ALLEGATO "A"

CAPITOLATO SPECIALE
PER IL MANTENIMENTO DELLA CERTIFICAZIONE ISO 27001
AL PROCESSO CRS E AL SERVIZIO ELETTRONICO DI RECAPITO CERTIFICATO

Oggetto

La presente Asta Pubblica, costituita da 3 lotti, ha per oggetto il mantenimento e il rinnovo dell'attuale certificazione ISO 27001" Sicurezza delle Informazioni dei servizi: CRS (Common Reporting Standard), SERC (Servizio Elettronico di Recapito Certificato), RDD (Registro dei Domicili Digitali), all'interno della IT (Information Technology) della Pubblica Amministrazione della Repubblica di San Marino. Dichiarazione di Applicabilità Rev. 3 del 20/09/2021".

Dichiarazione di confidenzialità

I documenti e le informazioni trasmessi nell'ambito della presente Asta pubblica, sono da considerarsi strettamente confidenziali; in particolare, le informazioni contenute nei relativi allegati non possono essere copiate, riprodotte, divulgate, trasferite, trasformate in qualsiasi forma, trasmesse o pubblicate.

Riservatezza

L'impresa partecipante, e tutte le figure ad essa collegate, dovrà tenere riservate tutte le informazioni concernenti le attività di cui sia venuta o potrà venire a conoscenza in occasione della definizione ed esecuzione della presente Asta. Il medesimo impegno sarà a carico dell'Ufficio Informatica, Tecnologia, Dati e Statistica dal momento della ricezione delle offerte.

LOTTO 1 – Attività di analisi, redazione della documentazione e coordinamento per mantenimento e rinnovo della certificazione ISO 27001

Le attività richieste per soddisfare la prima parte sono il mantenimento e il rinnovo della certificazione ISO27001 del processo di scambio automatico delle informazioni in ambito OCSE denominato CRS (Common Reporting Standard), SERC (Servizio Elettronico di Recapito Certificato) e RDD (Registro dei Domicili Digitali), all'interno della IT (Information Technology) della Pubblica Amministrazione. La certificazione già acquisita dal 13 ottobre 2016 (che comprendeva solo il servizio CRS) è stata annualmente revisionata mediante verifica ispettiva da parte dell'Ente Certificatore e rinnovata ad ottobre 2023 con l'aggiunta SERC (Servizio Elettronico di Recapito Certificato) e RDD (Registro dei Domicili Digitali).
Si allega il documento N°5 del Manuale ISO 27001 denominato ADC Analisi Del Contesto.
Le attività necessarie per il mantenimento ed il rinnovo della certificazione prevedono:

- Analisi ed eventuale aggiornamento delle politiche di sicurezza
- Analisi ed eventuale aggiornamento dell'ambito di applicazione del SGSI
- Analisi ed eventuale aggiornamento della valutazione del rischio
- Analisi ed eventuale aggiornamento della gestione del rischio
- Definizione degli obiettivi e dei relativi controlli da realizzare

- Analisi ed eventuale aggiornamento della dichiarazione di applicabilità
- Esecuzione audit interno di sistema in conformità allo Standard ISO 27001
- Attività di supporto nelle giornate di audit dell'Ente di Certificazione UKAS Numero UKAS: 0043 Denominazione: United Registrar of Systems Ltd
- Esecuzione audit interno generale di sistema in conformità allo standard ISO 27001;
- Attività di supporto nelle giornate di audit dell'Ente di Certificazione per la certificazione CRS+SERC.

Riferimenti normativi:
Decreto Delegato 30 gennaio 2020 n. 9
Regolamento 22 novembre 2018 n.7
Decreto Delegato 26 luglio 2018 n.92
Decreto Delegato 15 giugno 2018 n.65
Legge 23 agosto 2016 n.114
Decreto Delegato 11 aprile 2016 n.46
Legge 29 maggio 2013 n.58
Regolamento 30 dicembre 2015 n.20
Decreto 8 novembre 2005 n.156
Legge 20 luglio 2005 n.115

Le attività devono prevedere l'analisi del contesto, la predisposizione dei documenti, il coordinamento delle attività e tutto quanto necessario al fine di mantenere e rinnovare la certificazione ISO 27001.

In questo contesto viene richiesta anche l'attività di "Test di Sicurezza" attraverso tecniche di Vulnerability Assessment e Penetration Test in modalità Black Box su indirizzi esposti alle reti esterne ed in modalità Gray Box su due reti interne dove verranno allocati e messi a disposizione due server, attestati nelle opportune reti, per poter effettuare i test di vulnerabilità.
L'attività di "Test di Sicurezza" si dovrà svolgere in due fasi, la prima da remoto con l'esecuzione dei test e la raccolta delle vulnerabilità, la seconda presso il committente dove verranno presentati i report, discusse e analizzate le vulnerabilità riscontrate, valutando le possibili soluzioni applicabili per mitigare o eliminare le minacce riscontrate.
Il fornitore, nel pieno rispetto degli standard ISO, dovrà possedere un'organizzazione, mezzi e risorse idonee ed adeguate sotto il profilo dei servizi professionali ed essere in grado di offrire un servizio con elevato standard di qualità.
Il servizio dovrà essere eseguito dal fornitore, con la massima cura, diligenza, tempestività e riservatezza, mediante l'impiego di un'organizzazione efficiente, risorse e mezzi adeguati.
Il fornitore si impegna, inoltre, a svolgere tutte le attività, anche se non espressamente indicate negli atti di gara e nel contratto, al fine di garantire l'efficiente svolgimento del servizio.

