UBND TỈNH TÂY NINH
SỞ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 1774 /TB-STTTT

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

Tây Ninh, ngày 10 tháng 9 năm 2024

THÔNG BÁO

V/v mời chào thẩm định giá cho gói thầu: "Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh và diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng" (lần 2)

Căn cứ Kế hoạch số 1368/KH-UBND ngày 10/5/2024 của UBND tỉnh về Chuyển đổi số và đảm bảo an toàn thông tin mạng tỉnh Tây Ninh năm 2024.

Sở Thông tin và Truyền thông kính mời các đơn vị có chức năng thẩm định giá tham gia chào giá dịch vụ thẩm định giá cho gói thầu: "Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh và diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng" với các nội dung cụ thể như sau:

- Danh mục, số lượng, nội dung cần thẩm định giá: (*Phụ lục kèm theo)*

- Bảng chào giá lập chứng thư thẩm định giá (có đóng dấu ký tên Đại diện hợp pháp).

- Thời gian nhận Bảng chào giá là 7 ngày tính từ ngày ra thông báo. Địa điểm nhận hồ sơ: 006, Trần Quốc Toản, Phường 2, Thành phố Tây Ninh, tỉnh Tây Ninh. Điện thoại: 0276 3 611169 (gặp Tiến)./.

Trân trọng!

Nơi nhận:
- Các Công ty, đơn vị cung cấp dịch vụ thẩm định giá;
- Đăng thông báo lên cổng TTĐT Sở;
- Lưu: VT. TTGSĐH.

KT.GIÁM ĐỐC
PHÓ GIÁM ĐỐC

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TỈNH TÂY NINH

Nguyễn Trung Hiếu

PHỤ LỤC

Thông tin chi tiết danh mục, số lượng, nội dung cần thẩm định giá cho gói thầu "Đánh giá an toàn thông tin cho Trung tâm tích hợp dữ liệu tỉnh và diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng"

(Đính kèm Thông báo số /TB-STTTT ngày tháng năm 2024 của Sở Thông tin và Truyền thông tỉnh Tây Ninh)

1. Dịch vụ "Đánh giá an toàn thông tin cho trung tâm tích hợp dữ liệu tỉnh năm 2024 (hệ thống thông tin cấp độ 3)".

- Địa điểm thực hiện: Trung tâm tích hợp dữ liệu tỉnh Tây Ninh.
- Nội dung thực hiện:

1.1. Danh sách các website, máy chủ và ứng dụng trên nền tảng mobile.

Stt	Danh sách	Đơn vị tính	Số lượng	Mô tả
			4	
I	**Đánh giá ATTT hệ thống ứng dụng trên nền tảng WEB**			
1	Đánh giá ATTT hệ thống ứng dụng trên nền tảng WEB https://motcua.tayninh.gov.vn/	Website	01	Hệ thống Một cửa điện tử của tỉnh Tây Ninh
2	Đánh giá ATTT hệ thống ứng dụng trên nền tảng WEB https://dichvucong.tayninh.gov.vn/	Website	01	Hệ thống Dịch vụ công trực tuyến tỉnh Tây Ninh
3	Đánh giá ATTT hệ thống ứng dụng trên nền tảng WEB https://1022.tayninh.gov.vn/	Website	01	Hệ thống thông tin tiếp nhận phản ánh người dân
4	Đánh giá ATTT hệ thống ứng dụng http://lgsp.tyninh.gov.vn/	Website	01	Hệ thống tích hợp, chia sẻ dữ liệu dùng chung phục vụ kết nối các hệ thống thông tin trong nội bộ trong tỉnh và kết nối các hệ thống thông tin trong tỉnh với các hệ

				thống thông tin từ các bộ, ngành, địa phương khác.
II	**Ứng dụng trên nền tảng Mobile**		**01**	
1	Tây Ninh Smart (React-native)	Ứng dụng	01	
III	**Đánh giá các máy chủ**		**33**	
1	Hệ thống Một cửa điện tử và Dịch vụ công	Máy chủ	15	Gồm: 9 máy chủ hệ điều hành (HĐH) Microsoft Windows Server; 6 máy chủ HĐH CentOS.
2	Hệ thống Hệ thống thông tin tiếp nhận phản ánh 1022 Tây Ninh	Máy chủ	8	Gồm: 6 máy chủ HĐH Microsoft Windows Server ; 2 máy chủ HĐH Ubuntu.
3	Hệ thống LGSP	Máy chủ	10	Gồm: 10 máy chủ HĐH CentOS.

