SEGRETARIATO GENERALE della GIUSTIZIA AMMINISTRATIVA

Servizio per l'Informatica

Ufficio CED, Rete, Sicurezza e Dotazioni Informatiche

Capitolato tecnico

Strumenti McAfee

Licenze, servizi di manutenzione e supporto specialistico

Redatto da: Dott. Michele Tangi

Sommario

1. SITUAZIONE ATTUALE

Questa Amministrazione utilizza apparati e sistemi di sicurezza prodotti dalla società McAfee a partire dal 2009. Le tecnologie McAfee, integrate nei sistemi della G.A., sono state implementate sia a livello centralizzato, mediante l'uso di sistemi di prevenzione delle intrusioni e filtraggio del traffico web, sia a livello periferico con la diffusione di strumenti di antivirus e antimalware.

In particolare, *i prodotti oggi in possesso dell'Amministrazione* sono di seguito elencati:

1. **Suite protezione end point**
   - Console centralizzata ePO, per la gestione della suite di sicurezza del parco macchine;
   - Modulo Antivirus;
   - Host intrusion prevention;
   - MOVE, antivirus ottimizzazione per le macchine virtuali.
2. **Protezione navigazione web**
   - Webgateway implementato come proxy (su macchina virtuale) per il filtraggio delle URL e la protezione antimalware durante la navigazione web delle postazioni di lavoro.
3. **Network Intrusion Protection System**
   - Network Manager, per la gestione centralizzata del sistema di Intrusion Prevention;
   - Sensori di rete per il rilevamento di attacchi di rete e sistemi antibotnet.
4. **Vulnerability Manager**
   - Appliance per la verifica e la reportistica automatica delle vulnerabilità dei sistemi target.
5. **ATD, Advanced Threat Defense**
   - Appliance hardware sandbox che tramite macchine virtuali permette la individuazione e protezione da malware zero day utilizzando.
6. **TIE, Threat Intelligence Exchange**
   - Modulo software che permette lo scambio di informazioni tra le componenti di sicurezza presenti aumentando sensibilmente il livello di protezione su vettori di infezioni diversi (rete, web, chiavette usb, ecc.).
7. **SIEM e modulo DB**
   - Componente hardware che permette la storicizzazione e la correlazione dei log dei vari sistemi IT presenti in rete e, tramite il modulo DB, consente la storicizzazione delle informazioni di accesso ai database.

Per quanto riguarda *le componenti per la protezione end-point installate presso il Consiglio di Stato*, si specificano alcuni dettagli relativi a talune funzionalità core per ciascuna componente:

A. **ePolicy Orchestrator 5.1**: Console di Management centralizzata in grado di gestire la suite dei prodotti McAfee e che consente un controllo della conformità delle politiche di sicurezza e la protezione dei nodi dell'intera infrastruttura.
B. **Virus Scan Enterprise 8.8**: è un'applicazione che, tramite una tecnologia antivirus avanzata, consente di proteggere i server e le workstation dalle minacce più comuni derivanti da e-mail, connessioni web, accesso ai siti FTP, ecc. Essa integra anche il modulo software aggiuntivo (AntiSpyware Enterprise) che consente di identificare spyware e programmi potenzialmente dannosi con la stessa tecnologia di scansione dell'applicazione antivirus Database: consiste nello storage centrale utilizzato dall'applicazione ePolicy Orchestrator per memorizzare tutti i dati generati ed utilizzati.
C. **ePolicy Orchestrator Agent**: è un modulo software che consente lo scambio di informazioni tra il sistema gestito e l'ePolicy Orchestrator Server. L'agent è il mezzo con cui ogni nodo prende gli aggiornamenti, le politiche ed i task implementati sul server.
D. **Host Intrusion Prevention System**: con questa applicazione viene garantita la protezione dell'infrastruttura informatica dalle minacce complesse di sicurezza, mediante un livello di protezione basato su firme ed incorpora, inoltre, uno statefull firewall. Questo componente software ha pertanto il compito di proteggere l'Amministrazione dalle minacce note, inclusi gli attacchi zero-day. Gli aggiornamenti automatici delle firme consentono anche di bloccare l'esecuzione delle minacce emergenti compresi gli attacchi di buffer overflow.
E. **McAfee Management for Optimized Virtual Environments (MOVE)**: è una soluzione ottimizzata per la protezione antivirus avanzata nei desktop e nei server virtualizzati, installata sui sistemi dell'Amministrazione. Essa, utilizzabile con tutti i principali hypervisor, permette di non avere agent installati sui sistemi virtuali utilizzando VMware NSX e VMware vCloud Networking and Security.

