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: PTV38-2025: Cung cấp dịch vụ giám sát đảm bảo an toàn thông tin cho các địa chỉ IP và tên miền công khai trên Internet.

- Bên mời thầu: Công ty nhiệt điện Thái Bình.

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

- Loại hợp đồng: Hợp đồng trọn gói

- Địa điểm thực hiện: Công ty Nhiệt điện Thái Bình, địa chỉ: thôn Chỉ Thiện, xã Đông Thái Ninh, tỉnh Hưng Yên

- Thời gian thực hiện hợp đồng: 365 ngày

- Nguồn vốn: Vốn sản xuất kinh doanh

2. Mục tiêu công việc:

Giám sát an toàn thông tin (ATTT) từ bên ngoài được triển khai tự động, tập trung vào các dải địa chỉ IP Public, nhằm kịp thời phát hiện, phòng chống, đối phó các nguy cơ mất an toàn thông tin trong các hệ thống thông tin của Công ty Nhiệt điện Thái Bình.

Đánh giá an toàn thông tin cho ứng dụng (HTTT): Kiểm thử Gray box.

Đào tạo về kỹ năng đảo bảo an toàn thông tin hệ thống OT cho cán bộ quản trị, vận hành hệ thống.

3. Yêu cầu kỹ thuật của gói thầu:

Nhà thầu phải có phương án thuyết minh cụ thể đối với các dịch vụ.

3.1. Giám sát an toàn thông tin cho các địa chỉ IP/Domain công khai.

- Số lượng: tối đa 10 IP/Domain

- Thời gian thực hiện: 365 ngày

- Phát hiện các điểm yếu trong hệ thống, ứng dụng hoặc thiết bị có thể bị tin tặc khai thác để tấn công.

- Cảnh báo mã độc, phần mềm độc hại: Phát hiện hoạt động hoặc tập tin nghi ngờ chứa mã độc (virus, trojan, ransomware…) trong hệ thống.

- Cảnh báo tấn công có chủ đích (APT): Nhận diện hành vi tấn công tinh vi, có kế hoạch và mục tiêu rõ ràng nhằm xâm nhập hoặc chiếm quyền kiểm soát hệ thống.

- Cảnh báo rò rỉ dữ liệu: Phát hiện dữ liệu nhạy cảm (tài liệu, thông tin nội bộ, dữ liệu khách hàng…) bị truy xuất, sao chép hoặc truyền ra ngoài trái phép.

- Cảnh báo lộ lọt tài khoản: Phát hiện thông tin tài khoản người dùng (username, mật khẩu) bị rò rỉ trên internet, dark web hoặc qua kênh phi chính thống.

- Cảnh báo hệ thống nhiễm mã độc: Xác định máy chủ, máy trạm hoặc thiết bị đầu cuối đã bị mã độc xâm nhập và hoạt động trong môi trường mạng nội bộ.

- Cảnh báo port mở bất thường: Phát hiện cổng mạng (port) mở không đúng cấu hình, tiềm ẩn nguy cơ bị khai thác hoặc phục vụ cho kết nối trái phép.

- Tư vấn hỗ trợ xử lý các lỗ hổng, điểm yếu và sự cố ATTT.

- Hỗ trợ cảnh báo tức thì khi có thông tin về an toàn an ninh mạng qua Email.

- Có chuyên gia hỗ trợ và ứng cứu, xử lý tối đa 01 sự cố tấn công mạng nghiêm trọng.

- Báo cáo tổng hợp kết quả giám sát định kỳ hàng tháng.

2.2. Đánh giá an toàn thông tin cho ứng dụng (hoặc hệ thống thông tin)

- Số lượng: 1 hệ thống

- Thời gian thực hiện: 60 ngày.

- Hình thức đánh giá: Gray box

- Đơn vị đánh giá sẽ thực hiện đánh giá hệ thống khi được chủ đầu tư/quản trị hệ thống, ứng dung cung cấp thông tin mô tả về hệ thống và các tài khoản theo các mức quyền từ thấp đến cao để đánh giá, tìm ra nhiều điểm yếu nhất.

