ALLEGATO "A"

CAPITOLATO SPECIALE

PER LA FORNITURA DI UN SERVIZIO ANNUALE
DI CONTROLLO DELLA POSTA ELETTRONICA
ATTRAVERSO VERIFICA IN AMBIENTE SICURO (SAND BOX)

1 - OGGETTO

La Pubblica Amministrazione, gestendo direttamente il servizio di posta elettronica per diversi domini di posta ed in particolare avendo la responsabilità di garantire le migliori tecnologie per minimizzare il rischio di introduzione nei sistemi informatici di malware, virus e spam, vuole avvalersi di un servizio di controllo delle mail in arrivo, che agisca in tempi rapidi e che possa verificare in tempo reale la presenza di contenuti malevoli attraverso un ambiente sicuro. Questa richiesta vede come soluzione un servizio erogato su server remoti certificati, capaci di essere costantemente aggiornati rispetto alle tipologie di attacco tramite posta elettronica. In particolare la modalità di Sand Box identifica una metodologia che prevede, nei casi di eseguibili sconosciuti, l'attivazione di questi su diversi sistemi operativi per rendere evidente l'eventuale nocività.

L'amministrazione ricerca un prodotto erogato in CLOUD con queste caratteristiche generali:

1) il servizio di analisi e controllo mail dovrà essere configurato su diversi e distinti domini di posta per un totale di 3500 caselle mail registrate, prevedendo una certa variabilità durante l'anno;

2) l'analisi del contenuto mail deve avvenire come antispam, come analisi dei link attivi con controllo anche successivo nel tempo, come analisi degli allegati con verifica in Sand Box di eseguibili, come gestione di allegati zippati e crittati;

3) la consegna all'utente delle mail dannose come mail congelate senza allegati o link attivi;

4) la gestione e la garanzia di consegna di mail PEC o con contenuti firmati digitalmente .p7m e .p7e;

5) uno strumento di analisi e ricerca delle mail in quarantena con possibilità di creare dinamicamente regole di white list o black list;

6) una reportistica riassuntiva ed una reportistica di dettaglio selezionabile per periodi, analisi annuale, mensile, settimanale.

In particolare i requisiti attesi sono:

a. la soluzione deve essere un servizio erogato in Cloud, in grado di proteggere gli utenti su domini di posta multipli;

b. la soluzione deve fornire una protezione dalle email di spam consentendo di scartarle o metterle in quarantena in base al punteggio di spam effettivo;
c. la soluzione deve inoltre prevedere la possibilità di definire policy sulla base di utenti e gruppi;
d. la soluzione deve fornire all'utente finale la possibilità di segnalare un'email come spam utilizzando un link direttamente incluso nell'email ricevuta;
e. la soluzione deve fornire una protezione anti-malware utilizzando una combinazione di più motori;
f. la soluzione deve fornire all'utente finale la notifica degli eventi di quarantena e le eventuali funzionalità personalizzate (whitelist, blacklist, personalizzazione della frequenza di invio del report, lingua, ecc.);
g. l'accesso dell'utente finale alla quarantena antispam deve fornire le informazioni in lingua italiana e la lingua dovrebbe poter essere selezionata automaticamente in base alla localizzazione del browser;
h. la soluzione deve includere una specifica funzionalità di "Link Rewriting" che preveda la sostituzione delle URL sospette con un link a uno specifico servizio Cloud, che consenta di effettuare un'analisi in tempo reale del contenuto della pagina ad ogni "clic" dell'utente;
i. la soluzione deve includere una specifica funzionalità integrata per sensibilizzare gli utenti sul problema del phishing, che fornisca la possibilità di utilizzare le email di phishing ricevute, dopo averle rese innocue, per educare l'utente a riconoscere questo tipo di email e il pericolo che nascondono, senza richiedere un effort gestionale per la configurazione di campagne di phishing simulate;
j. la soluzione deve includere la detonazione in Sand Box per il rilevamento comportamentale di malware sconosciuto in file eseguibili, Microsoft Office e PDF. La soluzione Sand Box dovrebbe utilizzare la tecnologia di astrazione dell'hardware in grado di emulare sia l'hardware che il software della macchina su cui viene eseguita la detonazione dei file. Inoltre, la Sand Box non dovrebbe introdurre un "effort" gestionale per l'installazione, configurazione e aggiornamento periodico delle immagini delle virtual machine utilizzate per la detonazione;
k. la soluzione deve fornire una funzionalità di salvataggio temporaneo degli allegati rimossi dalle mail, da potersi utilizzare sia per la posta in entrata che per quella in uscita. Questa funzionalità dovrebbe consentire aggiungere un'annotazione allo stesso messaggio che includa il nome del file, la sua dimensione e un link web da cui il file possa essere successivamente recuperato;
l. la soluzione deve fornire una funzionalità specifica per contrastare gli attacchi di "executive spoofing" e Business Email Comprise (BEC), idealmente consentendo a un amministratore di configurare una lista di persone più esposte a tali attacchi;
m. la soluzione deve poter fornire l'accesso alla console di amministrazione nel Cloud anche utilizzando autenticazione a due fattori;
n. tutti i data center nel Cloud che possono essere utilizzati dalla soluzione, devono essere certificati ISO 27001, ISO 27018, CSA STAR e Privacy Shield;
o. in fase di attivazione del servizio Cloud deve essere possibile selezionare uno specifico Data Center primario e uno di backup per la gestione dei dati e metadati memorizzati nel Cloud. Tutti i dati devono inoltre essere sempre e solo memorizzati all'interno della comunità europea;

