Milano, 19 Novembre 2004

Spett.le
M&G Finanziaria
Centro Direzionale Milanofiori
Strada 4 Palazzo A6
20090 Assago, MI

Offerta n. 20041119.m05

Alla c. att.ne : Dott. Maurizio Garbelli

Oggetto: **Offerta per Proposta di innalzamento del livello di Sicurezza di M&G Piano 2004**

A seguito dei colloqui intercorsi vi sottoponiamo la nostra proposta per le soluzioni e i servizi come in oggetto.

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

Hacking Team Srl

Marco Bettini
Key Account Manager

1. ARCHITETTURA VPN SSL

1.1. Obiettivo

Le VPN basate su protocollo IPSEC si sono rivelate soluzioni semplici e facili da gestire nei collegamenti puntuali di tipo site-to-site, mentre hanno mostrato diverse lacune nell'utilizzo client-to-site sia dal punto di vista tecnologico, sia in termini di costi di gestione:

- Installazione di una componente client: operazione che una VPN SSL evita, utilizzando esclusivamente un browser (problematica meno sentita per chi utilizza una VPN IPSEC Microsoft il cui client è la piattaforma XP stessa)
- Installazione su stazioni fuori controllo: l'installazione di un client VPN IPSEC risulta ancora più problematica nel caso di consulenti o outsourcer dotati di un proprio strumento di lavoro, caso in cui non è possibile avere il controllo diretto della postazione
- Granularità della profilatura: nel caso di personale esterno all'azienda, risulta difficile gestirne l'accesso con maggiore granularità, allo scopo di limitare la visibilità alle risorse e alle informazioni strettamente necessarie. Una VPN IPSEC genera un IP virtuale interno e quindi il sorgente è a tutti gli effetti come se fosse collegato in rete interna, senza la possibilità quindi di restringere il suo campo d'azione.
- Incompatibilità tecnologica: un ulteriore vincolo delle VPN basate su IPSEC è dato dalla loro incompatibilità con le funzioni di Network Address Translation (NAT) svolte da dispositivi quali firewall o router, che di fatto impediscono o complicano notevolmente l'instaurazione del canale sicuro.

Una soluzione VPN SSL è quindi facile e veloce da implementare, completamente non intrusiva, che minimizza i costi di gestione e fornisce una mobilità davvero unica conservando lo stesso livello di sicurezza.

1.2. Soluzione

L'idea alla base delle VPN SSL è quella di far viaggiare tutto il traffico da proteggere all'interno di un canale crittografato dal protocollo Secure Socket Layer (SSL).

Nelle VPN SSL-based l'utente deve semplicemente avviare il proprio browser e collegarsi al dispositivo dedicato, come se si trattasse di una comune pagina web (sfruttando quindi le funzionalità crittografiche implementate nei più comuni browser). Una volta effettuata l'autenticazione, all'utente viene mostrato un portale che definisce con precisione tutte le risorse alle quali può accedere in termini di:

- Siti Web e portali aziendali
- Documenti e relativi file/directory
- Applicazioni client/server: posta, telnet IBM 3270, ssh, terminal service, etc…

Tutto il traffico legato all'utilizzo delle risorse precedenti sarà crittografato all'interno del canale SSL fino al dispositivo dedicato, il quale si occuperà di gestire la comunicazione con i server/applicazioni destinatari.

Le VPN SSL nascono per rispondere puntualmente alle esigenze che contraddistinguono l'accesso all'infrastruttura informatica da parte di utenze esterne. Per questa ragione le soluzioni VPN hanno diverse caratteristiche che le rendono uno strumento estremamente efficiente:

- Autenticazione: è previsto un sistema d'autenticazione integrabile con l'infrastruttura informativa esistente.
- Gestione delle utenze: è possibile definire gruppi d'utenze e i relativi diritti d'accesso.
- Risorse accessibili: è possibile accedere a file e directory, siti intranet e portali in generale, qualsiasi tipo di applicazione client/server e perfino accedere alla rete come una VPN tradizionale.

Il protocollo SSL prevede la possibilità di utilizzare un certificato lato client durante il processo d'autenticazione. Il certificato inviato al server, in questo caso il sistema VPN, consente il controllo della validità del client ottenendo quindi la mutua autenticazione. Nel caso quindi sia presente una Certification Authority aziendale è possibile utilizzare i certificati rilasciati all'utente come ulteriore strumento di autenticazione al sistema (anche strong con supporto di device hardware con token USB e smartcard.

