Südtiroler Informatik AG
Informatica Alto Adige SPA

Consultazione di mercato finalizzata all'acquisizione di un servizio di protezione da attacchi DDoS per collegamenti Internet Fastweb

Documento di Consultazione del Mercato

Informatica Alto Adige S.p.A., via Werner Von Siemens 29
39100 Bolzano
PEC: supply@pec.siag.it
http://www.siag.it

Bolzano,

PREMESSA

Informatica Alto Adige (di seguito IAA) eroga servizi informatici alla Provincia di Bolzano attraverso i suoi due Data Center di Bolzano e Brunico. Ogni Data Center è dotato di connettività Internet altamente ridondata e protetta dalle più avanzate tecnologie di Firewalling e IPS al fine di consentire la fruizione dei propri servizi anche su Internet e non solo sulla Intranet Provinciale.

Gli attacchi DDoS rappresentano un grande rischio per la rete e la disponibilità delle applicazioni. Le tradizionali soluzioni di sicurezza perimetrali, come i firewall e gli IPS (Intrusion Prevention System) non risolvono il problema, anzi sono loro stessi bersaglio degli attacchi DDoS.

Per contrastare in modo specifico le minacce alla disponibilità, è necessario disporre un Sistema di Mitigazione DDoS.

La presente iniziativa di consultazione di mercato nell'ambito dell'acquisto di "***Servizio di protezione da attacchi DDoS per collegamenti Internet Fastweb***", ai sensi degli artt.25 L.P. 16/2015 e ss.mm.ii. e dell'artt. 77 del D. Lgs. n. 36/2023 ha l'obiettivo di:

- garantire la massima pubblicità all'iniziativa, per assicurare la più ampia diffusione delle informazioni;
- ottenere la più proficua partecipazione da parte dei soggetti interessati e di verificare l'effettiva esistenza di più operatori economici interessati;
- pubblicizzare al meglio le caratteristiche qualitative e tecniche di beni e servizi oggetto di analisi;
- ricevere, da parte dei soggetti interessati, osservazioni e suggerimenti per una più compiuta conoscenza del mercato.

Si evidenzia che per la fornitura/servizio in oggetto, per le specifiche tecniche richieste in ragione delle peculiari esigenze da soddisfare, si ritiene sussistente una situazione di infungibilità quale definita dalle Linee Guida dell'ANAC n. 8 per il ricorso a procedure negoziate senza previa pubblicazione di un bando nel caso di forniture e servizi ritenuti infungibili. Ai sensi di quanto previsto dalle medesime Linee Guida, si rappresenta che:

- il fabbisogno e gli strumenti per farvi fronte sono rilevabili al punto 1 "Fabbisogno" del presente documento;
- il costo indicativo complessivo per l'acquisizione della fornitura/servizio è stimabile indicativamente in € 300.000,00 escl. IVA, come specificato al punto 2 "Costi attesi" del presente documento;

- la Stazione appaltante valuterà le soluzioni alternative ragionevoli eventualmente proposte nel contesto dei contributi forniti;
- l'eventuale affidamento, qualora a conclusione dell'istruttoria venga ravvisata la sussistenza dei relativi presupposti e non si ritengano quindi percorribili le soluzioni alternative ragionevoli eventualmente proposte, sarà effettuato ai sensi degli artt. 25 L.P. 16/2015 e ss.mm.ii. e 76 del D. Lgs. n. 36/2023.

Vi preghiamo di fornire il Vostro contributo a titolo gratuito - previa presa visione dell'informativa sul trattamento dei dati personali sotto riportata - compilando il presente questionario e inviandolo entro il **17.12.2025**, all'indirizzo e-mail supply@pec.siag.it**.**

Tutte le informazioni da Voi fornite con il presente documento saranno utilizzate ai soli fini dello sviluppo dell'iniziativa in oggetto.

Si prega di indicare se i contributi contengono informazioni e/o dati protetti da diritti di privativi o comunque rilevatori di segreti aziendali, commerciali o industriali, nonché ogni altra informazioni riservata utile a ricostruire la Vostra posizioni nel mercato e/o la Vostra competenza nel campo delle attività di cui alla presente consultazione.

Si chiede, altresì, di precisare, in vista dell'eventuale accesso da parte di altri operatori economici agli esiti della presente consultazione se la divulgazione di quanto contenuto nei Vostri contributi dovrà avvenire in forma anonima.

L'invio del documento al nostro recapito implica il consenso al trattamento dei dati forniti.