2. OGGETTO DELLA FORNITURA

Con la finalità di salvaguardare l'investimento tecnologico effettuato negli ultimi anni e dovendo assicurare il necessario aggiornamento e supporto tecnologico dei sistemi di sicurezza in uso, si rende indispensabile effettuare un'acquisizione che assicuri servizi "***Support Renewal***" e "***Professional Services***".

2.1 SUPPORT RENEWAL

Questo tipo di servizi è rappresentato dal rinnovo delle licenze software e dei canoni di manutenzione per gli apparati McAfee già in uso; nella tabella a seguire si riportano i codici e le descrizioni:

Nr.	Codice	Descrizione
1	IYVF35KADM	MFE Network Sec 3050 Sensor FO 1YrBZ+RMA
2	IYVM35KADM	MFE Network Sec 3050 Sensor 1Yr BZ+RMA
3	CTPYFM-AA	MFE Complete EP Threat Protect 1YrBZ[P+]
4	IMTYCM-AD	MFE Network Sec Starter Mngr 1Yr BZ
5	MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrBZ
6	WAMYCM-AA	MFE Web Anti-Malware 1Yr BZ
7	WSGYCM-AA	MFE Web Security 1Yr BZ
8	MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrBZ
9	TIEYFM-AA	MFE Threat Intel Exchange 1Yr BZ [P+]
10	RBX850CG1	MFE NetSec XFPGbic 850nm 8K/6050 1Yr RMA
11	ETM4600ELMNBD	MFE Ent Sec Mgr Log Mgr 4600 1YrBZ+NBD
12	ATD3000NBD	MFE Adv Threat Def 3000 Stand 1yrNBD
13	DSM2600NBD	MFE DB EvntMonitorforSIEM26001Yr BZ+NBD

2.2 PROFESSIONAL SERVICES CONSULTANT

Questo tipo di servizi è rappresentato dal supporto specialistico a consumo quantificabile in 40 giorni uomo; nella tabella a seguire si riporta il codice e la descrizione:

Nr.	Codice	Descrizione
14	MD-CONSULT-DY-Z1	Professional Services Consultant

Tali servizi riguarderanno, in particolar modo, il McAfee TIE, il SIEM, il MOVE, l'aggiornamento dei sistemi ePO, Webgateway e Network IPS e la formazione del personale del Consiglio di Stato; nei prossimi paragrafi si riporta il dettaglio informativo e la stima delle giornate uomo afferenti ai "*Professional Services Consultant*".

2.2.1 McAfee ENS 10.5 e TIE

Il McAfee TIE si compone di una piattaforma Server e un plug in sui client. Nella prevista migrazione dei client antivirus dalla attuale versione 8.8 alla nuova versione 10.5, sarà necessario supportare il Consiglio di Stato nella migrazione sia della piattaforma end point e sia del plug in TIE, in modo da connettere i client con l'ATD. La piattaforma End Point 10.5 fornisce notevoli miglioramenti in termini di sicurezza e performance. Le attività previste sono:

Attività prevista	Numero gg. stimati
Aggiornamento console ePO per caricare i nuovi software end point 10.5 e preparare le relative policy.	2
Progetto pilota per ENS 10.5, su parco macchine limitato. Verifica disinstallazione versione virus scan 8.8 e installazione della nuova versione end point 10.5.	3
Progetto pilota per plug in TIE (Moduli ATP).	2
Tuning policy.	1
Supporto al deploy di end point 10.5 e TIE sui sistemi del Consiglio di Stato.	2
Totale	**10**

2.2.2 SIEM e modulo DB

Il SIEM prevede la raccolta dei log di tutti i sistemi server e i sistemi critici, sia in ottemperanza alla legge italiana per la raccolta dei log di accesso degli amministratori di sistema, sia per avere una tracciatura degli accessi effettuati sui sistemi, in modo da verificare eventuali anomalie. Inoltre, in congiunzione con il SIEM, il modulo DB è in grado di raccogliere gli eventi di accesso sui sistemi DB.

