CONSORZIO LaMMA

RELAZIONE TECNICA

RELATIVA ALL'ACQUISIZIONE, INSTALLAZIONE, CONFIGURAZIONE E MIGRAZIONE DI UN CLUSTER FIREWALL COMPRENSIVO DI CORSI DI TRAINING E DEL SERVIZIO MANAGED DETECTION AND RESPONSE COMPLETE E RELATIVI SUPPORTI PER LA PROTEZIONE DI RETE DI TUTTA LA INFRASTRUTTURA DATI E UTENTI NELL'AMBITO DELLE ATTIVITÀ ORDINARIE E STRAORDINARIE DEL CONSORZIO

Consorzio LaMMA – Laboratorio di Monitoraggio e Modellistica Ambientale per lo sviluppo sostenibile
Area della Ricerca CNR – Edificio D - Via Madonna del Piano 10, 50019 Sesto Fiorentino FI
Tel. 055 448301 fax: 055 444083 info@lamma.rete.toscana.it www.lamma.rete.toscana.it

CONSORZIO LaMMA

Premessa

Nel Data Center del Consorzio LaMMA è presente da aprile 2019 un cluster Firewall configurato in alta affidabilità composto da due sistemi appliance Sophos XG 330 che gestiscono la totalità del traffico di rete e la sicurezza dell'Ente.

Tale gestione comprende la protezione completa sia dei sistemi esposti su Internet (es. server web e di posta elettronica, traffico internet generato dalla totalità dei client di rete) che delle postazioni utente e di elaborazione dati oltre all'accesso WiFi della sede di Firenze, Livorno e Grosseto.

La protezione è attuata mediante l'aggiornamento di questi sistemi in tempo reale con la casa madre e l'elaborazione approfondita dei pacchetti di traffico internet per la presenza di virus o programmi malevoli (IPS, Application control, etc).

Una delle caratteristiche più interessanti e avanzate di tale sistema è l'integrazione con i client Antivirus di ogni singolo utente all'interno della rete del LaMMA. E' infatti in uso per tutte le postazioni utente fisse e anche mobili l'antivirus centralizzato Sophos Central che comunica con il Firewall Sophos XG in modo proattivo, consentendo di individuare ed eventualmente bloccare (Security Hearbeat) granularmente a livello di traffico di rete il singolo computer, la postazione o il server infettato o compromesso o applicazioni specifiche e dannose.

Questa tipologia di implementazione di sicurezza risulta molto efficace nel combattere in modo rapido le minacce più avanzate ed in continua evoluzione e si è rivelata molto affidabile e funzionale.

Il supporto attuale scadrà il prossimo 15 settembre 2024 ed è necessario procedere all'acquisizione di un nuovo sistema di superiori prestazioni in ragione del notevole aumento di velocità del collegamento Internet, passato da 1Gbit a 10Gigabit/s con conseguente potenziale aumento di dieci volte delle performance richieste. L'attuale Firewall non è in grado di supportare tale velocità.

Sono inoltre presenti alcune problematiche di sicurezza e di rete:

- Nelle stazioni remote Radar presso Isola d'Elba e Monte Verrugoli non sono presenti dispositivi di collegamento di sicurezza adeguati. Essi risultano obsoleti e non più compatibili con i nostri standard di sicurezza della connettività con la sede centrale di Firenze.
- La copertura Wireless integrata attiva nelle tre sedi dell'Ente, non risulta più sufficiente per coprire tutti i dispositivi degli utenti in modo adeguato nei locali presenti.
- Con l'aumento dei dispositivi mobili e delle minacce di sicurezza come Ramsonware e Data Theft, malware, sono aumentati i rischi degli attacchi e la mole di lavoro necessaria a monitorare costantemente eventuali attacchi per evitare che vengano propagati all'interno dell'Ente.

Per poter risolvere queste problematiche e rendere omogeneo il livello di sicurezza di tutta l'infrastruttura è necessario acquisire per ogni sede prevista un nuovo sistema Firewall con relativi access point.

E' inoltre necessario acquisire il servizio Sophos MDR Complete (Sophos Managed Detection and Response) poter avere un supporto nel monitoraggio degli eventi di sicurezza H24/7.

Questo servizio è fondamentale nel caso di incidenti e per avere una compliance secondo i moderni standard di sicurezza, anche rispetto a polizze assicurative CyberRisk. Inoltre nel 2024 il Consorzio LaMMA trasferirà una parte delle proprie risorse al TIX di Regione Toscana, ed avere un sistema integrato di sicurezza monitorato remoto diventa essenziale per evitare eventuali data breach.

Sophos MDR Complete offre un monitoraggio continuo 24/7 di endpoint, rete e cloud, utilizzando intelligenza artificiale e machine learning per rilevare minacce sofisticate. Questo servizio permette di ottenere direttamente da Sophos, una risposta immediata e dettagliata agli incidenti, implementando strategie di risposta personalizzate. Il servizio automatizza le risposte e orchestra vari strumenti di sicurezza per migliorare l'efficienza operativa. Sono disponibili sempre le analisi post-incidente con i relativi dettagli accessibili tramite dashboard.

