LICENZA ANTIVIRUS ESET TRIENNALE 2022-2025 € 9.735,60 (IVA al 22% compresa) – DAL 1/4/2022 AL 31/3/2025 - AFFIDAMENTO. VARIAZIONE AI BUDGET DIREZIONALI 2022

CIG: ZA43586E9F

RELAZIONE

SITUAZIONE ATTUALE

La Camera ha confermato le configurazioni ICT standard camerali con la determinazione n. 85/AMM/2020 e tra queste il software antivirus aziendale Kaspersky di cui ha acquistato la licenza per il triennio 17/4/2021-16/4/2024 con determinazione n. 28/AMM del 10/3/2021.
La scelta di questo prodotto è stata quella di diversificare l'antivirus rispetto a quello adottato da Infocamere (la quale ha adottato per i propri sistemi il prodotto Trend Micro Security) in modo da aggiungere maggior copertura rispetto alle librerie antivirus del prodotto IC. Ci si è quindi orientati verso uno dei principali software sul mercato anti-malware e anti-virus già diffuso in circa 2.500 soggetti pubblici italiani tra cui: Polizia, Carabinieri, Ministero dell'Interno, Ministero della Giustizia, Ministero della Difesa.
Kaspersky ha la propria sede legale nel Regno Unito. La società ha però notevoli capacità di ricerca e sviluppo in Russia anche se dal 2017 il suo principale centro di ricerca e sviluppo è stato trasferito in Israele.

Ogni software antivirus, per poter funzionare, agisce ai livelli più profondi del computer o del server sul quale è installato e scarica quotidianamente, dalla società produttrice, le implementazioni software che lo mantengono aggiornato rispetto ai nuovi malware ed ai virus. Pertanto si tratta di uno strumento che ha una funzione delicata nell'ambito della cosiddetta cyber security. In seguito all'invasione dell'Ucraina da parte dell'esercito Russo ed in assenza di direttive da parte dell'agenzia nazionale per la sicurezza informatica o dall'Agid o da qualsiasi altra fonte governativa ho approfondito gli aspetti legati alla cyber security riguardo all'antivirus russo adottato.

In Italia, finora l'Agenzia di cybersicurezza nazionale, diretta da Roberto Baldoni, non ha diramato alcuna nota sul rischio rappresentato da Kaspersky.
Anzi, il MISE - direzione generale per le tecnologie delle comunicazioni e la sicurezza informatica e l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione (sulla base della elaborazione nella ungherese CCLab Software Laboratory) - ha rilasciato per Kaspersky Endpoint Security for Windows (version 11.6.0.394 AES256) una certificazione di sicurezza CC EAL2+ tale da rendere il software Kaspersky formalmente idoneo ad essere eseguito in ambiti classificati ai massimi livelli della PA

italiana. Il rapporto di certificazione è stato rilasciato dall'OCSI Organismo di certificazione della sicurezza informatica prot. OCSI/CERT/CCL/02/2021/RC del 31 Gennaio 2022.
Il sottosegretario alla presidenza del consiglio dei Ministri ha rilasciato un'intervista al Corriere della Sera del 13/3/2022 con la quale ha annunciato il bando all'antivirus Kaspersky e dichiarato che i server pubblici non sono sufficientemente protetti e che più il conflitto si prolunga più il rischio di attacchi cibernetici aumenta. L'indicazione, pur diffusa in modo informale, è di dismettere l'antivirus russo per evitare che da strumento di protezione possa diventare strumento di attacco.

Negli ultimi anni Kaspersky è finito sotto esame negli **Stati Uniti** da parte dell'Agenzia federale per la sicurezza nazionale americana(Dhs), come molta altra tecnologia considerata strategica, ad esempio la cinese Huawei per gli smartphone e soprattutto per le componenti delle centrali ICT.

In Europa **l'Olanda** aveva deciso nel 2018 di eliminare gradualmente Kaspersky dalle infrastrutture governative ed aveva invitato le aziende coinvolte nella salvaguardia dei servizi vitali, di fare lo stesso come misura precauzionale.
L'analisi del rischio condotta nel 2018 mostrava che non ci fossero indicazioni concrete che Kaspersky rappresentasse effettivamente un rischio per i Paesi Bassi. La conclusione fu che non si poteva né asserire né escludere se Kaspersky rappresentasse una minaccia per la sicurezza nazionale nei Paesi Bassi.
Inoltre, il rapporto olandese affermava anche che Kaspersky potesse essere stato infiltrato e compromesso da un governo diverso da quello russo (inconsapevolmente). Il rapporto riconosceva dunque che anche altre società di antivirus potessero essere a rischio. Il rischio zero anche in questo settore non esiste.

