Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu:

- Tên gói thầu: Gói thầu số 02: Thuê đơn vị kiểm tra đánh giá an toàn thông tin đối với hệ thống thông tin cấp độ 3 của thành phố Hải Phòng.

- Dự toán: Thuê đơn vị kiểm tra đánh giá an toàn thông tin đối với hệ thống thông tin cấp độ 3 của thành phố Hải Phòng.

- Chủ đầu tư: Công an thành phố Hải Phòng.

- Nguồn vốn: Kinh phí địa phương cấp năm 2025.

- Hình thức lựa chọn nhà thầu: Chào hàng cạnh tranh trong nước, qua mạng.

- Phương thức đấu thầu: Một giai đoạn, một túi hồ sơ.

- Thời gian bắt đầu tổ chức lựa chọn nhà thầu: Quý IV năm 2025.

- Loại hợp đồng: Trọn gói.

- Thời gian thực hiện hợp đồng: 20 ngày

2. Mục tiêu công việc:

Nhà thầu phải hoàn thiện kiểm tra đánh giá an toàn thông tin đối với hệ thống thông tin cấp độ 3 của thành phố Hải Phòng.

Nội dung dịch vụ đánh giá, kiểm tra, rà quét an toàn thông tin đối với hệ thống thông tin đạt cấp độ 3 của thành phố.

TT	Nội dung	Số lượng	Thời gian thực hiện	Số hệ thống	Đơn vị tính
I	**Chuyên gia thực hiện đánh đảm bảo an toàn thông tin cho 02 hệ thống thông tin cấp độ 3**				
1	Khảo sát thông tin chung: - Thông tin chung về đối tượng đánh giá: Tên đối tượng, mục đích sử dụng, mô tả về đối tượng cần đánh giá. - Thu thập thông tin về đơn vị chủ quản và vận hành: tổ chức, người dùng ứng dụng, cơ cấu tổ chức, đơn vị/cá nhân vận hành, năng lực,… - Thông tin về các chính sách an toàn thông tin; bảo vệ hệ thống,...	3	2	2	người/hệ thống/ngày

TT	Nội dung	Số lượng	Thời gian thực hiện	Số hệ thống	Đơn vị tính
	- Các biện pháp bảo đảm an toàn thông tin và bảo đảm hoạt động hiện có của hệ thống *(3 người * 2 ngày * 2 hệ thống)*				
2	Khảo sát thông tin về hệ thống - Thu thập thông tin public với mạng Internet: về danh sách tên miền, danh sách địa chỉ ip public ra mạng Internet, máy chủ webserver, máy chủ Proxy v.v.... - Mô hình kết nối chung của hệ thống - Thu thập thông tin nền tảng hệ thống cần đánh giá: Hệ điều hành, máy chủ Web, các cổng dịch vụ đang chạy, công nghệ phát triển, đơn vị phát triển v.v... - Hệ thống máy chủ hạ tầng phục vụ hệ thống: Danh sách các máy chủ; loại máy chủ (vật lý; ảo; cloud); chức năng của máy chủ; địa chỉ IP của máy chủ. (3 người * 3 ngày * 2 hệ thống)	3	3	2	người/ngày
3	Kiểm tra, đánh giá triển khai phương án quản lý đối với HTTT (3 người * 12 ngày * 02 hệ thống)	3	12	2	Người/ngày
4	Kiểm tra, đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt (3 người * 5 ngày * 2 hệ thống)	3	5	2	Người/ngày
5	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn mạng (3 người * 10 ngày * 2 hệ thống)	3	10	2	Người/ngày
6	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn máy chủ (3 người * 10 ngày * 2 hệ thống)	3	10	2	Người/ngày
7	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn ứng dụng (3 người * 8 ngày * 2 hệ thống)	3	8	2	Người/ngày