1.2. Nội dung thực hiện đánh giá:

STT	Nội dung công việc
A	**Kiểm thử, kiểm tra, đánh giá an toàn thông tin website**
1	Kiểm tra đánh giá cấu hình
1.1	*Khảo sát thu thập thông tin*
1.2	*Đánh giá cho ứng dụng dịch vụ Front end*
1.3	*Đánh giá cho ứng dụng dịch vụ Back end*
1.4	*Đánh giá quản lý định danh*
1.5	*Đánh giá tính xác thực*

1.6	*Đánh giá quá trình phân quyền*
1.7	*Đánh giá quản lý phiên đăng nhập*
1.8	*Đánh giá quá trình kiểm soát dữ liệu đầu vào*
1.9	*Đánh giá độ an toàn của mã hóa*
2	Dò quét lỗ hổng tồn tại trên ứng dụng
2.1	*Dò quét chủ động*
2.2	*Dò quét thụ động*
2.3	*Kiểm tra false positive*
2.4	*Đánh giá an toàn thông tin cho ứng dụng trên Web*
3	Báo cáo kết quả
3.1	*Quá trình đánh giá, phạm vi đánh giá*
3.2	*Quy mô đánh giá*
3.3	*Công cụ đánh giá*
3.4	*Hướng dẫn khắc phục các lỗ hổng an toàn thông tin*
B	**Kiểm thử, kiểm tra, đánh giá an toàn thông tin ứng dụng mobile**
1	Kiểm tra đánh giá cấu hình
1.1	*Khảo sát thu thập thông tin*
1.2	*Đánh giá cho ứng dụng dịch vụ Front end*
1.3	*Đánh giá cho ứng dụng dịch vụ Back end*
1.4	*Đánh giá quản lý định danh*
1.5	*Đánh giá tính xác thực*
1.6	*Đánh giá quá trình phân quyền*
1.7	*Đánh giá quản lý phiên đăng nhập*

1.8	*Đánh giá quá trình kiểm soát dữ liệu đầu vào*
1.9	*Đánh giá độ an toàn của mã hóa*
2	Dò quét lỗ hổng tồn tại trên ứng dụng
2.1	*Dò quét chủ động*
2.2	*Dò quét thụ động*
2.3	*Kiểm tra false positive*
2.4	*Đánh giá an toàn thông tin cho ứng dụng trên ứng dụng mobile*
3	Báo cáo kết quả
3.1	*Quá trình đánh giá, phạm vi đánh giá*
3.2	*Quy mô đánh giá*
3.3	*Công cụ đánh giá*
3.4	*Hướng dẫn khắc phục các lỗ hổng an toàn thông tin*
C	**Rà soát và làm sạch mã độc cho máy chủ/máy trạm quản trị**
1	Giám sát bất thường trên vùng mạng có hệ thống cần rà soát
1.1	*Triển khai công cụ giám sát mạng, rà soát theo danh mục*
1.2	*Triển khai công cụ giám sát bất thường lớp mạng, thu thập log hệ thống, phát hiện các dấu hiệu bất thường của mã độc, webshell cho vùng mạng giám sát*
1.3	*Triển khai các công cụ thu thập log dữ liệu trên máy chủ/máy trạm*
2	Rà soát phát hiện các đối tượng nhiễm mã độc
2.1	*Rà soát các mục tự khởi động cùng hệ thống, các tiến trình, các kết nối mạng, phát hiện các tập tin, tiến trình, kết nối độc hại*
2.2	*Rà soát các thư mục, tập tin, tiến trình, dấu hiệu thường gặp của các loại mã độc tấn công có chủ đích, đặc biệt là các loại mã độc nhắm vào Việt Nam*

2.3	*Rà soát các thành phần mức nhân hệ thống (kernel module), các driver, phát hiện mã độc mức nhân hệ thống (rootkit)*
3	Làm sạch, phân tích điều tra và thắt chặt an toàn thông tin trên các hệ thống
3.1	*Gỡ bỏ các mã độc phát hiện được trên hệ thống*
3.2	*Thu thập log hệ thống, xác định thời gian, nguồn lây nhiễm*
3.3	*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...)*
3.4	*Thực hiện siết cấu hình ATTT đối với các máy chủ/máy tính quản trị không phát hiện nhiễm mã độc*
3.5	*Thực hiện cài đặt lại, sau đó rà soát kiểm tra lại, siết cấu hình ATTT, tiến hành cài đặt lại hệ thống ứng dụng và online dịch vụ đối với các máy chủ/máy tính quản trị phát hiện bị mã hóa dữ liệu, không còn dấu vết mã độc*
3.6	*Thực hiện gỡ bỏ mã độc, siết cấu hình ATTT, online dịch vụ đối với các máy chủ/máy tính quản trị phát hiện nhiễm mã độc, chưa bị mã hóa dữ liệu*
4	Xây dựng báo cáo hồ sơ kết quả thực hiện
4.1	*Sau khi tất cả đã được làm sạch, giám sát không phát hiện dấu hiệu nghi ngờ, thực hiện xây dựng báo cáo chi tiết về nội dung kết quả thực hiện gồm: Báo cáo hiện trạng lây nhiễm, phá hoại của mã độc. Có hướng dẫn, khuyến nghị thực hiện sửa lỗi lại các server, hệ thống đang gặp tổn hại do mã độc gây nên. Nêu rõ các điểm yếu của hệ thống để có phương án khắc phục*
D	**Kiểm tra, đánh giá và quản lý rủi ro ATTT đối với các hệ thống thông tin**
1	Kiểm tra, rà soát, tư vấn khắc phục điểm yếu bảo mật của mô hình kết nối các máy chủ
1.1	*Tìm hiểu hoạt động, yêu cầu của hệ thống máy chủ*
1.2	*Khảo sát mô hình từng hệ thống máy chủ hiện tại*

