PHẦN 2. ĐIỀU KHOẢN THAM CHIẾU

CHƯƠNG V. ĐIỀU KHOẢN THAM CHIẾU

"Điều khoản tham chiếu" bao gồm những nội dung chủ yếu sau:

A. Mô tả khái quát về nhiệm vụ dịch vụ tư vấn và gói thầu.

A.1. Khái quát về nhiệm vụ dịch vụ tư vấn:

1. Giới thiệu về gói thầu:

- Tên gói thầu: Đánh giá an ninh mạng cho 07 hệ thống thông tin thuộc dự án nâng cấp hệ thống điều khiển bảo vệ (Ban AMN quản lý dự án).
- Giá dự toán gói thầu: 949.200.000 đồng;
- Nguồn vốn: Chi phí sản xuất;
- Hình thức LCNT: Đấu thầu rộng rãi trong nước (qua mạng);
- Loại hợp đồng: Trọn gói;
- Thời gian thực hiện gói thầu: 60 ngày.

2. Chủ đầu tư: Công ty truyền tải điện 4;

3. Địa điểm thực hiện: Các trạm biến áp 220kV của PTC4;

4. Nhiệm vụ và phạm vi thực hiện:

4.1. Nhiệm vụ:

Kiểm tra, đánh giá an toàn thông tin (ATTT) cho 07 hệ thống thông tin trạm biến áp nhằm đánh giá việc triển khai các phương án đảm bảo an toàn thông tin theo cấp độ ATTT đã được phê duyệt tuân thủ theo nghị định 85/2016/NĐ-CP ngày 01/07/2016, thông tư 12/2022/TT-BTTTT ngày 12/08/2022 và TCVN11930:2017.

- Trường hợp phát hiện những lỗ hổng, những điểm chưa đảm bảo ATTT của hệ thống thông tin theo thông tư 12/2022/TT-BTTTT ngày 12/08/2022 và TCVN 11930:2017 thì:
  + Đối với các cài đặt có thể thực hiện trên thiết bị/ phần mềm đã có sẵn trên hệ thống, nhà Thầu trình phương án thực hiện để đảm bảo an toàn thông tin. Sau khi chủ đầu tư thống nhất phương án thì nhà Thầu tiếp thực hiện cài đặt bổ sung.
  + Đối với những cài đặt cần phải thực hiện trên thiết bị/ phần mềm mà chưa có sẵn trên hệ thống thì đề xuất đầu tư bổ sung thiết bị và cấu hình cài đặt chi tiết để đảm bảo an toàn thông tin cho hệ thống phù hợp với cấp độ ATTT đã được duyệt. Nhà Thầu phải đề xuất đặc tính thiết bị cũng như cài đặt chi tiết trên thiết bị phù hợp với thiết kế hiện hữu của từng hệ thống thông tin. Nhà Thầu có thể tham khảo Đề án ATTT EVN giai đoạn 2023–2028 (Quyết định 168/QĐ-EVN ngày 23/02/2023) để đề xuất phương án.

– Thực hiện truy tìm nguy cơ an toàn thông tin – Threat Hunting cho máy chủ máy trạm tại 7 trạm biến áp.

4.2. Phạm vi công việc:

a. Số lượng hệ thống thông tin tự động hoá Trạm biến áp 220kV: gồm 07 trạm 220kV.

- Hệ thống tự động hoá trạm biến áp 220kV Rạch Giá.
- Hệ thống tự động hoá trạm biến áp 220kV Hóc Môn
- Hệ thống tự động hoá trạm biến áp 220kV Bình Hòa
- Hệ thống tự động hoá trạm biến áp 220kV Cát Lái
- Hệ thống tự động hoá trạm biến áp 220kV Long Bình
- Hệ thống tự động hoá trạm biến áp 220kV Long Thành
- Hệ thống tự động hoá trạm biến áp 220kV Nhà Bè

b. Số lượng thiết bị trong từng hệ thống thông tin:

STT	Trạm biến áp	Hệ thống điều khiển đang dùng	Máy tính điều khiển	Firewall	Switch layer 2	Ghi chú
1	220kV Rạch Giá	ATS	4	2	8	
2	220kV Hóc Môn	ATS	4	2	8	
3	220kV Bình Hòa	Toshiba	5	2	16	
4	220kV Cát Lái	Siemens	5	2	31	
5	220kV Long Bình	GE	6	2	14	
6	220kV Long Thành	Schneider	5	2	23	
7	220kV Nhà Bè	Siemens	5	2	31	

