

Spett.le
REGIONE DEL VENETO
U.O. Acquisti Centralizzati SSR - CRAV
Passaggio Gaudenzio 1
30131 PADOVA

Inviata via PEC acquisticentralizzati@pec.regione.veneto.it

Oggetto: Consultazione preliminare di mercato - Gara d'appalto per l'affidamento del "Sistema Informativo Regionale

Con riferimento all'oggetto si presentano di seguito le seguenti osservazioni:

Lotto 2

- 2.4.2.1 - Per dimensionare il servizio di housing sarà necessario disporre delle caratteristiche fisiche dei sistemi (spazi occupati, consumi elettrici e potenza termica impegnata).
- 2.4.2.1 - Si richiede di chiarire cosa si intenda per evoluzione prevista del 25% per la gestione del servizio di housing.
- 2.4.2.3 - Trattandosi di un servizio di housing, il criterio di valorizzazione per server logico o singola immagine (e non per server fisico), è inusuale perché il listino risulterebbe in parte scorrelato rispetto ai costi sostenuti dal fornitore (che sono impattati ad esempio dagli spazi occupati dai sistemi, dai loro consumi elettrici e dalla necessità di raffreddamento). Si propone quindi che tale criterio di valorizzazione venga perfezionato.
- 2.4.3.2 - Il criterio di valorizzazione e la correlata TBL010 dovrebbe tenere conto delle differenze fra sistemi virtualizzati x86, sistemi fisici x86, partizioni o sistemi enterprise dedicati ai servizi DB . Inoltre sarebbe importante avere evidenza di come viene valutata economicamente la predisposizione al DR\BC per ogni sistema istanziato.
- 2.4.4 (Premessa - 5.5) - Si chiede di precisare se è richiesto il servizio di Penetration Test Applicativo. In caso affermativo è necessario conoscere la dimensione / complessità del singolo applicativo e l'aspetto dimensionale. Se tale applicativo è un prodotto di mercato è sufficiente fornire informazioni che consentono la determinazione della complessità. Riguardo i singoli applicativi va esplicitata la condizione di test (se via Internet o su rete privata).
- 2.4.4 (Premessa - 5.5) - Si chiede di descrivere come le attività di monitoraggio degli eventi di sicurezza per FW, IDS, IPS, AV vengono implementate attraverso un sistema di notifica. Come sono gestiti attualmente gli eventi?

