

DELIBERAZIONE DEL DIRETTORE GENERALE

UNITÀ OPERATIVA: U.O.C. PROGETTAZIONE SVILUPPO E MANUTENZIONE IMMOBILI ED IMPIANTI, SISTEMI INFORMATICI E ICT

OGGETTO: INDIZIONE DI UNA PROCEDURA MEPA NEGOZIATA CON RDO A TRE OPERATORI ECONOMICI AI SENSI DELL'ART. 36 COMMA 2 LETT. B) E COMMA 6 DEL D.LGS. 50/2016, PER LA FORNITURA DI LICENZE SOPHOS ANTIVIRUS DA AGGIUDICARE CON IL CRITERIO DEL MINOR PREZZO AI SENSI DELL'ART. 95, CO. 4, LETT. B) D.LGS. 50/2016 –IMPORTO STIMATO A BASE DI GARA € 64.530,00 OLTRE IVA (22%) - Lotto CIG 9101780277

Tenuto conto che con la sottoscrizione del presente atto il Direttore della UOC attesta che l'affidamento di cui trattasi avviene nel rispetto della vigente normativa, in conformità della regolamentazione di cui all'oggetto.

Premesso che:

- Con nota prot. 17880 del 15/09/2021, a seguito del recente attacco hacker ai danni della Regione Lazio, il proponente ha richiesto ed ottenuto nulla osta dalla Direzione Generale ad incrementare i livelli di sicurezza della infrastruttura della rete aziendale;
- in particolare, per ciò che concerne la protezione da malware del sistema informativo aziendale, sin dal 2010 è stato adottato un sistema antivirus aziendale centralizzato su piattaforma SOPHOS End Point Protection, oggi evoluto da una versione client/server ad una cloud baased con consolle di gestione centralizzata mediante autenticazione a due fattori, per l'amministrazione degli host di rete e per il controllo degli eventi di sicurezza registrati.

Dato atto che:

- Le moderne minacce informatiche non sempre provengono dall'esterno, ma spesso si generano direttamente dalla rete aziendale, dove risulta fondamentale non solo la difesa dei singoli endpoint ma anche l'analisi e la ricerca delle sorgenti di attacco, al fine di isolare e scongiurare possibili perdite di dati;
- pertanto, è stata ravvisata la necessità di garantire una più elevata protezione del sistema informativo aziendale in caso di attacchi alla sicurezza informatica che possano compromettere l'operatività di ambienti ritenuti *mission critical*;
- questa U.O.C. ha avviato da tempo uno studio specifico delle tecnologie e delle soluzioni che il mercato può offrire a garanzia degli obiettivi di evoluzione ed elevazione dei sistemi di sicurezza informatici adeguati agli attacchi sempre più sofisticati degli hacker, in accordo con le direttive AGID;
- a tale scopo, sono stati presi in considerazione sia i sistemi di tipo Endpoint Detection and Response (EDR) sia i sistemi di tipo Extended Detection and Response (XDR), che si differenziano per il fatto che i primi (EDR) eseguono analisi dei dati e prevengono eventuali attacchi relativamente a quanto riportato nei singoli endpoint, mentre i secondi (XDR) svolgono tale compito non solo limitatamente agli endpoint,

ma integrando i dati che provengono dall'analisi della rete, delle e-mail, dei dispositivi mobili aziendali e del cloud;

- a parere di questa U.O.C. la soluzione migliore a garantire la sicurezza dei sistemi aziendali è rappresentata dai sistemi di tipo Extended Detection and Response (XDR) dal momento che tali sistemi di prevenzione sono in grado di debellare anche i cosiddetti "*attacchi laterali o movimenti laterali*";
- l'importanza di inserire tali sistemi di protezione all'interno della rete aziendale è evidente, poiché oltre a bloccare le menzionate minacce, consentono anche di risalire alla fonte dell'attacco e ricostruire la vulnerabilità sfruttata dai malintenzionati.

