PROGETTO

Acquisto ed attivazione di un sistema di sicurezza per la rete provinciale (a norma dell'art. 37, comma 1 del D.Lgs.vo n. 50/2016, con l'attivazione di una richiesta di offerta (RdO), nell'ambito del Mercato Elettronico della Pubblica Amministrazione (MePA))

La Provincia, per garantire la funzionalità dei propri uffici e degli uffici dei comuni che utilizzano la rete provinciale, ha la necessità di adottare tutte le misure di sicurezza e prevenzione così da ridurre al minimo il rischio di malfunzionamenti ed interruzioni di servizio.

Con deliberazione della Giunta Provinciale n. 133 del 2.5.2000, è stato approvato il progetto della prima rete telematica territoriale della Provincia di Reggio Emilia, che ha consentito di realizzare una rete di trasmissione dati 'protetta' tra i comuni e la Provincia di Reggio Emilia consentendo l'interoperabilità e lo scambio di dati in formato digitale tra le pubbliche amministrazioni del territorio provinciale; tale rete si è evoluta negli anni ed è stata integrata nella rete Lepida regionale. Con la creazione della rete telematica è stato costruito un modello topologico che ha visto la Provincia come snodo di collegamento della rete dei comuni verso il mondo Internet e la rete regionale e questo ha richiesto che nella realizzazione di tale rete fossero acquisiti e configurati adeguati apparati di protezione per la sicurezza della rete e dei dati degli enti coinvolti ed in coerenza con le tecnologie disponibili in quegli anni, è stato implementato uno strumento di firewall leader di mercato che ha garantito la massima sicurezza e stabilità.

Negli anni il sistema è stato adeguato alle evoluzioni tecnologiche, alle mutate caratteristiche della rete telematica regionale e all'aumento costante delle minacce alla sicurezza; in particolare con determinazione n. 853/2008 è stato acquisito un sistema firewall costituito da due apparati di rete Nokia/CheckPoint IP 560, aggiornato ora alla release software R 77.30: tale sistema al 31 dicembre 2016 non verrà più supportato dalla casa madre a livello di manutenzione hardware; si rende pertanto necessario sostituirlo, perché in caso di guasto e/o malfunzionamento non sarebbe garantito in alcun modo il suo ripristino.

Il sistema di sicurezza informatica dell'Ente negli anni è diventato sempre più importante e cruciale per via della crescente informatizzazione dei servizi in termini di apparati e sistemi informatici e della parallela diffusione e specializzazione delle minacce alla sicurezza: per l'operatività quotidiana degli uffici è necessario accedere a banche dati raggiunte tramite la rete Internet e molte di queste banche dati sono pubblicate con comunicazioni di tipo cifrato, proprio a causa dell'aumento delle minacce, che richiedono però tempi di controllo maggiori. Molte minacce arrivano poi dai file allegati o dai link inseriti nelle e-mail, strumento sempre più diffuso e indispensabile per tutti i dipendenti dell'Ente: è quindi fondamentale che tutte queste attività transitino dagli apparati di sicurezza garantendone la protezione da tutte le minacce presenti sulla rete internet e nelle mail, assicurando al contempo tempi di accesso soddisfacenti.

Attualmente la rete provinciale garantisce:

- l'accesso alla rete interna e alla navigazione a circa 400 postazioni utenti, utilizzano infatti la rete provinciale anche dipendenti regionali che operano dagli uffici provinciali e tutti necessitano costantemente di accedere a banche dati raggiungibili mediante internet (INSP, Agenzia delle Entrate, ANAC, Prefettura-BDNA, Agid, Sitar, Sistema Informativo Lavoro e Portale lavoro della Regione Emilia Romagna, sistema regionale di gestione delle autorizzazioni ai trasporti eccezionali e della formazione professionale, centrali di acquisto Mepa ed Intercenter, ACI e Motorizzazione civile, etc);

- l'accesso a sistemi informativi provinciali, sia ad accesso riservato agli uffici comunali (back office dello SUAP, di Rilfedeur e delle elezioni; strumenti di gestione della cartografia, dns) sia aperti a tutti (software di segnalazione per i cittadini, consultazione delle tornate elettorali, catalogo delle biblioteche provinciali, cartografia provinciale, etc), installati presso la sala macchine della Provincia;
- servizio di firewall per la rete interna e le pubblicazioni su internet per quattro comuni che non hanno un proprio apparato di protezione;
- servizio di firewall per la navigazione internet per tredici comuni che hanno un proprio apparato firewall per la rete interna, ma accedono a Internet mediante la rete provinciale;
- protezione del servizio di posta elettronica mediante il servizio di relay provinciale per dieci comuni;
- protezione del servizio di videosorveglianza di un comune