Oltre alla consulenza strategica, questo servizio aiuta a migliorare la sicurezza aziendale implementando best practice sempre concordate in coordinamento con il reparto IT. La fornitura è realizzata sia nell'ambito delle attività ordinarie che nell'ambito delle attività straordinarie relative ai progetti SCORE (rif. Attività 15 PDA) SINTETIC (rif. Attività 40 PDA) e DRT 11954/13 (rif. Attività 41 PDA).

Si intende acquisire il sistema di marchio Sophos, in quanto l'integrazione come sopra dettagliato, tra il sistema firewall Sophos XG e la parte antivirus Sophos Central presente sulle postazioni di lavoro e sui server critici di rete Windows, nonché il servizio MDR rende tecnicamente ed economicamente conveniente rimanere su questa tipologia e marca di prodotto.

Un eventuale cambiamento comporterebbe mesi di lavoro per poter riprogettare e re-installare tutti i software, nuovi punti di accesso Wireless e nuove configurazioni di sicurezza, con un impatto notevole per l'operatività dell'Ente. La perdita economica si realizzerebbe inoltre a causa della dismissione degli apparati wireless ancora funzionanti. Infine non potremmo attivare il servizio MDR che risulta essere fondamentale per poter supportare il reparto IT alle minacce di sicurezza sempre più complesse da affrontare.

Dettaglio tecnico

Sono state individuate le caratteristiche principali della fornitura e dei servizi che devono presentare le seguenti caratteristiche:

QTA'	Descrizione
1	XGS 4300 with Xstream Protection, 3-year - EU power cord
1	XGS 4300 with Xstream Protection, 3-year - EU power cord
1	XGS 4300 Enhanced to Enhanced Plus Support Upgrade - 39 MOS - GOV
4	10GbE Fiber Transceiver Short Range (10 Base-SR)
2	Generic Compatible SFP+ 10GBASE-T Copper 30m RJ-45 Transceiver Module
103	Central Email Advanced - 100-199 users - 36 MOS - Renewal
10	Sophos AP6 420 Access Point (EUK) plain, no power adapter/PoE Injector
10	Access Points Support for AP6 420 - 36 MOS
103	Central Intercept X Advanced with XDR - 100-199 users - 36 MOS - Renewal - GOV
14	Central Intercept X Advanced for Server - 10-24 servers - 36 MOS - Renewal - GOV
103	Managed Detection and Response Complete - 100-199 users - 36 MOS - Renewal - GOV
14	Managed Detection and Response Complete Server - 10-24 servers - 36 MOS - Renewal - GOV

117	Central Network Detection and Response - 100-199 users - 36 MOS - GOV
2	XGS 116 with Xstream Protection, 3-years - EU power cord
2	XGS 116w with Standard Protection, 3-years - EU power cord
4	3G/4G module Americas/EMEA
2	Certified Administrator Classroom Training - UTM o equivalente
2	Certified Administrator Classroom Training - Central o equivalente

Oltre alla consegna è richiesta l'installazione, la configurazione da remoto e migrazione dei sistemi firewall acquistati per le sedi del Consorzio di Firenze, Livorno e Grosseto da parte di personale specializzato e certificato Sophos da eseguirsi secondo le seguenti modalità:

- Revisione Central, applicazione nuova licenza MDR, centralizzazione access point su Central, revisione policy ed esclusioni, Migrazione configurazioni sui nuovi Firewall.
- Revisione policy Central Email
- Deploy sonda NDR su infrastruttura virtuale
- Check corretto funzionamento e approfondimento eventuali allarmi della sonda
- Redazione e consegna documentazione della configurazione eseguita.

L'Operatore è tenuto, su richiesta dell'Ente, attivare i corsi per n. 2 unità di personale inerenti il training finalizzati all'ottenimento della relativa certificazione.

Non sono consentite interruzioni riguardo alle prestazioni nel passaggio dal sistema attuale a quello oggetto dell'affidamento di cui alla presente Relazione.

Spetta all'Operatore intervenire per il ripristino di eventuali malfunzionamento.

Di seguito i dettagli delle licenze e degli apparati in uso:

Dati dei seriali dell'attuale Sistema Firewall:

- C330ACM49GX3C92
- C330ACRPGYX9Y65

Dati dell'attuale licenza Sophos Central:

LICENZE	TIPO	LIMITE	SCADENZA	N. DI LICENZA
Phish Threat	FULL	100	Nov 22, 2024	C549347844
Intercept X Advanced with	FULL	103	Set 15, 2024	L73728-84385

LICENZE	TIPO	LIMITE	SCADENZA	N. DI LICENZA
XDR				
Intercept X Advanced for Server	FULL	4	Set 15, 2024	L0007761875
Email Advanced	FULL	100	Nov 22, 2024	L0011527292

Procedura di gara

Non sono attualmente in corso presso la società concessionaria del Ministero dell'Economia e delle Finanze per i servizi informativi pubblici (Consip S.p.a.), convenzioni per la prestazione che si intende acquisire alle quali poter eventualmente aderire.

