ASLCagliari

ALLEGATO "A"
ALLA DETERMINA N° 501 DEL - 5 MAG. 2015

ASL8
NP.2014/29895 del 05/08/2014 ore 13:46
Mitt.: Sistemi Informativi e Tecnologie ...
Ass.: Patrimonio e Servizi Tecnici
Class.: 1.4.6.

Direzione Generale
Servizio Sistemi Informativi e Tecnologie Informatiche

Il presente allegato è composto di n° 3 fogli di n° 3 pagine.

Il Responsabile del Servizio Tecnico
(Ing. Massimo Masia)

Al Responsabile
Servizio patrimonio e Servizi Tecnologici
SEDE

AZIENDA U.S.L. N° 8 - CAGLIARI
06 AGO. 2014
ENTRATA SERVIZIO TECNICO

Oggetto: acquisizione apparato di sicurezza per l'alta affidabilità.

In relazione alle crescenti esigenze di trasmissione dati e alla necessità di disporre di collegamenti a larga banda sicuri e affidabili tra il Centro Stella della rete aziendale dislocato presso questa Direzione e le strutture territoriali, evitando nel contempo il verificarsi di tempi di fermo dell'infrastruttura e dei sistemi a causa dell'utilizzo di procedure non autorizzate che spesso portano alla saturazione della banda disponibile, si rende necessario acquisire un apparato specializzato per garantire la continua disponibilità e sicurezza relativamente alla gestione multilivello della sicurezza centralizzata, da configurare come apparato ridondante in alta affidabilità sul nodo di Network Core Switching direzionale.

Il governo dell'infrastruttura di sicurezza della rete aziendale e, quindi, della sicurezza perimetrale e interna rappresenta una criticità in quanto attualmente, ferme restando l'adeguatezza delle prestazioni e delle politiche di sicurezza, viene utilizzata ***un'unica apparecchiatura*** che a fronte di guasto o di temporaneo malfunzionamento renderebbe totalmente inaccessibile la rete da parte delle strutture aziendali, centrali e periferiche afferenti ai PP.OO. e Poliambulatori, determinando l'indisponibilità dei Sistemi Informatici e dell'accesso ad Internet direzionale, utilizzato anche dalle strutture territoriali. Nondimeno, verrebbero isolati i sistemi informatici relativi ai progetti regionali che prevedono la componente dipartimentale installata proprio nel data center direzionale aziendale.

A tal proposito si rende necessario acquisire un secondo apparato, da configurare opportunamente affinché sia disponibile la modalità cluster fault-tolerant HA (High Availability) che permetta di garantire completamente le medesime funzionalità dell'apparato principale in caso di malfunzionamento dello stesso.

Tra le specifiche funzionalità necessarie per il governo dell'infrastruttura di sicurezza della rete aziendale, attualmente presenti nell'apparato in uso, si indicano:

- Identificazione della applicazioni: la maggior parte delle applicazioni applica tecniche di evasione, che tendono a fare trovare sempre la possibile strada di uscita, anche quando i sistemi di perimetro la limitino. Di conseguenza l'unico modo che si ha di poterle raggruppare è eseguire una analisi approfondita per inserirle in famiglie comportamentali. Su queste famiglie, è quindi possibile creare dei permessi, come stringere al massimo i controlli applicativi su alcune di esse, oppure come definitivamente bloccarle qualora si ritengano dannose per la rete;
- Decifrazione del traffico SSL: molte applicazioni vengono utilizzate attraverso un canale cifrato SSL, per massimizzarne l'anominato. Questo vuol dire che i sistemi tradizionali non hanno la

AZIENDA U.S.L. N. 8 - CAGLIARI SERVIZIO TECNICO
07 AGO. 2014
PER PRESA IN CARICO

possibilità di interpretare il traffico originato, essendo in questo stato illeggibile. L'apparato in questione esegue una decrittazione del traffico SSL per analizzarne il contenuto, per quindi ri-decrittarlo dopo l'ispezione;

- Assegnazione dell'identità utente: attraverso un sistema di comunicazione con ActivDirectory l'apparato è in grado di assegnare l'identità agli utenti di dominio, in modo tale da creare delle politiche di sicurezza e controllo direttamente sugli utenti o sui gruppi, anziché ai singoli indirizzi IP o networks. E' disponibile anche un sistema embedded di Captive Portal per associare una identità ai client che non fanno parte del dominio aziendale (tipicamente i guest user);
- Connessione sicura: basata su standard site-to-site IPSec VPN e SSL VPN per accesso remoto garantendo la visibilità Policy-based e il controllo di applicazioni, utenti e contenuti per tutto il traffico VPN.