1.3	*Dựa trên các tiêu chuẩn và hướng dẫn ATTT đưa ra báo cáo đánh giá và các khuyến nghị khắc phục*
2	Kiểm tra, rà soát, tư vấn khắc phục điểm yếu bảo mật của các máy chủ
2.1	*Thu thập thông tin*
2.1.1	*Xác định sự tồn tại của các thiết bị filter: Firewall, IPS…*
2.1.2	*Thu thập thông tin phần cứng máy tính*
2.1.3	*Thu thập thông tin về hệ điều hành đang sử dụng.*
2.1.4	*Thu thập thông tin về danh sách các phần mềm và phiên bản đang cài đặt.*
2.1.5	*Thu thập thông tin về danh sách các dịch vụ đang chạy trên máy tính.*
2.1.6	*Thu thập phân loại các thông tin phần mềm thu thập được thành các danh mục tương ứng*
2.2	*Dò quét và phân tích lỗ hổng*
2.2.1	*Kiểm tra thông tin chi tiết về các bản vá cần cập nhật/đã cập nhật.*
2.2.2	*Kiểm tra thông tin chi tiết các lỗ hổng theo các chuẩn về lỗ hổng CVE, CPE và OVAL.*
2.2.3	*Kiểm tra thông tin về các tiến trình phần mềm đang thực thi.*
2.2.4	*Kiểm tra thông tin về các dịch vụ (services) đang được triển khai trên máy tính.*
2.2.5	*Kiểm tra thông tin về các chương trình khởi động cùng máy tính.*
2.2.6	*Kiểm tra thông tin về cấu hình kiểm soát truy cập của máy tính (User Account Control).*
2.2.7	*Kiểm tra thông tin về cấu hình hoạt động Internet của hệ thống (Internet Options).*
2.2.8	*Kiểm tra thông tin kiểm tra hệ thống file và tổng hợp những file nghi ngờ dẫn tới nguy cơ mất mát thông tin.*

2.2.9	*Dựa vào một số các thông tin thu thập được ở trên, phần mềm sẽ phát hiện thông minh các nguy cơ mất an ninh an toàn, thu thập các mẫu nghi ngờ mất an toàn.*
2.2.10	*Hỗ trợ phân tích đánh giá an ninh an toàn cho các tệp định dạng tệp thực thi trên Windows (exe, dll, com,...).*
2.2.11	*Phát hiện các hành vi mạng bất thường;*
2.2.12	*Phát hiện các cấu hình an toàn thông tin chưa phù hợp.*
2.2.13	*Điểm yếu mật khẩu: Không đặt mật khẩu xác thực, mật khẩu yếu dễ đoán.*
2.2.14	*Thu thập bằng chứng và xác nhận mức độ chính xác thông tin các lỗ hổng.*
2.3	*Thử nghiệm xâm nhập*
2.3.1	*Xác nhận, chứng minh sự tồn tại của điểm yếu trên hệ thống.*
2.3.2	*Loại bỏ những kết quả sai mà công cụ dò quét được.*
2.3.3	*Minh họa cách thức khai thác điểm yếu, giúp khách hàng hiểu rõ mức độ nguy hiểm và ảnh hưởng của điểm yếu đối với hệ thống mạng*
2.3.4	*Password attack: Thử nghiệm các kiểu tấn công password vào các thiết bị mạng, bảo mật và thiết bị truyền dẫn*
2.3.5	*Exploits: Thử nghiệm khai thác các lỗ hổng bảo mật được tìm thấy ở phần trước.*
2.4	*Tái đánh giá hệ thống*
2.4.1	*Tái đánh giá các điểm yếu trong lần đánh giá đầu tiên*
2.4.2	*Xác định có điểm yếu mới phát sinh hay không*
2.4.3	*Khẳng định hệ thống đã an toàn sau hai lần đánh giá.*
3	Kết quả đạt được: Báo cáo tổng kết Kiểm tra, đánh giá an toàn thông tin cho hệ thống máy chủ.
3.1	*- Phần 1: Đơn vị thực hiện sẽ mô tả chi tiết các điểm yếu bảo mật phát hiện được trên hệ thống máy chủ của hệ thống. Các lỗ hổng,*