Preso atto che:

- risulta, quindi, fondamentale integrare il sistema antivirus classico già in uso con un sistema di tipo Extended Detection and Response (XDR);
- lo studio svolto da questa U.O.C. ha portato ad individuare, tra i diversi sistemi XDR, una soluzione specifica evolutiva del sistema antivirus già in uso, così da implementare lo stesso senza sostituirlo, posto che le relative licenze d'uso verranno a scadere solo nel 2023;
- la specifica soluzione che risulterebbe dall'evoluzione individuata, che combina alle licenze CIXA (necessarie per il funzionamento dell'antivirus Sophos) già in uso, le licenze XDR (evolutive dell'antivirus Sophos già in uso) che verranno acquisite, è denominata "Advanced Intercept X", e rappresenta una soluzione pionieristica nella implementazione dei moduli di difesa dai Ransomware e Cryptovirus, software particolarmente malevoli che hanno lo scopo di alterare e rendere inutilizzabili i dati aziendali;
- il software "Advanced Intercept X", in particolare, offre le seguenti funzionalità:
 - Antiransomware
 - Web Security
 - Download Reputation
 - Controllo web / Blocco degli URL in base alla categoria di appartenenza
 - Controllo delle periferiche
 - Controllo delle applicazioni
 - Rilevamento antimalware con deep learning
 - Scansione antimalware dei file
 - Live Protection
 - Analisi del comportamento in pre-esecuzione (HIPS)
 - Blocco delle applicazioni potenzialmente indesiderate (PUA)
 - Intrusion Prevention System
 - Data Loss Prevention (prevenzione della perdita di dati)
 - Analisi del comportamento in fase di esecuzione (HIPS)
 - Antimalware Scan Interface (AMSI)
 - Rilevamento del traffico malevolo (Malicious Traffic Detection, MTD)
 - Exploit Prevention
 - Mitigazione del comportamento dei cybercriminali
 - Protezione antiransomware per i file (CryptoGuard)
 - Protezione del disco e del record di avvio (WipeGuard)
 - Protezione contro gli attacchi man-in-the-browser (Safe Browsing)
 - Ottimizzazione del lockdown delle applicazioni

- Rimozione automatizzata dei malware
- Synchronized Security Heartbeat
- Sophos Clean
- pertanto, le funzionalità aggiuntive che si potranno ottenere acquistando anche le licenze XDR Sophos sono:
 - Live Discover (formulazione di query SQL su ambienti diversi per il threat hunting e la protezione dell'integrità delle IT security operation)
 - Libreria di Query SQL (query pre-compilate e completamente personalizzabili), Rilevamento e definizione di priorità per gli eventi sospetti
 - Rilevamento e definizione di priorità per gli eventi sospetti
 - Accesso rapido, archiviazione dei dati su disco (fino a 90 giorni)
 - Origini di dati che coinvolgono prodotti multipli, ad es. Firewall, Email (Sophos XDR)
 - Query su prodotti multipli (Sophos XDR)
 - Archiviazione nel cloud con Sophos Data Lake 30 giorni
 - Query pianificate
 - Casi di minacce (Root Cause Analysis)
 - Analisi antim malware con Deep Learning
 - Dati di intelligence avanzata sulle minacce disponibili su richiesta, forniti direttamente dai SophosLabs
 - Esportazione dei dati attraverso analisi approfondite
 - Rimozione automatizzata dei malware
 - Synchronized Security Heartbeat
 - Sophos Clean
 - Live Response (per indagare e intraprendere azioni da remoto)
 - Isolamento degli endpoint su richiesta
 - "Clean and Block" Con Un Solo Clic

Dato altresì atto che:

- per l'individuazione dell'importo da porre a base di gara il proponente ha richiesto l'assistenza del Vendor Sophos, al quale è stato chiarito che le licenze CIXA già in possesso dell'AORN verranno a scadere solo il 25/06/2023 e, pertanto, occorre valorizzare il prezzo dell'acquisto delle licenze XDR per il solo periodo 25/03/2022 - 25/06/2023, mentre, per gli anni successivi al 2023, occorre valorizzare il prezzo sia delle licenze CIXA che delle licenze XDR, che, come precisato, solo se integrate, costituiscono il sistema denominato "Advanced Intercept X";
- da un confronto con il Vendor Sophos, l'acquisto delle singole licenze anno per anno è risultato essere più oneroso di quello pluriennale: precisamente l'incremento di prezzo tra una fornitura annuale ed una pluriennale è pari ad almeno il 10,60%;
- in ogni caso, in considerazione della rapida evoluzione delle tecnologie relative ai sistemi di protezione, onde escludere il possesso di strumenti di protezione che potrebbero risultare obsoleti, a parere del proponente, non è opportuno programmare l'acquisto di licenze di sistemi antivirus con scadenza superiore ai tre anni;
- il numero di licenze occorrenti ascende a 600 per "user" ed a 60 per "server";
- alcuni "user" sono rappresentati da macchine obsolete con sistemi operativi Win 7/8.1/2008, per i quali, affinché il sistema "Advanced Intercept X" funzioni correttamente,