In Francia l'Anssi (agenzia nazionale per la sicurezza dei sistemi informativi) il 2/3/2022 ha emesso un bollettino riguardo i potenziali effetti cyber legati all'invasione dell'Ucraina da parte della Russia su entità francesi. Scrive che, "nel contesto attuale, l'uso di alcuni strumenti digitali, in particolare gli strumenti della società Kaspersky, possono essere coinvolti a causa del loro legame con la Russia" da qui suggerisce di considerare nel medio termine una strategia di diversificazione delle soluzioni di cybersecurity". Inoltre, l'Anssi precisa che "in questa fase nessun elemento oggettivo giustifica una modifica della valutazione del livello di qualità dei prodotti e servizi forniti". Pertanto, "senza una soluzione sostitutiva, la disconnessione degli strumenti di sicurezza informatica può indebolire significativamente la sicurezza informatica [delle] organizzazioni […] non può essere raccomandata".

PROCEDURA OPERATIVA DI SOSTITUZIONE
Una volta acquisita la licenza le fasi di lavoro che verrebbero

attuate dal personale ICT sono le seguenti:

- configurazione di un nuovo server virtuale dedicato (fatto)
- installazione del software ESET con licenza di prova (fatto)
- configurazione di una policy "task A" per la rimozione di Kaspersky da ogni postazione fisica
- configurazione di una policy "task B" per la rimozione dell'Agent di Kaspersky da ogni postazione fisica
- download della licenza di ESET
- accensione del dispositivo (da parte di ogni operatore)
- rimozione manuale di Kaspersky e contestuale installazione di ESET sui n. 10 server
- rimozione con "TASK A" di Kaspersky e installazione di ESET su tutte le n. 200 postazioni VDI (virtuali)
- rimozione con "TASK B" dell'Agent Kaspersky e installazione di ESET su tutte le n. 200 postazioni VDI (virtuali)
- riavvio automatico delle VDI (nel weekend)
- rimozione con "TASK A" di Kaspersky e installazione di ESET su tuttI i pc fisici
- rimozione con "TASK B" dell'Agent Kaspersky e installazione di ESET su tutti i pc fisici
- riavvio dei pc fisici
- verifica del risultato della scansione di ogni dispositivo su console
- su console di ESET controllo di tutti i dispositivi ed eventuale classificazione nel relativo gruppo di categoria
- completare tutte le policy per gli aggiornamenti (nelle 8-10 settimane a seguire)

Questa attività dovrebbe richiedere da una a due settimane di lavoro del personale ICT con brevi interruzioni delle singole postazioni di lavoro del personale camerale durante la rispettiva fase di sostituzione del software. Seguirà poi un sistematico lavoro di messa a punto sistemistica che durerà in maniera non continuativa qualche mese.

PROPOSTA

Per tali motivi ritengo prudente sostituire il prima possibile l'antivirus in questione con un software alternativo di una società con base in uno dei paesi UE. La rimozione deve necessariamente essere immediatamente seguita dall'installazione di un antivirus alternativo.

I colleghi ICT ed il sistemista interno stanno testando da una settimana antivirus alternativi ed è stato individuato il prodotto Slovacco ESET che ha la propria base di sviluppo in un paese della UE ed è stato già utilizzato con altri clienti dal sistemista camerale; pertanto l'operazione di sostituzione dovrebbe avvenire in modo più veloce.

Il prezzo per l'acquisto del nuovo software è di € 2.660,00/annui (IVA al 22% esclusa). Per recuperare la somma necessaria all'acquisto propongo di ridurre il vincolo del contratto di

manutenzione per gli impianti di condizionamento della sede affidato con determinazione n. 105/AMM/2021, che prevede oltre ai canoni un importo a consumo, nell'eventualità di interventi su guasto. Per tale contratto, nel periodo già trascorso, la casistica degli interventi è stata poco frequente, per cui ritengo possibile diminuire il vincolo n. 53/2022 per l'anno 2022, dell'importo di € 2.542,53 pari alla somma necessaria a coprire il costo del canone dell'antivirus per il periodo residuale del 2022.

Sembra che il governo debba formalizzare a breve un DPCM con l'indirizzo di sostituire l'antivirus. Pur non essendo stata ancora emanata alcuna direttiva ufficiale sottolineo che operativamente questa attività non sarebbe istantanea e richiederebbe diversi giorni di lavoro dal download della licenza del nuovo antivirus fino alla copertura di tutte le macchine in servizio. Pertanto propongo di acquistare subito la nuova licenza.

Brescia, 15/3/2022

Il PROVVEDITORE
(geom. Marco Mosca)

IL SEGRETARIO GENERALE
(dr Massimo Ziletti)