Tra i punti di forza di una soluzione VPN SSL-based vi è la semplicità dell'architettura richiesta. Il sistema infatti è costituito (logicamente) da un unico device pronto per essere inserito con semplicità nell'infrastruttura informatica della propria azienda. I vantaggi di una soluzione appliance sono molti; i principali riguardano:

- Sistema operativo hardenizzato (nessuna piattaforma server aggiuntiva da gestire)
- Hardware dedicato: accelerazione SSL e compressione del traffico
- Alta affidabilità in funzionamento cluster pair (consigliata per la disponibilità e la continuità del servizio)

1.3. Quotazione Prodotto Aventail

La soluzione Aventail viene proposta nelle due modalità, in single appliance e in high availability.

Aventail EX – 1500 Single Appliance		**Prezzo di listino**	**Prezzo a Voi riservato**
1510	EX - 1500 Appliance with 25 Concurrent-User License	€ 10.445,00	**€ 9.800,00**
1510-AAG1	Aventail 1510 Assurance Gold for 1 year Next Business Day Delivery	€ 1.880,00	**€ 1.750,00**
1510-ADD-OD	On Demand for 1510	€ 2.200,00	**€ 2.050,00**
1510-ADD-OD-AAG1	Aventail On Demand for 1510 Assurance Gold for 1 year	€ 396,00	**€ 370,00**
TOTALE			**€ 13.970,00**

Aventail EX – 1500 Appliance in High Availability		**Prezzo di listino**	**Prezzo a Voi riservato**
1510 - X	EX - 1500 Appliance Pair with 25 Concurrent-User License	€ 16.715,00	**€ 14.800,00**
1510-X- AAG1	Aventail 1510 Assurance Gold for 1 year Next Business Day Delivery	€ 3.009,00	**€ 2.700,00**
1510-ADD-OD	On Demand for 1510	€ 2.200,00	**€ 2.050,00**
1510-ADD-OD-AAG1	Aventail On Demand for 1510 Assurance Gold for 1 year	€ 396,00	**€ 370,00**
TOTALE			**€ 19.920,00**

1.4. Quotazione Progetto

Il progetto chiavi in mano prevede l'implementazione di una infrastruttura VPN SSL basata su un cluster appliance consegnata completa di documentazione, configurazione e con un breve corso di amministrazione. Le attività previste sono le seguenti:

- Analisi dei requisiti, delle politiche e posizionamento architetturale
- Installazione e configurazione in alta affidabilità del cluster
- Configurazione delle applicazioni e profilatura di utenti e gruppi
- Testing del sistema
- Training di amministrazione
- Documento di progetto

Costo progetto € 6.000,00. Consegna prevista in 2 settimane dall'inizio lavori

2. AUTENTICAZIONE FORTE E GESTIONE DELLE PASSWORD (TOKEN USB E SMARTCARD)

2.1. Obiettivo

Le soluzioni di autenticazione forte e gestione delle credenziali hanno lo scopo di ridurre il rischio di accessi ai sistemi e alle applicazioni aziendali da parte di soggetti non autorizzati.

Autenticazione forte e gestione delle credenziali agiscono in modo complementare. La prima permette di realizzare meccanismi di identificazione degli utenti più sofisticati, basati sull'uso di credenziali complesse e quindi robusti a fronte di tentativi di intrusione. La seconda permette agli utenti autorizzati di conservare ed utilizzare credenziali complesse senza esporsi al rischio di furto o intercettazione delle stesse. In particolare, rendono più semplice la gestione di password lunghe (di difficile memorizzazione) e la modifica frequente delle stesse. In quest'ottica le soluzioni di autenticazione forte e gestione delle credenziali rappresentano una risposta tecnologica agli adempimenti imposti dalla normativa relativa alla privacy e dichiarata nella stesura del relativo documento programmatico (DPS).

Qualora questi sistemi venissero utilizzati in abbinamento ai certificati digitali, si otterrebbe una possibile scalabilità del sistema a innumerevoli funzionalità:

- Accesso autenticato al dominio
- Accesso autenticato alla VPN SSL e/o al sistema di lettura della posta via web
- Cifratura e firma della posta elettronica
- Cifratura del file system per la protezione delle informazioni sensibili dei portatili e delle postazioni
- Cifratura di file mediante ad esempio le funzionalità di EFS
- Firma digitale di documenti ad esempio utilizzando Adobe (che prevede anche la firma digitale multipla)
- In generale si potranno utilizzare tutti i tools che hanno la caratteristica di trattare certificati standard X.509

Si potrebbe arrivare quindi (a passi successivi e solo opzionalmente) ad avere una Company Card utilizzata come accesso fisico e come contenitore della propria identità digitale.

