Il sottoscritto Abraham Gebrehiwot in qualità di responsabile dell'unità tecnologica (UT) Computer and Communication Networks (CCN) dell'Istituto di Informatica e Telematica (IIT) del Consiglio Nazionale delle Ricerche (CNR)

CONSIDERATO

1. che, ad oggi, non esistono metodi standard (benchmark) per misurare e confrontare in modo oggettivo le prestazioni di apparati NGFW di produttori diversi e che solo un metodo oggettivo consentirebbe di effettuare in modo efficace una comparazione tra apparati di produttori diversi richiesta da una normale procedura d'acquisto;

2. che, per quanto specificato al punto 1, ciascun produttore riporta, nei documenti di specifica tecnica dei propri apparati NGFW, indicatori prestazionali non confrontabili tra loro. Infatti, sebbene tali indicatori mantengano nomi simili da produttore a produttore, nella maggior parte dei casi, questi fanno riferimento a misurazioni avvenute in contesti differenti, come ad esempio diverse configurazioni di networking e/o di firewalling. Inoltre, anche le comuni terminologie del settore cyber security assumono significati diversi a seconda del produttore che li utilizza;

3. che il sistema operativo e le interfacce di gestione di apparati NGFW sono differenti da produttore a produttore, essendo esse di tipo proprietario. Questo implica che il personale dell'UT CCN non può *a priori* conoscere approfonditamente i sistemi operativi e le interfacce di gestione di tutti i prodotti NGFW disponibili sul mercato;

4. che il supporto e la manutenzione delle soluzioni NGFW attualmente in uso sono scaduti in data 31 Maggio 2021 e che quindi il personale dell'UT CCN non ha a disposizione tempi sufficientemente lunghi per studiare nuove soluzioni appartenenti a prodotti diversi da quelli in uso;

5. che, per quanto specificato ai punti 3 e 4, se si avviasse una procedura di acquisto tradizionale (qualità/prezzo) potrebbe sussistere il rischio concreto di acquistare un prodotto scadente e/o sconosciuto al personale dell'UT CCN. Questo potrebbe comportare un ritardo nella messa in linea della soluzione e un aumento del rischio di incidenti di tipo cyber, con conseguenti disagi, anche gravi, al funzionamento del servizio della rete telematica dell'Area della Ricerca del CNR di Pisa;

6. che il personale dell'UT CCN ha diversi anni di esperienza sul campo, nei quali ha maturato un know-how specifico nella risoluzione di problemi cyber, mediante l'utilizzo di apparati del produttore Palo Alto Networks che costituiscono la soluzione attualmente in uso presso la rete telematica dell'Area della Ricerca del CNR di Pisa;

7. che, nel tempo, l'utilizzo degli apparati specificati al punto 6 ha giocato un ruolo centrale per la messa in sicurezza e il monitoraggio della rete telematica dell'Area della Ricerca del CNR di Pisa. Esiste quindi il rischio che soluzioni di altri produttori non siano compatibili con l'attuale configurazione, monitoraggio e funzionamento di rete;

8. che l'utilizzo di una soluzione che non sia in continuità con gli apparati specificati al punto 6 può far sì che il personale dell'UT CCN debba impiegare molto tempo prima di acquisire nuovamente un know-how paragonabile a quello raggiunto con la soluzione attualmente in uso;

9. che, tenendo in considerazione i punti 6 e 8, si potrebbero avere effetti negativi, almeno nel breve periodo, quali un livello di sicurezza più basso ed una soluzione operativa meno efficace;

CHIEDE

In base alle suindicate considerazioni, di procedere con Trattativa diretta su mepa aventi ad oggetto l'acquisizione di una manutenzione evolutiva su prodotti a Marca Palo Alto in quanto sussistono le condizioni di cui all'art 63 comma 3 lettera b)

Pisa, 22/06/2021

Ing. Abraham Gebrehiwot