Specificamente:

- Presentazione del team e delle responsabilità (profili professionali)
- Definizione dello "scope" e degli obiettivi
- Definizione delle regole di ingaggio per i diversi target
- Definizione delle linee di comunicazione
- Analisi delle tecnologie adottate
- Presentazione della strategia di analisi

Attività di preanalisi:

- Network Footprinting
- Definizione di Tool
- Preparazione e customizzazione dei server di analisi

Attività di enumeration:

- Enumerazione dei sistemi e degli indirizzi IP
- Information gathering passivo
- Information gathering attivo (previa autorizzazione)
- Protocolli
- Stato dei sistemi

Attività di analisi:

- Analisi avanzata basata su tool specifici
- Analisi manuale
- Vulnerability assessment dei sistemi ed applicazioni (attività manuale e con scansioni previa autorizzazione)

Verifica delle vulnerabilità Penetration Test (previa autorizzazione):

- Attacchi automatici
- Attacchi manuali
- Exploitation delle vulnerabilità scoperte escluso Denial of Service
- Client-side attacks
- Web Application Attacks
- Password Attacks
- Privilege escalation
- Network attacks (Port Forwarding / Redirection e Tunneling)
- Social engineering attacks (previa autorizzazione)

Documentazione e reportistica:

- Raccolta e registrazione delle evidenze informatiche
- Redazione della documentazione
- Consegna, presentazione e discussione dei risultati

Viene richiesta la produzione di due report, uno di carattere tecnico ed uno executive che descriva:

- il target analizzato
- le metodologie ed i riferimenti utilizzati per l'analisi
- tutte le vulnerabilità ed in genere le anomalie riscontrate e per ciascuna la nomenclatura standard CVE associata (dove possibile)
- classificazione oggettiva (possibilmente basata su scoring riconosciuti come CVSS)
- descrizione della segnalazione e riferimenti per poterla riprodurre
- IP e relativo hostname affetto dalla vulnerabilità
- impatti derivanti
- soluzioni concrete per la remediation
- presenza di exploit pubblici della vulnerabilità
- riassunto delle segnalazioni e relativa remediation di alto livello per il management

Per l'esecuzione di ciascuna delle richieste il fornitore dovrà indicare l'impegno espresso in giorni/uomo. Potranno essere richiesti maggiori dettagli per comprendere meglio le specificità, data la riservatezza del processo, alcune informazioni saranno fornite firmando un apposito accordo (NDA).
Il piano di lavoro sarà definito in comune accordo pianificando un calendario di incontri e di attività. Per ogni incontro/attività si dovrà produrre un report di quanto è stato svolto.

Si precisa che per il Vulnerability Assessment e Penetration Test possono essere considerati i seguenti numeri:
18 IP in uso da server http/https o sftp
58 IP in dbnet nella 172.30.2.0/24
1175 PC nel dominio
4130 utenti registrati a dominio (non tutti utenti attivi)
1293 gruppi registrati a dominio

In considerazione della scadenza della certificazione ad Ottobre 2023, le attività dovranno concludersi entro il mese di Settembre 2023 per poi procedere con la verifica ispettiva dell'organismo di sorveglianza dell'Ente di Certificazione, come indicato nel successivo Lotto 2.

L'offerta economica deve comprendere:

- le attività per la richiesta di mantenimento dell'attuale certificazione CRS SERC RDD ISO 27001;
- le attività di Vulnerability/Penetration Test;
- l'affiancamento nella fase di controllo/certificazione dell'ente accreditato.

LOTTO 2 – Audit della Certificazione ISO 27001

Il presente lotto riguarda esclusivamente l'attività di Audit finalizzata alla Certificazione ISO 27001 del processo CRS (Common Reporting Standard), SERC (Servizio Elettronico di Recapito Certificato) e RDD (Registro dei Domicili Digitali).
Per i sopra elencati, già certificato (71347/A/0001/UK/It), si richiede il mantenimento mediante visita ispettiva per gli anni 2023 e 2024 e il rinnovo dello stesso certificato nell'anno 2025.
Si ricorda che il Servizio Elettronico di Recapito Certificato (tNotice) è un servizio fornito da Poste San Marino in ATI con Inposte srl, la Pubblica Amministrazione di San Marino (PA) necessita della certificazione ISO 27001 in quanto fornisce servizi sistemistici, di hosting e di gestione dei processi collegati ai servizi della PA.
L'offerta dovrà essere comprensiva di tutti i costi relativi al mantenimento, al rinnovo della nuova certificazione e all'Audit compresa la visita di sorveglianza.
La certificazione potrà essere rilasciata esclusivamente da Organismi di Certificazione accreditati quali membri IAF (International Accreditation Forum).

LOTTO 3 - Microsoft Active Directory in ottica Assume Breach

Si richiedono 6 ore di istruzioni da erogarsi in 2 giornate con l'obbiettivo di formare il personale specialistico a recepire i risultati di un prossimo Assiume Breach condotto nella infrastruttura Microsoft Active Directory.

Al termine i tecnici dovranno essere in grado di comprendere i possibili gradi di libertà che un utente con privilegi minimi può avere per effettuare movimenti laterali ed intraprendere un percorso di privilege escalation.
Le figure che parteciperanno sono già esperte del mondo Microsoft e gestiscono l'infrastruttura Microsoft Active Directory. Si richiede che l'istruttore abbia un alto profilo e le certificazioni OSCP (Offensive Security Certified Professional), CRTP (Certified Red Team Professional).

Roberta Mularoni
Roberta Mularoni
2023.07.21 13:44:46+02'00'