TT	Nội dung	Số lượng	Thời gian thực hiện	Số hệ thống	Đơn vị tính
8	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn dữ liệu (3 người * 5 ngày * 2 hệ thống)	3	5	2	Người/ngày
9	Tổng hợp, hoàn thiện báo cáo đánh giá (3 người * 5 ngày * 2 hệ thống)	3	5	2	Người/ngày
II	**Chuyên gia thực hiện rà quét lỗ hổng, điểm yếu, săn lùng mối nguy hại trong hệ thống**				
1	Thực hiện rà quét, lỗ hổng điểm yếu cho ứng dụng, thiết bị trong hệ thống thông tin (5 người * 20 ngày)	5	20		Người/ngày
2	Thực hiện kiểm tra, rà quét phát hiện các nguy cơ từ các ứng dụng, dịch vụ trên internet, các nguy cơ từ bên ngoài (5 người * 9 ngày)	5	9		Người/ngày
3	Thực hiện kiểm tra, rà quét phát hiện nguy cơ trong mạng nội bộ (5 người *9 ngày)	5	9		Người/ngày
4	Tư vấn các biện pháp khắc phục: xác định các biện pháp khắc phục thích hợp cho các sự cố bảo mật và xác định mức độ ưu tiên để xử lý các sự cố bảo mật nghiêm trọng. (5 người * 7 ngày)	5	7		Người/ngày
5	Rà soát, kiểm tra lại hệ thống sau khi thực hiện các biện pháp khắc phục (5 người * 10 ngày)	5	10		Người/ngày
6	Tổng hợp, hoàn thiện báo cáo chi tiết (5 người * 5 ngày)	5	5		Người/ngày
III	**Công tác phí cho chuyên gia thực hiện nhiệm vụ**				
1	**Chuyên gia thực hiện đánh giá phương án bảo đảm an toàn thông tin đi khảo sát hệ thống (3 chuyên gia/hệ thống*2 hệ thống)**				

TT	Nội dung	Số lượng	Thời gian thực hiện	Số hệ thống	Đơn vị tính
1.1	Chi phí đi lại (6 người * 5 ngày)	30			Người/ngày
1.2	Tiền phòng nghỉ (6 người * 5 ngày)	30			Người/ngày
1.3	Chi tiền ăn (6 người * 5 ngày)	30			Người/ngày
2	**Chuyên gia thực hiện kiểm tra, rà quét phát hiện nguy cơ trong mạng nội bộ**				
2.1	Chi phí đi lại (6 người * 9 ngày)	45			Người/ngày
2.2	Tiền phòng nghỉ (6 người * 9 ngày)	45			Người/ngày
2.3	Chi tiền ăn (6 người * 9 ngày)	45			Người/ngày
IV	**Thuê phần mềm phục vụ đánh giá (bao gồm cài đặt, thiết lập cấu hình)**				
1	Phần mềm đánh giá lỗ hổng bảo mật cho hệ thống máy chủ, máy trạm (Phần mềm Nesus hoặc tương đương)	1			gói
2	Công cụ hỗ trợ khai thác, tấn công lỗ hổng an toàn thông tin (Phần mềm Burpsuite hoặc tương đương)	1			gói
3	Phần mềm đánh giá an ninh ứng dụng (Phần mềm Acunetix hoặc tương đương)	1			gói
4	Máy chủ	1			gói

3. Yêu cầu kỹ thuật của gói thầu:

Các nội dung thuộc phạm vi cung cấp của gói thầu phải đáp ứng những yêu cầu kỹ thuật cụ thể như sau:

3.1. Nội dung kiểm tra

Việc thuê dịch vụ kiểm tra, đánh giá an toàn thông tin đối với 02 hệ thống thông tin cấp độ 3 của thành phố Hải Phòng nhằm có cái nhìn toàn diện hơn về các mối nguy hại tồn tại trong hệ thống, có các giải pháp khắc phục những lỗ hổng bảo mật thông tin do sai sót trong quá trình cấu hình, lập trình, vận hành và giảm

thiểu được các rủi ro bảo mật thông tin có thể bị khai thác trên các thiết bị và ứng dụng gây hại cho hệ thống thông tin trọng yêu.

3.2. Quy mô kiểm tra:

Thuê kiểm tra, đánh giá rủi ro an toàn thông tin đối với 2 hệ thống thông tin cấp độ 3 của thành phố Hải Phòng:

- Hệ thống thông tin giải quyết hành chính thành phố

- Hệ thống thông tin điện tử thành phố

Phạm vi thực hiện: Kiểm tra đánh giá an toàn thông tin mạng đối với hạ tầng mạng, hạ tầng máy chủ, ứng dụng của 02 hệ thống thông tin cấp độ 3 của thành phố Hải Phòng.