Vista quindi la molteplicità e criticità di comunicazioni gestite dalla rete provinciale, si ritiene indispensabile acquisire un'infrastruttura diffusa e leader di mercato, che presenti tutte le migliori caratteristiche funzionali e che assicuri, anche rispetto alle valutazioni comparative effettuate da organismi internazionali, le migliori prestazioni e adeguamenti alla continua mutazione dei rischi informatici.
La scelta di uno strumento molto diffuso, potrà inoltre dare garanzia nel tempo, che su di esso possano operare una molteplicità di imprese con sedi operative tali da poter intervenire presso la sede della Provincia tempestivamente in caso di grave guasto.

Si sono individuate una serie di caratteristiche e funzionalità minime che dovrà garantire lo strumento che si va ad acquisire, così da assicurare i servizi sopra descritti, in particolare la soluzione proposta deve garantire le seguenti funzionalità:

- il sistema proposto deve essere configurato in **alta affidabilità**, tramite due dispositivi fisici distinti;
- il sistema e gli apparati proposti dovranno disporre, in maniera integrata, di tutte le diverse funzioni di sicurezza caratterizzanti un "***Next-Generation Firewall****",* ovvero garantire le funzionalità di: **Firewall/VPN di base con l'aggiunta di funzionalità di identificazione delle applicazioni e identificazione dell'utente, oltre ai servizi di Intrusion Prevention System (IPS), Antivirus, Anti-Spyware, Web/URL Filtering, Application Control ed Advanced Threat Protection/Detection**, senza necessità di utilizzare alcun modulo software o hardware aggiuntivo o ulteriore apparato esterno. Queste ultime funzionalità dovranno poter essere implementate ed attivate secondo i diversi profili legati alle singole regole di accesso definite sul sistema;
- la fornitura dovrà prevedere le **licenze e la manutenzione hardware e software annuale** per garantire le funzionalità sopra descritte;
- il sistema così configurato, con tutti i servizi attivi e configurati, dovrà garantire almeno il parametro di ***Threat prevention throughput (Firewall,Application Control, Url Filtering, IPS, Antivirus)*** **pari o superiore ad 1 Gbps**;
- il sistema dovrà disporre di un complesso di correlazioni di oggetti ed eventi relativi a tutte le diverse funzioni di sicurezza sopra descritte che sia integrato sullo stesso apparato del firewall e che garantisca una vista in tempo reale delle attività sospette e degli eventi relativi ad attività malevole;
- gli apparati dovranno disporre, di un servizio **"*Advanced Threat Protection/Detection*"** in Cloud con le seguenti caratteristiche:
  - ricezione e analisi proattiva di molteplici tipologie di file (es. "jar", "PE",

"flash",“pdf”, file Microsoft Office, pacchetti android e della copia di file eseguibili “exe”) sospetti in transito sull’apparato firewall stesso;
    - integrazione con l’apparato firewall sia in termini operativi che di gestione del servizio stesso;
    - verifica, analisi e report dettagliato dell’eventuale comportamento malevolo all’apertura o all'esecuzione dello stesso file sospetto;

- dovrà essere presente un **tool di migrazione** automatico che consenta di recuperare le configurazioni relativamente ad oggetti, host, network e regole presenti sull'attuale sistema Check Point;

Sulla base delle esigenze sopra indicate, sono stati analizzati diversi prodotti di mercato ed oltre **alla possibilità di aggiornare la soluzione esistente con appliance e tecnologia Check Point, si è individuata la soluzione “denominata PA 3020” in HA di Palo Alto Network** come quella più corrispondente alle caratteristiche e funzionalità richieste, il fornitore dovrà quindi proporre un progetto di migrazione dall'attuale soluzione ad una piattaforma tra quelle indicate o equivalente a livello di prestazioni, funzionalità e caratteristiche tecniche, con tutti i servizi attivi richiesti per un anno.