L'appliance di *security infrastructure* attualmente utilizzato è rappresentata dal prodotto Palo Alto Networks modello PA-2050, in produzione in azienda dal 2011 e caratterizzata da un throughput pari a 1 Gbps, con funzionalità e scalabilità attualmente sufficienti in seguito alle evoluzioni architetturali e infrastrutturali effettuate sui sistemi in questi ultimi anni. Sarebbe auspicabile l'acquisizione di una piattaforma più performante, quale la PA-3020 caratterizzata da un throughput doppio e pari a 2 Gbps.

A tal proposito, viene proposta dal produttore un' offerta che prevede il ritiro e la sostituzione dell'attuale appliance PA-2050 con il modello PA-3020 e congiuntamente la fornitura ad un prezzo simbolico di una seconda appliance PA-3020 come "onsite spares". Questa modalità prevede da parte del produttore la fornitura di una macchina identica alla prima ma per il primo anno priva della licenza software: in caso di guasto o malfunzionamento la licenza esistente può essere trasferita velocemente sulla seconda appliance che, in questo modo, divenendo attiva la sostituisce tutti gli effetti. Dopo il periodo di un anno l'unità "onsite spares" può essere convertita in una macchina attiva, con le medesime caratteristiche e funzionalità della prima e, quindi, con specifica licenza dedicata al fine di garantire l'alta affidabilità in cluster HA in maniera dinamica.

Gli attuali servizi di manutenzione ed aggiornamento, peraltro scaduti, verrebbero attivati sulla nuova piattaforma PA-3020 e non sull'attuale PA-2050, comprendendo anche il servizio WildFire per la protezione del malware moderno, unico nel suo genere e non previsto sull'attuale piattaforma.

Economicamente tale proposta risulta vantaggiosa in quanto portare in alta affidabilità l'attuale appliance avrebbe un costo di listino pari a circa € 20.000, cui si aggiungono i costi relativi all'estensione dei servizi di supporto pari a circa ulteriori € 8.000. La sostituzione dell'attuale modello (PA-2050) con la fornitura di due PA-3020, di cui uno "onsite spare", comporta un importo di spesa pari a circa € 16.000, cui si aggiungono i costi relativi al servizio di supporto pari a circa € 8.000, per un totale di circa € 24.000. Occorre

precisare che i servizi di supporto sono attualmente scaduti e, conseguentemente, da sottoscrivere comunque.

A tal proposito si allega il preventivo redatto dall'impresa Extra Informatica S.r.l., di cui al prot. PR14/00092 del 30.7.2014, precisando che l'importo previsto per la fornitura chiavi in mano dell'apparecchiatura sopra precisata, comprensivo di tutte le attività di installazione e configurazione, pari a €. 24.129,00 (ventiquattromilacentoventinove/00) + IVA è ritenuto congruo e assai vantaggioso considerando le quote di sconto riservato sulle diverse voci di spesa.

La fornitura richiesta è intendersi chiavi in mano nel pieno rispetto delle policy di sicurezza attualmente attive al fine di garantire l'integrità dei dati oltre che la sicurezza degli accessi locali e geografici.

Le motivazioni della scelta dell'Impresa sopracitata per la fornitura e messa in opera dell'apparecchiatura necessaria è da ricondursi al fatto che la stessa ha realizzato l'intera infrastruttura di rete cui gli apparati fanno riferimento, predisponendo il servizio di monitoraggio e gestione della stessa, attualmente in uso. Inoltre, l'Impresa in questione gestisce sotto l'egida di questo Servizio la sicurezza dell'intero network aziendale che, per ovvi motivi, non può essere parcellizzata, a tutto vantaggio oltreché di un più elevato livello di sicurezza anche di una più fluida gestione e migliore ottimizzazione delle risorse: a tal proposito si sottolinea l'elevato grado di sensibilità dei dati veicolati attraverso il network.

Distinti saluti.

Il Responsabile del Servizio
Ing. Marco Galisai

ASL Cagliari

pag. 3/3