AREA SISTEMI E SERVIZI INFORMATICI

RDO 2384571 CIG 8026696F11

Migrazione del sistema centralizzato di protezione dell'endpoint da on-premise a cloud (Sophos Central) e fornitura licenze Sophos Intercept X

Capitolato tecnico

ALMA MATER STUDIORUM - UNIVERSITÀ DI BOLOGNA

VIALE FILOPANTI 3 - 40126 BOLOGNA - ITALIA - TEL. +39 051 2095900 - FAX +39 051 2095919

Sommario

Premessa

Il presente capitolato disciplina gli aspetti tecnici della fornitura, per l'Area Sistemi e Servizi Informatici dell'Università di Bologna, del processo di migrazione dell'infrastruttura del sistema di protezione dell'endpoint e dei servizi a questa connessi, da on-premise alla soluzione Cloud. In ottemperanza con quanto previsto dalle misure minime di sicurezza ICT emanate da AgID, l'attività prevede anche l'innalzamento del livello di sicurezza tramite fornitura di specifico modulo, integrabile nel sistema in uso, per la protezione contro le infezioni di ransomware e più in generale contro gli attacchi zero-day. Inoltre dato che le licenze attuali scadranno il 17 maggio 2021, nell'offerta si chiede di acquisire il diritto all'utilizzo delle attuali 10.000 licenze di Sophos Endpoint Protection Advanced che diventeranno Sophos Central Endpoint Advanced e delle nuove 5.000 licenze di Sophos Intercept X.

Oggetto della fornitura

La gara ha per oggetto la fornitura di un adeguato numero di giorni (almeno 5) di **supporto specialistico** alla migrazione da Endpoint Protection advanced a Central Endpoint Advanced degli asset informatici gestiti tramite console dell'Università di Bologna, la fornitura di Sophos Intercept X per **5.000 licenze** e durata fino al **31 dicembre 2021**, la fornitura di Sophos Server Advanced per **10 licenze** e durata fino al **31 dicembre 2021**, l'estensione della scadenza delle attuali **10.000 licenze** di Sophos Endpoint Protection al **31 dicembre 2021**, il **servizio di Technical Account Manager (TAM) fino al 31 dicembre 2021** e uno specifico **training per due persone** sull'utilizzo della nuova console di gestione.

L'iniziativa che prevede la migrazione della console di gestione consta dei seguenti step:

- Attivazione Sophos Central – console cloud
- Attivazione Enterprise Dashboard per la gestione multi tenant
- Migrazione policy on-premise -> cloud
- Setup Server di Cache per la gestione degli aggiornamenti e per il setup iniziale
- Setup Active Directory Sync
- Test migrazione manuale
- Pilota migrazione di un set di computer
- Training console cloud

ed è richiesto il supporto specialistico del fornitore, sia in on-site che da remoto.

La fornitura comprenderà la soluzione Sophos per proteggere gli endpoint dalle seguenti tecniche di attacco (exploit):

- Enforce Data Execution Prevention
- Mandatory Address Space Layout Randomization
- Bottom-up ASLR
- Null Page (Null Deference Protection)
- Heap Spray Allocation
- Dynamic Heap Spray
- Stack Pivot
- Stack Exec (MemProt)
- Stack-based ROP Mitigations (Caller)

- Branch-based ROP Mitigations (Hardware Assisted)
- Structured Exception Handler Overwrite (SEHOP)
- Import Address Table Filtering (IAF)
- Load Library
- Reflective DLL Injection
- Shellcode
- VBScript God Mode
- Wow64
- Syscall
- Hollow Process
- DLL Hijacking
- Squiblydoo Applocker Bypass
- APC Protection (Double Pulsar / AtomBombing)
- Process Privilege Escalation

La soluzione deve avere le seguenti funzionalità di protezione:

- Protezione del dumping delle credenziali dal “credentials store” di Windows sul disco, dai registri, dalla memoria. Protezione in grado di bloccare attacchi fatti con tool come Mimikatz
- Mitigazione di attacchi eseguiti con la tecnica di Code Cave
- Protezione dalla tecnica di attacco Man-in-the-Browser
- Rilevamento del traffico di rete malevolo verso i server di contollo e comando
- Rilevamento di Shell Meterpreter

La soluzione deve proteggere da attacchi ransomware impedendo la cifratura non autorizzata dei file e, in caso di attacco, il prodotto deve essere in grado di ripristinare in modo automatico allo stato originale i file criptati. Questo motore deve proteggere anche da attacchi ransomware remoti. Deve inoltre proteggere da attacchi di ransomware in grado di cifrare il master boot record del disco, e deve essere in grado di prevenire comportamenti malevoli attraverso l’application lockdown delle seguenti applicazioni:

- Web Browsers (including HTA)
- Web Browser Plugins
- Java
- Media Applications
- Office Applications

La soluzione deve disporre di un motore di deep learning basato sulla tecnologia delle reti neurali per il riconoscimento, senza necessità di aggiornamenti, del malware, delle applicazioni potenzialmente indesiderabili e dei programmi leciti.