2.2. Soluzione

Hacking Team progetta ed implementa soluzioni di autenticazione forte e gestione delle credenziali che automatizzano i processi di emissione/revoca/rinnovo delle credenziali. In base alle specifiche esigenze, tali soluzioni possono comprendere diversi insiemi di funzionalità: gestione centralizzata di credenziali, servizi di single-sign-on, servizi di self service per gli utenti finali, ecc. I vantaggi che ne derivano riguardano sia le problematiche di amministrazione, che risultano snellite e semplificate, sia le problematiche degli utenti finali, che accedono ad infrastrutture complesse ed eterogenee in modo trasparente ed uniforme ma soprattutto utilizzando una sola password e/o la propria identità digitale.

Le componenti dell'architettura sono le seguenti:

- ActivCard ActivClient 5.0 - E' il layer software che deve essere installato sulle workstation da cui gli utenti effettuano richieste di autenticazione. ActivClient offre inoltre all'utente funzionalità di gestione della propria smart card o token (cambiamento PIN, visualizzazione credenziali, strumenti di diagnostica).
- ActivCard Card Management System - E' un sistema per la gestione del ciclo di vita degli utenti e dei dispositivi loro assegnati. Il Card Management System si interfaccia con, e consente l'amministrazione centralizzata di tutti gli altri componenti dell'infrastruttura di controllo dell'accesso:
  - Certification Authority che emettono certificati memorizzati su smart card o USB key;
  - Directory LDAP contenenti informazioni sugli utenti.
- *Back-end*: il Card Management System espone le proprie funzionalità mediante interfacce Web che permettono di svolgere funzioni di amministrazione/configurazione. L'interazione con il back-end riguarda due categorie di utenza:
  - *Amministratori*: sono gli utenti che gestiscono l'infrastruttura di strong authentication. Hanno accesso alle funzionalità di emissione, gestione e revoca dei token e delle singole credenziali.
  - *Utenti Finali*: il modulo di back-end espone, via HTTP, alcune funzionalità di self-service che supportano gli utenti nella risoluzione dei problemi legati all'utilizzo del token (smarrimento del token, smarrimento del PIN, blocco, etc.).

L'infrastruttura di strong authentication offrirà le seguenti funzionalità:

- ***Emissione dei token***: prima dell'utilizzo, i token devono essere configurati per gestire l'insieme di credenziali (certificati digitali, password, etc.) che sarà memorizzato su di essi. L'insieme di credenziali che un token può gestire costituisce il *profilo* del token stesso.
- ***Assegnazione dei token***: affinché un utente possa usufruire dei servizi di strong authentication, è necessaria una operazione di assegnazione, mediante la quale un token, identificato da un serial number unico, viene associato ad un account del dominio Windows 2000. Nel caso di nuovi utenti, questa operazione può comportare la creazione contestuale di nuovi account nel dominio. L'assegnazione di un token ad un account comporta la creazione di opportuni record nel DBMS su cui si appoggia la soluzione, che consentono di effettuare le successive operazioni di gestione e tenere traccia di tutte le operazioni compiute.
- ***Gestione dei token***: gli amministratori dell'infrastruttura di strong authentication possono monitorare lo stato dei token (emessi, attivi e/o revocati) e, se necessario, modificarlo (sblocco, reset, modifica del profilo, etc.).
- ***Gestione delle credenziali***: gli amministratori dell'infrastruttura di strong authentication possono monitorare lo stato dei token (emessi, attivi e/o revocati) e, se necessario, modificare ogni singola credenziale memorizzata su di essi.
- ***Revoca dei token***: gli amministratori dell'infrastruttura di strong authentication possono revocare i token emessi. L'operazione di revoca comporta la revoca di tutte le credenziali presenti sul token, ma non la rimozione dell'account a cui il token è associato.