- 2.4.4 – Servizio di Firewalling e VPN. Si richiedono informazioni riguardo il numero di subnet da proteggere, il numero di VPN e la tipologia richiesta, il numero di IP pubblici e privati da gestire, il numero di regole attualmente presenti su quanto è in esercizio. Al fine di dimensionare il servizio da offrire, si richiedono informazioni riguardo le licenze attive, i servizi per ogni apparato, tutti gli elementi dimensionali che caratterizzano il servizio come ad esempio il numero di sessioni contemporanee, la banda supportata nella specifica modalità. Il servizio di FW dev'essere esteso a singolo host della rete oppure è sufficiente a livello perimetrale?
- 2.4.4 – Servizio IDS/IPS. Si richiede se il servizio dev'essere di tipo Host e/o Network o è ininfluente come implementato dal fornitore? Quali sono i vincoli minimali riguardo il servizio richiesto al fornitore (ad esempio, la capacità di inspection SSL su http)?
- 2.4.4 – Servizio di Content Security. E' necessario conoscere il numero di client e server da proteggere per ciascun sistema operativo implementato.
- 2.4.4 – Servizio di Data Loss Prevention. Si richiede se il tipo di servizio è previsto a livello network e se è attualmente già in essere un sistema di catalogazione delle informazioni sensibili. Si richiede inoltre se è stata sviluppata la profilatura delle utenze e i relativi grant per l'accesso strutturato alle informazioni sensibili.
- 2.4.4.3 - Patch Management. Riguardo le vulnerabilità, si richiede se sono attualmente utilizzati tool automatici e procedure periodiche di valutazione delle vulnerabilità presenti. Quanti sono gli IP privati e pubblici sottoposti a monitoraggio e con quale frequenza viene effettuato il monitoraggio?
- 2.5 - Si richiede di chiarire che la progettazione e l'evoluzione architettura è da intendersi successiva alla fase di Take-in.
- 2.6.2 - Erogazione di servizi di "Threat Intelligence". Si chiede di confermare che il servizio richiesto prevede la fornitura di una interfaccia GUI attraverso la quale sono esposte, per categorie, le potenziali minacce informatiche raccolte sul web e che superino il concetto del "bollettino delle vulnerabilità".
- 2.6.2 - Implementazione/valutazione di avanzati sistemi di rilevamento per la prevenzione di attacchi cibernetici. Si richiede se l'implementazione di sistemi avanzati di rilevamento implicano la difesa via Web Application Firewall dei servizi Web esposti su Internet e la difesa da attacchi applicativi con soluzioni in cloud o on-premises.
- 2.6.2 - Attività di Cyber Security Assessment verticale per servizi esposti in cloud (Attacchi DDoS / DNSSEC / Patch Monitoring ...). Si richiede se oltre all'assessment indicato sono da considerare anche servizi di protezione volumetrica che riesca a proteggere attacchi volumetrici con una capacità di cleaning fino a 160 Gbps.
- 2.6.2 - Penetration test, anche per web services e servizi REST. Si chiede conferma che i penetration test indicati sono limitati ai servizi infrastrutturali e ai sistemi gestiti dal fornitore senza entrare nella componente specifica applicativa. Inoltre si chiede con quale frequenza, quanti IP pubblici e privati sono coinvolti. Se si tratta di PT per Web Services e REST si chiede di dare il dettaglio del contesto oggetto di analisi.
- 2.6.2 - Formazione al personale in merito alle principali tematiche riguardante la cyber security. Si chiede un dettaglio di quali moduli di sicurezza si parla. La formazione deve essere erogata ad un certo numero di persone coinvolte e con una certa frequenza, nonché su specifiche tematiche come il phishing per esempio. Si chiede un dettaglio riguardo il

numero di persone coinvolte, se una formazione di tipo e-learning può essere considerata come condizione minimale di fornitura, la frequenza e il tipo di formazione attese.

- 2.8 - Si è inteso che nel caso di riuso dell'attuale Data Center, i servizi di condizionamento, anti intrusione, antincendio, ecc. saranno erogati da terze parti con cui il fornitore dovrà coordinarsi. Nel caso in cui con il Take-in si intenda proporre l'evoluzione verso il cloud computing o in linea più generale si intendano proporre soluzioni di hosting/housing presso Data Center di terze parti, tali servizi sarebbero invece a carico del fornitore, compresi i relativi costi. In questi casi è quindi opportuno che venga adottato un sistema di valutazione dell'offerta che tenga conto del trasferimento dei costi di tali servizi dall'appaltatore al fornitore.
- 2.9 - Per i rinnovi delle licenze a cura del fornitore in Allegato C è necessario indicare la scadenza dei contratti e si chiede di chiarire se il fornitore debba farsi carico o meno dei costi delle licenze fino alla loro scadenza.

