

RICHIESTA DI OFFERTA PER SERVIZI DI VERIFICA SICUREZZA INFRASTRUTTURE
CIG Z1625944D1

SPECIFICHE DEL SERVIZIO

1	GENERALITÀ DELLA FORNITURA	2
1.1	Oggetto.....	2
1.2	Durata	2
1.3	Tipologia dei servizi richiesti	2
2	DESCRIZIONE DELLA FORNITURA	2
2.1	Verifica sicurezza infrastrutture	2
2.1.1	Verifica delle vulnerabilità applicative.....	3
2.1.2	Scansione delle vulnerabilità degli apparati di rete	3
2.1.3	Analisi del codice sorgente.....	3
2.1.4	Tempi di attivazione del servizio	3
3	QUADRO SINOTTICO	3
4	PROPOSTA ECONOMICA.....	4

1 GENERALITÀ DELLA FORNITURA

1.1 Oggetto

E' oggetto del presente affidamento l'insieme dei servizi di verifica sicurezza delle infrastrutture e dei sistemi di seguito meglio dettagliati.

1.2 Durata

Il contratto avrà durata di 12 mesi dalla data di sottoscrizione con la possibilità da parte di DigiCamere di disporre una proroga opzionale di ulteriori 12 mesi dalla scadenza del contratto nel caso in cui l'importo residuo per i servizi opzionali non sia stato ancora utilizzato completamente e sia sufficientemente capiente per tale proroga.

1.3 Tipologia dei servizi richiesti

DigiCamere ha la necessità di monitorare costantemente la sicurezza dei propri sistemi e delle proprie applicazioni. Per far questo DigiCamere intende acquisire un servizio che copra le seguenti tre tipologie di attività:

- Identificazione delle vulnerabilità dei dispositivi delle infrastrutture informatiche (penetration test);
- Verifica dei livelli di sicurezza dei siti e delle applicazioni web (vulnerability assessment);
- Analisi del codice sorgente delle applicazioni alla ricerca di vulnerabilità conosciute.

DigiCamere è alla ricerca di un fornitore che possa erogare i servizi richiesti con le seguenti caratteristiche:

- in modalità SaaS (non deve richiedere costi aggiuntivi, per installazioni SW o server, fatto salvo quelli per eventuali connessioni VPN);
- utilizzo in autonomia dei singoli servizi all'interno della durata contrattuale;
- verifiche di vulnerabilità basate sui DB standard di fatto CVE (*Common Vulnerability Exposure*) e CWE (*Common Weakness Enumeration*);
- con reportistica semplice e chiara visibile online o esportabile in pdf e csv.

E' soluzione preferibile quella che propone servizi integrati ed utilizzabili all'esigenza all'interno dei 12/24 mesi.

Il servizio deve comprendere manutenzione e assistenza per la durata contrattuale e tutti gli eventuali costi accessori.

Nei capitoli successivi sono descritte in dettaglio le specifiche che dovrà avere ciascun servizio richiesto.

2 DESCRIZIONE DELLA FORNITURA

Nei paragrafi successivi vengono descritte le caratteristiche della fornitura nonché vincoli e requisiti richiesti al fornitore in merito all'oggetto del capitolo.

2.1 Verifica sicurezza infrastrutture

Per "Verifica sicurezza infrastrutture" si intendono tutte le attività e servizi necessari a verificare i livelli di sicurezza di sistemi, infrastrutture ed applicazioni che possano dare indicazioni a DigiCamere sulle priorità e modalità di intervento.

I tre filoni di intervento sono:

- Verifica delle vulnerabilità applicative;

- Scansione delle vulnerabilità degli apparati di rete;
- Analisi del codice sorgente.

2.1.1 Verifica delle vulnerabilità applicative

Il "vulnerability assessment" è il processo di identificazione, quantificazione e prioritizzazione (o classificazione) delle vulnerabilità di un servizio o applicazione web.

A questo scopo si richiede un servizio automatico che permetta la scansione automatica di 40 siti/applicazioni web, anche in intranet (anche più scansioni per sito nell'arco del periodo contrattuale) con le caratteristiche descritte al paragrafo 1.3 della presente e che abbia le seguenti funzioni:

- riconoscere ed identificare un ampio numero di differenti vulnerabilità come l'SQL injection, il Cross-site Scripting, etc coprendo come minimo la top ten delle vulnerabilità OWASP;
- classificare le vulnerabilità per livello di rischio (es. basso, medio e alto);
- fornire un report con le soluzioni per eliminare, o quantomeno mitigare, le vulnerabilità;
- verificare la conformità alle normative vigenti.