A.2 Các nhiệm vụ cụ thể:

Nhà thầu phải đề xuất giải pháp và phương pháp luận với các nhiệm vụ cụ thể đáp ứng những yêu cầu sau:

Kiểm tra, đánh giá an toàn thông tin (ATTT) cho 07 hệ thống thông tin trạm biến áp nhằm đánh giá việc triển khai các phương án đảm bảo an toàn thông tin theo cấp độ ATTT được phê duyệt tuân thủ theo nghị định 85/2016/NĐ-CP ngày 01/07/2016, thông tư 12/2022/TT-BTTTT ngày 12/08/2022 và TCVN 11930:2017 trong hồ sơ đề xuất cấp độ của từng trạm bao gồm:

1. Đánh giá an toàn thông tin hệ thống thông tin từng trạm biến áp:

STT	YÊU CẦU	Các chỉ mục tham chiếu trong TCVN 11930:2017	
		Cấp độ 4 ATTT	Cấp độ 5 ATTT
I. YÊU CẦU QUẢN LÝ		**8.1**	**9.1**
1.1	**Thiết lập chính sách an toàn thông tin**	**8.1.1**	**9.1.1**
1.1.1	Chính sách an toàn thông tin	8.1.1.1	9.1.1.1
1.1.2	Xây dựng và công bố	8.1.1.2	9.1.1.2

1.1.3	Rà soát, sửa đổi	8.1.1.3	9.1.1.3
1.2	**Tổ chức bảo đảm an toàn thông tin**	**8.1.2**	**9.1.2**
1.2.1	Đơn vị chuyên trách về an toàn thông tin	8.1.2.1	9.1.2.1
1.2.2	Phối hợp với những cơ quan/tổ chức có thẩm quyền	8.1.2.2	9.1.2.2
1.3	**Bảo đảm nguồn nhân lực**	**8.1.3**	**9.1.3**
1.3.1	Tuyển dụng	8.1.3.1	9.1.3.1
1.3.2	Trong quá trình làm việc	8.1.3.2	9.1.3.2
1.3.3	Chấm dứt hoặc thay đổi công việc	8.1.3.3	9.1.3.3
1.4	**Quản lý thiết kế, xây dựng hệ thống**	**8.1.4**	**9.1.4**
1.4.1	Thiết kế an toàn hệ thống thông tin	8.1.4.1	9.1.4.1
1.4.2	Phát triển phần mềm thuê khoán	8.1.4.2	9.1.4.2
1.4.3	Thử nghiệm và nghiệm thu hệ thống	8.1.4.3	9.1.4.3
1.5	**Quản lý vận hành hệ thống**	**8.1.5**	**9.1.5**
1.5.1	Quản lý an toàn mạng	8.1.5.1	9.1.5.1
1.5.2	Quản lý an toàn máy chủ và ứng dụng	8.1.5.2	9.1.5.2
1.5.3	Quản lý an toàn dữ liệu	8.1.5.3	9.1.5.3
1.5.4	Quản lý an toàn thiết bị đầu cuối	8.1.5.4	9.1.5.4
1.5.5	Quản lý phòng chống phần mềm độc hại	8.1.5.5	9.1.5.5
1.5.6	Quản lý giám sát an toàn hệ thống thông tin	8.1.5.6	9.1.5.6
1.5.7	Quản lý điểm yếu an toàn thông tin	8.1.5.7	9.1.5.7
1.5.8	Quản lý sự cố an toàn thông tin	8.1.5.8	9.1.5.8
1.5.9	Quản lý an toàn người sử dụng đầu cuối	8.1.5.9	9.1.5.9
1.6	**Phương án quản lý rủi ro an toàn thông tin**	Phụ lục IV, thông tư 12	Phụ lục V, thông tư 12
1.7	**Phương án kết thúc vận hành, khai thác, thanh lý, huỷ bỏ**	Phụ lục IV, thông tư 12	Phụ lục V, thông tư 12
II. YÊU CẦU KỸ THUẬT		**8.2**	**9.2**
2.1	**Bảo đảm an toàn mạng**	**8.2.1**	**9.2.1**
2.1.1	**Thiết kế hệ thống**	8.2.1.1	9.2.1.1
a.	Thiết kế các vùng mạng trong hệ thống theo chức năng, các vùng mạng tối thiểu bao gồm:	8.2.1.1.a.	9.2.1.1.a.
	- Vùng mạng nội bộ;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng mạng biên;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng DMZ;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng máy chủ nội bộ;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng mạng không dây (nếu có) tách riêng, độc lập với các vùng mạng khác;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng mạng máy chủ cơ sở dữ liệu;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng quản trị;	8.2.1.1.a.	9.2.1.1.a.
	- Vùng quản trị thiết bị hệ thống.	8.2.1.1.a.	9.2.1.1.a.
b.	Phương án thiết kế bảo đảm các yêu cầu sau:	8.2.1.1.b.	9.2.1.1.b.
	- Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn;	8.2.1.1.b.	9.2.1.1.b.

- Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án dự phòng cho các thiết bị mạng và phương án cân bằng tải, dự phòng nóng cho thiết bị mạng chính ;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án bảo đảm an toàn cho máy chủ cơ sở dữ liệu;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án chặn lọc phần mềm độc hại trên môi trường mạng;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án phòng chống tấn công từ chối dịch vụ;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án phòng chống tấn công mạng cho ứng dụng web;sử dụng tường lửa ứng dụng web đối với các hệ thống thông tin được quy định tại khoản 2, điều 10, nghị định 85/2016/NĐ-CP hoặc hệ thống trung tâm dữ liệu, điện toán đám mây, định danh, xác thực điện tử, chứng thực điện tử, chữ ký số, kết nối tích hợp, chia sẻ dữ liệu đáp ứng tiêu chí quy định tại khoản 3 điều 10 nghị định 85/2016/NĐ-CP	8.2.1.1.b.	9.2.1.1.b.
- Có phương án đảm bảo an toàn thông tin cho hệ thống thư điện tử; sử dụng sản phẩm bảo đảm an toàn thông tin cho hệ thống thư điện tử;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án quản lý truy cập lớp mạng; sử dụng sản phẩm quản lý truy cập lớp mạng đói với hệ thống mạng nội bộ, trung tâm giám sát điều hành an toàn thông tin mạng, đáp ứng tiêu chí tại khoản 3 điều 10 nghị định 85/2016/NĐ-CP;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án giám sát hệ thống thông tin tập trung sử dụng sản phẩm giám sát hệ thống thông tin tập trung;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án giám sát an toàn hệ thống thông tin tập trung sử dụng sản phẩm quản lý và phân tích sự kiện an toàn thông tin hoặc sản phẩm tương đương;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án quản lý sao lưu dự phòng tập trung sử dụng hệ thống lưu trữ tập trung và sản phẩm quản lý lưu trữ tập trung;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án quản lý phần mềm phòng chống mã độc trên máy chủ/ máy tính người dùng, sử dụng sản phẩm phòng, chống mã độc và/ hoặc sản phẩm phát hiện và phản ứng sự cố ATTT trên thiết bị đầu cuối, có chức năng quản lý tập trung;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án phòng, chống thất thoát dữ liệu; sử dụng sản phẩm phòng, chống thất thoát dữ liệu đối với hệ thống thông tin có xử lý thông tin bí mật nhà nước hoặc hệ thống cơ sở dữ liệu dùng chung đáp ứng tiêu chí quy định tại khoản 3 điều 10 nghị định 85/2016/NĐ-CP.	8.2.1.1.b.	9.2.1.1.b.
- Có phương án dự phòng kết nối mạng internet cho các máy chủ dịch vụ;	8.2.1.1.b.	9.2.1.1.b.
- Có phương án đảm bảo an toàn cho mạng khong dây (nếu có)	8.2.1.1.b.	9.2.1.1.b.
- Có phương án quản lý tài khoản đặc quyền, sử dụng sản phẩm quản lý tài khoản đặc quyền	8.2.1.1.b.	9.2.1.1.b.

	- Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30km.		9.2.1.1.b.
	- Có phương án dự phòng cho kết nối mạng giữa hệ thống chính và hệ thống dự phòng		9.2.1.1.b.
III. YÊU CẦU VỀ THIẾT LẬP, CẤU HÌNH HỆ THỐNG			
1.1	**Bảo đảm an toàn mạng**	**8.2.1**	**9.2.1**
1.1.1	Kiểm soát truy cập từ bên ngoài mạng	8.2.1.2	9.2.1.2
1.1.2	Kiểm soát truy cập từ bên trong mạng	8.2.1.3	9.2.1.3
1.1.3	Nhật ký hệ thống	8.2.1.4	9.2.1.4
1.1.4	Phòng chống xâm nhập	8.2.1.5	9.2.1.5
1.1.5	Phòng chống phần mềm độc hại trên môi trường mạng	8.2.1.6	9.2.1.6
1.1.6	Bảo vệ thiết bị hệ thống	8.2.1.7	9.2.1.7
1.2	**Bảo đảm an toàn máy chủ**	**8.2.2**	**9.2.2**
1.2.1	Xác thực	8.2.2.1	9.2.2.1
1.2.2	Kiểm soát truy cập	8.2.2.2	9.2.2.2
1.2.3	Nhật ký hệ thống	8.2.2.3	9.2.2.3
1.2.4	Phòng chống xâm nhập	8.2.2.4	9.2.2.4
1.2.5	Phòng chống phần mềm độc hại	8.2.2.5	9.2.2.5
1.2.6	Xử lý máy chủ khi chuyển giao	8.2.2.6	9.2.2.6
1.3	**Bảo đảm an toàn ứng dụng**	**8.2.3**	**9.2.3**
1.3.1	Xác thực	8.2.3.1	9.2.3.1
1.3.2	Kiểm soát truy cập	8.2.3.2	9.2.3.2
1.3.3	Nhật ký hệ thống	8.2.3.3	9.2.3.3
1.3.4	Bảo mật thông tin liên lạc	8.2.3.4	9.2.3.4
1.3.5	Chống chối bỏ	8.2.3.5	9.2.3.5
1.3.6	An toàn ứng dụng và mã nguồn	8.2.3.6	9.2.3.6
1.4	**Bảo đảm an toàn dữ liệu**	**8.2.4**	**9.2.4**
1.4.1	Nguyên vẹn dữ liệu	8.2.4.1	9.2.4.1
1.4.2	Bảo mật dữ liệu	8.2.4.2	9.2.4.2
1.4.3	Sao lưu dự phòng	8.2.4.3	9.2.4.3

Tương ứng với các yêu cầu đảm bảo ATTT ở bảng trên (từng nội dung), nhà Thầu phải ghi rõ hệ thống hiện hữu đã thực hiện biện pháp/ cấu hình gì để đảm bảo ATTT kèm theo kết luận đánh giá (các mục thiếu nội dung này được xem là chưa thực hiện). Các trao đổi giữa nhà Thầu và chủ Đầu Tư trong quá trình triển khai (có liên quan đến thông tin được quy định là "mật") phải thực hiện theo quy định về bảo mật thông tin

2. Rà quét lỗ hổng bảo mật và đánh giá xâm nhập, gỡ bỏ mã độc, điểm yếu bảo mật trên máy chủ, thiết bị mạng.

2.1. Rà quét lỗ hổng bảo mật và đánh giá xâm nhập (Pentest) cho hệ thống máy chủ, máy trạm:

- Quy trình khảo sát, phương pháp luận thực hiện dựa theo các tiêu chuẩn hàng đầu như OWASP (v4), NIST 800-115 (Technical Guide to Information Security Testing), ISSAF (Information System Security Assessment), OSSTMM (The Open Source Security Testing Methodology Manual). Thực hiện dò quét sử dụng các công cụ dò quét lỗ hổng bảo mật hàng đầu như: NeXpose, Nessus, Metasploit, … kết hợp với đánh giá thủ công để đảm bảo phát hiện tối đa các lỗ hổng tồn tại trên hệ thống máy chủ.

2.1.1. Kiểm tra, rà soát, tư vấn khắc phục điểm yếu bảo mật của các máy chủ, máy trạm

Đánh giá phát hiện lỗ hổng, điểm yếu, thử nghiệm xâm nhập hệ thống là việc thực hiện dò quét, phát hiện lỗ hổng, điểm yếu của hệ thống, thử nghiệm tấn công xâm nhập hệ thống và đánh giá nguy cơ, thiệt hại có thể có của hệ thống thông tin khi bị đối tượng tấn công xâm nhập.

Bước 1: Thu thập thông tin

- Xác định sự tồn tại của các thiết bị filter: Firewall, IPS…
- Thu thập thông tin phần cứng máy tính
- Thu thập thông tin về hệ điều hành đang sử dụng.
- Thu thập thông tin về danh sách các phần mềm và phiên bản đang cài đặt.
- Thu thập thông tin về danh sách các dịch vụ đang chạy trên máy tính.
- Thu thập phân loại các thông tin phần mềm thu thập được thành các danh mục tương ứng

Bước 2: Dò quét và phân tích lỗ hổng

Đơn vị thực hiện tiến hành dò quét các nguy cơ an ninh trên hệ thống máy chủ sử dụng các công cụ hỗ trợ có bản quyền và dò quét thụ động để phát hiện bất thường, không thực hiện dò quét chủ động trong hệ thống thông tin đang hoạt động.

