Milano, 25 luglio 2005

Spett.le
Banca 247 S.p.A.
Via Moretti, 11
24121 Bergamo (BG)

Offerta n. 20050725.08GP

Alla cortese attenzione: Sig. Davide Biscaro

Oggetto: Offerta per attività Ethical Hacking

A seguito dei colloqui intercorsi vi sottoponiamo la nostra proposta per il servizio in oggetto.

In attesa di un vostro gradito riscontro, vi porgiamo i nostri più cordiali saluti.

Hacking Team S.r.l.
Gabriele Parravicini
Responsabile commerciale

Offerta
Ethical Hacking – B@nca 24-7

SOMMARIO

STORIA DEL DOCUMENTO

Versione:	Data:	Modifiche effettuate:
1.0	25 luglio 2005	Emissione

RICHIESTA DEL CLIENTE

B@nca 24-7 richiede di formulare una proposta, con relativa offerta economica, relativa ad interventi di Ethical Hacking su 4 indirizzi IP pubblici corrispondenti a 4 domini.

In altre parole, si richiede una consulenza di security assessment che verifichi, secondo una logica indipendente e supra partes, l'*effettiva* sicurezza dei server e degli applicativi di B@nca 24-7 relativi ai seguenti domini:
www.bankyou.it – www.banca247.it – www.cartalibra.it – www.cartakalia.it .

Più precisamente, il dimensionamento delle attività e' il seguente:

- Attività di Ethical Hacking applicativo sugli applicativi sopraindicati in modalità Black box ovvero senza alcuna credenziale utente.

Il cliente specifica inoltre che i seguenti punti devono essere compresi nei risultati della consulenza in oggetto:

- Documento tecnico che riporti le vulnerabilità individuate e i passi necessari per eliminarle.
- Documento di presentazione per il management in forma di *slides*
- Presentazione di quest'ultimo punto al management

SOLUZIONE PROPOSTA

L'intervento proposto si compone delle seguenti parti:

- Ethical Hacking applicativo dall' esterno:
  - Verifica della sicurezza simulando un attacco applicativo che origini da Internet.

DETTAGLI TECNICI DELLA SOLUZIONE PROPOSTA

Analisi applicativa

Questa analisi è costituita da una serie di tentativi d' attacco che coinvolgono solo i protocolli di comunicazione utilizzati dagli utenti finali per interagire con le applicazioni. Nel caso specifico delle applicazioni web, tali attacchi sono basati su manipolazioni dei pacchetti HTTP che vengono scambiati fra i browser degli utenti ed il web server. Esistono diverse categorie di attacchi verso applicazioni web, che possono portare alla compromissione di uno o più layer dell'intera infrastruttura applicativa: web server, application server, data tier.

Caratteristica comune a tutti gli attacchi applicativi è la completa trasparenza ad ogni sistema di difesa perimetrale (firewall, ids, ecc.): manipolazioni dei protocolli di layer 7 (applicativi) non possono essere rilevate da dispostivi che analizzano il traffico a layer 3 (network).

Il test sarà condotto in modalità anonima ed in "user-mode". Ciò significa che, preventivamente, dovra' essere creato un account tramite le usuali procedure di attivazione al fine di permettere a Hacking Team di accedere come utente autorizzato. Non saranno accettati account di altro tipo (di test interno, amministrativi, etc.) poiché non fornirebbero la corretta valutazione circa il rischio che un utente registrato possa cercare di accedere in modo fraudolento ad informazioni per cui non è autorizzato. L' attività comprende l' analisi dell' applicazione in termini architetturali, verranno analizzate le configurazioni delle macchine interessate, sia a livello di sistema operativo che applicativo.

L' attivita' di security audit dell' applicazione web identifica in modo completo le classi di attacco, in particolare saranno testate:

- Cross-site scripting: attacchi che sfruttano una non corretta vaidazione dei contenuti restituiti dal server in risposta a richieste HTTP opportunamente modificate.

