

Spett.le
Amministrazione Provinciale di Roma
Dipartimento II - Direzione
Via delle Tre Cannelle, 1/b
00187 - ROMA

c.a. Dirigente Servizio Monitoraggio Investimenti, Dott. Fresilli Francesco

Roma, 19/09/2013

Prot. N°13/WPR/0073/GL

Oggetto: Offerta per servizi professionali di Sicurezza.

Come da accordi intercorsi, ci preghiamo di sottoporre alla Vs. attenzione la ns. migliore offerta relativa a quanto sottoindicato.

L'offerta prevede a carico di Wizards Progetti s.r.l. la fornitura di due differenti tipologie di attività di sicurezza:

- 1) Un Web Application Penetration Test (WAPT) che permette di identificare eventuali vulnerabilità presenti nel Portale de Pagamenti
- 2) Il servizio di Computer Forensics (CF) che ha lo scopo di acquisire informazioni onde determinare, approfondire e documentare quali attività sono state effettuate a causa della compromissione sui sistemi oggetto dell'analisi.

Nel documento allegato "Offerta Servizio" sono descritti i dettagli di quanto in oggetto, le condizioni economiche e le modalità contrattuali applicate, le responsabilità di Wizards Progetti S.r.l. e gli adempimenti a Vostro carico.

Per qualsiasi ulteriore chiarimento Vi invitiamo a contattare i seguenti riferimenti Wizards Progetti S.r.l.:

Dott. Giuseppe Lorenzetti - tel. 06 91.80.29.1 - e-mail giuseppe.lorenzetti@wizardsgroup.it

Cogliamo l'occasione per porgere i nostri migliori saluti.

Amministratore Unico

Fulvio Duse

OFFERTA SERVIZIO

CLIENTE	Amministrazione Provinciale di Roma Dipartimento II - Direzione
INDIRIZZO	Via delle Tre Cannelle, 1/b 00187 - ROMA
RIFERIMENTI CLIENTE	Dirigente Servizio Monitoraggio Investimenti, Dott. Fresilli Francesco
DESCRIZIONE SERVIZIO	Web Application Penetration Test e Analisi Forense sull' applicazione Portale dei Pagamenti della Provincia di Roma.
PROTOCOLLO NOSTRA OFFERTA	
DATA EMISSIONE OFFERTA	19/09/2013

DOCUMENTO EMESSO DA:	NOME	DATA
ACCOUNT	Giuseppe Lorenzetti	19/09/2013
VERIFICATO DA:	NOME	DATA
PRODUZIONE	Giuseppe Lorenzetti	19/09/2013
APPROVATO DA:	NOME	DATA
DIRETTORE GENERALE	Roberto Nocentini	19/09/2013

1 OGGETTO DELL'OFFERTA

1.1 Premessa

Lunedì 08/04/2013 Wizards Progetti, nella figura del dott. Lorenzetti Giuseppe, informa la Provincia di Roma nella figura del responsabile dei Sistemi Informativi, sig. Stefano Iacobucci che il sistema web "Portale dei Pagamenti" della Provincia di Roma presentava delle anomalie (l'accesso al sistema era molto lento).

Giovedì 11/04/2013 la Provincia di Roma nella figura del dott. Lo Franco informa il dott. Lorenzetti di che aver constatato la medesima anomalia del servizio.

Mentre il gruppo tecnico di Wizards Progetti, recandosi in Provincia di Roma il 12/04/2013 costata, dopo il riavvio del server, che l'anomalia riscontrata in precedenza non è più presente, il gruppo tecnico della Provincia di Roma costata alcune anomalie presenti sul server; il giorno stesso, in serata, la Provincia di Roma nella figura del sig. Stefano Iacobucci, comunica a Wizards Progetti che per motivi di sicurezza, il server è stato messo fuori rete.

Nella raccomandata, anticipata via FAX il 18/04/2013, che ha come oggetto "Il Portale dei Pagamenti – messa in sicurezza" la Provincia di Roma chiede a Wizards Progetti la messa in opera di tutte le opportune misure tecniche necessarie per garantire la sicurezza e l'impenetrabilità del Sistema ivi incluso il Penetration Test.

