]HackingTeam[

Spett.
T.S.F. - Tele Sistemi Ferroviari S.p.A.
Acquisti e Servizi Confronti Competitivi
Via Vito Giuseppe Galati, 71
00155 Roma

All'attenzione del ***Dott. Antonio Buongiorno***
c.c. ***Ing. Giovanni Riggio***

Milano, 22 Ottobre 2008

Oggetto: Offerta Servizi Security

A seguito della Vs. gentile richiesta siamo con la presente ad inviarVi la ns. migliore offerta relativa ad un attività di VA/PT Wireless, come di seguito meglio descritto.

Nelle pagine seguenti troverete la quantificazione economica dei servizi richiesti.

I prezzi riportati in offerta si intendono privi di ogni eventuale servizio aggiuntivo, fatta eccezione per i casi in cui questi non vengano specificatamente evidenziati.

Il contenuto della presente documento è strettamente riservato a TSF e al meglio delle nostre condizioni economiche.

Rimaniamo a Vostra disposizione per ogni ulteriore chiarimento in merito e, in attesa di un vostro cortese riscontro, cogliamo l'occasione per porgere distinti saluti

HT S.r.l.

Ivan Roattino

1. TARGET

L'oggetto delle attività è una verifica di Sicurezza della connessione wireless presso la stazione Ferrovie dello Stato di Bologna.

2. DESCRIZIONE DEI SERVIZI OGGETTO DELL'ATTIVITA'

- ✓ Vulnerability Assessment e penetration test wireless
- ✓ Verifica raggiungibilità e servizi con utenze fornite
- ✓ Raccolta eventuali evidenze
- ✓ Considerazioni generali ed executive report
- ✓ Redazione Report

3. METODOLOGIA DELLA SOLUZIONE PROPOSTA

3.1. Premessa

La possibilità di integrare il wireless alla rete cablata aziendale con una spesa minima rappresenta un'attrazione per molti IT manager. Per contro, il compromesso sta nel fattore sicurezza. Punti di accesso pubblici rendono le reti poco sicure e rappresentano l'anello debole della catena dell'intero network se non si adottano accorgimenti di sorta.

Di conseguenza l'introduzione di infrastrutture Wifi all'interno dell'azienda deve essere accompagnata da una policy di sicurezza forte, mirata a prevenire l'insorgenza di possibili rischi che potrebbero ripercuotersi sull'integrità di tutta la struttura aziendale.

3.2. I rischi

Nella realizzazione dei sistemi wireless, a causa di scelte tecniche non propriamente oculate, si sono venute a delineare alcune debolezze che derivano sia dalla scelta degli standard, sia dalla loro implementazione da parte dei produttori.

Ad alto livello si possono prospettare alcuni scenari di attacco che per praticità potremmo suddividere nelle seguenti categorie:

1. attacchi di inserimento

2. intercettazione e monitoraggio non autorizzato del traffico
3. jamming
4. attacchi da client a client
5. attacchi brute force all'access point
6. attacchi crittografici
7. errata configurazione

Capire come funzionano gli attacchi e utilizzare queste informazioni per prevenirli, sono passi fondamentali nella stesura di una policy di sicurezza per una qualsiasi soluzione wireless.

Di seguito vengono riassunte brevemente le caratteristiche delle tipologie di attacco.

3.3. Attacchi di inserimento

Consistono nella distribuzione incontrollata e non autorizzata di periferiche wireless e/o sulla creazione di reti wireless abusive, aggirando qualsiasi tipo di revisione architetturale.

In questo caso gli scenari possono essere due:

- Client non autorizzati: un attaccante tenta di connettersi abusivamente, tramite un notebook all'access point più vicino, in special modo se questi ultimi non sono configurati per richiedere una password all'atto della connessione del client.
- Access point non autorizzato: questa tecnica prevede l'installazione di 'rogue' access point, punti di connessione clandestini o altamente insicuri, che danno la possibilità di avere accesso alle risorse della rete da client fuori perimetro.

Entrambe le tecniche consentono l'accesso non autorizzato a sistemi wireless, e nel caso peggiore anche la possibilità di raggiungere le risorse aziendale poste sulla rete cablata.

La gravità dell'intrusione é in diretta relazione con il contenuto informativo dei sistemi connessi dal sistema di distribuzione (DS): si parte dalla semplice visione di documenti riservati, fino ad arrivare alla distruzione degli stessi o addirittura al reperimento e diffusione di dati riservati.

3.4. Intercettazione e monitoraggio del traffico

Come nelle reti a cavo, è possibile intercettare e monitorare (sniffare) il traffico sulle reti 802.11[x].

Il punto di forza di questo attacco rispetto a un ambiente wired è che l'attaccante non ha bisogno di compromettere un sistema collegato alla rete per depositare un agente o un Trojan che faccia da sniffer.