- Parameter tampering: attacchi che sfruttano una non corretta vaidazione dei parametric passati dal browser al web server.
- Hidden field manipulation: attacchi che, sfruttando paradigmi di programmazione non sicuri, alterano il valore di parametri applicativi fra due successive richieste HTTP.
- Backdoors e opzioni di debug: attacchi basati su errori di configurazione e/o di programmazioni molto noti e diffusi.
- Stealth commanding: attacchi che mediante tecniche di injection mirano ad eseguire comandi sui server.
- Forceful browsing: attacchi che mirano ad accedere a risorse protette seguendo percorsi di navigazione non previsti.
- Buffer overflow: attacchi che comportano l'esecuzione di codice arbitrario in assenza di opportuna validazione dei parametri in ingresso.
- Cookie poisoning: attacchi basati sulla manipoloazione dei coockie di sessione HTTP.
- Configurazioni errate: attacchi che sfruttano comuni errori di configurazione.
- Vulnerabilita' note: attacchi che sfruttano la mancata applicazione di patch.
- SQL injection: attacchi che mirano all'esecuzione di query non previste sui DBMS di backend
- Attacchi http: manipolazioni degli Header HTTP.

DOCUMENTAZIONE UTENTE

Oltre a ciò specificatamente richiesto nel capitolo 2 (RICHIESTA DEL CLIENTE), al termine dell'attività sarà fornito un report che conterrà:

a. **Topologia rilevata**
b. **Dettagliata descrizione del metodo e degli strumenti**
c. **L'elenco dei sistemi/apparati acceduti in modo non autorizzato**
d. **Descrizione della catena di eventi che hanno portato all'accesso della rete/sistema/applicazione**
e. **Log degli eventi**
f. **Eventuali esempi delle informazioni ottenute**

Sarà inoltre allegata una descrizione dei possibili miglioramenti che potrebbero essere applicati alla rete, ai sistemi o ai servizi, unita all'elenco, supra vendor, delle soluzioni tecnologiche e/o dei prodotti da adottare per incrementare il livello di security del sistema informativo.

PIANO DI INTERVENTO

Attività (tipologie)

Attività
Attività di Ethical Hacking applicativo dall'esterno
Incontro per la presentazione dei risultati e di tutto il materiale prodotto: • Report Direzionale. • Report tecnico dettagliato con indicazione delle possibili soluzioni.

Documenti necessari

Per dare inizio alle attività sarà necessaria la sottoscrizione dei due allegati:

- Allegato A: Accordo Legale
- Allegato B: Accordo di Non Divulgazione

RESPONSABILITÀ

Sarà responsabilità di Hacking Team completare il presente progetto secondo quanto specificato nella definizione delle funzionalità iniziali, fornendo al Cliente la documentazione citata.

Sarà responsabilità del Cliente garantire l'accesso ai locali preposti, nonché la disponibilità di una persona durante le attività previste dal presente progetto.

La presenza di tale persona permetterà a Hacking Team di spiegare nel modo più rapido ed efficace le attività svolte, sia in termini di tecniche che di strumenti.

Documentazione Utente

La documentazione e la reportistica sono comprese nei servizi sopra esposti.

Piano di manutenzione

In questa offerta non e' previsto piano di manutenzione.

OFFERTA ECONOMICA

Servizi

Servizi	Descrizione	Costo
Ethical Hacking	Applicativo	**€ 15.000,00**
	Totale	**€ 15.000,00**

I costi indicati si intendono al netto delle imposte.

Totale a voi riservato

Servizi	Descrizione	Costo
Ethical Hacking	Applicativo	**€ 12.000,00**
	Totale	**€ 12.000,00**

I costi indicati si intendono al netto delle imposte.

CONDIZIONI GENERALI DI OFFERTA

Modalità di pagamento e condizioni generali di fornitura

Validità offerta:	30 gg
Fatturazione servizi	50% all'ordine – 50% a fine lavori
Spese di trasferta	Incluse
Liquidazione fatture	30 D.F.F.M.
Trasporti	Ns.carico
Garanzia	A norma di legge

Tutti i prezzi esposti nella presente offerta sono da intendersi IVA esclusa.