Wizards Progetti, ha proceduto alla fase di analisi propedeutica la fase operativa, al fine di individuare gli step necessari alla messa in sicurezza del Sistema.

Tali step sono riportati di seguito nel paragrafo "Descrizione del Servizio".

1.2 Descrizione del servizio

Le attività di sicurezza da eseguire sul Sistema sono:

1. Un Web Application Penetration Test (WAPT) che permette di identificare eventuali vulnerabilità presenti nel Portale de Pagamenti
2. Il servizio di Computer Forensics (CF) che ha lo scopo di acquisire informazioni onde determinare, approfondire e documentare quali attività sono state effettuate a causa della compromissione sui sistemi oggetto dell'analisi.

Nel dettaglio, il Web Application Penetration Test includerà le seguenti sotto attività:

- Valutazione della sicurezza delle applicazioni attraverso tentativi di intrusione mirati a:
 - eludere i meccanismi di autenticazione ed autorizzazione.
 - Ottenere privilegi amministrativi o di altri utenti (privilege escalation).
 - Ottenere l'accesso ai dati gestiti dall'applicazione od alterare le modalità di presentazione degli stessi.
 - Violare i meccanismi di validazione e gestione delle sessioni.
 - Individuare problematiche relative alla validazione degli input attraverso l'invio di caratteri malformati.
- Valutazione dell'architettura e del design applicativo al fine di individuare problematiche che potrebbero portare ad accessi non autorizzati o alla perdita di confidenzialità ed integrità delle informazioni gestite dall'applicazione.
- identificazione di campi ed informazioni nascoste all'interno delle pagine, componenti di test, interfacce amministrative e debolezze relative all'installazione e configurazione di web ed application server.
- Validazione delle vulnerabilità e raccolta di proof of concept,
- Valutazione e classificazione delle vulnerabilità individuate secondo le seguenti dimensioni:
 - Impegno richiesto ad un attaccante per sfruttare con successo la vulnerabilità.
 - Impatto che si avrebbe sul business aziendale qualora la vulnerabilità venisse effettivamente sfruttata.
 - Impegno richiesto al Cliente per correggere la problematica.

- Sviluppo di un piano di azioni immediato, atto mitigare il rischio associato alle vulnerabilità a maggior impatto.

Il servizio di Computer Forensics (CF) ha lo scopo di acquisire informazioni onde determinare, approfondire e documentare quali attività sono state effettuate a causa della compromissione sui sistemi oggetto dell'analisi.

L'attività include le seguenti fasi:

- Acquisizione delle memorie dei server compromessi, tramite il sistema e la tecnologia più idonea.
- Analisi e Valutazione tramite l'analisi dei file presenti quali presenza di file sospetti, analisi dei log di sistema, del web server e del database server.
- Presentazione tramite la redazione di un documento, i risultati dell'analisi e il procedimento utilizzato.

Per ogni vulnerabilità effettivamente verificata i consulenti renderanno disponibili le evidenze e predisporranno un report dettagliato con suggerimenti per l'attività di mitigazione o eliminazione della vulnerabilità stessa, utili ad elevare il livello di sicurezza dell'ambiente testato.

Trattandosi di servizi esposti su Internet le attività vengono tipicamente eseguite a partire da postazioni esterne all'infrastruttura del cliente, con tentativi di attacco effettuati dalla rete internet.

1.3 Vincoli e Prerequisiti

Le attività di WAPT verranno effettuate su un ambiente messo a disposizione da Wizards Progetti che dal punto di vista applicativo corrisponda a quello rilasciato alla Provincia di Roma il 20/03/2013.

1.4 Durata

Il servizio proposto sarà svolto per un massimo di 14 giorni lavorativi a partire dalla data di accettazione di codesta offerta.