p. tutte le componenti Cloud della soluzione devono basarsi su un'infrastruttura multi-tenant;
q. la licenza d'uso della soluzione deve consentire di poter cambiare la modalità di deployment durante la durata contrattuale. Le modalità di deployment disponibili devono includere On-premise, Hybrid e Cloud;
r. il servizio SaaS di Email Security deve essere disponibile per il 99,999% del tempo come parte dello SLA.

La soluzione deve comprendere l'attività di configurazione iniziale.

2 – MODALITA' E TEMPI DI CONSEGNA

La Stazione Appaltante si riserva, a suo insindacabile giudizio, il diritto di non procedere all'effettiva aggiudicazione, anche a seguito dell'emissione del presente bando.
Pertanto la presente richiesta di preventivo **NON** comporta alcun impegno da parte della Stazione Appaltante e non sorgeranno nei partecipanti diritti di sorta fino a quando l'eventuale aggiudicazione non sia stata deliberata con formale provvedimento del Congresso di Stato, reso esecutivo a norma di legge e firmato il relativo contratto.
Il servizio si intenderà attivato con l'avvio operativo della soluzione, che dovrà avvenire entro e non oltre 25 (venticinque) giorni lavorativi (dal lunedì al venerdì) dalla data di sottoscrizione del contratto.

3 – ORARIO DI LAVORO

Gli orari degli interventi dovranno essere concordati con il Direttore dell'esecuzione.

4 – ESECUZIONE DELLA FORNITURA

Il servizio dovrà essere conforme alle specifiche tecniche descritte nella documentazione di gara. Non saranno accettate caratteristiche tecniche inferiori o diverse da quelle previste.

5 - INTERFERENZE CON ALTRE IMPRESE

L'Impresa Appaltatrice dovrà prendere atto che durante il servizio potrà incontrarsi con altre ditte, di conseguenza, s'impegna a condurre i propri lavori in armonia con le esigenze delle anzidette ditte, senza recare intralcio ed evitando contestazioni pregiudizievoli per l'andamento generale dei lavori. Resta inteso che per le accennate interferenze e per gli oneri conseguenti, l'Impresa Appaltatrice non potrà accampare nessuna pretesa, richiesta di compenso o richiesta di proroga. In caso di divergenza, l'Impresa Appaltatrice s'impegna ad accettare ed osservare le disposizioni e decisioni che il Direttore dell'esecuzione, a suo insindacabile giudizio, riterrà opportuno prendere, tenendo presente il migliore andamento dei lavori, salvo esporre le proprie riserve.

6 - NOMINA DEL DIRETTORE DELL'ESECUZIONE

Divenuta efficace la delibera di aggiudicazione, a seguito del controllo preventivo di legittimità da parte del competente organo di controllo, la Stazione Appaltante nominerà il Direttore dell'esecuzione, in conformità a quanto previsto all'articolo 30, comma 2, del Decreto Delegato n. 26/2015 e successive modifiche. Nel contratto sarà indicato il nominativo ed il recapito del Direttore dell'esecuzione.