Si propone, quindi, di procedere con un affidamento diretto ai sensi dell'art. 50, comma 1, lett. b), D. Lgs 31 marzo 2023 n. 36 attraverso una trattativa diretta su START in favore dell'azienda sotto riportata che ha garantito il supporto all'attivazione della fornitura mantenendo la continuità dei servizi critici del Consorzio alla luce delle scadenze delle licenze:

Rag. Sociale: WETECH'S S.P.A.

Partita IVA: 05174160480 - Codice Fiscale: 05174160480

Indirizzo: VIA FRATELLI ALINARI 76/80/82 - 52025 - MONTEVARCHI (AR)

Rea: 134136

PEC: wetechs@legalmail.it

Il suddetto Operatore ha dichiarato di aver svolto nel triennio precedente 2021-2023 attività analoghe per importi superiori al servizio di cui alla presente relazione.

Tempi di consegna e di attivazione ed esecuzione del servizio

La consegna dovrà avvenire presso la sede legale dell'Ente entro 30 giorni naturali e consecutivi dalla stipula del contratto e, comunque, non oltre la data di scadenza dell'attuale servizio Sophos:

Consorzio LaMMA

Via Madonna del Piano, 10

50019 Sesto Fiorentino

FIRENZE

L'installazione, configurazione e migrazione dei sistemi dovranno essere avviati entro 15 gg. lavorativi dalla consegna o e completati entro i successivi 15 gg solari e, comunque, non oltre la data di

scadenza dell'attuale servizio Sophos. Non ci dovranno essere interruzioni del servizio di sicurezza. Dovranno essere effettuate almeno 3 giornate di supporto sistemistico professionale da remoto.

Supporto triennale: dovrà essere garantito con decorrenza dalla scadenza dell'attuale contratto.

Corsi inerenti il training: dovranno essere tenuti su richiesta dell'Amministrazione.

In caso di malfunzionamento dovranno essere effettuati gli interventi per il ripristino dei sistemi:

- per il firewall XGS 4300 e gli apparati collegati il supporto richiesto è h24/7 con primo contatto entro 1 ora in caso di guasto di livello gravità massimo (critico) ed anticipo della parte guasta in caso di malfunzionamento hardware,
- per i firewall XGS 116 è richiesto una tempistica di risposta h24/7 entro 4 ore in caso di guasto di livello gravità massimo critico) ed anticipo della parte guasta in caso di malfunzionamento hardware,
- per Sophos Central è richiesto il contatto entro 4 ore in caso di guasto di livello gravità massima (critico).

Stima dei Costi

Il costo complessivo stimato è di **105.989,08 € oltre IVA** secondo il dettaglio della tabella seguente come comunicato da Sophos Italia e trova copertura nel DRT-11954-23 e nei progetti europei SCORE e SINTETIC.

QTY	Descrizione	HARDWARE e Licenze	SERVIZI
1	XGS 4300 with Xstream Protection, 3-year - EU power cord	€ 26.018,82	
1	XGS 4300 with Xstream Protection, 3-year - EU power cord	€ 7.751,76	
1	XGS 4300 Enhanced to Enhanced Plus Support Upgrade - 39 MOS - GOV		€ 2.208,88
4	10GbE Fiber Transceiver Short Range (10 Base-SR)	€ 2.082,70	
2	Generic Compatible SFP+ 10GBASE-T Copper 30m RJ-45 Transceiver Module	€ 358,80	
103	Central Email Advanced - 100-199 users - 36 MOS - Renewal	€ 5.428,10	
10	Sophos AP6 420 Access Point (EUK) plain, no power adapter/PoE Injector	€ 1.316,25	
10	Access Points Support for AP6 420 - 36 MOS		€ 218,75
103	Central Intercept X Advanced with XDR - 100-199 users - 36 MOS - Renewal - GOV	€ 16.504,46	
14	Central Intercept X Advanced for Server - 10-24 servers - 36	€ 2.878,58	

	MOS - Renewal - GOV		
103	Managed Detection and Response Complete - 100-199 users - 36 MOS - Renewal - GOV		€ 16.842,56
14	Managed Detection and Response Complete Server - 10-24 servers - 36 MOS - Renewal - GOV		€ 4.124,12
117	Central Network Detection and Response - 100-199 users - 60 MOS - GOV		€ 10.744,99
2	XGS 116 with Xstream Protection, 3-years - EU power cord	€ 2.789,41	
2	XGS 116w with Standard Protection, 3-years - EU power cord	€ 2.480,35	
4	3G/4G module Americas/EMEA	€ 1.540,55	
	TOTALE	**€ 69.149,78**	**€ 34.139,30**

Il costo della Installazione è di circa **€ 2.700 oltre IVA.**.

Sesto Fiorentino, 20 Giugno 2024

Il referente Tecnico

Simone Montagnani

Consorzio LaMMA – Laboratorio di Monitoraggio e Modellistica Ambientale per lo sviluppo sostenibile
Area della Ricerca CNR – Edificio D - Via Madonna del Piano 10, 50019 Sesto Fiorentino FI
Tel. 055 448301 fax: 055 444083 info@lamma.rete.toscana.it www.lamma.rete.toscana.it