Bolzano,

Dati Azienda

Ragione Sociale Azienda
C.F.
P.IVA
Indirizzo
PEC
Nome e Cognome del referente
Ruolo in azienda
Telefono
Fax
Indirizzo e-mail

INFORMATIVA AI SENSI DELL'ART. 13 DEL REGOLAMENTO (UE) 2016/679

Ai sensi degli artt. 13 e seguenti del GDPR - Regolamento UE 2016/679 si invita a prendere visione dell'informativa presente al link: https://assets-eu-01.kc-usercontent.com/482bf257-c7e4-01f3-0b5d-5f9ff7229638/94a355de-c818-4689-aada-1bdc498b7611/informativa-supply-siag-it.pdf

Breve descrizione dell'iniziativa

IAA ha attivo un sistema di mitigazione degli attacchi DDoS sui propri collegamenti Internet che erogano servizio ai propri clienti e necessita predisporre il rinnovo contrattuale di tale servizio.

Il contrasto più efficace per gli attacchi DDoS, per la loro stessa natura, può essere realizzato esclusivamente proteggendo le risorse trasmissive che forniscono la connettività Internet. Nel caso di attacchi DDoS la protezione risulta tanto più efficace quanto più è realizzata in prossimità delle sorgenti degli attacchi e quindi lontano dai target.

1. Fabbisogno

Il servizio di protezione da attacchi di DDoS ricercato da IAA si deve basare su piattaforme distribuite, presenti nei DC e sulle reti di accesso del fornitore senza la necessità di aggiungere apparati dedicati al servizio presso i locali di IAA e senza la necessità di apportare modifiche architetturali all'infrastruttura di IAA. In particolare, si richiede che, in condizioni normali, il traffico Internet SIAG non subisca deviazioni e fluisca direttamente verso l'upstream provider per garantire la compatibilità del servizio con l'architettura

di rete esistente, a tutela dell'investimento effettuato e in quanto progettata e dimensionata per operare con un instradamento diretto verso gli upstream provider con flussi già ottimizzati e testati in esercizio. Tali infrastrutture devono essere in grado di monitorare costantemente il traffico diretto verso i Data Center di IAA e, **solo in caso di anomalie**, devono avere la possibilità di intervenire deviando il traffico verso appliance in grado di filtrare le connessioni lecite e deviare le sessioni reputate malevole.

Per questo motivo va posta particolare attenzione al flusso di traffico che, annunciato verso l'Autonomous System dell'operatore (AS 12874), dovrà seguire il normale flusso verso Internet ed essere dirottato verso gli scrubbing center **solo in caso di attacco DDoS**.

La soluzione proposta deve permettere di effettuare:

- **Analisi** del traffico proveniente da Internet in tempo reale;
- **Detection** di eventuali anomalie rilevate nel traffico;
- **Mitigation** delle anomalie riscontrate eliminando il traffico malevolo.

Dovrà inoltre essere in grado di mitigare le principali tipologie di attacchi volumetrici DDoS descritte nell'elenco che segue, a titolo esemplificativo ma non esaustivo:

- **Attacchi di Flood ICMP**: Questi attacchi sfruttano il protocollo ICMP (Internet Control Message Protocol) per inviare un grande numero di pacchetti ICMP, sovraccaricando la banda e consumando le risorse di rete.
- **Attacchi di Flood UDP**: Questi attacchi coinvolgono l'invio massiccio di pacchetti UDP (User Datagram Protocol) verso un obiettivo, spesso utilizzando port scanning o altre tecniche per identificare e sfruttare servizi vulnerabili.
- **Attacchi di Amplificazione**: Questi attacchi sfruttano server aperti o mal configurati per inviare grandi quantità di dati verso l'obiettivo, amplificando così l'intensità dell'attacco. Alcuni esempi di protocolli utilizzati per gli attacchi di amplificazione includono DNS (Domain Name System), NTP (Network Time Protocol) e SNMP (Simple Network Management Protocol).
- **Attacchi SYN Flood**: Gli attacchi SYN Flood sfruttano il protocollo TCP (Transmission Control Protocol) inviando un grande numero di richieste di connessione SYN incomplete verso un obiettivo, sovraccaricando le risorse del server e impedendo l'accesso legittimo agli utenti.

- **Attacchi di Reflection/Amplification HTTP/HTTPS**: Questi attacchi sfruttano i server Web aperti per riflettere e amplificare il traffico verso l'obiettivo, utilizzando richieste HTTP/HTTPS malformate o manipolate.
- **Attacchi di Reflection/Amplification DNS**: Questi attacchi sfruttano server DNS aperti o male configurati per riflettere e amplificare il traffico verso l'obiettivo, sfruttando le richieste DNS malformate o manipolate.

