HP Inc
Government Relations

Senato della Repubblica

8ª Commissione Lavori Pubblici, Comunicazioni

Indagine conoscitiva sull'applicazione del codice dei contratti pubblici

Audizione di HP Inc.

11 Aprile 2019

Garantire la sicurezza cibernetica nel Public Procurement: le raccomandazioni di HP Inc.

Executive summary

La consapevolezza dei rischi cibernetici è ormai abbondantemente radicata, ma le strategie di risposta risultano spesso essere concentrate quasi esclusivamente sul rafforzamento dei *software* di sicurezza e sulla protezione dei *data center*, anziché sulla sicurezza a livello *hardware*.

Al fine di intervenire in modo proattivo sulle minacce informatiche rivolte all'intero sistema nazionale, pare ineludibile l'avvio di iniziative volte a rendere i device utilizzati dalle Istituzioni italiane capaci di rispondere alle crescenti minacce cyber.

Sulla base delle considerazioni sopra esposte e in vista di un probabile intervento di revisione normativa da parte del Legislatore, HP Inc. ritiene fermamente che per garantire la sicurezza delle infrastrutture critiche nazionali sia necessario:

1. **Stabilire requisiti minimi di sicurezza in materia di appalti**. Gli appalti non possono essere unicamente basati sul mero criterio del minor prezzo.
2. **Acquisire *hardware* con standard di sicurezza elevati a tutela delle infrastrutture critiche**. È necessario investire nella sicurezza delle infrastrutture critiche per il Paese a livello pratico andando a rafforzare il parco macchine degli uffici governativi, amministrativi e delle agenzie di sicurezza.

Considerazioni preliminari sullo stato dell'arte

Mantenere elevato il livello di sicurezza cibernetica di informazioni, infrastrutture e cittadini è una delle più grandi sfide del nostro tempo, dal momento in cui i bersagli dei *cyber* attacchi sono molteplici.

Secondo un rapporto PwC[1], infatti, i danni causati da debolezze dei sistemi informatici sono saliti di circa il 40% nel triennio 2015-2017. Con riguardo al contesto nazionale, il recente Rapporto Clusit del 2018 sulla sicurezza ICT[2] in Italia ha rilevato in media 94 incidenti gravi al mese nei 14 trimestri precedenti. Un numero estremamente preoccupante se si considera che «*[…] il fenomeno mira a interferire in maniera pesante non solo nella vita privata dei cittadini (peraltro vittime nel 2017 di crimini estorsivi su larghissima scala) quanto invece sul piano finanziario e geopolitico*»[3].

I danni potenziali generati da inefficienze dei sistemi di sicurezza sono, inoltre, notevoli anche da un punto di vista economico: le stime inducono a ritenere che nel 2016 il nostro Paese abbia subito danni derivanti da attività di cyber crimine per quasi 10 miliardi di euro.

Il Legislatore europeo, dal 2013, ha definito una strategia ben delineata per difendersi da tali minacce. La Direttiva *Network and Information Security* (NIS), il *Cyber Act*, regolamento adottato dal Parlamento Europeo nel marzo 2019 che stabilisce lo sviluppo di cyber-certificazioni per prodotti connessi, il

[1] HP, *La sicurezza IT nel settore pubblico: Rafforzare la sicurezza dei dispositivi*, Gennaio 2017.
[2] Rapporto Clusit 2018 sulla sicurezza ICT in Italia.
[3] Rapporto, *cit.*, p. 5.

Regolamento Europeo sulla *Privacy* (GDPR), le soluzioni *Smart Border*, i maggiori poteri conferiti all'Europol, così come la recente Direttiva sull'uso dei dati del codice di prenotazione (PNR), rappresentano passaggi fondamentali del piano strategico voluto dalla Commissione Europea.

Nella passata legislatura l'Esecutivo ha avviato una serie di iniziative per elevare il livello di *cyber* sicurezza delle proprie infrastrutture e dei propri cittadini, che andrebbero accompagnate da concreti piani di azione e dall'introduzione di regole di Public Procurement maggiormente stringenti sui criteri di sicurezza e di qualità per quanto concerne l'approvvigionamento dei prodotti informatici.

La visione di HP Inc.

La consapevolezza dei rischi cibernetici è ormai abbondantemente radicata, ma **le strategie di risposta risultano spesso essere concentrate quasi esclusivamente sul rafforzamento dei *software* di sicurezza e sulla protezione dei *data center*, sottovalutando la sicurezza a livello *hardware***. Le aziende si trovano oggi ad affrontare una serie innumerevole di minacce cibernetiche, che hanno come punto di accesso gli *endpoint device*, ovvero i dispositivi che si trovano in prima linea nel mondo iper connesso dell'IoT.

