



PROVVEDIMENTO

**AFFIDAMENTO DIRETTO
PER L'ACQUISIZIONE DEL SERVIZIO DI SICUREZZA "IN CLOUD"
ANTIMALWARE/BOTNET DENOMINATO "UMBRELLA INSIGHT"
(ES19_028_MEPA)**

PREMESSE

Viste le motivazioni di cui all'Allegato 1 "Motivazioni dell'approvvigionamento", ai sensi del D. Lgs. 50/2016 e s.m.i. (cd. Codice dei Contratti Pubblici), si rende necessario procedere all'acquisizione del servizio di sicurezza "in cloud" antimalware/botnet denominato "Umbrella Insight" dalla società Maticmind S.p.A., che ha presentato la migliore offerta nell'ambito di una preliminare esplorativa di mercato, nei termini di seguito specificati.

PROSPETTO ECONOMICO COMPLESSIVO DELL'APPALTO E IMPORTO DI AGGIUDICAZIONE

Il prospetto economico complessivo degli oneri necessari per il servizio in oggetto, individua le seguenti voci:

A) Importo servizio oggetto d'appalto

A1	Importo a base d'asta per il servizio di sicurezza "in cloud" antimalware/botnet denominato "Umbrella Insight"	Euro 30.000,00
	Totale A	Euro 30.000,00

B) Importo per oneri per la sicurezza da interferenza non soggetti a ribasso

B1	Oneri per la sicurezza da interferenza	Euro 0,00
	Totale B	Euro 0,00

	Totale A + B	Euro 30.000,00
--	---------------------	-----------------------

C) Somme a disposizione dell'Amministrazione

C1	Spese per contributo ANAC (Autorità Nazionale Anticorruzione Vigilanza Contratti Pubblici)	Euro 0,00
	IVA ed eventuali altre imposte:	
C2	IVA (al 22%) di A)	Euro 6.600,00
C3	IVA (al 22%) di B)	Euro 0,00
	Totale C	Euro 6.600,00

	Totale A + B + C	Euro 36.600,00
--	-------------------------	-----------------------

Il valore dell'appalto, ai sensi dell'art. 35 del D. Lgs. 50/2016 e s.m.i., comprensivo degli oneri per la sicurezza da interferenza non soggetti a ribasso pari a Euro zero, è pari a **Euro 30.000,00** (oltre oneri di legge), salvo eventuali

maggiori oneri derivanti da rischi da interferenza come definiti preliminarmente alla stipula del Contratto.

L'importo di aggiudicazione della fornitura in oggetto è pari a **Euro 29.160,00** (oltre oneri di legge e oneri per la sicurezza da interferenza pari a Euro zero).

DURATA

Il servizio di sicurezza "*in cloud*" *antimalware/botnet* denominato "*Umbrella Insight*" dovrà essere garantito per un periodo di 12 mesi a decorrere dalla data di attivazione del servizio medesimo.

TIPOLOGIA DI PROCEDURA E CRITERIO DI AGGIUDICAZIONE

Visti il "Regolamento in materia di appalti pubblici" del CSI-Piemonte e la normativa in materia di appalti pubblici e, in particolare, l'art. 36, comma 2, lett. a) del D. Lgs. 50/2016 e s.m.i., si procede con l'acquisizione tramite affidamento diretto a favore della società Maticmind S.p.A. che ha presentato la migliore offerta nell'ambito di una preliminare esplorativa di mercato, espletata dalla scrivente Amministrazione tra più Operatori Economici (Fornitori consultati: Italtel S.p.A. – Accenture S.p.A. – Maticmind S.p.A. – Sirti S.p.A. – Dimension Data Italia S.p.A. – Vem Sistemi S.p.A. – Lutech S.p.A. – Lantech Longwave S.p.A. – IBM Italia S.p.A. – BT Italia S.p.A. – Alpitel S.p.A. – Axians SAIV S.p.A. – Next-Era Prime S.r.l. – Alascom Services S.r.l.; Fornitore partecipante: Maticmind S.p.A.).

Ai fini della definizione dell'elenco degli operatori economici da consultare, sono state individuate le società partner CISCO di livello GOLD, abilitate al Bando MEPA "Servizi-Prestatori di Servizi al Mercato Elettronico della Pubblica Amministrazione", nell'ambito della categoria "Servizi per l'Information & Communication Technology", ad esclusione del Fornitore uscente.

La documentazione relativa all'esplorativa di mercato citata è agli atti degli uffici competenti del CSI-Piemonte e non materialmente allegata al presente Provvedimento.

Si applica il criterio di aggiudicazione del minor prezzo ai sensi dell'art. 95, comma 4 del D. Lgs. 50/2016 e s.m.i.

L'acquisizione sarà gestita tramite il canale del Mercato Elettronico per la Pubblica Amministrazione (MEPA) (Rif. "Procedura di acquisto tramite Trattativa diretta").