2.1.2 Scansione delle vulnerabilità degli apparati di rete

Per scansione delle vulnerabilità di rete si intende l'attività di ricerca e mappatura delle debolezze di una rete attraverso la ricerca di indirizzi attivi e porte aperte individuando quindi sistemi e applicazioni per poi approfondire il livello di analisi fino ad arrivare ad identificare il livello di patch dei sistemi e le relative vulnerabilità.

A questo scopo si richiede un servizio per la scansione di 250 indirizzi IP (anche di classi diverse, o ripetute sullo stesso sottoinsieme di IP, ad esempio 50 IP verificati 5 volte) con le caratteristiche descritte al paragrafo 1.3 della presente e che abbia le seguenti funzioni:

- riconoscere ed identificare le vulnerabilità di rete;
- classificare le vulnerabilità per livello di rischio (es. basso, medio e alto);
- fornire un report con le soluzioni per eliminare, o quantomeno mitigare, le vulnerabilità;
- verificare la conformità alle normative vigenti.

2.1.3 Analisi del codice sorgente

Per analisi del codice sorgente si intende Il fornitore si impegna a mettere a disposizione personale con idonee certificazioni per l'espletamento delle attività previste dal presente documento.

A questo scopo si richiede un servizio per la scansione di un milione di linee di codice (almeno linguaggi java, javascript e php) con le caratteristiche descritte al paragrafo 1.3 della presente e che abbia le seguenti funzioni:

- riconoscere ed identificare le vulnerabilità presenti nel codice;
- classificare le vulnerabilità per livello di rischio (es. basso, medio e alto);
- fornire un report con le soluzioni per eliminare, o quantomeno mitigare, le vulnerabilità;
- verificare la conformità alle normative vigenti.

2.1.4 Tempi di attivazione del servizio

Il Fornitore dovrà attivare il servizio entro 5 giorni lavorativi dalla data affidamento dello stesso, permettendo a DigiCamere di disporre della piattaforma e di tutti gli strumenti necessaria ad effettuare le attività sopraelencate.

3 QUADRO SINOTTICO

Nella tabella seguente riepiloghiamo le specifiche del servizio richiesto, tabella che comunque non sostituisce e/o annulla quanto sopra descritto in dettaglio.

Tabella riepilogativa	
Tipologia	<u>Servizio, preferibilmente in modalità SaaS ed in cloud con funzionalità integrate</u>
Servizi richiesti	<ul style="list-style-type: none"> • 40 scansioni di vulnerabilità applicative su siti e applicazioni web, anche intranet; • Scansione vulnerabilità di rete su 510 indirizzi IP (anche ripetuti e/o di classi diverse); • Analisi di 1 milione di righe di codice; • 3gg training on the job / supporto avvio attività.
Tempi di attivazione del servizio	<u>Entro 5 giorni lavorativi dall'affidamento</u>

4 PROPOSTA ECONOMICA

L'importo massimo per il servizio della durata di 12 mesi è di Euro 18.000,00 + IVA e deve comprendere tutti i costi accessori di start-up ed assistenza. La proposta deve esplicitare eventuali prerequisiti (vpn, configurazioni firewall, etc) necessari affinché possano essere erogati tutti i servizi richiesti.

Si chiede inoltre di indicare nella proposta economica il costo unitario, da prevedere in caso di ulteriori esigenze, per le seguenti voci:

- Scansione vulnerabilità applicativa per 1 sito/applicazione web;
- Scansione vulnerabilità di rete per 255 indirizzi IP, ad uso interno DigiCamere;
- Scansione di 1 milione di linee di codice, ad uso interno DigiCamere;
- Un giorno/uomo aggiuntivo di supporto.

Tali servizi aggiuntivi saranno attivati a consumo solo su eventuale richiesta di DigiCamere nell'arco del periodo contrattuale per un importo massimo raggiungibile di ulteriori 12.000,00 Euro + IVA.

Tabella riepilogativa costi	
Servizio richiesto (12 mesi)	Base d'asta: 18.000,00 Euro
Servizi opzionali (Attivabili fino ad un massimo di 12.000,00 Euro)	
Scansione vulnerabilità applicativa per 1 sito/applicazioni web	Base d'asta: 600,00 Euro
Scansione vulnerabilità di rete per 255 indirizzi IP	Base d'asta: 600,00 Euro
Scansione di 1 milione di righe di codice	Base d'asta: 3.500,00 Euro
Un giorno/uomo aggiuntivo di supporto	Base d'asta: 800,00 Euro

Canone aggiuntivo per la proroga del servizio di 12 mesi con utilizzo della piattaforma fornita	Non è prevista una base d'asta
---	--------------------------------