Specifiche del servizio

Oggetto: Richiesta di preventivo per la fornitura di un servizio di audit sulla sicurezza dell'infrastruttura "IBM Business Process Manager" in uso presso la Camera di Commercio di Milano, e delle applicazioni ad esso collegate.

1 DESCRIZIONE SCENARIO

DigiCamere utilizza il sistema di Business Process Management "IBM – BPM" per fornire servizi alla Camera di Commercio di Milano e alle sue Aziende speciali e partecipate.

Le caratteristiche e il contenuto informativo delle attività che vengono gestite tramite la piattaforma BPM rendono particolarmente critico l'aspetto di presidio e miglioramento della sicurezza del sistema e delle applicazioni ad esso collegate. Si rende perciò necessaria un'attività di verifica costante, volta a individuare ed eliminare possibili falle di sicurezza.

Attualmente tale attività interessa innanzitutto le modalità di sviluppo dei flussi, che devono tendere a garantire il massimo grado di sicurezza rispetto alle principali possibilità di attacco.

E' però necessario procedere ad un'indagine ad ampio raggio su tutti gli aspetti, sia di sviluppo che architetturali, della piattaforma, per verificare la presenza di eventuali problemi.

2 DESCRIZIONE DELLA FORNITURA

DigiCamere ha l'esigenza di individuare un fornitore che si occupi di eseguire un'indagine approfondita su ogni aspetto della piattaforma BPM che possa rappresentare un punto di vulnerabilità ad attacchi informatici, e successivamente proceda alla redazione di un piano di messa in sicurezza nonché, a richiesta e compatibilmente con le risorse economiche disponibili, alla sua messa in atto.

2.1 Perimetro dell'indagine

Il perimetro dell'assessment di sicurezza e delle successive attività di correzione sarà circoscritto ai seguenti sistemi, di diretta pertinenza dell'infrastruttura di Business Process Management:

- **Piattaforma WebSphere:** La piattaforma BPM risiede su un application server IBM WebSphere, versione 8.5.5.1, ottimizzato tramite personalizzazioni sulla configurazione standard;
- **Piattaforma BPM:** DigiCamere utilizza la versione 8.5.0.1 della piattaforma IBM Business Process Manager. Su tale piattaforma sono installate in ambiente di produzone 14 process app di varia complessità. Il sistema utilizza a supporto un database DB2 versione 10.1;

- **Web Application di supporto ai processi BPM:** Si tratta di applicazioni scritte in linguaggio Java, installate sull'application server WebSphere su cui risiede la piattaforma BPM. Esse dialogano con i sistemi collegati (BPM, ESB) tramite web service e connessione diretta ai database di supporto dei processi BPM.

Maggiori dettagli sulle architetture, sugli strumenti a supporto e sulle metodologie di sviluppo del sistema BPM verranno forniti al paragrafo 3.

2.2 Descrizione delle attività

Le attività del presente documento si svolgeranno in due fasi. La prima fase sarà l'assessment di sicurezza, in cui verrà fatta l'attività di ricerca e successiva documentazione delle eventuali vulnerabilità individuate sulle componenti della piattaforma; la seconda fase sarà quella di intervento sulle vulnerabilità stesse, per la messa in sicurezza del sistema.

2.2.1 Assessment di sicurezza sulle componenti della piattaforma

Dal momento che, dal punto di vista dell'utilizzo, BPM può essere assimilato a una complessa applicazione web, si è definito che le linee guida che dovranno guidare l'indagine possano essere individuate prevalentemente tra quelle definite dal progetto OWASP, attualmente in fase di aggiornamento (per i dettagli del progetto OWASP si invita a visitare il sito web della community, all'indirizzo https://www.owasp.org). Sarà comunque richiesta un'analisi preliminare, in collaborazione con i referenti di progetto DigiCamere, finalizzata a individuare le aree di maggiore attenzione nonché l'ordine di priorità rispetto alle vulnerabilità oggetto dell'indagine.