RESPONSABILE UNICO DEL PROCEDIMENTO

Visti i poteri delegati dal Consiglio di Amministrazione al Direttore Generale, il Responsabile Unico del Procedimento (RUP) per la presente procedura, nominato dal Direttore Generale, è Stefano Lista, in qualità di Direttore della Direzione "Infrastrutture" (già Direzione "Gestione Datacenter e Rete") del CSI-Piemonte.

Considerato quanto sopra descritto, il Direttore Acquisti:

- autorizza, ai sensi della normativa vigente in materia, la procedura di affidamento diretto per l'acquisizione del servizio di sicurezza "in cloud" *antimalware/botnet* denominato "Umbrella Insight" dalla società Maticmind S.p.A., per un periodo di 12 mesi a decorrere dalla data di attivazione del servizio medesimo, per un importo pari a **Euro 29.160,00** (oltre oneri di legge), da esperirsi tramite il canale del Mercato Elettronico per la Pubblica Amministrazione (MEPA) (Rif. "Procedura di acquisto tramite Trattativa diretta").

Gli oneri per la sicurezza da interferenza non soggetti a ribasso sono pari a Euro zero (oltre oneri di legge), salvo maggiori oneri derivanti da rischi da interferenza come definiti preliminarmente alla stipula del Contratto;

- approva il prospetto economico complessivo degli oneri necessari per l'appalto in oggetto;
- approva la documentazione della procedura: Capitolato Speciale d'Appalto – Requisiti Tecnici, Condizioni Particolari di Contratto e relativi allegati.

Si allega:

- Motivazioni dell'Approvvigionamento della Direzione Infrastrutture (Allegato 1)
- Capitolato Speciale d'Appalto – Requisiti Tecnici, Condizioni Particolari di Contratto e relativi allegati (Allegato 2)

Torino, 26.07.2019

Il Direttore Acquisti

FIRMATO IN ORIGINALE

(Paola Tavella)

RdA	WBS	Codice Materiale CSI	CUI	Approvvigionamento continuativo
2019000283	N17-1028-PSD3	72510000-3-000	n.a.	SI

MOTIVAZIONI DELL'APPROVVIGIONAMENTO

SERVIZIO DI SICUREZZA "IN CLOUD" ANTI MALWARE/BOTNET DENOMINATO "UMBRELLA INSIGHT"

1. Oggetto

Oggetto dell'affidamento è il servizio di sicurezza "in cloud" anti malware/bonet denominato "Umbrella Insight" della Cisco Systems Inc. per un periodo di 12 mesi a decorrere dall'attivazione del servizio medesimo. Nel dettaglio:

Codice Prodotto	Descrizione
UMB-INSIGHTS-K9	Umbrella Insights per 1500 user
UMB-SUPT-B	Umbrella Insights Support – Basic

2. Motivazione della richiesta e contesto in cui si inserisce l'approvvigionamento

La gestione della sicurezza informatica è tra i principali obiettivi del CSI Piemonte nell'erogazione dei servizi IT agli Enti Consorziati, per cui si pone particolare attenzione al miglioramento costante del livello di sicurezza delle infrastrutture e delle diverse componenti applicative dei servizi IT.

Gli strumenti di governo della sicurezza informatica del Consorzio hanno evidenziato come, nell'ultimo anno, siano aumentati i tentativi d'attacco usando postazioni infette all'interno dell'amministrazione. Ciò si evince in particolar modo dall'indice di "reputation" associato allo spazio di indirizzamento pubblico del CSI Piemonte (tecnicamente conosciuto come "security rating"¹) relativo al diffondersi di infezioni di postazioni afferenti a "botnet"² che potenzialmente trasformano il computer infetto in un soggetto attivo in campagne di attacco verso soggetti esterni all'amministrazione.

¹ Con il termine "Security Rating" si intende la misura espressa da un indice numerico che identifica il posizionamento di un'organizzazione nell'ambito delle prestazioni di sicurezza informatica. L'indice è utilizzato per valutare il rischio informatico dell'organizzazione e per confrontarlo con quello di organizzazioni analoghe. Da gennaio 2017 il CSI ha acquisito tramite Procedura Negoziata un servizio di Security Reputation (Security Scoring) fornito dalla azienda Bitsigh Technologies Inc., leader mondiale nel settore specifico, tramite il rivenditore autorizzato Eurosel Moma S.r.l. (ora Cybersel S.r.l.) che permette di verificare dall'esterno il grado di sicurezza dell'infrastruttura e delle postazioni del CSI Piemonte, basandosi su operazioni di analisi dei dati pubblici di compromissione (appartenenza a botnet, ip black list, report di scansione, etc) ed assegnando una classificazione (Scoring) in base al livello di sicurezza riscontrato.

