Procedura aperta, ai sensi del D.Lgs. n. 50/2016 e ss. mm. e ii., per l'affidamento della fornitura delle infrastrutture hardware e software, nel rispetto del regolamento GDPR, e dell'insieme delle attività necessarie alla predisposizione di un sistema di Disaster Recovery per le piattaforme IT di RSM. CIG 7541613FE9. CUP J81B15000920001.

RISPOSTE A QUESITI POSTI DA SOCIETÀ CONCORRENTI

Quesito n. 44: Capitolo 4.4 CONNETTIVITA' E SICUREZZA

In riferimento al capitolo, si da evidenza di un un cluster checkpoint su cui sono attestati i collegamenti internet e MPLS. In ottica di replicarlo sul sito DR si richiede:

a) Di specificare modello di firewall impiegato e di come esso è configurato in termini di zone , clustering active-standby/active-active, integrazione con AD, come e se è configurato in termini di Virtual Space.

b) Se la gestione avviene attraverso una console di management, in tal caso specificarne il tipo e modello e se il cliente prevede di darne accesso e ai soli fini dell'installazione.

c) Essendo richiesta infrastruttura per un DR si chiede conferma che la soluzione di sicurezza fornita sul sito di DR non debba seguire un normale processo di policy change manuale o in alternativa di specificare uno SLA relativo.

d) Se è ammessa la fornitura di un singolo fw sul sito di DR.

Risposta n. 44:

a) La soluzione in uso è costituita da due firewall Checkpoint SG5600, con virtual system distribuiti su entrambi in configurazione VSLS, ed integrazione con AD.

b) La gestione avviene attraverso una virtual appliance alla quale si prevede di dare un accesso opportunamente regolato per le attività specifiche.

c) La soluzione di sicurezza non deve seguire un normale processo di policy change manuale.

d) Sì, è ammessa la fornitura di un singolo fw sul sito di DR ma è premiante una soluzione in cluster.

Quesito n. 45: Si richiede se la Licenza Veeam Enterprise Plus copra tutti i socket di tutti i Cluster.

Risposta n. 45:

La licenza Veeam Enterprise Plus copre i socket dei seguenti cluster:

1) cluster basato su VMware vSphere 6.0 composto da n. 5 server blade HP (n. 4 BL685c G7, n. 1 BL465c G8) per un totale di 14 CPU e 900 GB di ram inseriti all'interno di un enclosure blade HP C7000 equipaggiato con 2 switch VC Flex-10/10D e 2 switch FC B-series 8/12c e collegato ad una SAN basata su storage Netapp FAS8020;

2) cluster basato su VMware vSphere 6.0 composto da n. 2 server blade HP (n. 2 BL460c G9) per un totale di 4 CPU e 256 GB di ram inseriti all'interno dello stesso enclosure blade HP C7000 sopra citato e collegato alla stessa SAN basata su storage Netapp FAS8020.

Quesito n. 46: Il Capitolato prescrive: "Questi firewall permettono qualsiasi combinazione di protezione su più livelli, tra cui: firewall, VPN, IPS, Application Control, Mobile Access, Anti-Bot, Identity Awareness, URL Filtering, Anti-spam e Antivirus.....che interessano l'architettura al di fuori del perimetro, e sono in grado di prevenire le minacce derivanti dai comportamenti anomali degli utenti o dalla presenza di app malevoli."
Si richiede conferma che le prevenzioni delle minacce siano relative al solo perimetro , agentless e basate sulle features presenti sul NGFW/X.

Risposta n. 46: Si conferma che le prevenzioni delle minacce sono relative al solo perimetro, agentless e basate sulle features presenti nel pacchetto NGTX.

Quesito n. 47: Con riferimento all'assistenza in garanzia il Capitolato prevede:

"Assistenza in garanzia hardware e software: a partire dalla data di sottoscrizione del verbale di conformità e per la durata di 36 mesi, il fornitore dovrà assicurare un periodo di assistenza in garanzia hardware e software che copra tutta l'infrastruttura di DR; durante detto periodo l'aggiudicatario dovrà garantire altresì il mantenimento e l'aggiornamento delle procedure di DR, adeguando i sistemi e le configurazioni secondo le variazioni sul sito primario".

Si chiede di specificare l'assistenza attesa ed il tempo di ripristino specifico per la garanzia HW della soluzione di sicurezza attesa sul sito di DR sia in ottica cluster che eventuale single mode se ammesso.
Inoltre, affinché l'aggiudicatario garantisca gli adeguamenti alle configurazioni della soluzione di sicurezza si richiede :
1) Di specificare se la PA intende propagarli al sito DR attraverso una management rimanendo tale funzione di sua gestione e competenza;
2) Di specificare se la PA si aspetta un processo di policy change direttamente a WEBUI ed in tal caso specificare uno SLA specifico;

3) In caso contrario specificare il tipo di gestione attesa propedeutica agli adeguamenti.

Risposta n. 47: Nell'assistenza in garanzia sono compresi tutti gli interventi atti a garantire il perfetto funzionamento del sistema fornito oltre al mantenimento e all'aggiornamento delle procedure di DR, adeguando i sistemi e le configurazioni secondo le variazioni sul sito primario. I tempi di intervento e/o ripristino saranno di volta in volta concordati con il committente e comunque non superiori all'intervallo del "Next Business Day".

1) Sì, il processo di propagazione policy change rimane di gestione e competenza della PA.

2) No, si tratta di una funzione di competenza della PA.

3) Vedi risposta sub 2.

Angelo Marinetti