La soluzione deve essere in grado di visualizzare nella console in cloud un motore grafico di analisi delle cause alla base degli attacchi rilevati mostrando tutti gli eventi che hanno portato al rilevamento. Questa funzionalità deve permettere di capire quali sono stati i file, i processi e le chiavi di registro colpiti dal malware e le eventuali comunicazioni in rete fatte durante l’attacco.

La soluzione deve supportare sistemi operativi client Windows 7 o superiori.

Deve essere possibile abilitare e gestire da un'unica console cloud ulteriori feature mediante il solo acquisto di licenze aggiuntive. Queste le feature richieste:

- Full disk Encryption mediante la gestione di Microsoft Bitlocker
- gestione e protezione di dispositivi mobile (Smartphone e Tablet Android, Ios e Windows Mobile)

- antivirus e antispam sulla posta attraverso un relay di posta in cloud
- gestione del wifi attraverso access point del vendor gestiti da cloud

La soluzione deve essere compatibile con soluzioni antivirus di altri vendor.

Il vendor deve avere anche una soluzione di protezione tradizionale (a signature) acquistabile separatamente, gestita dalla stessa console e integrabile nello stesso agente di protezione richiesto in questo bando.

Architettura

Attualmente è in esercizio un sistema antivirus on-premise, di classe enterprise, dedicato alla protezione delle postazioni di lavoro di tipo client (desktop, laptop). Di seguito un disegno schematico dell'infrastruttura.

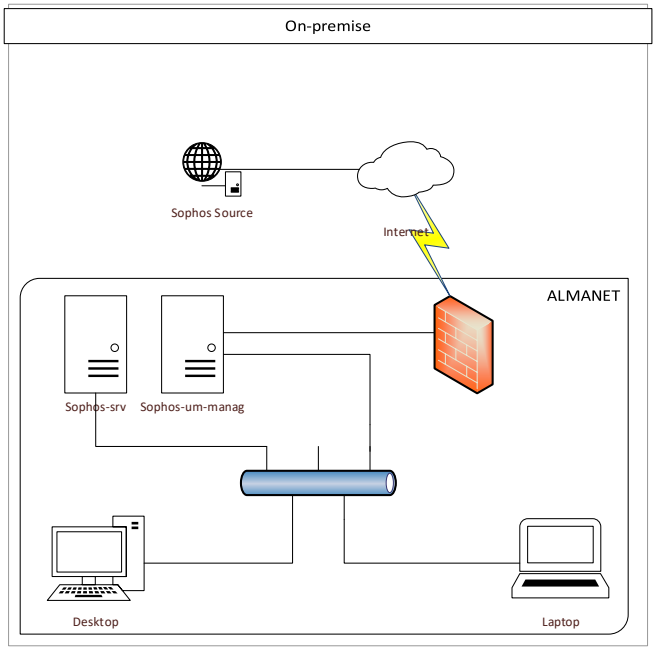

Figura 1 – Attuale architettura

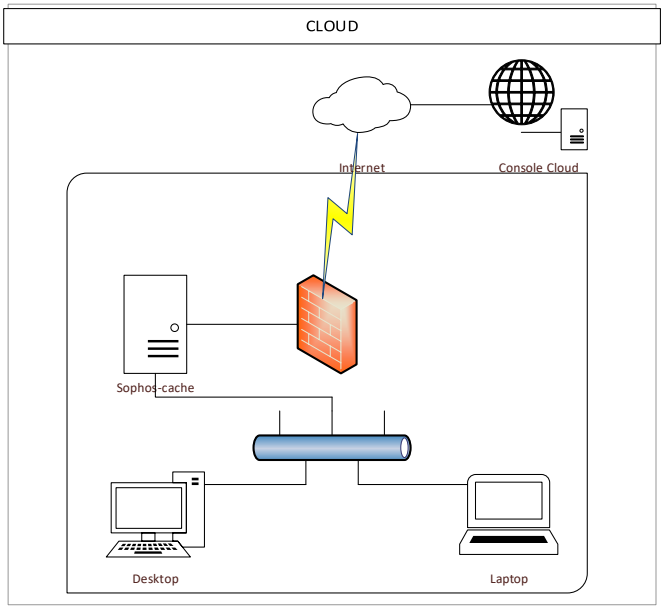

Figura 2 – Architettura prevista

Durata del contratto

Il servizio avrà decorrenza dalla stipula del contratto al 31/12/2021, con esclusione di tacito rinnovo.