² Botnet: Una botnet è una rete controllata da un botmaster e composta da dispositivi infettati da malware specializzato, detti bot o zombie.

In particolare si è rilevato come queste infezioni siano per la quasi totalità legate agli utenti dei servizi “free-wi-fi” erogati dal Consorzio.

La continua evoluzione delle minacce portate da malware e *Advanced Persistent Threat* (APT) può essere intercettata analizzando le richieste DNS³ e lavorando su due approcci diversi:

- 1) prevenzione su domini conclamati come malevoli;
- 2) investigazione finalizzata a capire come la registrazione di un nuovo dominio individui l’inizio di una nuova campagna d’infezione.

Nel 2018, anche sulla base di quanto emerso nel corso della POC (Proof of Concept) svolta nel corso del 2017 descritta nel seguito, il CSI-Piemonte ha valutato, in questo scenario, l’adozione di uno strumento del secondo tipo, considerando che l’analisi è rivolta sui soli domini “DNS” e non sul traffico reale generato dai *client*, che richiede normalmente l’adozione di complesse ed onerose architetture hardware “on-premise”.

Il primo servizio di questa tipologia è nato nel 2006 con il nome “OpenDNS” (sia in versione “open” per utenze *consumer*, sia a pagamento per utenze di tipo *enterprise*). Nel corso degli anni la società OpenDNS è diventata *leader* mondiale, potendo contare su oltre 65 milioni di accessi giornalieri e diventando il secondo DNS al mondo dopo quello di Google.

Nel 2015 la società OpenDNS è stata acquisita da Cisco Systems Inc. che, relativamente al servizio di sicurezza sopra citato, ha mantenuto la modalità “open” per le utenze *consumer* e quella a pagamento per le utenze di tipo *enterprise*.

Una POC (*Proof of Concept*) sul prodotto “Cisco Umbrella” (nuova denominazione del prodotto “OpenDNS”) svolta nel corso del 2017, ha evidenziato l’efficacia del prodotto, che ha consentito l’eliminazione della quasi totalità delle infezioni da *botnet* riportando l’indice di *reputation* del CSI-Piemonte a livelli ottimali.

Tali risultati sono stati presentati dal DPO (*Data Protection Officer*) al Comitato di Sicurezza del CSI-Piemonte del 20 settembre 2017, che ha avallato l’adozione del servizio di sicurezza in oggetto.

I punti di forza di questa soluzione sono:

- l’erogazione in modalità “SaaS” senza necessità di HW/SW dedicato, che consente un’attivazione pressoché immediata e trasparente alle tecnologie di rete e sicurezza utilizzate;
- costante aggiornamento in modo dinamico del *database* che contiene l’elenco dei domini malevoli, al momento il più grande e completo *database* esistente.

Poiché la soluzione individuata si basa sul controllo delle richieste DNS, si è evidenziato il vantaggio derivante dall’assenza di installazione di alcun software o hardware e la necessità di configurazioni. Questa peculiarità del servizio consente di non avere “*lock-in*” tecnologici (a differenza di altre soluzioni) in quanto l’eventuale sostituzione del servizio con uno analogo (basato su DNS) non ha costi di *change* significativi ed è indipendente dalla tecnologia utilizzata in CSI per l’erogazione dei servizi Wi-Fi.

³ Domain Name System

Altre soluzioni tecnologiche – sempre di mercato - che offrono servizi comunque analoghi, sono basate sull'utilizzo di piattaforme *hardware* “*on-premise*”. Questo implica da un lato l'adattamento della configurazione di rete Wi-Fi dei clienti ed un “*lock-in*” sulla soluzione del *vendor*. Viceversa, non sono emerse soluzioni percorribili, ovvero tecnicamente idonee e rispondenti alle esigenze qualitative e quantitative proprie del Consorzio, acquisibili in modalità aperta e/o altrimenti disponibili a riuso sulla piattaforma AGID.

A tale proposito, nel corso del 2018, il CSI-Piemonte, al fine di garantire il servizio di sicurezza a protezione di tutti gli accessi Wi-Fi di tipo “*guest*”, ovvero FreeTorinoWiFi, FreePiemonteWiFi ed Area Ospiti ha acquisito – in esito alla consultazione del mercato (Rif. ES18_166_MEPA) - il servizio “*in cloud*” denominato “Umbrella Insight” dalla società Novanext S.r.l. per un importo complessivo pari a Euro 26.790,00 (oltre oneri di legge, inclusi oneri di sicurezza da interferenza pari a Euro 0,00), per un periodo di 12 mesi.

Pertanto, alla luce di quanto sopra esposto, in considerazione dell'esigenza sopra descritta, delle peculiarità del servizio e degli ottimi risultati prodotti nell'ultimo anno di utilizzo, si rende ora necessario procedere con l'acquisizione del servizio in oggetto - denominato “Umbrella Insight” - per un periodo di 12 mesi a decorrere dalla data di attivazione del servizio medesimo, mediante la consultazione del mercato secondo la normativa di riferimento.