3.3. Yêu cầu đối với dịch vụ đánh giá, kiểm tra, rà quét an toàn thông tin:

Dịch vụ đánh giá, kiểm tra, rà quét an toàn thông tin đối với hệ thống thông tin cấp độ 3 bao gồm các nội dung sau:

I	**Thực hiện kiêm tra, đánh giá phương án đảm bảo an toàn thông tin đôi với hệ thông thông tin cập độ 3**
1	Khảo sát thông tin chung: - Thông tin chung về đối tượng đánh giá: Tên đối tượng, mục đích sử dụng, mô tả về đối tượng cần đánh giá. - Thu thập thông tin về đơn vị chủ quản và vận hành: tổ chức, người dùng ứng dụng, cơ cấu tổ chức, đơn vị/cá nhân vận hành, năng lực,... - Thông tin về các chính sách an toàn thông tin; bảo vệ hệ thống,... Các biện pháp bảo đảm an toàn thông tin và bảo đảm hoạt động hiện có của hệ thống
2	Khảo sát thông tin về hệ thống - Thu thập thông tin public với mạng Internet: về danh sách tên miền, danh sách địa chỉ ip public ra mạng Internet, máy chủ webserver, máy chủ Proxy v.v... - Mô hình kết nối chung của hệ thống - Thu thập thông tin nền tảng hệ thống cần đánh giá: Hệ điều hành, máy chủ Web, các cổng dịch vụ đang chạy, công nghệ phát triển, đơn vị phát triển v.v... - Hệ thống máy chủ hạ tầng phục vụ hệ thống: Danh sách các máy chủ; loại máy chủ (vật lý; ảo; cloud); chức năng của máy chủ; địa chỉ IP của máy chủ

3	Kiểm tra, đánh giá triển khai phương án quản lý đối với HTTT: - Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý - Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin - Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin
4	Kiểm tra, đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin được phê duyệt
5	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn mạng
6	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn máy chủ
7	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn ứng dụng
8	Kiểm tra, đánh giá các tiêu chí bảo đảm an toàn dữ liệu
9	Tổng hợp, hoàn thiện báo cáo đánh giá
II	**Dịch vụ rà quét lỗ hổng, điểm yếu, săn lùng mối nguy hại trong hệ thống**
1	Thực hiện kiểm tra, đánh giá, rà quét lỗ hổng an toàn bảo mật trên các ứng dụng, thiết bị trong hệ thống thông tin.
2	Thực hiện kiểm tra, rà quét phát hiện các nguy cơ từ các ứng dụng, dịch vụ trên internet, các nguy cơ từ bên ngoài
3	Thực hiện kiểm tra, rà quét phát hiện nguy cơ trong mạng nội bộ.
4	Tư vấn các biện pháp khắc phục: xác định các biện pháp khắc phục thích hợp cho các sự cố bảo mật và xác định mức độ ưu tiên để xử lý các sự cố bảo mật nghiêm trọng
5	Thực hiện rà soát, kiểm tra, đánh giá lại hệ thống sau khi thực hiện các biện pháp khắc phục.
6	Tổng hợp, hoàn thiện báo cáo kiểm tra, đánh giá chi tiết

3.4. Yêu cầu về phạm vi đánh giá, kiểm tra, rà quét an toàn thông tin:

Triển khai đánh giá, kiểm tra an toàn thông tin cho 2 hệ thống quan trọng của thành phố Hải Phòng, bao gồm:

- Hệ thống thông tin giải quyết hành chính thành phố.
- Hệ thống thông tin điện tử thành phố.

3.5. Các yêu cầu về dịch vụ:

Thực hiện kiểm tra, đánh giá phương án đảm bảo an toàn thông tin đối với hệ thống thông tin cấp độ 3.

3.1. Khảo sát thông tin hệ thống thông tin cần thực hiện đánh giá:

* Khảo sát thông tin chung:

- Thông tin chung về đối tượng đánh giá: Tên đối tượng, mục đích sử dụng, mô tả về đối tượng cần đánh giá.
- Thu thập thông tin về đơn vị chủ quản và vận hành: tổ chức, người dùng ứng dụng, cơ cấu tổ chức, đơn vị/cá nhân vận hành, năng lực,...
- Thông tin về các chính sách an toàn thông tin; bảo vệ hệ thống,...
- Các biện pháp bảo đảm an toàn thông tin và bảo đảm hoạt động hiện có của hệ thống.

