**Avviso per Indagine di Mercato per servizi di vulnerability assessment e remediation relativi alla sicurezza informatica**

LepidaSpA, società in house con oltre 430 Soci pubblici sul territorio dell'Emilia-Romagna, con azioni nel campo dell'ICT, intende verificare, attraverso il presente Avviso di Indagine di Mercato (pubblicato anche sul sito www.lepida.it), per sé e per i propri Soci, quali servizi sono presenti sul mercato con le caratteristiche di seguito riportate. Tali servizi devono essere già disponibili sul mercato, possibilmente su Consip o su IntercentER, con tutte le caratteristiche richieste, e non realizzati su commessa o mediante azioni evolutive future. LepidaSpA si riserva di utilizzare i risultati di questo Avviso per sé e per i propri Soci e di effettuare eventuali acquisizioni, per sé, per i propri Soci o dirette dai propri Soci utilizzando i risultati di questo Avviso, anche mediante ulteriori procedure da identificare in funzione dei riscontri ricevuti proprio da questa procedura.

I servizi di interesse per la presente indagine di mercato sono i seguenti:

- Vulnerability Assessment (VA) distinti nelle seguenti tipologie:
    A. VA Infrastrutturale: attività di verifica finalizzata a rilevare eventuali vulnerabilità, errori di configurazione o carenze in termini di sicurezza su sistemi server, postazioni di lavoro e apparati di rete, che li rendano esposti ad attacchi. Può essere:
        - Esterno: attività condotta sugli host esposti sul perimetro della rete pubblica Internet;
        - Interno: attività condotta sugli host attestati alla rete interna del cliente.
    B. VA Applicativo: attività di verifica basata su analisi dinamiche finalizzata a rilevare eventuali vulnerabilità, errori di configurazione o carenze in termini di sicurezza su applicazioni web basate su tecnologie eterogenee (es. .NET, PHP, C/C++, Java, J2EE, ASP), che consentano interazioni illecite con i servizi o accessi non autorizzati ai dati contenuti nei database di backend. Può essere:
        - Esterno: attività condotta su applicazioni esposte sul perimetro della rete pubblica Internet;
        - Interno: attività condotta su applicazioni raggiungibili dalla rete interna del cliente;

    e inoltre:
        - White Box: attività condotta dopo aver ricevuto dal cliente opportune informazioni tecniche relative alle applicazioni da testare;
        - Black Box: attività condotta senza disporre di alcuna informazione tecnica relativa alle applicazioni da testare.
- Vulnerability Remediation (VR) distinti nelle seguenti tipologie:
    C. VR Infrastrutturale: implementazione di contromisure di sicurezza volte a risolvere vulnerabilità, errori di configurazione o carenze in termini di sicurezza su sistemi server, postazioni di lavoro e apparati di rete rilevate a seguito di un vulnerability assessment;
    D. VR Applicativo: implementazione di contromisure di sicurezza volte a risolvere vulnerabilità, errori di configurazione o carenze in termini di

sicurezza su applicazioni web basate su tecnologie eterogenee (es. .NET, PHP, C/C++, Java, J2EE, ASP) e database (es. SQL Server, Oracle, DB2, MySQL, PostgreSQL) rilevate a seguito di un vulnerability assessment.

I servizi di vulnerability assessment devono essere erogati nelle seguenti modalità vincolanti e non derogabili:

1. definizione degli obiettivi e delle modalità operative con il cliente e successiva esecuzione delle attività in autonomia;
2. esecuzione di scansioni automatizzate e attività manuali per test specifici o verifiche volte a eliminare eventuali falsi positivi;
3. utilizzo delle best practices di settore (es. OSSTMM, OWASP);
4. produzione di un report compatto e dettagliato riassuntivo dei risultati dell'attività e suddiviso in tre differenti aree: Executive Summary, riassunto di alto livello destinato al management del cliente; Technical Details, parte tecnica che descrive nel dettaglio gli asset verificati, le relative caratteristiche hardware e/o software, le vulnerabilità riscontrate, il loro impatto e la relativa severità; Remediation Plan, sezione tecnica con istruzioni precise su come risolvere le problematiche identificate;
5. svolgimento delle attività da parte di personale altamente qualificato e referenziato, avente esperienza di almeno 4 anni e in possesso di certificazioni professionali riconosciute internazionalmente (es. CISSP, OPSA, OPST, CISA, CEH) relative al servizio in oggetto.

I servizi di vulnerability remediation devono essere erogati nelle seguenti modalità vincolanti e non derogabili:

1. definizione degli obiettivi e delle modalità operative con il cliente e successiva esecuzione delle attività in autonomia, avendo a disposizione il remediation plan prodotto a seguito di un vulnerability assessment precedentemente condotto;
2. esecuzione di attività di aggiornamento o configurazione sui più diffusi sistemi operativi, database, web server, content management system, application server, linguaggi e framework di sviluppo, apparati di rete e dispositivi di sicurezza;
3. produzione di un report compatto e dettagliato, di natura tecnica, riassuntivo delle attività svolte e delle problematiche corrette;
4. svolgimento delle attività da parte di personale altamente qualificato e referenziato, avente esperienza di almeno 4 anni e in possesso di certificazioni professionali riconosciute internazionalmente relative al servizio in oggetto.

E’ ammesso che un fornitore risponda unicamente per i servizi della tipologia VA o per quelli della tipologia VR, ma non per entrambi, al fine di garantire la dovuta indipendenza tra le attività di assessment e di remediation eventualmente richieste da un medesimo cliente.

Si richiede di rispondere, entro e non oltre Martedì 06.12.2016 alle ore 12, per email a gianluca.mazzini@lepida.it, illustrando dettagliatamente per ciascuno dei servizi richiesti le caratteristiche e le modalità di erogazione della propria offerta, con particolare riferimento ai singoli requisiti richiesti, e, relativamente ai servizi di VA, di fornire report di esempio.

Si richiede inoltre di indicare quale potrebbe essere una base di costo, possibilmente orientata ad un meccanismo scalabile in funzione della popolazione, meglio se con un costo a singolo cittadino, altrimenti per fasce.

Responsabile unico del Procedimento è Gianluca Mazzini, gianluca.mazzini@lepida.it 3358160916

Data di pubblicazione: 21.11.2016