consip

Nota stampa di approfondimento

29 aprile 2021

OGGETTO DELLA CONVENZIONE

La convenzione "Videosorveglianza 1" è stata bandita il 26/11/2015 e riguarda la fornitura di **sistemi di videosorveglianza e servizi connessi** per le PA, prima edizione, del valore complessivo di € **53.700.000**, suddivisa in **tre lotti** geografici:

- Lotto 1 (€ 19.000.000) riferito alle regioni Piemonte, Liguria, Valle d'Aosta, Lombardia, Veneto, Trentino Alto Adige, Friuli Venezia Giulia: aggiudicato a Fastweb S.p.A. Attivo dal 22/03/2017 e conclusosi il 22/09/2018
- Lotto 2 (€ 14.300.000) riferito alle regioni Emilia Romagna, Toscana, Lazio, Marche, Abruzzo, Molise, Umbria, Sardegna: aggiudicato al RTI Telecom Italia S.P.A. – Leonardo-Finmeccanica S.P.A. – Ingegneria & Software Industriale S.P.A. Attivo dal 17/05/2017 conclusosi il 17/01/2018
- Lotto 3 (€ 23.400.000) riferito alle regioni Campania, Basilicata, Puglia, Sicilia, Calabria: aggiudicato a Fastweb S.p.A. Attivo dal 22/03/2017 e conclusosi il 14/06/2018.

NOTE GENERALI

La **sicurezza di un qualsiasi sistema informatico dipende da diversi fattori** che devono essere globalmente considerati:

- **caratteristiche** del prodotto (di competenza del produttore dei beni)
- **progettazione e realizzazione** del sistema (di competenza dell'esecutore del contratto)
- **gestione e conduzione** del sistema (effettuata dal beneficiario e/o da terzi)
- **utilizzo** che ne fa il beneficiario.

Ne deriva che nel **caso specifico della convenzione "Videosorveglianza 1"** - oltre alle caratteristiche tecniche proprie dei prodotti offerti in gara - la sicurezza dipende sia dalla progettazione e realizzazione del sistema di videosorveglianza, affidata al Fornitore (Fastweb o RTI Telecom come sopra indicato nel dettaglio), sia dall'utilizzo che ne fa la PA attraverso l'adozione delle proprie

procedure (es: politiche di creazione e uso delle credenziali di accesso, modalità di accesso alle immagini registrate) e il monitoraggio del loro effettivo rispetto da parte del personale interno e/o di soggetti terzi, qualora affidatari della conduzione del sistema .

A rafforzare ciò, alcune brevi considerazioni:

1. **TEMA DI QUALITÀ E SICUREZZA DEL PRODOTTO**. La **nazionalità dei produttori delle tecnologie non è sempre, né automaticamente, sinonimo di garanzia di sicurezza**. A titolo di esempio le seguenti fattispecie:
   - l'attacco di tipo "*supply chain*" di vasto impatto subito dall'azienda americana SolarWinds
   - la vulnerabilità riscontrata sui prodotti NVR del vendor tedesco Bosch, concretizzatasi nella possibilità di compromettere la riservatezza e la disponibilità dei video, in diretta e registrati, dalle telecamere associate al NVR
   - la vulnerabilità riscontrata sulle telecamere della serie 8000 del vendor americano Cisco, consistente nel poter rendere inattive le telecamere
   - la vulnerabilità riscontrata su una serie di prodotti del vendor svedese Axis, consistente nel poter prendere il controllo delle telecamere
2. **TEMA VULNERABILITÀ E ATTACCHI INFORMATICI**. La **grande diffusione di una tecnologia** (Hikvision e Dahua sono i primi due produttori mondiali nel mercato della videosorveglianza) **tipicamente corrisponde anche alla presenza di una "superficie di attacco" maggiore**. In altri termini, il numero di attacchi informatici che interessano una tecnologia ampiamente diffusa è sicuramente superiore se paragonato a quelli ricevuti da tecnologie scarsamente diffuse e, quindi, su tale tecnologia sarà più facile rilevare eventuali vulnerabilità associate
3. **TEMA DI INTERESSI NAZIONALI E SPIONAGGIO**. L'**eventuale condotta fraudolenta di un produttore straniero** che deliberatamente inserisca backdoor e vulnerabilità di sicurezza per scopi malevoli, per il cui accertamento sarebbero, comunque, necessarie verifiche tecniche particolarmente complesse, **non può essere rimesso alla valutazione della Stazione Appaltante che bandisce la gara** per l'affidamento di sistemi di videosorveglianza, anche laddove a procedere in tal senso sia una centrale di committenza. Non è immaginabile, infatti, che gli esiti di questi accertamenti tecnici possano differire a seconda del soggetto che li esegue.

   Dovrebbe essere **compito delle autorità nazionali competenti in materia di sicurezza effettuare valutazioni tecniche** finalizzate ad identificare tali problematiche e **adottare provvedimenti formali** nei confronti di produttori stranieri non affidabili, di modo che, poi,

gli eventuali esiti negativi delle predette valutazioni siano veicolati per tempo, e in maniera uniforme, alle PA che di tali prodotti abbisognano traducendosi in una vera e propria preclusione all'impiego degli stessi quando, in particolare, trattasi di amministrazioni che, per le funzioni espletate e i servizi erogati, necessitano di una particolare protezione dagli attacchi informatici.