* Khảo sát thông tin về hệ thống

- Thu thập thông tin public với mạng Internet: về danh sách tên miền, danh sách địa chỉ ip public ra mạng Internet, máy chủ webserver, máy chủ Proxy v.v...
- Mô hình kết nối chung của hệ thống
- Thu thập thông tin nền tảng hệ thống cần đánh giá: Hệ điều hành, máy chủ Web, các cổng dịch vụ đang chạy, công nghệ phát triển, đơn vị phát triển v.v...

Hệ thống máy chủ hạ tầng phục vụ hệ thống: Danh sách các máy chủ; loại máy chủ (vật lý; ảo; cloud); chức năng của máy chủ; địa chỉ IP của máy chủ.

3.2. Kiểm tra, đánh giá triển khai phương án quản lý đối với HTTT

a. Kiểm tra tính đầy đủ và phù hợp của Quy chế bảo đảm an toàn thông tin theo phương án bảo đảm an toàn thông tin về quản lý được phê duyệt:

- Các quy định trong Quy chế: (1) Thiết lập chính sách an toàn thông tin; (2) Tổ chức bảo đảm an toàn thông tin; (3) Bảo đảm nguồn nhân lực; (4) Quản

lý thiết kế, xây dựng hệ thống; (5) Quản lý vận hành hệ thống;

- Các quy trình kèm theo Quy chế: (1) Quy trình tuyển dụng cán bộ; (2) Quy trình chấm dứt hoặc thay đổi công việc; (3) Quy trình thử nghiệm và nghiệm thu hệ thống; (4) Quản lý an toàn mạng; (5) Quản lý an toàn máy chủ và ứng dụng; (6) Quản lý an toàn dữ liệu; (7) Quản lý an toàn thiết bị đầu cuối; (8) Quản lý phòng chống phần mềm độc hại; (9) Quản lý giám sát an toàn hệ thống thông tin; (10) Quản lý điểm yếu an toàn thông tin; (11) Quản lý sự cố an toàn thông tin; (12) Quản lý an toàn người sử dụng đầu cuối; (13) Quản lý rủi ro an toàn thông tin; (14) Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

b. Đánh giá việc tuân thủ các quy định, quy trình trong Quy chế bảo đảm an toàn thông tin trong quá trình vận hành, khai thác, kết thúc hoặc hủy bỏ hệ thống thông tin, cụ thể:

- Thiết lập chính sách an toàn thông tin trong quy chế, chính sách bảo đảm an toàn thông tin mạng hệ thống
- Tổ chức bảo đảm an toàn thông tin trong quy chế, chính sách bảo đảm an toàn thông tin mạng hệ thống
- Bảo đảm nguồn nhân lực trong quy chế, chính sách bảo đảm an toàn thông tin mạng hệ thống
- Quản lý thiết kế, xây dựng hệ thống trong quy chế, chính sách bảo đảm an toàn thông tin mạng hệ thống
- Quản lý vận hành hệ thống trong quy chế, chính sách bảo đảm an toàn thông tin mạng hệ thống
- Phương án Quản lý rủi ro an toàn thông tin
- Phương án Kết thúc vận hành, khai thác, thanh lý, hủy bỏ.

3.3. *Đánh giá việc thiết kế hệ thống theo phương án bảo đảm an toàn thông tin :*

- Kiểm tra tài liệu thiết kế, xây dựng, vận hành hệ thống
- Kiểm tra, xác minh tính tuân thủ của cấu hình thực tế theo thiết kế

3.4. Kiểm tra, đánh giá các tiêu chí về đảm bảo an toàn mạng

- Kiểm tra thiết kế phân vùng hệ thống:

+ Thiết kế phân tách vùng mạng nội bộ

+ Thiết kế phân tách vùng mạng biên

+ Thiết kế phân vùng DMZ

+ Thiết kế phân vùng máy chủ nội bộ

+ Thiết kế phân vùng máy chủ cơ sở dữ liệu

+ Thiết kế phân vùng quản trị thiết bị hệ thống

+ Thiết kế phân vùng mạng quản trị

+ Thiết kế phân vùng mạng không dây

- Kiểm tra, đánh giá hệ thống có phương án thiết kế bảo đảm an toàn thông tin theo yêu cầu của HTTT cấp độ 3