Le attività previste per il SIEM e il modulo DB sono:

Attività prevista	Numero gg. stimati
Configurazione iniziale SIEM	1
Predisposizioni policy di ricezione eventi dei vari sistemi datasource.	1
Predisposizione policy di correlazione eventi	1
Aggancio dei primi datasource per diverse fasce di sistema operativo e applicazioni (Sistemi Windows, Web server ecc.).	2
Configurazione iniziale modulo DB e aggancio alla rete (modalità span port).	1
Configurazione policy per raccolta connessioni sui sistemi DB	1
Inizio raccolta eventi sui DB	1
Rilascio reportistica iniziale del sistema SIEM	1
Totale	**9**

2.2.3 Sistema MOVE

Durante il 2017 è stata rilasciata la nuova versione della piattaforma MOVE, sistema antivirus ottimizzato per gli ambienti virtuali. La nuova versione 4,6 introduce molte nuove features tra cui la possibilità di bilanciare il carico tra gli off line scan server in modo automatico, la possibilità di mandare in time-out la scansione in caso di problemi o rallentamento del sistema target o server. Possibilità di fare esclusioni sui processi (MOVE multiplatform).

Le attività previste per questa attività di aggiornamento sono:

Attività prevista	Numero gg. stimati
Predisposizione di ePO per l'aggiornamento software di MOVE	0,5
Predisposizioni policy per la nuova versione MOVE	0,5
Aggiornamento sistema MOVE e dei Scan server distribuiti sui vari sistemi hypervisor VMware presenti in CdS	2
Tuning del sistema	2
Totale	**5**

2.2.4 Mantenimento e Aggiornamento dei Sistemi

Per l'aggiornamento dei sistemi ePO, Web Gateway e Network IPS normalmente si prevedono circa 6 giorni l'anno.

Attività prevista	Numero gg. stimati
Aggiornamento dei Sistemi ePO, Web Gateway e Network IPS	5
Totale	**5**

2.2.5 Training per i Sistemi in uso

Si stimano le seguenti giornate di formazione da erogare al personale del Consiglio di Stato:

Attività prevista	Numero gg. stimati
Training per il Sistema ***Network Intrusion Detection***	2
Training per il Sistema ***ePO*** e il sistema ***ENS 10.5***	2
Training per il Sistema ***ATD*** e il Sistema ***TIE***	2
Training per il Sistema ***SIEM*** e il Sistema ***DB***	3
Training per il Sistema ***Webgateway***	2
Totale	**11**

3. RIEPILOGO DELLA FORNITURA

Nella tabella a seguire, si fornisce il dettaglio riepilogativo della fornitura, con l'indicazione del numero progressivo, del codice prodotto sul Mercato elettronico, della descrizione del prodotto, delle quantità, della data inizio e della data fine, della durata in mesi.

Nr.	Prodotto Codice	Prodotto Descrizione	Tipo Programma	Quantità (Nodi)	Data Inizio	Data Fine	Durata Mesi
1	IYVF35KADM	MFE Network Sec 3050 Sensor FO 1YrBZ+RMA	Support Renewal	1	12/1/2017	11/30/2018	12
2	IYVM35KADM	MFE Network Sec 3050 Sensor 1Yr BZ+RMA	Support Renewal	1	12/1/2017	11/30/2018	12
3	CTPYFM-AA	MFE Complete EP Threat Protect 1YrBZ[P+]	Support Renewal	2200	12/1/2017	11/30/2018	12
4	IMTYCM-AD	MFE Network Sec Starter Mngr 1Yr BZ	Support Renewal	1	12/1/2017	11/30/2018	12
5	MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrBZ	Support Renewal	50	12/1/2017	11/30/2018	12
6	WAMYCM-AA	MFE Web Anti-Malware 1Yr BZ	Support Renewal	2200	12/1/2017	11/30/2018	12
7	WSGYCM-AA	MFE Web Security 1Yr BZ	Support Renewal	2200	12/1/2017	11/30/2018	12
8	MOVYCM-AT	MFE MOVE AV for Virtual Servers OS 1YrBZ	Support Renewal	70	12/17/2017	11/30/2018	11
9	TIEYFM-AA	MFE Threat Intel Exchange 1Yr BZ [P+]	Support Renewal	2200	12/22/2017	11/30/2018	11
10	RBX850CG1	MFE NetSec XFPGbic 850nm 8K/6050 1Yr RMA	Support Renewal	2	12/29/2017	11/30/2018	11
11	ETM4600ELMNBD	MFE Ent Sec Mgr Log Mgr 4600 1YrBZ+NBD	Support Renewal	1	1/9/2018	11/30/2018	11
12	ATD3000NBD	MFE Adv Threat Def 3000 Stand 1yrNBD	Support Renewal	1	1/9/2018	11/30/2018	11
13	DSM2600NBD	MFE DB EvntMonitorforSIEM26001Yr BZ+NBD	Support Renewal	1	1/9/2018	11/30/2018	11
14	**MD-CONSULT-DY-Z1**	**Professional Services Consultant**	**Professional Services**	**40**	**N/A**	**N/A**	**12**

La somma dei prezzi di listino ufficiale McAfee, escluse le giornate di "Professional Services Consultant" è pari a euro 106.893,14 oltre IVA.

