thống điều hòa trung tâm, bảo đảm về nhiệt độ, độ ẩm ổn định trong phòng máy chủ.

- Nguồn điện trong phòng máy chủ phải được đảm bảo ổn định UPS, chống quá tải; hệ thống UPS đảm bảo hoạt động liên tục.

- Có nguồn cung cấp điện dự phòng, máy phát điện để có thể thay thế nguồn cung cấp điện chính khi có sự cố mất điện xảy ra./.