Al fine di procedere con un'indagine a tutto campo sull'infrastruttura BPM e sulle applicazioni installate, al fornitore verrà richiesto di procedere con le seguenti attività:

- **Ricerca delle vulnerabilità all'interno dei sistemi oggetto dell'indagine:** la ricognizione delle problematiche di sicurezza dovrà seguire un approccio di tipo gray-box; il fornitore avrà accesso alle informazioni relative all'infrastruttura e alla relativa architettura, e disporrà di un account utente per l'utilizzo della piattaforma; in questa prima fase dell'attività non verranno forniti ulteriori accessi o informazioni sul codice e sulle configurazioni;
- **Resoconto sulle aree di maggior rischio individuate:** Al termine dell'attività di ricognizione, il fornitore produrrà una relazione dettagliata in cui dovrà indicare l'elenco delle eventuali vulnerabilità individuate, il grado di severità, e le attività necessarie per la loro eliminazione;
- **Definizione di un piano di attività per l'eliminazione delle eventuali vulnerabilità e del relativo ordine di priorità:** il fornitore fornirà un piano di lavoro completo finalizzato alla risoluzione delle eventuali problematiche di sicurezza individuate nella relazione, ordinato secondo il grado di severità; per ogni attività verrà specificata la quantificazione in giornate uomo, e in base a severità e stima verrà definito, in collaborazione con DigiCamere, l'ordine di esecuzione del piano;
- **Definizione delle procedure atte ad evitare il ripresentarsi delle eventuali vulnerabilità:** sulla scorta delle problematiche riscontrate il fornitore produrrà un documento contenente linee guida di sviluppo software finalizzate a prevenire il ripresentarsi delle problematiche di sicurezza legate al codice e alle metodologie di sviluppo; tali indicazioni entreranno a far parte delle linee guida per lo sviluppo di software BPM in uso presso DigiCamere;

Per il suddetto servizio, Digicamere ha previsto una modalità di svolgimento del servizio a corpo quindi con la formula "chiavi in mano"**.**

2.2.2 Interventi di messa in sicurezza della piattaforma

Per la messa in sicurezza delle vulnerabilità eventualmente individuate, il fornitore eseguirà le seguenti azioni di intervento, su esplicita richiesta di Digicamere.

- **Eliminazione delle eventuali vulnerabilità individuate secondo l'ordine di priorità definito:** a richiesta di DigiCamere, il fornitore interverrà, anche in momenti distinti, sulle componenti della piattaforma per risolvere le problematiche di sicurezza eventualmente individuate; in questa attività sono compresi ulteriori test per verificare le vulnerabilità risolte, e resoconto delle risultanze dei test;
- **Documentazione delle attività di messa in sicurezza, stato di avanzamento delle attività, indicazione del residuo:** il fornitore produrrà adeguata documentazione di ogni intervento, redigendo ed integrando volta per volta un documento complessivo in cui saranno indicate le attività eseguite, le attività ancora da eseguire, ed eventuali problematiche a vario titolo non risolvibili, con relativa motivazione.
- **Relazione sullo stato dell'arte dei sistemi oggetto dell'indagine per quanto riguarda la sicurezza al termine degli interventi:** Il fornitore redigerà un documento che illustrerà lo stato della sicurezza della piattaforma BPM a termine degli interventi, sulla falsariga della relazione di sicurezza post-assessment. Tale documento non riporterà le attività eseguite (che saranno comunque contenute nella documentazione delle attività di sicurezza), bensì rappresenterà un quadro della situazione "as is" della piattaforma al termine degli interventi.

Per il suddetto servizio invece Digicamere ha previsto una modalità di svolgimento del servizio a consumo, quindi sulla base delle effettive esigenze di Digicamere.

3 CONTESTO OPERATIVO

L'ambiente di esercizio di Digicamere si avvale di piattaforme tecnologiche messe a punto al fine di ridurre al massimo i rischi di interruzione del servizio e nel contempo garantire livelli di performance elevate: l'orientamento seguito in questi anni si è focalizzato, soprattutto, sull'individuazione di ambienti open-source su cui basare le piattaforme di produzione.

3.1 Sistemi orientati all'automazione dei processi interni

E' sempre presente l'integrazione con il sistema di single sign on e l'integrazione con database interni e con portali. Digicamere dispone di un sistema proprietario middleware che consente il colloquio tra la piattaforma BPM e altri sistemi/database con i quali i flussi devono colloquiare.

3.2 Tecnologie e ambienti

Dal punto di vista dei sistemi e degli ambienti, Digicamere dispone oggi, in rete interna, di tre server OS Windows 2008 R2 STD 64 bit, uno per il process center, uno per il process server di quality, e uno per il process server di produzione. Sono presenti tre DBMS DB2 Enterprise Edition 10.1, uno per ogni ambiente, per la persistenza dei dati del process center e del process server.

Per quanto riguarda gli ambienti, Digicamere opera distribuendo le attività su server differenti, ciascuno specializzato per le seguenti attività:

- *Sviluppo*: attività per la quale è previsto un server interno. Il processo di deploy del codice prevede ampie possibilità di accesso alle macchine da parte degli sviluppatori.
- *Quality* (o pre-produzione): attività per la quale è previsto un server dedicato e il deploy prevede qualche possibilità di accesso da parte degli sviluppatori, in funzione del tipo di progetto;

- *Produzione*: attività per la quale sono previsti server inaccessibili agli sviluppatori, sui quali le applicazioni e i database sono installati/modificati da sistemisti con opportuni privilegi.

