CAPITOLATO TECNICO

FORNITURA DI ACCESSI E LICENZE D'USO RELATIVE ALLA PIATTAFORMA PROOFPOINT SECURITY AWARENESS PER 12 MESI

INDICE

1 PREMESSA

1.1 DEFINIZIONI

Nel corpo del documento, ai termini di cui appresso, viene attribuito il significato riportato a fianco di ciascuno di essi:

- CONSIP: la società che, in qualità di stazione appaltante, affida la fornitura oggetto del presente Capitolato;
- SOGEI: la Società Generale di Informatica S.p.A.,;
- Agenzia delle Entrate: beneficiaria della Fornitura;
- Capitolato tecnico: il presente documento che enuncia le specifiche tecniche alle quali dovrà conformarsi la fornitura;
- Contratto: il contratto che verrà stipulato tra la SOGEI e l'impresa che enuncia le regole giuridiche alle quali si dovrà conformare la fornitura;
- Fornitura: il complesso delle attività oggetto del presente Capitolato;
- Società: la società aggiudicataria della fornitura;
- Malfunzionamento: qualsiasi anomalia funzionale dei prodotti software e, in ogni caso, ogni difformità del prodotto in esecuzione rispetto alla relativa documentazione tecnica e manualistica d'uso;
- Produttore: la società Proofpoint LTD;
- Responsabile delle attività contrattuali: la persona individuata dalla Società come interlocutore di Sogei e responsabile di tutte le attività contrattuali;
- Sistema Informativo: il sistema informativo gestito da Sogei con sede in Via Mario Carucci 99.

1.2 CONTESTO DI RIFERIMENTO

Come pubblicizzato dalla letteratura di settore e dalla quotidiana osservazione degli eventi di sicurezza informatica, il fattore umano è una delle principali fonti di rischio cibernetico, contribuendo ad incrementare sia l'impatto che la probabilità di accadimento di un incidente. Una azione umana poco consapevole è uno dei mezzi maggiormente utilizzati dai cybercriminali per aggirare le protezioni poste a difesa di una infrastruttura informatica, sia tecniche che organizzative. A riguardo, ne è evidenza anche il notevole aumento, negli ultimi anni, dei fenomeni di malspam e phishing perpetrati attraverso lo strumento della posta elettronica, così come per più generiche attività di ingegneria sociale.

Come riferito in una nota ufficiale da Martin McKeay, direttore editoriale del rapporto sullo stato di Internet – Security della società Akamai: «Il phishing è un problema a lungo termine e prevediamo

che i malintenzionati continueranno a colpire indistintamente consumatori e aziende fino a quando non verranno messi in atto programmi di formazione per aumentare la consapevolezza degli utenti riguardo ai rischi e verranno implementate tecniche di difesa a più livelli. Lo stile degli attacchi di phishing ha diverse forme, pertanto le aziende devono impegnarsi per rimanere un passo avanti rispetto ai criminali che tentano di abusare della loro fiducia».

Appare quindi evidente come la formazione sul tema costituisca un elemento strategico per la prevenzione degli incidenti cyber ed è parte integrante di una strategia di sicurezza completa.

Una delle principali preoccupazioni del Management è la bassa sensibilità e consapevolezza da parte di tutto il personale sui rischi legati al mondo Cyber.

Dall'analisi degli incidenti di Cyber Security emerge che il fattore umano contribuisce in maniera determinante alla riuscita degli attacchi, in particolare quelli che mirano ad ingannare i dipendenti, ad esempio con false e-mail. La formazione su questi temi è un elemento fondamentale nella prevenzione degli incidenti di Cyber Security ed è parte integrante di una strategia di sicurezza completa. Un personale formato e consapevole è una prima linea di difesa e segnalazione contro gran parte degli attacchi Cyber.

L'Agenzia delle Entrate, con scopo di diffondere la cultura della sicurezza cibernetica e fornire elementi essenziali ma concreti relativamente a questa tematica, intende proseguire ad erogare una formazione specifica per la prevenzione degli incidenti cyber, destinandola a tutti i propri dipendenti che ancora non l'hanno effettuata.

1.3 NORMATIVA DI RIFERIMENTO

Il fatto che la sicurezza di dati, reti e informazioni sia un obiettivo strategico oramai non più di interesse di una singola azienda o settore, ma di dominio nazionale e internazionale è ben noto alle Istituzioni di riferimento, come testimoniato dal fermento normativo in materia.