Thực hiện dò quét, phân tích xác định các điểm yếu tồn tại trên hệ thống bao gồm:

- Kiểm tra thông tin chi tiết về các bản vá cần cập nhật/đã cập nhật.
- Kiểm tra thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng CVE, CPE và OVAL.
- Kiểm tra thông tin về các tiến trình phần mềm đang thực thi.
- Kiểm tra thông tin về các dịch vụ (services) đang được triển khai trên máy tính.

- Kiểm tra thông tin về các chương trình khởi động cùng máy tính.

- Kiểm tra thông tin về cấu hình kiểm soát truy cập của máy tính (User Account Control).

- Kiểm tra thông tin về cấu hình hoạt động Internet của hệ thống (Internet Options).

- Kiểm tra thông tin kiểm tra hệ thống file và tổng hợp những file nghi ngờ dẫn tới nguy cơ mất mát thông tin.

- Dựa vào một số các thông tin thu thập được ở trên, phần mềm sẽ phát hiện thông minh các nguy mát an ninh an toàn, thu thập các mẫu nghi ngờ mất an toàn.

- Hỗ trợ phân tích đánh giá an ninh an toàn cho các tệp định dạng tệp thực thi trên Windows (exe, dll, com, …).

- Phát hiện các hành vi mạng bất thường;

- Phát hiện các cấu hình an toàn thông tin chưa phù hợp.

- Điểm yếu mật khẩu: Không đặt mật khẩu xác thực, mật khẩu yếu dễ đoán.

- Thu thập bằng chứng và xác nhận mức độ chính xác thông tin các lỗ hổng.

Bước 3: Thử nghiệm xâm nhập

Đánh giá điểm yếu và kiểm thử xâm nhập (Pentest) theo phương thức thử nghiệm thâm nhập lỗ hổng bảo mật, quá trình này có sự thực hiện trực tiếp thủ công của các chuyên gia thay vì chỉ sử dụng các công cụ dò quét tự động theo phương thức dò quét điểm yếu.

Không áp dụng phương pháp Black-box (đánh giá hộp đen, người đánh giá không có thông tin gì của hệ thống được đánh giá), chỉ lựa chọn phương pháp White-box (đánh giá toàn bộ các điểm yếu) hoặc Grey-box (đánh giá mức độ tổn thương nếu có nguy cơ từ nội bộ).

Từ danh sách các lỗ hổng và điểm yếu bảo mật xác định được từ bước trước, chuyên gia của nhà Thầu đánh giá ATTT sẽ thực hiện thử nghiệm tấn công, khai thác vào các hệ thống có điểm yếu bảo mật trong một số tình huống. Công việc này được thực hiện với mục đích:

- Xác nhận, chứng minh sự tồn tại của điểm yếu trên hệ thống.

- Loại bỏ những kết quả sai mà công cụ dò quét được (các file hệ thống mà công cụ rà quét hiểu là mã độc). Chấp nhận xác nhận của các tổ chức phòng chống virus, an toàn thông tin uy tín (Norton, Bitdefender, McAfee, VirusTotal,…) đối với file nghi ngờ mã độc trong quá trình rà quét.

- Phân tích các nguy cơ và rủi ro an ninh thông tin tương ứng với các lỗ hổng.

- Minh họa cách thức khai thác điểm yếu, giúp chủ đầu tư hiểu rõ mức độ nguy hiểm và ảnh hưởng của điểm yếu đối với máy chủ.

2.2. Rà quét và gỡ bỏ mã độc cho máy chủ, máy trạm

Để đảm bảo cho hệ thống CNTT thực sự được dò quét toàn bộ và sạch sẽ, an toàn trước khi bước vào giai đoạn quy hoạch và triển khai các giải pháp đảm bảo an toàn thông tin, việc thực hiện các công việc rà soát và loại bỏ mã độc là quan trọng và cần thực hiện sớm.

Dịch vụ dò quét được thực hiện bởi các chuyên gia bảo mật thông tin, những người có nhiều năm kinh nghiệm trong việc kiểm tra hệ thống, phân tích phần mềm độc hại, điều tra tấn công bằng phần mềm. Quá trình làm sạch được thực hiện trên kinh nghiệm của chuyên gia kết hợp với công cụ hoàn toàn không ảnh hưởng đến quá trình vận hành của hệ thống, đảm bảo khắc phục các nguy cơ mất an toàn thông tin do mã độc gây ra. Nhà Thầu phải thống nhất với Chủ đầu tư phương án xử lý trước khi loại bỏ các mã độc.