I tre ambienti sopra indicati possiedono le seguenti caratteristiche:

Sviluppo
n.1 server OS Windows 2008 R2 STD Edition con installati il WAS IBM WebSphere release 8.5.5.1 e il Process Center di IBM BPM release 8.5.0.1
n.1 server OS Windows 2008 R2 STD Edition su cui è installata un'istanza DB2 release 10.1

Quality
n.1 server OS Windows 2008 R2 STD Edition con installati il WAS IBM WebSphere release 8.5.5.1 e il Process Server di IBM BPM release 8.5.0.1 per ambienti non di produzione
n.1 server OS Windows 2008 R2 STD Edition su cui è installata un'istanza DB2 release 10.1

Produzione
n.1 server OS Windows 2008 R2 STD Edition con installati il WAS IBM WebSphere release 8.5.5.1 e il Process Server di IBM BPM release 8.5.0.1
n.1 server OS Windows 2008 R2 STD Edition su cui è installata un'istanza DB2 release 10.1
n.1 server Linux con http Server Apache

3.3 Profilazione utenti

Il sistema autorizzativo del sistema IBM BPM viene gestito tramite LDAP di Single Sign On: SSO di test per gli ambienti di sviluppo e test, mentre SSO di produzione per l'ambiente di produzione.

3.4 Strumenti di sviluppo

L'ambiente di sviluppo applicativo adottato per le Process App è l'IBM Process Designer, l'attuale versione in uso è la 8.5.0.1

L'ambiente di sviluppo in uso per le web application Java di supporto è Eclipse.

Lo strumento di sviluppo per la progettazione e la gestione dei database applicativi in uso è IBM Data Studio.

4 CARATTERISTICHE DELLA FORNITURA

Data la natura delle attività richieste, che potranno prevedere interventi sia di tipo sistemistico che di sviluppo sui sistemi oggetto dell'indagine, oltre alla necessaria presenza di figure competenti sulle tematiche della sicurezza il fornitore dovrà disporre al suo interno figure professionali che possiedano competenze specifiche sui sistemi IBM WebSphere e BPM, nonché di sviluppo Java. Il fornitore dovrà pertanto garantire lo stesso livello di competenza richiesto da DigiCamere ai fornitori di attività di sviluppo BPM, e nello specifico:

- IBM BPM Developer
- IBM BPM Analyst
- IBM BPM Solution Architect

Digicamere ha stimato che per lo svolgimento del servizio circa l'80% delle giornate saranno svolte dal figura professionale di IBM BPM Developer. Qualora, nel corso della durata contrattuale e per lo svolgimento dell'attività, il numero di giornate offerte dal fornitore per una figura professionale sopraindicate dovesse esaurirsi, Digicamere in accordo con il Fornitore ha la facoltà di utilizzare i residui economici delle altre figure professionali per impiegarle sulla figura professionale con giornate esaurite.

Il fornitore potrà indicare, quale condizione migliorativa, l'eventuale possesso delle certificazioni legate ai profili IBM indicati, a patto che le risorse in possesso di tali certificazioni facciano parte dei team messi a disposizione dal fornitore per l'esecuzione attività richieste da Digicamere.
Nel corso della durata contrattuale, qualora dovesse emergere la necessità di Digicamere di rivedere il mix di giorni uomo offerti dal Fornitore per figura professionale, può concordare con quest'ultimo di rivedere il mix di gg uomo offerto al fine di garantire un team di lavoro maggiormente allineato con le esigenze e caratteristiche di progetto.

Il Team di Lavoro che sarà dedicato al progetto dovrà rimanere quantitativamente e qualitativamente immutato nel corso della prestazione del servizio. Eventuali avvicendamenti e sostituzioni dei relativi componenti dovranno comunque avvenire nel rispetto della consistenza qualitativa e quantitativa originaria e dovranno essere preventivamente autorizzati da Digicamere. Il Fornitore dovrà garantire che il sostituto abbia equivalenti competenze tecniche ed esperienza tali da garantire la continuità del Servizio e dovrà farsi carico del periodo di affiancamento/istruzione necessario per rendere la nuova risorsa autonoma sul progetto.

Digicamere avrà la facoltà, a suo insindacabile giudizio, di chiedere al Fornitore la sostituzione di uno o più componenti del team ove questi non rispettino i requisiti di conoscenze e capacità richiesti nell'ottica della realizzazione del servizio richiesto. La sostituzione dovrà avvenire entro il termine massimo di 5 giorni lavorativi con personale dotato delle competenze necessarie per l'esecuzione delle attività.