+ Phương án quản lý truy cập, quản trị hệ thống từ xa an toàn

+ Phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập

+ Phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính

+ Phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu

+ Phương án chặn lọc phần mềm độc hại trên môi trường mạng

+ Phương án phòng chống tấn công từ chối dịch vụ

+ Phương án phòng, chống tấn công mạng cho ứng dụng web

+ Phương án bảo đảm an toàn thông tin cho hệ thống thư điện tử

+ Phương án quản lý truy cập lớp mạng

+ Phương án giám sát hệ thống thông tin tập trung

+ Phương án giám sát an toàn hệ thống thông tin tập trung

+ Phương án quản lý sao lưu dự phòng tập trung

+ Phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung

+ Phương án phòng, chống thất thoát dữ liệu.

+ Phương án duy trì ít nhất 02 kết nối mạng Internet từ các ISP sử dụng hạ tầng kết nối trong nước khác nhau.

+ Phương án bảo đảm an toàn cho mạng không dây

- Kiểm tra, đánh giá cấu hình tường lửa thiết lập các yêu cầu về kiểm soát truy cập từ bên ngoài mạng

+ Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc quản trị hệ thống từ các mạng bên ngoài và mạng Internet.

+ Kiểm soát truy cập từ bên ngoài vào hệ thống theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các dịch vụ, ứng dụng mà hệ thống không cung cấp hoặc không cho phép truy cập từ bên ngoài

+ Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi hệ thống không nhận được yêu cầu từ người dùng.

+ Phân quyền và cấp quyền truy cập từ bên ngoài vào hệ thống theo từng người dùng hoặc nhóm người dùng căn cứ theo yêu cầu nghiệp vụ, yêu cầu quản lý.'

+ Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống

- Kiểm tra, đánh giá cấu hình tường lửa thiết lập các yêu cầu về kiểm soát truy cập từ bên trong mạng

+ Chỉ cho phép truy cập các ứng dụng, dịch vụ bên ngoài theo yêu cầu nghiệp vụ, chặn các dịch vụ khác không phục vụ hoạt động nghiệp vụ theo chính sách của tổ chức

+ Giới hạn truy cập các ứng dụng, dịch vụ bên ngoài theo thời gian

+ Phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chức năng và chính sách của tổ chức

- Kiểm tra cấu hình lưu log hệ thống trên các thiết bị mạng/bảo mật (Router, Switch, Firewall, NIPS,...): Thiết lập chức năng ghi, lưu trữ nhật ký hệ thống trên các thiết bị hệ thống

- Kiểm tra cấu hình đồng bộ thời gian trên các thiết bị mạng/bảo mật (Router, Switch, Firewall, NIPS,...): Sử dụng máy chủ thời gian trong hệ thống để đồng bộ thời gian

- Kiểm tra cấu hình lưu trữ và quản lý tập trung nhật ký hệ thống của các thiết bị mạng/bảo mật (Router, Switch, Firewall, NIPS,...)

+ Lưu trữ và quản lý tập trung nhật ký hệ thống

+ Lưu trữ nhật ký hệ thống của thiết bị tối thiểu 03 thâng

- Rà soát việc định kỳ cập nhật CSDL dấu hiệu phát hiện tấn công mạng trên sản phẩm IPS

+ Phương án phòng chống xâm nhập để bảo vệ các vùng mạng trong hệ thống

+ Định kỳ cập nhật cơ sở dữ liệu dấu hiệu phát hiện tấn công mạng

- Rà soát việc định kỳ cập nhật CSDL dấu hiệu phát hiện tấn công mạng trên sản phẩm có tính năng phòng chống mã độc trên môi trường mạng

+ Có phương án phòng chống phần mềm độc hại trên môi trường mạng

+ Định kỳ cập nhật dữ liệu cho hệ thống phòng chống phần mềm độc hại

- Rà soát, kiểm tra cấu hình quản trị đảm bảo yêu cầu về bảo vệ thiết bị hệ thống trên các thiết bị mạng

+ Cấu hình chức năng xác thực trên các thiết bị

+ Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị thiết bị từ xa

+ Hạn chế các địa chỉ mạng có thể kết nối, quản trị thiết bị từ xa

+ Hạn chế được số lần đăng nhập sai

+ Phân quyền truy cập, quản trị thiết bị

Rà soát chính sách ATTT về xử lý thiết bị mạng trước và sau khi sử dụng: Nâng cấp, xử lý điểm yếu an toàn thông tin của thiết bị hệ thống trước khi đưa vào sử dụng.