occorre acquistare anche apposite licenze "estensive" di supporto, della durata di almeno 6 mesi, posto che in tale lasso temporale l'AORN dovrebbe aver terminato le operazioni di sostituzione di tali macchine obsolete;

- dunque, l'importo da porre a base di gara ai sensi dell'art. 35 co. 4 D.Lgs. 50/2016, è stato individuato per l'acquisto di n. 600 licenze per user e n. 60 licenze per server XDR con scadenza triennale, per l'acquisto di 600 licenze per users e n. 60 licenze per server CIXA con scadenza biennale e per l'acquisto e di un numero massimo di 499 licenze estensive di supporto per macchine con sistemi obsoleti della durata di 6 mesi e, richiesto al Vendor, è stato da esso valorizzato in complessivi € 64.530,00 oltre IVA (22%);
- ai sensi dell'art. 36, comma 6 del Codice dei contratti pubblici, per lo svolgimento delle procedure d'importo inferiore alle soglie comunitarie, le stazioni appaltanti possono procedere attraverso un mercato elettronico che consenta acquisti telematici basati su un sistema che attua una procedura di scelta del contraente interamente gestita per via elettronica, tra i quali, quello istituito dal Ministero dell'economia e delle finanze, che avvalendosi di CONSIP S.p.A., mette a disposizione delle stazioni appaltanti il mercato elettronico delle pubbliche amministrazioni.

Preso atto che:

- Non sono attualmente attive su Consip convenzioni per l'acquisto di licenze CIXA Sophos ed XDR Sophos;
- i diversi sistemi di protezione acquistabili in convenzione non sarebbero, in ogni caso, idonei a soddisfare lo specifico fabbisogno di tutela dei dati di questa A.O.R.N.;
- in particolare, il sistema combinato di licenze CIXA ed XDR, denominato "Advanced Intercept X" della Sophos - la cui tecnologia, nell'ambito dei sistemi antivirus, è riconosciuta essere posizionata nel quadrante dei "leader" nel relativo Magic Quadrant di Gartner - presenta tutte le caratteristiche architetture, tecniche, di sicurezza e certificazione in grado di garantire la migliore protezione possibile in caso di attacco hacker;
- per tale motivo, questa U.O.C. inviterà a partecipare alla R.D.O. tre operatori economici selezionando gli stessi solo tra i rivenditori autorizzati di licenze CIXA ed XDR Sophos, iscritti al Me.PA., nell'elenco della categoria merceologica "Informatica, Elettronica, Telecomunicazioni e Macchine per Ufficio".

Considerato che:

- l'affidamento attiene ad una fornitura con caratteristiche standardizzate e circoscritte ai requisiti specificamente indicati nel Disciplinare di gara, pertanto, ai sensi dell'art. 95, co. 4, lett. b, del D.Lgs. 50/2016, il criterio di aggiudicazione sarà il minor prezzo;
- la documentazione di gara è costituita dai seguenti atti, ivi complessivamente richiamati per costituirne parte integrante e sostanziale:
 - LETTERA DI INVITO
 - DISCIPLINARE DI GARA
 - ALLEGATI AL DISCIPLINARE DI GARA:
 - Allegato A – Dichiarazione di partecipazione;
 - Allegato B – DGUE;