- ***Help Desk***: la soluzione proposta permette agli utenti di modificare un sottoinsieme (definito dagli amministratori) delle caratteristiche del proprio token, come ad esempio il PIN, e di eseguire operazioni di restore in seguito al blocco o smarrimento.
- ***Integrazione con sistemi vari***: la soluzione proposta prevede la possibilità di integrarsi con qualsiasi applicazione che permette l'uso di certificati digitali standard con supporto di decive crittografici. Sarà quindi possibile integrare la posta elettronica cifrata e firmata, la cifratura dei dati sul file system, la cifratura dei portatili, la firma digitale dei documenti, l'accesso ad OWA, l'accesso remoto via VPN SSL, etc etc…

2.3. Quotazione Prodotti ActivCard

ActivCard		Prezzo per 25 utenti	Prezzo per 100 utenti
BAK300P025	ActivCard USB Key Java64K - No profile - 25 Units	€ 625,00	€ 2.500,00
EAE50WP	Enterprise Access Card Solution v5.0 (CMS + ActivClient PKI Only) for Windows – 25 users	€ 2.150,00	€ 7.000,00
EAE50WLAM	Maintenance	€ 430,00	€ 1.400,00
TOTALE		**€ 3.205,00**	**€ 10.900,00**

2.4. Quotazione Progetto

Il progetto chiavi in mano prevede l'implementazione di una infrastruttura ActiveCard completa di tutte le funzionalità di gestione delle identità digitali e dei token, di tutte le procedure necessarie al corretto funzionamento ed utilizzo del sistema, della parte di integrazione con applicazioni di terze parti (soddisfacimento dei requisiti di posta elettronica, file system, portatili, VPN…) e di un corso di amministrazione.
Le attività previste sono le seguenti:

- Analisi dei requisiti e posizionamento architetturale
- Installazione e configurazione delle componenti server
- Definizione profili dei token, delle politiche e dei ruoli
- Integrazione con la cifratura EFS
- Integrazione con l'accesso remoto VPN e OWA
- Testing del sistema
- Training di amministrazione
- Documento di progetto
- Stesura delle procedure di Amministrazione
- Stesura delle procedure di Help Desk
- Stesura della procedura di Backup
- Stesura delle procedure Utente Finale

Costo progetto € 12.000,00. Consegna prevista in 3 settimane dall'inizio lavori

3. CENTRALIZZAZIONE DEI SYSLOG

3.1. Obiettivo

L'esigenza è quella di centralizzare i log dei server critici e di alcuni apparati di rete con il fine di costruire uno storico caratterizzato da una ben precisa finestra temporale, oltre la quale si provvederà ad uno storage. Questo permetterà di avere un unico punto di raccolta dei log, di poter effettuare complete analisi forensi, di debuggare più agevolmente i sistemi e di conservare gli eventi per un certo periodo di tempo.

3.2. Soluzione

Si propone un sistema basato su syslog in maniera tale da non dover installare agent sulle sorgenti dei log e da non dover acquisire un prodotto commerciale per un'attività ritenuta per ora secondaria.
Con questo primo step, si potranno quindi perseguire tutti gli obiettivi sopra citati: un server syslog deamon provvederà alla ricezione dei syslog sorgenti, li visualizzerà e li memorizzerà. Si potrà scegliere tra due possibili piattaforme: linux con syslogd oppure windows con kiwi.
In un secondo momento, dei piccoli script o moduli software sviluppati ad hoc da Hacking Team, potranno implementare controlli di contenuto, alert sulla base di determinati eventi, semplici regole di correlazione…

3.3. Progetto

Si propone, come primo approccio alla tematica, un'attività di consulenza per la definizione delle guidelines e delle politiche che dovranno essere seguite dal sistema. Per analizzare meglio la tipologia dei log, la loro quantità e per approfondire gli obiettivi del cliente, si ritiene necessaria l'installazione test di un syslog server per poter essere supportati, a livello decisionale, da riscontri pratici.
Le attività previste sono le seguenti:

- Analisi dei requisiti e posizionamento architetturale
- Installazione e configurazione del server syslog
- Testing del sistema
- Analisi della tipologia, della quantità dei log
- Studio conclusivo su obiettivi, politiche e linee guida
- Stesura delle Guidelines

Costo progetto € 4.000,00. Consegna prevista in 1 settimana dall'inizio lavori

4. CONDIZIONI GENERALI

Tutti i prezzi sono da considerare IVA esclusa.
Validità offerta: 30 gg dalla presente
Fatturazione prodotti : - alla consegna
Fatturazione servizi : - 50% all'ordine
- 50% alla collaudo
Pagamento: 30 gg data fattura
Coordinate Bancarie: Unicredit Banca
L.go Donegani - Milano
ABI 02008 CAB 01621 C/C 000010228244 CIN A