3. Spesa prevista

L'importo a base d'asta previsto per l'acquisizione del servizio in oggetto è pari a Euro 30.000,00 (oltre oneri di legge e inclusi oneri per la sicurezza derivanti da interferenza pari a Euro zero).

L'importo a base d'asta è stato determinato sulla base del costo dell'attuale servizio, ed è in linea con i costi sostenuti nell'ambito del precedente approvvigionamento (rif. ES18_166_MEPA).

4. Fonti di finanziamento e Pianificazione aziendale

L'importo di spesa previsto trova copertura nella PTE della Regione Piemonte relativa al “Vulnerability Assessment”.

5. Istruttoria ex Legge 208/2015 e s.m.i.

La Legge 208/2015 del 28 dicembre 2015 e s.m.i. (nota anche come "Legge di Stabilità 2016"), in particolare all'art. 1, commi 512-516 pone in capo alle Pubbliche Amministrazioni ed alle società inserite nel conto economico consolidato della PA (c.d. "elenco ISTAT") l'obbligo di provvedere ai propri approvvigionamenti di beni e servizi informatici e di connettività esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip S.p.A. o dei "Soggetti Aggregatori", ivi comprese le Centrali di Committenza regionali, per i beni e i servizi disponibili presso gli stessi soggetti.

Il CSI-Piemonte, pur non rientrando, alla lettera, nelle categorie sopra citate, ha comunque conformato - in via prudenziale - il proprio iter autorizzativo per gli acquisti IT a quanto disposto dalla normativa sopra richiamata.

Poiché l'appalto in questione si configura come "acquisto IT", si è quindi proceduto alla verifica della sussistenza di eventuali Convenzioni attive, Accordi Quadro e/o strumenti analoghi nei cataloghi di Consip S.p.A., della Centrale di Committenza Regionale (SCR-Piemonte S.p.A.) e del soggetto aggregatore Città Metropolitana di Torino, che potessero soddisfare le esigenze cui l'appalto intende rispondere.

Alla data del 28 giugno 2019, il riscontro è il seguente:

- sui cataloghi di Consip S.p.A., SCR-Piemonte S.p.A. e della Città Metropolitana di Torino non è presente alcuna Convenzione o Accordo Quadro o Avviso avente ad oggetto il servizio oggetto di appalto;
- per quanto concerne il canale Consip del "Mercato Elettronico della Pubblica Amministrazione (MEPA)", dalla consultazione del bando "Servizi-Prestatori di Servizi al Mercato Elettronico della Pubblica Amministrazione", nell'ambito della categoria "Servizi per l'Information Communication Technology" risulta disponibile il prodotto "Servizi di sicurezza informatica".

Configurandosi il presente affidamento come servizio riconducibile al prodotto sopra citato, risulta possibile formalizzare l'affidamento tramite MEPA e pertanto esso rientra nella fattispecie di cui all'art.1, c. 512 della L. 208/2015 e s.m.i.

6. Conformità alle disposizioni ISO 27001:2013

Il presente approvvigionamento non rientra nell'ambito di applicazione delle disposizioni ISO 27001:2013.

7. Conformità alla norma UNI CEI EN ISO 50001:2011

Il presente approvvigionamento, non rientra nell'ambito di applicazione delle disposizioni UNI CEI EN ISO 50001:2011.

8. Conformità alle disposizioni BS OHSAS 18001:2007

Il presente approvvigionamento risulta conforme alle disposizioni BS OHSAS 18001:2007 e non richiede verifica preventiva di conformità da parte del Servizio Prevenzione e Protezione del CSI-Piemonte.

9. Conformità alle disposizioni in materia di protezione dei dati personali

Il presente approvvigionamento non rientra nell'ambito di applicazione delle disposizioni in materia di protezione dei dati personali.

10. Modalità di approvvigionamento

Alla luce di quanto sopra esposto, visti il "Regolamento in materia di approvvigionamenti" del CSI Piemonte e la normativa in materia di appalti pubblici, e in particolare l'art. 36, comma 2, lett. a) del D. Lgs. 50/2016 e s.m.i., si richiede di procedere all'approvvigionamento in oggetto applicando il criterio di aggiudicazione del minor prezzo ai sensi dell'art. 95, comma 4 del D. Lgs. n. 50/2016 e s.m.i., sulla base della comparazione di preventivi.

Torino, 28 giugno 2019

Il RUP
Direzione Infrastrutture
(Stefano Lista)

FIRMATO IN ORIGINALE

Responsabile Acquisti Beni e Servizi ICT
(Barbara Gallizia)

FIRMATO IN ORIGINALE