3.5. *Kiểm tra, đánh giá các yêu cầu về đảm bảo an toàn máy chủ*

- Kiểm tra, đánh giá cấu hình hệ thống trên các máy chủ theo yêu cầu về xác thực

+ Thiết lập chính sách xác thực trên máy chủ

+ Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa

+ Thiết lập chính sách mật khẩu an toàn

+ Hạn chế số lần đăng nhập sai

+ Vô hiệu hóa tài khoản nếu tài khoản đó đăng nhập sai nhiều lần vượt số lần quy định

- Rà soát, kiểm tra cấu hình về việc kết nối, quản trị từ xa trên máy chủ

+ Chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa

+ Thiết lập giới hạn thời gian chờ (timeout)

+ Thay đổi cổng quản trị mặc định của máy chủ

+ Giới hạn địa chỉ mạng được phép truy cập, quản trị máy chủ từ xa

- Rà soát, kiểm tra cấu hình về việc lưu trữ nhật ký hệ thống trên máy chủ

+ Thiết lập lập chức năng ghi nhật ký hệ thống trên các máy chủ

+ Đồng bộ thời gian giữa máy chủ với máy chủ thời gian

+ Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống để không mất hoặc tràn nhật ký hệ thống

+ Quản lý và lưu trữ tập trung nhật ký hệ thống thu thập được từ máy chủ

+ Lưu nhật ký hệ thống trong khoảng thời gian tối thiểu là 03 tháng

- Rà soát, kiểm tra cấu hình hệ thống về phòng chống xâm nhập trên máy chủ

+ Loại bỏ các tài khoản không sử dụng, các tài khoản không còn hợp lệ trên máy chủ

+ Sử dụng tường lửa của hệ điều hành và hệ thống để cấm các truy cập trái phép tới máy chủ

+ Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng

+ Thực hiện nâng cấp, xử lý điểm yếu an toàn thông tin trên máy chủ trước khi đưa vào sử dụng

- Kiểm tra Quy chế an toàn thông tin về quy trình đánh giá máy chủ trước khi đưa vào sử dụng

- Rà soát việc cài đặt phần mềm phòng chống mã độc trên tất cả máy chủ

+ Cài đặt phần mềm phòng chống mã độc và thiết lập chế độ tự động cập nhật

+ Kiểm tra, dò quét, xử lý phần mềm độc hại cho các phần mềm trước khi cài đặt

+ Quản lý tập trung các phần mềm phòng chống mã độc cài đặt trên máy chủ

- Kiểm tra tính năng quản lý tập trung trên các sản phẩm AV, EDR

- Kiểm tra quy trình, chính sách về việc xử lý máy chủ khi chuyển giao: Phương án xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng

- Rà soát chính sách sao lưu dự phòng dữ liệu máy chủ: Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành

- Rà soát quy trình xóa, hủy dữ liệu trên các thiết bị: Biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa

3.6. Kiểm tra, đánh giá các yêu cầu về đảm bảo an ứng dụng

- Kiểm tra, đánh giá cấu hình hệ thống trên ứng dụng/dịch vụ web theo yêu cầu về xác thực

+ Thiết lập cấu hình ứng dụng để xác thực người sử dụng khi truy cập, quản trị, cấu hình ứng dụng

+ Hạn chế số lần đăng nhập sai trong khoảng thời gian nhất định với tài khoản nhất đinh

+ Lưu trữ có mã hóa thông tin xác thực hệ thống

+ Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng

+ Mã hóa thông tin xác thực trước khi gửi qua môi trường mạng

- Kiểm tra cấu hình kiểm soát, phân quyền và giới hạn truy cập, quản trị ứng dụng/dịch vụ

+ Thiết lập cấu hình ứng dụng để đảm bảo an toàn mật khẩu người sử dụng

+ Thiết lập giới hạn thời gian chờ (timeout) để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng

+ Giới hạn địa chỉ mạng quản trị được phép truy cập, quản trị ứng dụng từ xa

+ Phân quyền truy cập, quản trị, sử dụng tài nguyên khác nhau của ứng dụng với từng người/nhóm sử dụng

+ Giới hạn số lượng các kết nối đồng thời (kết nối khởi tạo và đã thiết lập) đối với các ứng dụng

- Rà soát, kiểm tra việc cấu hình ghi nhật ký hệ thống trên ứng dụng

Ghi nhật ký hệ thống bao gồm những thông tin cơ bản sau:

(1) Thông tin truy cập ứng dụng

(2) Thông tin đăng nhập khi quản trị ứng dụng;

(3) Thông tin các lỗi phát sinh trong quá trình hoạt động

(4) Thông tin thay đổi cấu hình ứng dụng

Quản lý và lưu trữ nhật ký hệ thống trên hệ thống quản lý tập trung

Nhật ký hệ thống phải được lưu trữ trong khoảng thời gian tối thiểu là 03 tháng

- Kiểm tra tính năng mã hóa thông tin, dữ liệu quan trọng trước khi truyền thông tin qua mạng: Mã hóa thông tin, dữ liệu (không phải là thông tin, dữ liệu công khai) trước khi truyền đưa, trao đổi qua môi trường mạng; sử dụng phương án mã hóa theo quy định về bảo vệ bí mật nhà nước đối với thông tin mật: Sử dụng kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền

Rà soát phương án sử dụng chữ ký số cho hệ thống ứng dụng/dịch vụ: Sử dụng chữ ký số khi trao đổi thông tin, dữ liệu quan trọng.

3.7. Kiểm tra, đánh giá các yêu cầu về đảm bảo an dữ liệu

- Rà soát quy trình lưu trữ dữ liệu bảo đảm dữ liệu được lưu cùng mã kiểm tra tính nguyên vẹn

- Kiểm tra việc lưu trữ có mã hóa các thông tin không công khai trong hệ thống CSDL

- Rà soát quy trình, chính sách về việc sao lưu dự phòng dữ liệu

- Kiểm tra việc sao lưu dự phòng dữ liệu thực tế được thực hiện như thế nào.

- Rà soát quy trình, chính sách về phân loại dữ liệu.

- Kiểm tra phương án triển khai hệ thống SAN ở phân vùng riêng với các

máy chủ

3.6. Kiểm tra, đánh giá, rà soát các nguy cơ, lỗ hổng bảo mật trong hệ thống thông tin:

Thực hiện kiểm tra, đánh giá, rà quét lỗ hổng an toàn bảo mật trên các ứng dụng, thiết bị trong hệ thống thông tin.

Thực hiện kiểm tra, rà quét phát hiện các nguy cơ từ các ứng dụng, dịch vụ trên internet, các nguy cơ từ bên ngoài

Thực hiện kiểm tra, rà quét phát hiện nguy cơ trong mạng nội bộ.

Tư vấn các biện pháp khắc phục:

Phân tích chi tiết các điểm yếu và lỗ hổng bảo mật đã được xác định;

Đánh giá và phân loại các lỗ hổng theo mức độ nghiêm trọng, xác định những lỗ hổng có nguy cơ cao và ảnh hưởng lớn đến hoạt động, cần ưu tiên xử lý;

Đồ xuất các giải pháp và biện pháp cụ thể để đóng hoặc giảm thiểu các lỗ hổng, đảm bảo phù hợp với đặc điểm của hệ thống, tính chất và mức độ nghiêm trọng của từng lỗ hổng.

Thực hiện rà soát, kiểm tra, đánh giá lại hệ thống sau khi thực hiện các biện pháp khắc phục.

Tổng hợp, hoàn thiện báo cáo kiểm tra, đánh giá chi tiết

3.7. Yêu cầu đon vị cung cấp dịch vụ:

- Nhà cung câp dịch vụ phải có: Giây phép kinh doanh sản phâm, Dịch vụ an toàn thông tin mạng được đơn vị có thâm quyên câp.

4. Giải pháp và phương pháp luận:

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

1. Giải pháp và phương pháp luận;

2. Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

Mục này quy định về quy trình kiểm tra, nghiệm thu sản phẩm, trình tự giao nộp sản phẩm (nếu có)... để phục vụ công tác thanh, quyết toán hợp đồng.