In **Italia ci si sta muovendo proprio in tal senso con l'introduzione del *Perimetro di Sicurezza Nazionale***, conseguente all'approvazione della legge 18/11/19 n. 133 "*Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica e di disciplina dei poteri speciali nei settori di rilevanza strategica*" e relativa normativa attuativa (in parte ancora in corso di adozione), che prevede, tra le altre cose, la costituzione del Centro di Valutazione e Certificazione Nazionale (CVCN) attraverso cui possono essere eseguite specifiche attività di test in vista del successivo affidamento di forniture di beni, sistemi e servizi ICT destinati a essere impiegati sulle reti, sui sistemi informativi e per l'espletamento dei servizi informatici identificati dai soggetti che sono inclusi nel perimetro di sicurezza nazionale cibernetica.

* * *

Fermo quanto premesso, si riportano nel seguito le risposte alle domande specifiche.

Se al momento dell'assegnazione dei lotti si era a conoscenza del tipo di dispositivi di videosorveglianza (marca, modello, funzionalità) che le società vincitrici avrebbero installato

Sì, l'aggiudicazione dei tre lotti della convenzione "Videosorveglianza 1" è avvenuta successivamente alla presentazione dell'offerta tecnica da parte dei concorrenti, in cui sono state riportate le tecnologie offerte (brand e modello dei dispositivi offerti).

Ci risulta che tramite bandi Consip, numerose forniture siano state aggiudicate da società che utilizzano apparecchiature/strumenti di videosorveglianza delle società cinesi DAHUA e HIKVISION. Queste società sono note per la vulnerabilità informatica dei loro apparecchi, per essere strettamente collegate al governo cinese e per essere in diverse blacklist, tra cui quella dell'agosto del 2019 in cui il governo statunitense ha bandito i loro prodotti da tutti gli edifici pubblici/governativi. CONSIP ha avuto modo di valutare la criticità di queste forniture?

I due aggiudicatari dei tre lotti di gara (Fastweb e il RTI Telecom) hanno offerto varie tecnologie tra cui, nell'ambito delle telecamere e dei Network Video Recorder, è stata preponderante quella Hikvision, mentre la tecnologia Dahua non è stata offerta.

Consip ha previsto - al termine della fase di valutazione delle offerte e sui concorrenti primi in graduatoria - l'effettuazione di verifiche tecniche relative all'esame della documentazione di prodotto presentata dai concorrenti volta a garantire la corrispondenza tra il prodotto offerto e le specifiche tecniche richieste nel capitolato tecnico di gara.

Il collaudo dei sistemi di videosorveglianza realizzati in fase esecutiva del contratto (a seguito di ciascun ordinativo di fornitura) è, invece, in capo alle PA che hanno aderito alla convenzione stipulando autonomi contratti.

Avete strumenti per penalizzare nel punteggio di gara soggetti che offrono strumentazioni con problematiche di sicurezza?

Le regole sull'affidamento dei contratti pubblici - fermo il rispetto degli standard minimi di qualità richiesti - prevedono esclusivamente punteggi incrementali volti a premiare i miglioramenti tecnici offerti dal concorrente.

In questa logica - relativamente agli aspetti di sicurezza - nella convenzione "Videosorveglianza 1" erano presenti sia requisiti minimi (es. le immagini delle riprese rimangono unicamente nella disponibilità delle Amministrazioni) nonché requisiti premianti (es. relativi all'archiviazione e gestione delle immagini).

A fronte della successiva adozione del GDPR e delle normative sopravvenute in materia di sicurezza nazionale, la successiva edizione "Videosorveglianza 2" rafforza ulteriormente le soluzioni offerte in termini di sicurezza, ampliando i requisiti minimi ed introducendo nuovi requisiti premianti.

In ultimo, l'individuazione dell'operatore economico aggiudicatario deriva, oltre che dagli elementi economici, dalla valutazione della pluralità di requisiti sottoposti a valutazione tecnica, di cui la sicurezza costituisce uno degli elementi di rilievo.

Quali istituzioni/enti che rientravano nei lotti previsti dal bando hanno completato la procedura di acquisto di forniture di sistemi di videosorveglianza?

L'informazione non è divulgabile. Il Ministero dell'Economia e Finanze è l'unico soggetto titolare del trattamento dei dati per le attività svolte da Consip nell'ambito del Programma di razionalizzazione degli acquisti della PA.

In ogni caso - sulla specifica iniziativa di videosorveglianza - la divulgazione dei dati delle PA acquirenti potrebbe aumentare il rischio di attacco e non può, pertanto, avvenire senza il consenso della stessa PA acquirente.

In relazione alla Gara a procedura aperta per la fornitura di sistemi di sorveglianza e servizi connessi per le pubbliche amministrazioni (edizione 2) si richiede lo stato di avanzamento dei lavori e la data prevista di pubblicazione dei vincitori della gara.

La gara per l'aggiudicazione della convenzione ""Videosorveglianza 2" è in fase di "esecuzione dei controlli" sui requisiti soggettivi dei partecipanti (ex art. 80 Codice Appalti). Si prevede l'aggiudicazione per IV Trimestre 2021.