Il RUP si riserva la facoltà di ordinare, mediante comunicazione scritta, l'avvio delle prestazioni oggetto del contratto nelle more della stipula dello stesso, ai sensi dell'art. 32, co. 13 D.Lgs. 50/2016. In tal caso la Stazione Appaltante potrà ordinare all'aggiudicatario l'avvio di tutte o di parte delle prestazioni oggetto del contratto.

L'aggiudicatario assume l'obbligo di dare immediato adempimento. In caso di mancata successiva stipula del contratto l'aggiudicatario avrà diritto soltanto al pagamento delle spese sostenute per l'esecuzione delle attività ordinate dal RUP.

Fatturazione elettronica e pagamenti

L'appaltatore dovrà emettere fattura elettronica con cadenza annuale e pari ad 1/3 dell'importo offerto in sede di gara.

Le fatture, oltre ad essere emesse in termini corretti e rispondenti alle specifiche tecniche, dovranno riportare i seguenti dati:

- codice univoco ufficio: OAHLWA
- CIG: 8026696F11
- numero della RDO: 2384571

Il fornitore inoltre si impegna a riportare sulla fattura la seguente dicitura: "Scissione di pagamento ai sensi dell'art. 2, co.1 del DM 23 gennaio 2015".

I pagamenti saranno subordinati all'esito positivo del procedimento di verifica di conformità della prestazione rispetto a quanto indicato nel presente Capitolato e negli altri atti di gara e alla regolarità contributiva verificata tramite la richiesta di rilascio agli Enti competenti del Documento Unico di Regolarità contributiva (DURC) e degli accertamenti Equitalia.

L'impresa aggiudicataria, ai sensi dell'art. 3 della L. 136/2010, deve comunicare, prima della stipula del contratto, gli estremi del conto corrente su cui effettuare il pagamento (codice IBAN …….., intestato a …….., presso ……..) nonché le generalità delle persone delegate ad operarvi.

La cessazione e la decadenza dall'incarico dell'Istituto sopra designato, per qualsiasi causa avvenga, deve essere tempestivamente notificata all'Università che non assume alcuna responsabilità per i pagamenti eseguiti a Istituto non più autorizzato a riscuotere.

Il pagamento avverrà entro 30 giorni dalla data di ricezione della fattura.

Il ritardato pagamento della fattura determina il diritto alla corresponsione degli interessi legali di mora, calcolati sulla base del tasso di riferimento maggiorato di 8 punti percentuali. Il tasso di riferimento è il tasso di interesse applicato dalla BCE alle operazioni di rifinanziamento principali, come definito dal D.lgs. 231/2011, modificato dalla Legge 192/2012.

Garanzie di esecuzione

L'Aggiudicatario per la sottoscrizione del contratto deve costituire una garanzia, a sua scelta sotto forma di cauzione o fideiussione ai sensi di quanto previsto dall'articolo 103 del d.lgs. 50/2016.

Detta cauzione definitiva può essere prestata mediante polizza fidejussoria o fideiussione bancaria presso gli Istituti legalmente autorizzati.

La fideiussione bancaria o la polizza assicurativa deve prevedere espressamente:

- la rinuncia al beneficio della preventiva escussione del debitore principale;

- la rinuncia all'eccezione di cui all'articolo 1957, co. 2 del Codice Civile,

- l'operatività della garanzia medesima entro quindici giorni a semplice richiesta scritta della stazione appaltante;

L'importo della garanzia è ridotto del 50% per gli operatori economici ai quali sia stata rilasciata, da organismi accreditati, la certificazione di qualità.

Per fruire di tale beneficio, il gestore segnala il possesso del requisito, e lo documenta allegando la certificazione di qualità conforme alle norme europee, in originale o in copia conforme all'originale.

Spese contrattuali

Tutte le spese e gli oneri fiscali inerenti al contratto, compresi i bolli, saranno a carico dell'Aggiudicatario, al quale verrà successivamente comunicato le modalità di versamento dell'importo relativo alle marche da bollo.

Norma di rinvio

Per quanto non espressamente previsto nel presente capitolato si rinvia alle condizioni generali di contratto di cui al bando MEPA relativo alle forniture/servizi "Beni-Informatica, Elettronica, Telecomunicazioni e Macchine per Ufficio""

https://www.acquistinretepa.it/opencms/opencms/scheda_iniziativa.html?idIniziativa=365a72f5d8c80c09

Foro competente

Per tutte le controversie comunque attinenti all'interpretazione o all'esecuzione del contratto, è stabilita la competenza esclusiva del Foro di Bologna.