Il nuovo Piano Nazionale per la protezione cibernetica e la sicurezza informatica riporta i seguenti 11 indirizzi operativi, tra i quali il terzo investe il presente capitolato tecnico:

1. Potenziamento capacità di intelligence, di polizia e di difesa civile e militare;
2. Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;
3. Promozione e diffusione della cultura della sicurezza informatica. Formazione ed addestramento;
4. Cooperazione internazionale ed esercitazioni;
5. Operatività delle strutture nazionali di incident prevention, response e remediation;
6. Interventi legislativi e compliance con obblighi internazionali;
7. Compliance a standard e protocolli di sicurezza;

8. Supporto allo sviluppo industriale e tecnologico;
9. Comunicazione strategica e operativa;
10. Risorse;
11. Implementazione di un sistema di cyber risk management nazionale.

2 OGGETTO DEL SERVIZIO

Il presente Capitolato disciplina la fornitura di accesso e delle licenze d'uso relative alla Security Awareness Platform di Proofpoint, da erogarsi in favore dell'Agenzia delle Entrate, ivi comprese tutte le attività connesse allo svolgimento delle prestazioni medesime così come regolamentate, oltre che dal presente Capitolato, anche dallo Schema di contratto e dalle Condizioni Particolari.

La piattaforma resa disponibile dalla Società dovrà essere attiva per 12 (dodici) mesi a decorrere dalla data di stipula del contratto, con un limite di n. 7500 licenze nominative attivabili.

La piattaforma dovrà fornire moduli formativi in forma di video-diapositive, con possibilità di gestire centralmente la relativa amministrazione e somministrazione, prevedendo altresì una componente di interazione con l'utente per la verifica del livello raggiunto, tramite apposita piattaforma web based.

I Moduli formativi online dovranno coprire le seguenti tematiche:

- Anti-Phishing;
- Data Protection and Destruction;
- Safe Social Networks;
- Safer Web Browsing;
- Security Beyond the Office;
- Social Engineering;
- URL Training;
- Email Security;
- Passwords.

La verifica delle conoscenze pregresse e post-formazione dovrà prevedere:

- questionari con domande interattive pre-selezionate per argomento;
- interazione con l'utente mediante la possibilità di eseguire attacchi simulati, con modelli di e-mail di phishing pronte all'uso e personalizzabili su varie tematiche lavorative e livelli di difficoltà.

In base al risultato dell'assessment ad ogni dipendente potranno essere assegnati uno o più corsi di formazione specifici mediante meccanismi automatici sulla base del comportamento dell'utente.

Devono, inoltre, essere presenti funzionalità specifiche di analisi e reportistica quali ad esempio:

- tracciatura dei risultati delle campagne di assessment/assegnazione;

- reporting dei risultati dell'assessment e dei corsi effettuati per categoria di utenti, per livello di conoscenza su specifici temi per singolo utente e per gruppi utenti;

- console di amministrazione centralizzata per governare il processo formativo.

Si fa presente che il corso è stato erogato già per circa 4.000 utenti dell'Agenzia nel 2020 e per continuità e coerenza del contenuto formativo occorre erogarlo per le restanti utenze con le stesse modalità.

2.1 ATTIVAZIONE DELLE CREDENZIALI

La Società dovrà attivare e fornire le credenziali amministrative per l'accesso al portale entro 10 (dieci) giorni decorrenti dalla data di stipula del contratto.

Le credenziali dovranno essere inviate all'indirizzo di posta elettronica indicato dalla Committente all'atto della stipula del contratto.

La Società dovrà inviare alla medesima casella di posta elettronica ogni informazione necessaria al fine di permettere l'identificazione del prodotto e la conseguente possibilità di utilizzarlo.

2.2 VERIFICA DI CONFORMITÀ

Entro 15 (quindici) giorni a decorrenti dalla consegna e attivazione delle credenziali dei prodotti software, di cui al precedente par. 2.1, queste ultime saranno sottoposte a verifica di conformità, volta a certificare che le prestazioni contrattuali siano eseguite a regola d'arte sotto il profilo tecnico-funzionale. La Società è tenuta a prestare alla Sogei, a propria cura e spese, l'assistenza tecnica necessaria e a mettere a disposizione della Sogei quanto necessario alle operazioni di verifica di conformità.

La Società potrà intervenire alla verifica di conformità, anche attraverso propri rappresentanti. In tal caso detti rappresentanti sono tenuti a sottoscrivere i documenti di verifica di conformità che verranno redatti da Sogei (verbali, certificato, ecc.)

In caso di esito negativo della verifica di conformità, ferma restando l'applicazione delle penali, di cui al successivo paragrafo 4, la Società dovrà provvedere, a propria cura e spese, entro il termine che le verrà comunicato dalla Sogei, alla eliminazione dei difetti e/o delle carenze riscontrati entro il termine massimo di 5 giorni lavorativi, oppure di 3 giorni lavorativi se il malfunzionamento segnalato riguarda problemi di sicurezza del prodotto, ovvero una vulnerabilità tecnica che metta in pericolo l'integrità della piattaforma e dei contenuti esposti. Dopo la comunicazione, da parte della Società, dell'avvenuta eliminazione dei difetti e/o delle carenze, la Sogei procederà a nuova verifica di conformità nei termini e con le modalità di cui ai commi precedenti.