I concorrenti dovranno **formulare una relazione descrittiva** che presenti dettagliatamente il sistema di sicurezza che intendono proporre, sulla base delle caratteristiche tecniche minime come dettagliate dal produttore, l'implementazione e configurazione che intendono effettuare sul sistema perché sia rispondente alle necessità dell'Ente. Dovrà inoltre essere presente un crono programma che dettagli le modalità e le tempistiche per la conversione delle configurazioni e delle regole attualmente presenti sul sistema firewall per garantire il minimo disservizio: tali attività dovranno essere effettuate in affiancamento al personale interno all'Ente, che si occuperà poi della gestione del sistema a regime.

dato atto che:

- al momento presente, nell'ambito del programma "Acquisti in Rete della PA", attuato dal Ministero dell’Economia e delle Finanze attraverso la gestione di Consip S.p.A, a norma dell'articolo 26 della legge 23 dicembre 1999, n. 488 "Legge finanziaria 2000", relativamente alla categoria “Telecomunicazioni, elettronica e servizi accessori ”, è attiva la convenzione “Reti Locali 5 – Lotto 2“ che propone dispositivi di sicurezza, ma si valuta di non procedere all'acquisizione di tali apparati in quanto:
    - ✓ in data 16 novembre 2016 sul programma "Acquisti in Rete della PA" è stata pubblicata una segnalazione che precisa che '*in data 16/11/2016, relativamente al Lotto 2 della convenzione Reti Locali 5, si è verificato l’esaurimento del massimale,* comprensivo di estensioni 6° e 7° quinto;
    - ✓ i sistemi di sicurezza e relativi servizi software presenti in convenzione non si ritengono adeguati, relativamente a funzionalità, diffusione sul mercato, presenza di aziende sul territorio italiano con esperienza nella loro configurazione e migrazione dal precedente sistemi di sicurezza CheckPoint, attualmente in uso, in particolare:
        - ✗ i dispositivi presenti in convenzione, comprendono quattro soluzioni, dalla fascia base (meno performante) alla fascia top (con grandi prestazioni), e nella comparazione si valuta sempre il sistema di fascia top, denominato USG6650;
        - ✗ il prodotto in convenzione è poco diffuso in Italia al momento e le aziende che possono garantire assistenza e raggiungere in tempi stretti la sede della Provincia in caso di malfunzionamenti gravi e bloccanti sono limitate (l'acquisto di un prodotto più diffuso e presente nel territorio ci dà molte più garanzie in tal senso);

- ✗ rispetto ai sistemi di valutazione internazionale dei prodotti di questa tipologia il prodotto in convenzione è in possesso delle certificazioni ICSA Labs e NSS Labs, ma per Gartner (www.gartner.com) è un prodotto ancora di nicchia, indicato nelle situazioni in cui gli apparati di rete e di amministrazione sono del medesimo costruttore, invece la Provincia non possiede alcun altro prodotto Huawei;
- ✗ non risulta avere integrata la funzionalità di 'a*dvanced threat protection',* come sopra descritta tra le funzionalità di grande importanza nella soluzione che si intende acquisire;

b) al momento presso la Centrale di committenza regionale Intercent-ER è presente la convenzione 'Servizi convergenti ed integrati di trasmissione dati e voce su reti fisse e mobili' che propone a listino, tra i servizi aggiuntivi e non previsti inizialmente, alcune licenze di sistemi di protezione dati, ma si ritiene che non siano adeguati relativamente alle funzionalità e ai costi, così come indicati su tali listini;

L'aggiudicatario dovrà dimostrare di avere esperienza in precedenti migrazioni da sistema firewall CheckPoint esistente alla soluzione proposta e dovrà indicare una proposta di pianificazione delle attività tale da garantire il minimo disservizio.
La ditta dovrà inoltre indicare con precisione il livello di assistenza proposto, successivo alle attività di migrazione, ovvero specificare le modalità con cui sarà possibile segnalare le problematiche evidenziate dal sistema e i tempi di presa in carico, sulla base della gravità del problema riscontrato e dovrà specificare la durata di tale servizio compresa nella fornitura.

Con riferimento alla Legge n. 123 del 03/08/2007 e alla successiva determinazione n. 3 del 05/03/2008 sulla “Sicurezza nell'esecuzione degli appalti relativi a servizi e forniture. Predisposizione del documento unico di valutazione dei rischi (DUVRI) e determinazione dei costi della sicurezza” (emanata dall'AVCP - AUTORITA' per la Vigilanza sui contratti pubblici di lavori, servizi e forniture), trattandosi di affidamento di attività principalmente di natura intellettuale, non sono previsti rischi da interferenza né oneri per la sicurezza.

L'azienda affidataria del servizio dovrà poi dichiarare l'entità dei costi generali per gli adempimenti in materia di sicurezza che sostiene.

La base d'asta ammonta a € 39.900,00.

Per ogni altro dettaglio si rimanda al Capitolato.