- Allegato C – Dichiarazioni integrative operatore economico singolo o associato;
- Allegato D – Dichiarazioni integrative altri soggetti;
- Allegato E – Protocollo di legalità;
- CODICE DI COMPORTAMENTO da visionare per l'accettazione nella Dichiarazione di partecipazione visionabile al seguente indirizzo: www.santobonopausilipon.it al seguente percorso "home/atti generali/codice disciplinare e di condotta".
- COMUNICAZIONE EMERGENZA COVID da visionare per l'accettazione nella dichiarazione di partecipazione.
- NOTA PROT. 8187/21 relativa al versamento dell'Imposta di Bollo sul contratto.
- il contratto sarà concluso mediante piattaforma Me.PA, da intendersi nella forma della scrittura privata a norma dell'art. 32, comma 14 del Codice dei contratti pubblici, e sarà regolamentato dalle Condizioni Generali di Contratto stabilite da Consip S.p.A.;
- non verrà applicato il termine dilatorio di cui all'art. 32, comma 9 del Codice Appalti, come previsto dal comma 10, lett. b) del medesimo articolo;
- in ottemperanza alle disposizioni dell'Ufficiale Rogante aziendale con nota prot. 8187 del 20.04.2021, entro 5 giorni dalla stipulazione del contratto, l'aggiudicatario si impegna all'assolvimento dell'imposta di bollo di € 16,00, secondo le modalità previste dall'art. 3 del DPR 642/1972, acquisita a cura del RUP della precedente UOC.

Ritenuto pertanto opportuno:

- procedere all'indizione di una procedura negoziata sotto soglia con RDO a tre operatori economici ai sensi dell'art. 36 comma 2 lett. b) e comma 6 del d.lgs. 50/2016, per la fornitura di n. 600 licenze per users e n. 60 licenze per server XDR della durata di 36 mesi, di n. 600 licenze per users e n. 60 licenze per server CIXA della durata di 24 mesi e di un numero massimo di 499 licenze estensive di supporto per macchine con sistemi obsoleti della durata di 6 mesi, da aggiudicare con il criterio del minor prezzo ai sensi dell'art. 95, co. 4, lett. b) D.Lgs. 50/2016, per un importo a base d'asta pari ad € 64.530,00 oltre IVA (22%).

Visti:

- L'art. 36, co. 6 che consente alle stazioni appaltanti di avvalersi del sistema Me.PA. per lo svolgimento di procedure sottosoglia;
- Le Linee Guida n. 4, di attuazione del Decreto Legislativo 18 aprile 2016, n. 50, recanti *"Procedure per l'affidamento dei contratti pubblici di importo inferiore alle soglie di rilevanza comunitaria, indagini di mercato e formazione e gestione degli elenchi di operatori economici"*;
- le Linee Guida n. 4 aggiornate al Decreto Legislativo 19 aprile 2017, n. 56 con delibera del Consiglio n. 206 del 1 marzo 2018, recanti *«Procedure per l'affidamento dei contratti pubblici di importo inferiore alle soglie di rilevanza comunitaria, indagini di mercato e formazione e gestione degli elenchi di operatori economici»*;
- la comunicazione del Direttore Generale acquisita al prot. n. 17979 del 04/10/2019, confermativa della disposizione dell'Ufficiale Rogante di cui al prot. n. 9542 del 25/05/2019, che ha previsto che per le procedure di affidamento diretto ex art. 36 D.Lgs.

50/2016, espletate sui mercati elettronici, quest'AORN provveda alla sola verifica del possesso da parte dell'affidatario dei requisiti speciali, qualora previsti, essendo demandata al gestore del mercato elettronico la verifica della sussistenza del requisito generale di assenza di motivi di esclusione ex art. 80 del D.Lgs. 50/2016 con le modalità prescritte dall'art. 36, comma 6-bis del D.Lgs. 50/2016;

Il Direttore
Ing. Gennaro Sirico
f.to digitalmente

Acquisito il parere favorevole del Direttore Sanitario che sottoscrive per conferma

Il Direttore Sanitario
Dott. Vincenzo Giordano
f.to digitalmente

IL DIRETTORE GENERALE

In virtù dei poteri conferitigli con D.P.G.R.C. N. 171 DEL 09/12/2020

Alla stregua dell'istruttoria compiuta dalla Unità Operativa proponente, nonché dell'espressa dichiarazione di regolarità resa dal responsabile di tale Unità Operativa con la firma apposta in calce.