Il costo di listino di una giornata di Professional Services Consultant è pari a euro 1.260,00 oltre IVA, per un totale (40 gg/uomo) di euro 50.400,00 oltre IVA.

La base d'asta, dunque, è pari a euro 157.293,14 oltre IVA.

Devono ritenersi comprese nel costo della fornitura le licenze d'uso dei prodotti e il relativo servizio di manutenzione. Il servizio di manutenzione delle licenze software dovrà comprendere tutte quelle attività necessarie per mantenere continuamente aggiornati i prodotti con le versioni rilasciate dalla casi produttrici.

Il fornitore dovrà mettere a disposizione dell'amministrazione un numero unico per la ricezione delle chiamate.

4. VERIFICHE DI CONFORMITÀ

A seguito di comunicazione da parte del Fornitore, e comunque entro e non oltre 60 giorni dalla data di stipula del contratto, l'Amministrazione procederà alla verifica di conformità della fornitura, che si concluderà con la redazione di apposito certificato di conformità. Le operazioni di verifica di conformità si svolgeranno in due fasi; la prima di tipo *Inventariale* e la seconda di tipo *Funzionale*.

Durante la **Verifica Inventariale**, il Fornitore dovrà presentare ogni documentazione necessaria ad attestare l'effettiva consistenza della fornitura, sia in termini di licenze che di manutenzione. La documentazione, che dovrà comprendere i codici dei prodotti forniti dalle case produttrici, sarà sottoposta ad approvazione da parte dell'Amministrazione.

Durante la **Verifica Funzionale**, l'Amministrazione si riserva la facoltà di effettuare ulteriori motivate verifiche che ritenga opportuno, mirate ad accertare l'effettiva consistenza delle licenze software dei prodotti; in tal caso sarà possibile concordare un nuovo piano per terminare la verifica di conformità complessiva.

Il Fornitore deve garantire tutta l'assistenza necessaria e mettere a disposizione dell'Amministrazione tutte le apparecchiature e i mezzi essenziali per l'effettuazione delle verifiche.

5. RESPONSABILE DEL SERVIZIO

Al fine di consentire una ordinata e regolare esecuzione contrattuale, all'atto della stipula del contratto di fornitura, il fornitore dovrà indicare un responsabile del servizio, eventualmente coincidente con il soggetto firmatario del contratto, che funga da interfaccia con l'Amministrazione per le comunicazioni relative ad aspetti logistici ed amministrativi, e più in generale che possa rappresentare il Fornitore.

Le comunicazioni, gli eventuali disservizi e/o inadempienze, comunicate al responsabile del servizio si intendono come direttamente presentate al Fornitore.

6. LIVELLI DI SERVIZIO E PENALI

L'impresa è obbligata in caso di malfunzionamento dei sistemi di sicurezza forniti, vale a dire in caso di qualsiasi anomalia funzionale che, anche indirettamente, provochi l'interruzione o la non completa disponibilità del servizio all'utenza, a ripristinare la piena funzionalità del sistema.

Tale servizio di ripristino deve essere garantito tutti i giorni, compresi i festivi, dalle ore 8.00 alle ore 19.00, per qualunque tipo di problema, con i seguenti livelli di servizio:

LIVELLO DI SERVIZIO	CASO DI APPLICAZIONE
SLA.1	Presa in carico del problema entro **2 ore dalla chiamata**.
SLA.2	Intervento in loco entro **4 ore dalla chiamata**.

Il mancato rispetto dei termini previsti per gli **SLA** comporterà l'applicazione delle seguenti penalità:

MANCATO RISPETTO TERMINI PREVISTI	LIVELLO DI SERVIZIO	PENALE
PE.1	**SLA.1**	Prevedere una penale pari al **0,15 per mille** dell'importo netto contrattuale per ogni ora solare di ritardo.
PE.2	**SLA.2**	Prevedere una penale pari al **0,10 per mille** dell'importo netto contrattuale per ogni ora solare di ritardo.

DE ROGATIS DANILO
11.12.2017 11:39:05 UTC