2.2.1 Rà quét phát hiện mã độc

- Rà soát các mục khởi động cùng hệ điều hành: Rà soát toàn bộ các mục, tệp tin, chương trình, câu lệnh, dịch vụ có tính chất khởi động cùng với hệ điều hành hoặc sau khi người dùng đăng nhập vào hệ thống.
- Rà soát các tiến trình đang hoạt động: Rà soát toàn bộ các tiến trình đang chạy trên máy tính.
- Rà soát các kết nối mạng trên máy tính: Thực hiện rà soát toàn bộ kết nối mạng đang hoạt động. Giám sát các kết nối TCP/IP, DNS Query trong khoảng thời gian thực hiện rà soát.
- Rà soát các thư mục nhạy cảm: Rà soát các thư mục phổ biến mà mã độc thường được cài đặt.
- Thu thập nhật ký rà soát: Thu thập các nhật ký (log) đã thực hiện rà soát: các mục khởi động cùng hệ điều hành, các kết nối mạng, nhật ký của hệ điều hành (Windows Event Logs).
- Kiểm tra hoạt động của ứng dụng dịch vụ: Sau khi thực hiện rà soát xong, kiểm tra lại hoạt động của dịch vụ của ứng dụng, đảm bảo vẫn hoạt động bình thường như trước thời điểm thực hiện rà soát.
- Kiểm tra chéo kết quả rà soát: Người kiểm tra chéo thực hiện phân tích lại các nhật ký rà soát đã thu thập được.

2.2.2 Làm sạch, phân tích điều tra và thắt chặt an toàn thông tin

- Gỡ bỏ các mã độc phát hiện được trên hệ thống.
- Thu thập log hệ thống, xác định thời gian, nguồn lây nhiễm.
- Phân tích các mã độc phát hiện được, xác định các tên miền/IP điều khiển để thực hiện chặn lọc trên các hệ thống (firewall, proxy, DNS...).

2.3. Rà quét lỗ hổng bảo mật và đánh giá xâm nhập (Pentest) cho thiết bị

mạng:

Kiểm tra, rà soát, tư vấn khắc phục điểm yếu bảo mật của thiết bị mạng (Router, Switch, Firewall)

Bước 1: Khảo sát thu thập thông tin

- Khảo sát thông tin về sơ đồ hệ thống mạng,
- Khảo sát thông tin về thiết bị mạng bao gồm:
    - Địa chỉ IP
    - Địa chỉ MAC
    - Tên thiết bị
    - Hãng sản xuất
    - Dòng thiết bị (Model, Name, Family)
- Thông tin về hệ điều hành/firmware đang sử dụng.
- Thông tin về số hiệu các cổng dịch vụ đang mở.

Bước 2: Dò quét điểm yếu

Nhà Thầu thực hiện tiến hành dò quét các nguy cơ an ninh trên các thiết bị mạng sử dụng các công cụ hỗ trợ có bản quyền và dò quét thụ động để phát hiện bất thường, không thực hiện dò quét chủ động trong hệ thống thông tin đang hoạt động.. Thực hiện dò quét, phân tích xác định các điểm yếu tồn tại trên hệ thống bao gồm:

- Kiểm tra thông tin chi tiết về các bản vá cần cập nhật/đã cập nhật.
- Kiểm tra thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng.
- Phát hiện các cấu hình an toàn thông tin chưa phù hợp.
- Điểm yếu mật khẩu: Không đặt mật khẩu xác thực, mật khẩu yếu dễ đoán
- Thu thập bằng chứng và xác nhận mức độ chính xác thông tin các lỗ hổng
- Các lỗ hổng do lỗi cấu hình, triển khai cài đặt
- Dò quét điểm yếu trên các dịch vụ đang chạy
- Dò quét điểm yếu trên các ứng dụng đang cài trên các thiết bị

Bước 3: Thử nghiệm xâm nhập

Đây là quá trình quan trọng nhất của quá trình đánh giá điểm yếu và kiểm thử xâm nhập (Pentest) theo phương thức thử nghiệm thâm nhập lỗ hổng bảo mật. Quá trình này có sự thực hiện trực tiếp thủ công của các chuyên gia vì chỉ sử dụng các công cụ dò quét tự động theo phương thức dò quét điểm yếu. Từ danh sách các lỗ hổng và điểm yếu bảo mật xác định được từ bước trước, nhà Thầu thử nghiệm tấn công, khai thác vào các hệ thống có điểm yếu bảo mật trong một số tình huống. Không áp dụng phương pháp Black-box (đánh giá hộp đen, người đánh giá không có thông tin gì của hệ thống được đánh giá), chỉ lựa chọn phương pháp White-box (đánh giá toàn bộ các điểm yếu) hoặc Grey-box (đánh giá mức độ tổn thương nếu có nguy cơ từ nội bộ).