Per permettere l'erogazione delle attività, il fornitore dovrà dotare le proprie risorse di:

- Proprie apparecchiature di lavoro (Notebook);
- Proprie licenze IBM Process Designer, per permettere l'analisi sul codice delle process application.

Per poter permettere di lavorare in modo efficiente e con feedback costanti da entrambi i lati, tutte le attività dovranno essere svolte presso gli uffici di DigiCamere o presso i clienti (sempre sul territorio di Milano).

5 MODALITÀ DI EROGAZIONE DEL SERVIZIO

5.1 Assessment di sicurezza, relazione e documentazione

La durata dell'attività di assessment è prevista in 30 giorni di calendario a partire dalla data di avvio. Al termine di questo periodo il fornitore dovrà aver completato tutte le attività previste per questa fase: effettuato le attività di analisi, ricerca delle vulnerabilità, redazione della relazione sulle vulnerabilità individuate, del piano di attività di bonifica e delle linee guida di sviluppo. Vista la tipologia dell'attività Digicamere prevede che lo svolgimento dell'attività avvenga con la modalità "a corpo".

5.2 Attività sistemistiche e di sviluppo – modalità di ingaggio

Data l'esigenza da parte di DigiCamere di poter richiedere le attività di eliminazione delle vulnerabilità anche in momenti diversi, la fornitura delle attività di sviluppo sarà effettuata con la modalità "a consumo", in pacchetti minimi di 5 giorni lavorativi complessivi del team di lavoro, salvo l'utilizzo con quantità inferiori di eventuali residui, con relativa pianificazione e in base alla seguente procedura di affidamento:

- Digicamere, tramite Richiesta di intervento, comunicherà al Fornitore l'ambito di intervento e il n. di giornate/uomo che prevede di utilizzare;
- Il Fornitore, definirà e trasmetterà una proposta di fornitura con il/i cv della/e figura/e professionale/i da dedicare al progetto entro il termine massimo di **3 giorni lavorativi** dalla ricezione della Richiesta di intervento dando disponibilità ad un incontro preliminare nella quale vengono approfondite le attività e chiariti eventuali dubbi;

- Digicamere provvederà a valutare la proposta (se necessario previo incontro con il Fornitore come sopra indicato) e in caso di valutazione positiva, Digicamere comunicherà per iscritto al Fornitore l'attivazione del Progetto. Da quel momento lo stesso Fornitore dovrà rendersi disponibile ad iniziare le attività entro il termine massimo di **5 giorni lavorativi**;
- In caso di valutazione negativa della proposta, Digicamere ne darà comunicazione al Fornitore invitandolo a produrre, entro il termine massimo di **2 giorni lavorativi** dalla richiesta una nuova proposta da sottoporre ad approvazione;
- Digicamere provvederà all'analisi della seconda proposta di fornitura. In caso di valutazione positiva, Digicamere comunicherà per iscritto al Fornitore l'attivazione del Progetto, e a partire da quel momento il Fornitore dovrà rendersi disponibile ad iniziare le attività entro **2 giorni lavorativi**.

In caso di valutazione negativa della seconda proposta, Digicamere lo comunicherà per iscritto al Fornitore riservandosi la facoltà di non affidare allo stesso lo specifico Progetto.

Data la necessità di continuità, DigiCamere richiede che su una stessa attività venga fornita sempre la stessa figura professionale, l'eventuale sostituzione di figura sarà a totale carico del fornitore che dovrà garantire il completo passaggio di consegne nel tempo massimo di 5 giorni lavorativi.

All'interno della fornitura, il fornitore dovrà mettere a disposizione fino a due figure professionali in parallelo con le caratteristiche indicate.

6 NON-DISCLOSURE AGREEMENT

Il fornitore non dovrà per nessun motivo divulgare nessuna delle informazioni e del materiale al quale avrà accesso durante la fornitura.

7 LIVELLI DI SERVIZIO (SLA)

Il servizio offerto dovrà rispettare i livelli di servizio (SLA) riportati di seguito:

- Durata massima dell'attività di cui al paragrafo 2.2.1: 30 giorni di calendario;
- Attivazione di figure professionali per interventi di cui al paragrafo 2.2.2: 5 giorni lavorativi dall'approvazione della proposta di intervento;
- Sostituzione di una figura attiva su un intervento di cui al paragrafo 2.2.2: 5 giorni lavorativi dalla richiesta di sostituzione.

Per accettazione

_____

(Timbro e Firma del Legale Rappresentante dell'impresa)