Tutto quello di cui si ha bisogno è riuscire a raggiungere la portante dei segnali usati dai sistemi Wifi. Visto che il segnale viene distribuito in maniera circolare sui tre assi dimensionali, il risultato è che questo può essere intercettato da posizioni esterne all'azienda o da un piano all'altro del palazzo.

L'analisi passiva del traffico e/o la clonazione di un Access Point, se non venissero adottate precise contromisure, potrebbero consentire la visione del traffico non cifrato tra utenti e servizi o il reperimento di credenziali di accesso ai sistemi applicativi dell'azienda.

3.5. Attacchi da client a client

Gli standard prevedono che due client wireless possano colloquiare direttamente tra loro, senza utilizzare l'access point del loro Service Set. Di conseguenza gli utenti, hanno bisogno di essere protetti non solo dai rischi esterni, ma anche da elementi sconosciuti.

Le risorse condivise e i servizi messi a disposizione sulla rete Wifi divengono oggetto di possibili attacchi, come se fossero posti su di una normale rete cablata; attacchi che vanno dal semplice DoS, fino ad attacchi evoluti che consentono di prendere il controllo dei sistemi e delle informazioni in esso residenti.

3.6. Attacchi Brute Force vs. access point

Diversi sistemi di distribuzione usano una singola chiave o password per autenticare tutti i client.

Il brute forcing, tramite dizionario o tentativi sequenziali, consente l'accesso al dispositivo di accesso ed di ottenere comodamente tutti i dati utente. Attacchi di questo tipo sono molto diffusi e di grande impatto, sopratutto in ambienti in cui le infrastrutture sono complesse ed eterogenee.

Questi fattori spingono gli amministratori di sistema ad adottare politiche di sicurezza lascive a vantaggio della interoperatività e della semplicità di gestione.

3.7. Attacchi crittografici

Lo standard 802.11b usa un sistema di autenticazione chiamato WEP. Questo standard è potenzialmente soggetto a diversi tipi di attacco:

1. passivo, basato su analisi statistica del traffico
2. attivo, con iniezione di nuovo traffico da una stazione non autorizzata, basato sull'analisi del testo in chiaro passante
3. attivo, basato sulla compromissione dell'access point
4. attivo, tramite il monitoraggio continuato del traffico in un certo lasso temporale dell'ordine di qualche giorno, permettendo la decifrazione in tempo reale di tutto il traffico

Sia la versione 40bit che la 128bit sono soggette a questi attacchi.

L'invito è di considerare altamente insicuro lo standard WEP e di integrare soluzioni per la sicurezza dell'infrastruttura aggiuntive o standard che utilizzano sistemi di integrità e cifratura più evoluti.

3.8. Errata configurazione

Di solito i sistemi di accesso vengono distribuiti con una configurazione standard per una facile messa in produzione ed un utilizzo immediato.

Visto l'obiettivo di avere un apparato pronto all'uso e utilizzabile nei più disparati ambienti, di solito porta a definire configurazioni di default in cui la sicurezza viene posta in secondo piano.

Gli amministratori dovrebbero considerare i rischi che comporta l'utilizzo di questa configurazione , prima di procedere all'installazione, onde evitare di esporre i sistemi ospiti a rischi inutili.

4. QUOTAZIONE ECONOMICA

Descrizione Attività	Figura professionale	Stima GG.	Prezzo
VULNERABILITY ASSESSMENT E PENETRATION TEST WIRELESS	Senior Security Engineer	5 GG	**€ 3.000**
Totale a Voi riservato			**€ 3.000**

5. CONDIZIONI GENERALI DI FORNITURA

1. l'offerta con relativa quotazione economica è modulare, i servizi ai punti sopra esposti, possono essere attivati singolarmente.

2. i prezzi esposti sono omnicomprensivi di ogni onere e spesa sostenuta da HT.

3. il pagamento è a 120 gg d.f.f.m

4. di aver preso cognizione di tutte le circostanze generali e speciali espresse nel presente invito e nell'allegato che possono interessare la fornitura;

5. di rinunciare a richiedere la risoluzione del contratto per eccessiva onerosità sopravvenuta ai sensi dell'art. 1467 c.c. e la revisioen dei corrispettivi, anche ove la variazione dei costi siano superiori al 10% (dieci percento) dei corrispettivi offerti che non saranno, pertanto, soggetti di revisione;

6. di garantire, anche a nome del personale impiegato nello svolgimento delle attività relative al servizio in oggetto, che l'erogazione avverrà secondo criteri di correttezza e moralità, in modo conforme a tutta la vigente normativa civile, amministrativa e penale ad essa applicabile. In particolare la Società garantisce che sarà evitato a carico di TSF ogni e qualsiasi effetto pregiudiziale ai sensi del D. lgs 231/01