Công việc này được thực hiện với mục đích:

- Xác nhận, chứng minh sự tồn tại của điểm yếu trên hệ thống.

- Loại bỏ những kết quả sai mà công cụ dò quét được.

- Minh họa cách thức khai thác điểm yếu, giúp chủ đầu tư hiểu rõ mức độ nguy hiểm và ảnh hưởng của điểm yếu đối với hệ thống mạng

- Password attack: Thử nghiệm các kiểu tấn công password vào các thiết bị mạng, bảo mật và thiết bị truyền dẫn

- Exploits: Thử nghiệm khai thác các lỗ hổng bảo mật được tìm thấy ở phần trước.

3. Tiêu chuẩn, quy chuẩn kỹ thuật áp dụng:

- Nghị định số 85/2016/NĐ-CP ngày 01/07/2016 của Chính phủ về đảm bảo an toàn hệ thống thông tin theo cấp độ;

- Thông tư 12/2022/TT-BTTTT ngày 12/8/2022 của Bộ Thông tin và Truyền thông về việc hướng dẫn Nghị định 85/2016/NĐ CP về bảo đảm an toàn hệ thống thông tin theo cấp độ và hướng dẫn chi tiết tại tiêu chuẩn quốc gia TCVN 11930:2017;

- Nghị định 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ về việc Quy định chi tiết một số điều của Luật An ninh mạng;

- Quyết định số 168/QĐ-EVN ngày 23/02/2023 của EVN về việc phê duyệt Đề án "Đảm bảo an toàn thông tin cho hệ thống thông tin của Tập đoàn Điện lực quốc gia Việt Nam giai đoạn 2023 – 2028";

- 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.

- Các tiêu chuẩn kỹ thuật khác có liên quan.

4. Kết quả đầu ra của dịch vụ:

a. Đối với công tác đánh giá ATTT cho 07 trạm biến áp theo Đề án ATTT EVN giai đoạn 2023–2028 (Quyết định 168/QĐ-EVN ngày 23/02/2023) và đáp ứng theo tiêu chí TCVN 11930:2017 trong hồ sơ đề xuất cấp độ của từng trạm: Báo cáo chi tiết công tác đánh giá, đề xuất và thực hiện:

- Đánh giá mức độ bảo mật từng hệ thống thông tin (từng trạm biến áp) hiện hữu.

- Đề xuất phương án tăng cường bảo mật trên hạ tầng các giải pháp ATTT sẵn có đáp ứng theo tiêu chí TCVN 11930:2017 trong hồ sơ đề xuất cấp độ (như thực hiện bổ sung các cấu hình bảo mật cần thiết, thay đổi quy hoạch mạng, chính sách kết nối mạng, tối ưu các giải pháp bảo mật…trên các thiết bị hiện hữu).

- Thực hiện bổ sung các cấu hình bảo mật cần thiết, tối ưu các giải pháp bảo mật…trên các thiết bị hiện hữu.

- Đề xuất phương án đầu tư tăng cường bảo mật và cấu hình cài đặt trên thiết bị đầu tư mới đảm bảo an toàn thông tin đáp ứng theo tiêu chí TCVN 11930:2017 trong hồ sơ đề xuất cấp độ.

b. Đối với công tác rà quét lỗ hổng bảo mật và đánh giá xâm nhập, gỡ bỏ mã độc, điểm yếu bảo mật trên máy chủ, thiết bị mạng:

b1. Đánh giá lỗ hổng, điểm yếu và kiểm thử xâm nhập (Pentest) cho hệ thống máy chủ

Sau khi hoàn thành quá trình đánh giá lỗ hổng, điểm yếu và kiểm thử xâm nhập (Pentest) cho hệ thống máy chủ, nhà Thầu thực hiện tổng hợp lại tất các các thông tin thu thập được, nội dung của quá trình làm việc và kết quả thu được để đưa ra *"Báo cáo tổng kết Kiểm tra, đánh giá an toàn thông tin cho hệ thống máy chủ".* Bản báo cáo sẽ bao gồm các nội dung chính như sau:

- Phần 1: Kết quả quá trình đánh giá: Mô tả chi tiết các nguy cơ an ninh trên hệ thống máy chủ. Các lỗ hổng, điểm yếu bảo mật phát hiện được sẽ được phân loại theo mức độ rủi ro: Cao, Thấp và Trung Bình.