Il servizio dovrà inoltre avere le seguenti caratteristiche:

- Capacità di cleaning di volumi di traffico pari a 10 Gbps
- Numero illimitato di mitigazioni
- Protezione puntuale fino al singolo IP (anche all'interno di subnet più estese)
- Incident Report entro NBD dalla disattivazione della diversion
- Ampia scelta di profili di servizio al fine di prevedere eventuali ottimizzazioni future
- Assistenza h24x7 con supporto tecnico in lingua italiana erogato dall'Italia

Il Fornitore dovrà erogare il servizio in modalità **proattiva** attraverso un monitoring costante e, in caso di rilevamento di anomalie di traffico riferibili ad attacchi di tipo DDoS, il Fornitore informerà IAA per richiederne l'autorizzazione a procedere con le azioni di contenimento (applicazione della diversion). Per tutta la durata dell'attacco il personale del Fornitore sarà costantemente impegnato a monitorarne l'evoluzione.

La Diversion dovrà essere disabilitata su conferma di IAA a fronte degli aggiornamenti da parte del Fornitore sul rientro dell'attacco. Il Fornitore dovrà sempre informare IAA ad ogni cambio di stato della configurazione del Servizio.

2. Costi attesi

I costi attesi ammontano a € 300.000,00 oltre iva per 36 mesi.

Per l'effetto di quanto precede, sulla base delle proposte che saranno ricevute dalle Società partecipanti alla presente consultazione e indipendentemente dalle stime sopra identificate, Informatica Alto Adige S.p.A. - procederà ad avviare una procedura di acquisto coerente con i risultati dell'indagine stessa, al fine di ottenere la soluzione il più possibile rispondente alle proprie esigenze.

In proposito, si precisa che, ove all'esito della presente consultazione risultassero sussistenti i presupposti di cui agli artt. 25 L.P. 16/2015 e ss.mm.ii. e del 76 D. Lgs. n. 36/2023, Informatica Alto Adige S.p.A. si riserva sin d'ora di procedere all'acquisto mediante procedura negoziata senza pubblicazione del bando.

3. Domande

1. Qual è il fatturato annuo medio realizzato dall'Azienda nell'ultimo biennio relativamente alla vendita di servizi di protezione anti DDoS sia nel mercato italiano che, nello specifico, nel mercato della Pubblica Amministrazione?

Risposta:

_____
_____
_____
_____

2. Si chiede di elencare le precedenti e principali forniture di servizi di protezione anti DDoS dell'Azienda e descrivere le loro principali caratteristiche:

Risposta:

_____
_____
_____
_____

3. Descrivere il mercato di riferimento, chi sono i clienti e quali sono i segmenti di mercato coperti.

Risposta:

_____
_____
_____
_____

4. Descrivere le modalità di distribuzione sul mercato, descrivere la filiera ed indicare come arriva il prodotto/servizio al mercato (vendita diretta, distributori, retail ecc.).

Risposta:

_____
_____
_____
_____

5. Quali sono i punti di forza rispetto alla concorrenza?

Risposta:

_____
_____
_____
_____

6. Quali sono le certificazioni di qualità, di processo, ambientali, ecc. di cui dispone la Vostra Azienda? Quali elementi dei vostri prodotti e servizi vengono valorizzati da tali certificazioni? Perché?

Risposta:

_____
_____
_____
_____

7. Qual è la veste contrattuale con cui l'Azienda intende partecipare? Specificare se si intende partecipare in veste di produttore, di distributore, in esclusiva o non in esclusiva. Nelle ipotesi di partecipazione in virtù di diritti esclusivi il fornitore dovrà dare evidenza del diritto esclusivo (v. allegato) Nell'ipotesi di partecipazione in qualità di distributore, si chiederà all'Azienda di fornire evidenza degli eventuali accordi commerciali col produttore in ordine alla vendita/distribuzione, alla manutenzione e ai servizi connessi relativamente alle licenze oggetto del fabbisogno.

Risposta:

_____
_____
_____
_____

8. Condizioni di prezzo mediamente praticate (prezzi di listino, tipologia di sconti praticati per le licenze, la manutenzione, prezzi e sconti per tutti i servizi richiesti) dettagliata per ogni esigenza elencata nel precedente Capitolo 1 – Fabbisogno.

Risposta:

_____
_____
_____
_____

Firma Fornitore

_____