7. Referente commerciale/responsabile di contratto HT:
   Marco Bettini marco.bettini@hackingteam.it tel 02.29060603 - mobile 3488291450

Spese di trasferta	Se non diversamente specificato in offerta le tariffe professionali esposte nella presente offerta sono riferite ad attività presso la sede di clienti localizzati a Roma.
Orario di lavoro	L'orario di lavoro va dalle ore 9:00 alle 13:00, e dalle ore 14:00 alle 18:00 dal lunedì al venerdì a meno di indicazioni specifiche inserite nell'allegato tecnico. Il tempo di viaggio è incluso nella stima dei giorni.
Validità dell'Offerta	**a)** La presente offerta e' da ritenersi valida per un periodo di 30 (trenta) giorni dalla data di emissione della presente, ai sensi e per gli effetti dell'articolo 1331 primo comma del Codice Civile. Qualsiasi ordine ricevuto da HT in relazione alla presente offerta è subordinato all'accettazione dello stesso da parte di HT, che provvederanno a darne notizia al Cliente **b)** I prezzi dei servizi si intendono fissi ed invariabili, e validi qualora non siano previste penali nel Vs. ordine d'acquisto
Informazioni e specifiche tecniche	I Servizi saranno eseguiti in base alle esigenze e specifiche tecniche individuate e descritte nell'ordine o nel relativo allegato della cui esatta indicazione e descrizione il Cliente si assume piena ed esclusiva responsabilità. Sulla base di quanto specificato l'Azienda sua volta dichiara e garantisce che i Servizi saranno eseguiti da personale dotato di adeguata preparazione professionale. Il Cliente sarà il solo responsabile delle attività oggetto dei Servizi, svolte dal personale dell' Azienda e sarà altresì responsabile del risultato di tali attività.
Proprietà intellettuale	I concetti, le idee, il know-how o le tecniche relative alla elaborazione dei dati sviluppati dal personale dell'Azienda o con la sua collaborazione in connessione alla prestazione dei servizi potranno essere usati da entrambe le parti senza limitazione alcuna. Resta peraltro inteso che qualora detti concetti, idee, know-how o tecniche si concretino in invenzioni, scoperte o altri beni protetti da un diritto di proprietà intellettuale essi saranno di proprietà dell'Azienda, la quale peraltro concede fin d'ora al Cliente licenza non esclusiva irrevocabile e gratuita di sfruttamento di tali invenzioni, scoperte o altri beni
Ritardo del pagamento	In caso di ritardo nei pagamenti, verrà calcolato a favore di HT, un interesse finanziario che sarà definito in fase di stipula del Contratto.
I.V.A.	Tutti i prezzi riportati in offerta sono da considerarsi al netto di I.V.A.;
Foro competente	Per qualsiasi controversia riguardante l'interpretazione e/o l'applicazione delle presenti condizioni di vendita sarà esclusivamente competente il Tribunale di Roma;
Trattamento dati personali	Le società HT si impegna, nel caso in cui durante l'espletamento delle attività descritte in offerta questo si renda necessario, a far ottemperare i propri dipendenti, a quanto prescritto dalla legge n.675 del 31.12.1996 e ss.
Responsabilità del contratto	Ciascuna delle ha nominato, un proprio responsabile che dovrà mantenere i collegamenti con l'altra parte in merito all'oggetto del presente contratto. Questi, in particolare, avranno il compito di: - coordinare le attività del proprio gruppo di lavoro; - mantenere i contatti con la controparte; - tenere le comunicazioni previste dal contratto o comunque utili allo svolgimento delle attività oggetto dello stesso. Le parti si impegnano, qualora le persone nominate non potessero più svolgere, per qualunque ragione, tali funzioni, a sostituirle immediatamente con persone aventi capacità e qualifiche analoghe. Qualora una parte non nomini il proprio responsabile o non provveda tempestivamente alla sua sostituzione, l'altra parte farà riferimento al firmatario del contratto.
Distrazione del Personale	Il Cliente si impegna, per la durata di vigenza del presente accordo e per i due anni successivi al termine dello stesso a non assumere alle proprie dipendenze e/o utilizzare, direttamente od indirettamente, anche per tramite di interposta persona e /o società controllate e/o collegate, i dipendenti o collaboratori dell'Azienda che abbiano in qualsiasi modo partecipato all'erogazione del servizio oggetto del presente contratto. In caso di violazione di quanto previsto al comma precedente, Il Cliente dovrà pagare all'Azienda una penale pari a dodici (12) mensilità della retribuzione corrisposta da questa al dipendente prima dell'assunzione in violazione di quanto previsto dalla presente clausola, salvo il risarcimento del maggior danno.
Riservatezza	HT si impegna a mantenere riservata ogni informazione relativa alle attività svolte presso il cliente di cui verrà a conoscenza in relazione alla prestazione dei servizi richiesti e a richiedere analogo impegno al proprio personale.