2 CONDIZIONI ECONOMICHE

2.1 Costi del Servizio/Sviluppo Progetto

Item	Descrizione	Qt.	Corrispettivo economico
1	Web Application Penetration Test	1	€5.000,00
2	Attività di Forensic	1	€4.000,00

Come concordato il pagamento sarà posto a carico del soggetto nella misura in cui sarà imputabile la o le lacune eventualmente riscontrate.

2.2 Imposte e Tasse

Tutti gli importi convenuti saranno fatturati applicando l' I.V.A. secondo l'aliquota vigente.

2.3 Modalità di fatturazione e pagamento

Fatturazione 100% all'ordine.

Validità della presente offerta 30gg.

3 CONDIZIONI GENERALI

3.1 Impegno Risorse e Tempificazione

Tutte le risorse impiegate sono dipendenti e/o consulenti della WIZARDS PROGETTI S.R.L., assolutamente competenti in relazione all'incarico loro affidato e regolarmente assunti nel pieno rispetto dei contratti di lavoro applicabili e delle eventuali prescrizioni della Pubblica Autorità.

La WIZARDS PROGETTI S.R.L. esonera la Committente da ogni obbligo, onere e responsabilità di cui alla legge n. 877/1973.

Il servizio verrà svolto nell'ambito di otto ore lavorative in orario di ufficio, dal lunedì al venerdì.

La WIZARDS PROGETTI S.R.L. si dichiara disponibile ad effettuare, con congruo preavviso e se sussistono gravi e comprovate ragioni, sostituzioni temporanee del personale impiegato con altro di pari requisiti e competenze. Decorsi 5 giorni dall'inizio di esecuzione dell'accordo, il servizio si intenderà da Voi definitivamente accettato.

3.2 Coordinamento

Ciascuno dei contraenti ha facoltà di designare un proprio Responsabile che avrà il compito di rappresentare ciascuna parte nei confronti dell'altra durante lo svolgimento dell'incarico affidato.

La WIZARDS PROGETTI S.R.L. si impegna a fornire mensilmente alla committente dei "rapporti" con la indicazione delle ore lavorate e, se richiesta espressamente, una descrizione delle attività già eseguite. Compete alla Vs. società il diritto di indire riunioni periodiche di verifica di completamento delle singole attività in relazione all'iniziale piano di realizzazione; i soggetti designati avranno i poteri per impegnare ciascuna delle parti rappresentate.

E' prevista la possibilità per ciascuna parte di indire con congruo preavviso riunioni straordinarie con ordine del giorno da definire di volta in volta al fine del miglior andamento del rapporto.

3.3 Responsabilità della WIZARDS PROGETTI S.R.L.

La WIZARDS PROGETTI S.R.L. riconosce a proprio carico tutti gli oneri inerenti alla assicurazione del proprio personale occupato nelle attività connesse all'oggetto della presente offerta e dichiara di assumere in proprio ogni responsabilità in caso di infortunio e di danni direttamente arrecati da detto personale alle persone e alle cose sia del committente che di terzi, in dipendenza di colpa o negligenza nell'esecuzione presso il committente, delle prestazioni di cui alla presente offerta.

La WIZARDS PROGETTI S.R.L. s'impegna inoltre ad ottemperare a tutti gli obblighi verso i propri dipendenti e/o consulenti in base alle disposizioni vigenti in materia di lavoro e di assicurazioni sociali, assumendo a proprio carico tutti gli oneri relativi; si obbliga ad attuare nei confronti dei propri dipendenti occupati nelle attività di cui all'offerta, le condizioni normative e retributive contemplate nei contratti collettivi di lavoro applicabili, alla data dell'accettazione della presente, alla categoria e nella località dove si svolgerà il lavoro.

3.4 Riservatezza

La WIZARDS PROGETTI S.R.L. si obbliga a mantenere strettamente confidenziali e riservati i progetti, i dati e ogni altra informazione ricevuta dalla Committente, impegnandosi anche per i soggetti che forniranno le attività necessarie all'esecuzione del presente accordo, a non divulgare i dati e le informazioni inerenti alla Committente che potranno rendersi disponibili o note nello svolgimento del servizio offerto.