Per tutto quanto in premessa espresso e che qui si intende integralmente richiamato

DELIBERA

1. **Di prendere atto** della opportunità di garantire una più elevata protezione del sistema informativo aziendale in caso di attacchi alla sicurezza informatica, integrando il sistema antivirus classico già in uso (CIXA Sophos) con un sistema di tipo Extended Detection and Response (XDR Sophos) mediante l'acquisto delle necessarie licenze;
2. Per l'effetto, **di indire** procedura negoziata sotto soglia con RDO a tre operatori economici ai sensi dell'art. 36, comma 2 lett. b) e comma 6 del D.Lgs. 50/2016, per la fornitura di n. 600 licenze per user e n. 60 licenze per server XDR della durata di 36 mesi, di n. 600 licenze per users e n. 60 licenze per server CIXA della durata di 24 mesi e di un numero massimo di 499 licenze estensive di supporto per macchine con sistemi obsoleti della durata di 6 mesi, da aggiudicare con il criterio del minor prezzo ai sensi dell'art. 95, co. 4, lett. b) D.Lgs. 50/2016, per un importo a base d'asta pari ad € 64.530,00 oltre IVA (22%);
3. **Di approvare** la seguente documentazione di gara, costituente parte integrante e sostanziale del presente provvedimento:
 - LETTERA DI INVITO
 - DISCIPLINARE DI GARA
 - ALLEGATI AL DISCIPLINARE DI GARA:
 - Allegato A – Dichiarazione di partecipazione;
 - Allegato B – DGUE;

- Allegato C – Dichiarazioni integrative operatore economico singolo o associato;
 - Allegato D – Dichiarazioni integrative altri soggetti;
 - Allegato E – Protocollo di legalità;
 - CODICE DI COMPORTAMENTO da visionare per l'accettazione nella Dichiarazione di partecipazione visionabile al seguente indirizzo: www.santobonopausilipon.it al seguente percorso "home/atti generali/codice disciplinare e di condotta".
 - COMUNICAZIONE EMERGENZA COVID da visionare per l'accettazione nella dichiarazione di partecipazione.
 - NOTA PROT. 8187/21 relativa al versamento dell'Imposta di Bollo sul contratto.
4. **Di dare atto** che la spesa derivante dall'affidamento *de quo* sarà addebitata a seguito dell'aggiudicazione sui Bilanci di relativa competenza come immobilizzazione immateriale;
 5. **Di nominare** RUP e DEC del procedimento il Direttore della UOC Tecnico Patrimoniale e ICT, ing. Gennaro Sirico;
 6. **Di precisare** che la presente deliberazione è soggetta a pubblicazione sul profilo del Committente, nella sezione "Amministrazione trasparente" ai sensi dell'art. 37, commi 1 e 2 del D.Lgs. 33/2013 e dell'art. 29 del D.Lgs. 50/2016;
 7. **Di dare atto** che il contratto sarà concluso mediante piattaforma Me.PA., da intendersi nella forma della scrittura privata a norma dell'art. 32, comma 14 del Codice dei contratti pubblici, e sarà regolamentato dalle Condizioni Generali di Contratto stabilite da Consip S.p.A.;
 8. **Di dare atto altresì** che non verrà applicato il termine dilatorio di cui all'art. 32, comma 9 del Codice Appalti, come previsto dal comma 10, lett. b) del medesimo articolo;
 9. **Di prendere atto** che, in ottemperanza alle disposizioni dell'Ufficiale Rogante aziendale con nota prot. 8187 del 20.04.2021, entro 5 giorni dalla stipulazione del contratto, l'aggiudicatario si impegna all'assolvimento dell'imposta di bollo di € 16,00, secondo le modalità previste dall'art. 3 del DPR 642/1972, acquisita a cura del RUP della precedente UOC;
 10. **Di conferire immediata esecutività** alla presente determinazione, ai sensi e per gli effetti dell'art. 21-quater L. 241/90, stante la necessità di procedere in tempi rapidi all'incremento della sicurezza della infrastruttura di rete considerato il recente aumento degli attacchi hacker nei confronti degli Enti Pubblici

Visto

Il Dirigente Amministrativo
(*Dr.ssa Antonella Giuliani*)
f.to digitalmente

IL DIRETTORE GENERALE
Dott. Rodolfo Conenna
f.to digitalmente