In caso di ulteriore esito negativo della verifica di conformità, la Sogei avrà facoltà di risolvere il contratto e di fare eseguire tutta o in parte la fornitura a terzi in danno della Società e fatto salvo in ogni caso il diritto al risarcimento di tutti i danni comunque subiti. A completamento della verifica positiva sarà prodotto la "Nota di Verifica di conformità" che dovrà essere sottoscritta dal Responsabile della Fornitura e dal Responsabile Sogei.

3 GESTIONE DEL SERVIZIO

Il contratto avrà efficacia dalla data della sua stipula e avrà una durata di 12 (dodici) mesi, e comunque, sino al completo adempimento di tutte le obbligazioni contrattuali.

3.1 RESPONSABILE DELLE ATTIVITÀ CONTRATTUALI

La Società dovrà comunicare, trasmettendolo con la documentazione per la stipula, il nominativo del Responsabile della fornitura, nonché un numero di telefono e un indirizzo e-mail al quale indirizzare eventuali comunicazioni. La Società deve provvedere in piena autonomia al coordinamento e all'organizzazione delle attività nel rispetto delle specifiche e dei tempi forniti da Sogei.

Sarà compito del Responsabile curare la gestione amministrativa del contratto e delle attività legate alla fatturazione e verificare il rispetto di tutti gli adempimenti contrattuali.

3.2 MODALITÀ DI COMUNICAZIONE

La Società si impegna a comunicare, contestualmente alla presentazione della documentazione per la stipula, un numero di fax, un indirizzo e-mail, un indirizzo pec e un numero di telefono al quale rivolgersi, senza alcun limite sul numero di chiamate, per ogni comunicazione relativa alla fornitura.

Resta inteso che, per tutta la durata contrattuale, la Società dovrà garantire la piena funzionalità dei suddetti mezzi di comunicazione comunicando tempestivamente a Sogei eventuali modifiche.

3.3 ADEMPIMENTI PER LA SICUREZZA

La Società s'impegna a porre in essere quanto necessario a garantire l'esecuzione delle attività in piena aderenza con le disposizioni del D. Lgs. 81/2008 "Testo Unico sulla sicurezza durante il lavoro", cooperando e coordinandosi, in particolare, con i referenti della Committente e degli uffici dell'Amministrazione Finanziaria presso cui dovranno essere svolte le attività contrattuali, ai fini degli adempimenti di cui al comma 2 dell'art. 26 del citato decreto.

Si evidenzia che le attività di cui al presente capitolato rientrano nelle fattispecie di cui al comma 3-bis del suddetto articolo, per le quali non sussiste l'obbligo di redigere il DUVRI (Documento Unico di Valutazione dei Rischi da Interferenze).

3.4 LINGUA

Tutte le attività e la documentazione sarà in lingua italiana e/o lingua inglese.

3.5 RISERVATEZZA

Tutte le informazioni trattate e tutti i documenti, anche parziali, scambiati tra la Società e Sogei sono riservati, pertanto è richiesta la massima attenzione per il loro utilizzo, in particolare se questo avviene al di fuori delle sedi Sogei.

La Società non potrà utilizzare o condividere con terzi, a nessun titolo e in nessun modo, la documentazione, i dati o qualsiasi altra informazione fornita da Sogei, ancorché inserita attraverso la piattaforma Proofpoint o al di fuori delle attività oggetto del contratto.

4 PENALI

Sogei applicherà le penali, secondo le modalità previste in contratto, nei seguenti casi:

- per ogni giorno lavorativo di ritardo nell'attivazione delle credenziali si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale;
- in caso di esito negativo della verifica di conformità di cui al paragrafo 2.2, si applicherà una penale pari all'1‰ (uno per mille) dell'importo contrattuale, per ogni giorno intercorrente tra la data del verbale negativo e quello positivo.

Nell'ipotesi in cui l'importo delle penali applicabili superi l'ammontare del 10% (diecipercento) dell'importo contrattuale complessivo, la Sogei avrà il diritto di risolvere, totalmente o parzialmente, il contratto in danno della Società, salvo il diritto dell'eventuale maggior danno.

5 MODALITÀ DI FATTURAZIONE

La Società potrà emettere fattura successivamente alla sottoscrizione della nota di verifica di conformità positiva. La fattura dovrà riportare il numero di repertorio del contratto ed il codice CIG.

Si precisa che la mancanza di uno di questi elementi consente al committente di rifiutare la fattura entro il termine previsto.