3.5 Adempimenti del Committente

Il Committente si impegna a mettere a disposizione del personale della WIZARDS PROGETTI S.R.L. l'utilizzo di hardware, locali e logistica per lo svolgimento dell'attività presso la propria sede o presso la sede dell'utente finale.

Il Committente si obbliga espressamente a non fare proposte di assunzione e/o di collaborazione autonoma ovvero comunque a non concludere alcun accordo con il personale e i consulenti utilizzati dalla WIZARDS PROGETTI S.R.L. per il servizio, sia durante l'erogazione dello stesso, sia nei dodici mesi successivi alla conclusione delle attività.

Il Committente si riserva la facoltà di controllare l'esecuzione delle attività oggetto del presente accordo e di verificarne lo stato di avanzamento a sua cura e spese.

3.6 Richiesta di informazioni su rischi specifici e misure di prevenzione (D.LGS 81/2008)

Ai sensi

dell'art. 26 comma 1, lettera b) del D. Lgs. 81/08 e s.m.i., che impone al datore di lavoro dell'impresa committente l'obbligo di fornire «dettagliate informazioni sui rischi specifici esistenti nell'ambiente in cui sono destinati ad operare» i lavoratori dell'impresa appaltatrice e «sulle misure di prevenzione e di emergenza adottate in relazione alla propria attività»,

dell'art. 26, comma 2 del D. Lgs. 81/08 e s.m.i. che impone sia al datore di lavoro dell'impresa committente sia al datore di lavoro dell'impresa appaltatrice gli obblighi di cooperazione e coordinamento in merito all'attuazione delle «misure di prevenzione e protezione dai rischi sul lavoro» nonché di informazione reciproca «al fine di eliminare rischi dovuti alle interferenze tra i lavori delle diverse imprese coinvolte nell'esecuzione dell'opera complessiva»,

viste le sanzioni previste per i datori di lavoro dall'art. 55 del D. Lgs. 81/08 e s.m.i., allo scopo di realizzare una proficua cooperazione per l'attuazione delle misure di prevenzione e protezione, nonché un coordinamento degli interventi, e per eliminare eventuali rischi dovuti alle interferenze tra il lavoro dell'impresa appaltatrice con quello dell'impresa committente o di altre imprese presenti negli ambienti oggetto della commessa, il committente si impegna a fornire a WIZARDS PROGETTI S.R.L. le seguenti informazioni necessarie per soddisfare agli obblighi sopra indicati:

A) Informazioni sui rischi specifici esistenti nell'ambiente di lavoro:

- caratteristiche dell'ambiente nel quale sarà effettuato il lavoro;
- presenza di aree ad accesso controllato, zone di stazionamento e percorsi da rispettare;
- macchine e/o impianti per i quali devono essere adottate misure di protezione particolari;
- ambienti e/o attrezzature con esposizione a rischio elettrico;
- ambienti e/o attrezzature con esposizione a rischio di scoppio, incendio o esplosione;
- zone nelle quali è possibile un' esposizione ad agenti fisici, chimici e biologici.

B) Informazioni sulle misure di prevenzione e di emergenza adottate in relazione all'attività:

- nominativo del Responsabile del Servizio di Prevenzione e Protezione;
- nominativo dell'incaricato del coordinamento tra impresa committente e impresa appaltatrice;
- nominativo dei lavoratori dell'impresa committente che collaboreranno con quelli dell'impresa appaltatrice;
- estratto del documento di valutazione dei rischi redatta dal committente;
- servizi igienici, mensa (se presente) e sala ristoro a disposizione dei lavoratori;
- piano di emergenza e comportamenti da adottare in caso di evacuazione;
- locale di pronto soccorso e referenti per il primo soccorso sanitario;
- numeri telefonici interni di interesse.

3.7 Controversie

I diritti ed obblighi nascenti fra le Parti per effetto del rapporto instaurato saranno sottoposti alle norme sopra previste e a quelle che il Codice Civile detta in materia.

Per qualsiasi controversia è competente in via esclusiva il Tribunale di Roma.