- Phát hiện các điểm yếu, lỗ hổng trong hệ thống, phân tích mức độ ảnh hưởng của các lỗ hổng, điểm yếu.

- Tư vấn phương án khắc phục đối với từng điểm yếu, lỗ hổng (nếu có).

- Báo cáo chi tiết về các điểm yếu, lỗ hổng đã tìm thấy.

2.3. Đào tạo an toàn thông tin đối tượng cán bộ quản trị vận hành hệ thống, tổ ứng cứu sự cố ATTT.

- Tên khóa đào tạo: Đào tạo về kỹ năng phòng chống tấn công website cho cán bộ quản trị vận hành hệ thống, tổ ứng cứu sự cố ATTT.

- Thời gian đào tạo: 01 ngày.

- Hình thức thực hiện: Trực tuyến

- Số lượng học viện: Tối đa 15 người

- Nội dung khóa học: Đào tạo an toàn thông tin hệ thống OT, cụ thể:

+ TCVN 14423:2025 an ninh mạng - yêu cầu đối với hệ thống thông tin quan trọng.

+ Quy định 717/QĐ- EVN ngày 31/5/2025 đảm bảo an ninh mạng và an toàn thông tin trong Tập đoàn Điện lực Việt Nam.

+ Các rủi ro an toàn thông tin phổ biến với hệ thống công nghệ thông tin của ngành điện lực Việt Nam.

+ Các giải pháp kỹ thuật nghiệp vụ an toàn thông tin chuyên sâu (tối thiểu 03 giải pháp) cần triển khai để đảm bảo an toàn thông tin với hệ thống công nghệ thông tin của ngành điện lực Việt Nam.

+ Hướng dẫn cách phát hiện và cách khắc phục tối thiểu 03 sự cố an toàn thông tin (Case study) điển hình đã xảy ra với hệ thống công nghệ thông tin ngành điện lực.

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:

5.1. Giám sát an toàn thông tin cho các địa chỉ IP/Domain công khai

- Báo cáo hàng tháng kết quả giám sát do lãnh đạo đơn vị thực hiện giám sát, rà quét ký (bản cứng).
- Đề xuất giải pháp và hỗ trợ xử lý các lỗ hổng bảo mật (nếu có) khi phát hiện lỗ hổng bảo mật của Công ty.

5.2. Đánh giá an toàn thông tin cho ứng dụng

Báo cáo chi tiết về các điểm yếu, lỗ hổng đã tìm thấy, tư vấn phương án khắc phục đối với từng điểm yếu, lỗ hổng (nếu có).

5.3. Đào tạo an toàn thông tin

- Chứng nhận các học viên tham gia khóa học.
- Báo cáo tổng kết khóa đào tạo.

6. Yêu cầu về bản quyền phần mềm sử dụng trong quá trình kiểm tra đánh giá an toàn thông tin

- Nhà thầu cung cấp chứng nhận bản quyền các phần mềm sử dụng trong quá trình kiểm tra đánh giá ATTT. Các công cụ nhà thầu sử dụng trong công tác, kiểm tra đánh giá ATTT phải có chứng nhận bản quyền hoặc tương đương.

7. Các yêu cầu Cam kết về việc tuân thủ quy định

Nhà thầu phải cam kết đáp ứng các yêu cầu về đảm bảo an toàn bảo mật thông tin đối với toàn bộ các hệ thống, dịch vụ của hệ thống trong phạm vi gói thầu khi thực hiện triển khai.

Nhà thầu phải cam kết chịu hoàn toàn trách nhiệm về mọi thiệt hại phát sinh do việc khiếu nại của bên thứ ba về việc vi phạm bản quyền sở hữu trí tuệ liên quan đến dịch vụ do nhà thầu cung cấp cho Bên mời thầu.