	điểm yếu bảo mật phát hiện được sẽ được phân loại theo mức độ rủi ro: Cao, Thấp và Trung Bình. Kèm theo đó là hình ảnh minh họa cách thức, kết quả quá trình đánh giá. *- Phần 2: Đơn vị thực hiện 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 khách hàng*

2. **Dịch vụ "Diễn tập thực chiến ứng phó sự cố an toàn thông tin mạng".**

- Địa điểm thực hiện: tỉnh Tây Ninh.
- Nội dung thực hiện: Chi tiết nội dung diễn tập thực chiến ATTT.

Stt	Nội dung công việc thực hiện
I	**Xây dựng phương án diễn tập**
1	Xây dựng phương án cho Đội tấn công: - Các công cụ, kỹ thuật sử dụng để khai thác lỗ hổng bảo mật, tấn công hệ thống; - Các lỗ hổng bảo mật khai thác; - Các kịch bản tấn công khai thác, tấn công leo thang, lưu vết tấn công cho 02 ứng dụng. - Phương án thực hiện gồm các nội dung sau: + Mô tả theo các vector tấn công từ Internet; + Các kịch bản gồm các bước: Thăm dò (Reconnaissance), Chuẩn bị công cụ (Weaponization), Khai thác (Exploitation), Dọn dẹp (Closure). Trong kịch bản thực hiện có thể bao gồm Social Engineering.
2	Xây dựng phương án diễn tập chung: - Điều phối hoạt động chung của buổi diễn tập; - Điều phối hoạt động Đội tấn công, Đội phòng thủ, ... - Phương án thực hiện gồm: + Khai mạc: thực hiện bằng hình thức trực tuyến giới thiệu về mục tiêu diễn tập, các quy định trong quá trình diễn tập, thời gian bắt đầu và kết thúc diễn tập, ... ; + Diễn tập chính thức: trong vòng 14 ngày tính từ thời điểm khai mạc; + Đào tạo, tổng kết, bế mạc: 01 ngày, hình thức trực tiếp, các đội báo cáo về kết quả diễn tập, tổng kết chung.

II	**Xây dựng nội dung đào tạo nâng cao trình độ chuyên môn**
1	Xây dựng nội dung đào tạo bao gồm: - Các hình thức tấn công và phòng thủ đã thực hiện trong thời gian diễn tập; - Các hình thức và cách xử lý, giảm thiểu tấn công trên ứng dụng web (XSS, SQL Injection, File Upload, Directory Traversal, …); - Rà soát, phân tích và xử lý mã độc webshell; - Kỹ năng điều tra xử lý sự cố, phân tích các dấu hiệu tấn công, điều tra về lỗ hổng, kiểm thử ứng dụng web; - Nội dung gồm lý thuyết và thực hành với các tình huống giả định.
III	**Triển khai hoạt động diễn tập (15 ngày)**
1	Tổ chức hoạt động diễn tập thực chiến (14 ngày):
1.1	*Tổ chức hoạt động ngày khai mạc trực tuyến (0,5 ngày): giới thiệu mục tiêu, nội quy diễn tập, giải đáp các thắc mắc,…*
1.2	*Triển khai diễn tập của Đội tấn công:* *- Thực hiện tấn công hệ thống mục tiêu theo phương án đã xây dựng;* *- Báo cáo kết quả tấn công vào các hệ thống mục tiêu;* *- Làm sạch hệ thống bị xâm nhập sau khi kết thúc diễn tập.*
1.3	*Điều phối hoạt động giữa các đội trong quá trình diễn tập.*
2	Tổ chức đào tạo, tổng kết và bế mạc hoạt động diễn tập hình thức trực tiếp (01 ngày):
2.1	*Đào tạo nâng cao trình độ chuyên môn cho đội ngũ cán bộ làm về công tác ATTT theo nội dung đã xây dựng.*
2.2	*Tổng kết, bế mạc diễn tập:* *- Tổng hợp báo cáo của Đội tấn công, Đội phòng thủ;* *- Đánh giá kết quả diễn tập;* *- Tổ chức hoạt động tổng kết, bế mạc diễn tập.*
2.3	*Lập báo cáo triển khai công tác diễn tập đã thực hiện.*

IV	**Công tác hậu cần phục vụ diễn tập**
1	Chi phí Teabreak giữa giờ trong ngày đào tạo, tổng kết trực tiếp (60 người/01 buổi).
2	- Chi phí ấn phẩm truyền thông (standee, backdrop, nametag, bandroll, …). - Truyền thông, chụp ảnh, đưa tin sự kiện. - Chi phí in ấn tài liệu phục vụ đào tạo, diễn tập.