- Phần 2: Đề xuất, khuyến nghị: Đề xuất các phương án, giải pháp để khắc phục các lỗ hổng, điểm yếu bảo mật được phát hiện trên hệ thống máy chủ của chủ đầu tư.

b2. Rà soát mã độc trên danh sách máy chủ, máy trạm:

- Biên bản thực hiện rà soát mã độc trên danh sách máy chủ, máy trạm đã cung cấp: nêu rõ thời gian, cách thức, người thực hiện, kết quả sơ bộ.

- Trường hợp phát hiện mã độc/ lỗ hổng bảo mật thì nhà Thầu đánh giá ATTT phải liên hệ với nhà Thầu cung cấp phần mềm điều khiển để thống nhất kết quả đánh giá và phương án xử lý và cùng ký biên bản đánh giá.

- Báo cáo kết quả thực hiện dịch vụ dò quét, gỡ bỏ mã độc: nêu chi tiết thời gian, nội dung công việc, kết quả, nhận xét đánh giá, đề xuất.

b3. Rà quét lỗ hổng bảo mật và đánh giá xâm nhập (Pentest) cho thiết bị mạng.

Sau khi hoàn thành quá trình đánh giá lỗ hổng, điểm yếu và kiểm thử xâm nhập (Pentest) cho hệ thống, đơn vị thực hiện sẽ tổng hợp lại tất các các thông tin thu thập được, nội dung của quá trình làm việc và kết quả thu được để đưa ra cho chủ đầu tư *"Báo cáo tổng kết Kiểm tra, đánh giá an toàn thông tin cho thiết bị mạng"*. Bản báo cáo sẽ bao gồm các nội dung chính như sau:

- Phần 1: Kết quả quá trình đánh giá: Mô tả chi tiết các điểm yếu bảo mật phát hiện được trên hệ thống mạng LAN của chủ đầu tư. Các lỗ hổng, điểm yếu bảo mật phát hiện được sẽ được phân loại theo mức độ rủi ro: Cao, Thấp và Trung Bình.

- Phần 2: Đề xuất, khuyến nghị: Đề xuất các phương án, giải pháp để khắc

phục các lỗ hổng, điểm yếu bảo mật được phát hiện trên hệ thống thiết bị mạng của chủ đầu tư.

c. Đào tạo, hướng dẫn:

- Thực hiện đào tạo, chia sẻ quy trình thực hiện đánh giá an toàn thông tin; Quy trình, công cụ đã thực hiện để rà quét mã độc, phát hiện các lỗi bảo mật của hệ thống, ứng dụng của PTC4; Hướng dẫn tái hiện lại các lỗ hổng và lỗi đã tìm ra trong các report để PTC4 có thể chủ động nhân rộng phạm vi thực hiện. Thời gian đào tạo: tối thiểu 1 ngày làm việc qua hình thức Online hoặc Onsite.

5. Thời gian dự kiến bắt đầu thực hiện DVTV:

- Thời gian dự kiến Nhà thầu bắt đầu thực hiện triển khai công việc DVTV: Ngay sau khi hợp đồng giữa Chủ đầu tư và Nhà thầu có hiệu lực.
- Thời gian thực hiện: 60 ngày

6. Kinh nghiệm và nhân sự của nhà thầu:

Căn cứ Nghị định 108/2016/NĐ-CP của Chính phủ ban hành ngày 01 tháng 07 năm 20216; Căn cứ văn bản 1337/EVNNPT-VTCNTT+ĐT+PC ban hành ngày 11 tháng 03 năm 2024 yêu cầu về năng lực các đơn vị cung cấp các hạng mục liên quan đến an toàn thông tin phải có Giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng, trong đó phải có nội dung doanh nghiệp được phép kinh doanh cung cấp dịch vụ tư vấn an toàn thông tin mạng.

7. Trách nhiệm của chủ đầu tư:

Phối hợp cung cấp những tài liệu có liên quan đến nhiệm vụ của tư vấn nhằm tạo điều kiện thuận lợi cho nhà thầu thực hiện nhiệm vụ của mình.