Lotto 3

- 3.1 - Si propone di considerare una soluzione tecnica con erogazione del servizio anche su rete privata (VPN MPLS) al fine di aumentare la disponibilità del servizio e poter assicurare da parte del fornitore la gestione end-to-end del servizio.
- 3.2 - Si ritiene utile evidenziare come all'interno di realtà ICT complesse come quella di Regione Veneto sia opportuno richiedere anche la disponibilità di servizi di MailGateway per l'invio massivo di posta elettronica da applicativi e/o dispositivi multifunzione.
- 3.2 - Servizi di posta elettronica possono essere integrati con soluzioni di VirtualFax e VirtualSMS. Si chiede se possono essere di interesse di Regione Veneto.
- 3.2 (6) - Andrebbe specificato che si può assumere la disponibilità degli editor da parte degli utenti per modificare i file.
- 3.2 (10) - Sono necessari i requisiti di dettaglio per valutare la fattibilità tecnico/economica al fine di poter offrire la specifica soluzione richiesta.
- 3.2 (13) - Si chiede di indicare a chi spetti l'utilizzo della console di gestione del servizio e di richiedere che la soluzione di gestione venga adeguatamente descritta nell'offerta tecnica. Si propone di premiare soluzioni completamente integrate.
- 3.2 (13) - Si chiede di precisare a chi spetti l'help desk di primo livello e quali funzionalità svolga.
- 3.4 (1) - Sono necessari i requisiti di dettaglio per valutare la fattibilità tecnico/economica al fine di poter offrire la specifica soluzione richiesta.
- Con riferimento all'Avviso GUUE (Allegato B - Punto 5), è opportuno specificare nel Capitolato Tecnico che la soluzione deve poter gestire l'accounting e il billing per le diverse ragioni sociali che accederanno al servizio e che le aziende utilizzeranno gli stessi servizi offerti a Regione Veneto, rendendo possibile utilizzare una multi-tenant platform architecture.

Altre osservazioni

Certificazioni del fornitore

Si ritiene opportuno segnalare la necessità di richiedere al fornitore il possesso di adeguate certificazioni per le offerte dei servizi infrastrutturali IT e relativamente ai data center da cui si intendono erogare i servizi. Ciò al fine di garantire adeguate caratteristiche di qualità, sicurezza, affidabilità e disponibilità del servizio offerto alla Regione Veneto ed ai suoi utenti.

Offerte infrastrutturali

- 1) ISO 9001 Quality Management Systems
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62085)
- 2) ISO/IEC 27001 Information technology - Security techniques - Information security management systems
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435)
- 3) ISO/IEC 27018 Information technology - Security techniques - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
(http://www.iso.org/iso/catalogue_detail.htm?csnumber=61498)
- 4) ISO 20000 Information Technology - Service Management
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51986)

Data Center

- 1) Uptime Institute Tier III o Tier IV (<https://uptimeinstitute.com/tiers>). Il possesso della certificazione Tier IV andrebbe adeguatamente premiato.
- 2) ISO/IEC 27001 Information technology - Security techniques -- Information security management systems
(http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=66435)

Software Defined Solutions

Tramite la virtualizzazione del data center, è possibile astrarre tutte le risorse quali ad esempio i server, lo storage, il networking e la sicurezza. Le risorse dei data center possono quindi essere fruite dai clienti in modalità as-a-service. Inoltre al cliente viene data la possibilità di gestire in autonomia i propri servizi attraverso strumenti di self-provisioning. Il fornitore dovrebbe essere in grado di dimostrare capacità di implementazione di:

1. Soluzioni di Software Defined Data-Center, attraverso infrastrutture hyperconverged, in grado di offrire benefici quali ad esempio per la rapidità di implementazione, la scalabilità lineare e la semplicità di gestione.
2. Soluzioni di Software Defined Storage e di Storage Grid attraverso le quali è possibile garantire un incremento delle performance e del throughput, mantenendo inalterati i tempi di accesso al variare della quantità di dati.
3. Soluzioni di Software Defined Network (SDN) che permettono di accelerare il delivery, di rendere le connessioni dinamiche e di aprire le infrastrutture all'uso di componenti Virtual Network Function. La SDN, attraverso un'unica interfaccia di controllo, consente di gestire il layer virtuale e il fisico unificandone la gestione. La realizzazione di una Network Function Virtualization Infrastructure abilita alla realizzazione di componenti virtuali di Firewalling, Load Balancing ed altri elementi di rete, permettendo di pianificare l'ampliamento delle infrastrutture in modo più omogeneo e con i benefici di un dimensionamento granulare. Le soluzioni indicate consentono di ridurre i rischi legati al demand management, agevolando i processi di capacity management e limitando al minimo la necessità di avere una visione accurata sulle attività future di business aziendale.

Cordiali saluti

Mestre 17/3/2017

Telecom Italia Spa
Il Procuratore
Lisa Bassetto