Dagli attacchi mirati alle frodi, dal *phishing* al *malware*, passando per il semplice *spam*, la lista dei pericoli è lunga e in continua evoluzione. Negli ultimi anni questa tendenza è stata particolarmente marcata per quanto riguarda gli attacchi ad *hardware* e *firmware* dei dispositivi. Questo tipo di minacce è rilevante in quanto dota l'*hacker* di capacità di controllo su tutto il *software* e il sistema operativo, oltre a una posizione privilegiata di invisibilità rispetto ai sistemi di protezione anti-*malware*. Ciononostante le componenti *hardware* e *firmware* dei dispositivi più comuni in case e uffici, quali PC e, soprattutto, stampanti vengono presi solo eccezionalmente in considerazione come oggetti da tutelare con maggior attenzione.

L'Agenzia per l'Italia Digitale (AgID) con la pubblicazione delle Misure Minime di Sicurezza ICT per le Pubbliche Amministrazioni ha sottolineato che in prima istanza, al fine di proteggere la sicurezza dei cittadini, occorre procedere alla redazione di un inventario di tutti i dispositivi connessi e assicurarsi che essi siano configurati secondo i più alti standard di sicurezza possibili. Da ciò si evince che **il ruolo dei *device*, in particolare PC e stampanti ritenuti punti di accesso privilegiati a differenti tipologie di *cyber* attacchi (il 71% dei *data breaches* comincia da un *device*[4]), diviene fondamentale.**

La maggior parte degli *information security officers* è ben consapevole della vulnerabilità di questo tipo di *device*, come si evince da un sondaggio del *Ponemon Institute*[5], e che la loro sicurezza richieda maggiori precauzioni di base.

Proteggere i dispositivi dagli attacchi cibernetici è divenuta una priorità che non può più essere procrastinata. **HP da tempo si sta impegnando per innalzare gli standard di sicurezza di *device*, quali PC e stampanti. Le soluzioni proposte mirano a garantire *hardware* sicuri anche attraverso**

[4] Idtheftcentre.org
[5] Ponemon Institute, *Annual Global IT Security Benchmark Tracking Study*, Marzo 2015.

il rafforzamento della capacità di rilevare tempestivamente violazioni dei dati a seguito di un *cyber* attacco e di recuperare gli stessi nel minor tempo possibile, ripristinando così uno stato di lavoro sicuro.

La visione di HP si basa su un principio fondamentale, che va oltre i semplici meccanismi di protezione: considerare le criticità legate alla sicurezza dei dispositivi come centrali sin dal momento della progettazione del *device* stesso (*security by design*) e non una volta che esso è stato realizzato. Questo consente alla nostra azienda di garantire standard di sicurezza unici per PC e stampanti di ultima generazione. In questo scenario, sono soprattutto i governi a essere esposti in prima linea alle minacce *cyber*, con l'evidente necessità di innalzare i livelli di sicurezza dei sistemi di governo e delle infrastrutture critiche nazionali.

HP ritiene pertanto che, nell'ottica di un innalzamento del livello di sicurezza cibernetica, sia assolutamente necessario garantire standard di sicurezza elevati dei *device*, oltre che dei *software*. Per tale ragione è auspicabile che nel processo di revisione del Codice dei Contratti Pubblici l'Esecutivo e il Legislatore prestino adeguata attenzione alla necessità di introdurre criteri *ad hoc* relativi a tale aspetto.

La revisione del Codice dei Contratti Pubblici: le raccomandazioni di HP

In premessa, HP intende esprimere il proprio favore in relazione all'indagine conoscitiva avviata in seno all'8ª Commissione del Senato sull'applicazione del Codice dei Contratti Pubblici.

Con riguardo al tema specifico del public procurement dei prodotti informatici, al fine di intervenire in modo proattivo sulle minacce informatiche rivolte all'intero sistema nazionale, pare **ineludibile l'avvio di iniziative volte a rendere i device utilizzati dalle Istituzioni italiane capaci di rispondere alle crescenti minacce cyber.** Ciò vale soprattutto nella fase attuale, caratterizzata da un una crescente percezione dei rischi *cyber* e da una maggiore produzione normativa e regolamentare in tema di *cybersecurity*.

Sulle base delle suddette considerazioni, paiono necessarie misure ulteriori alla pur opportuna modifica introdotta nel recente passato al Codice dell'amministrazione digitale che introduce il carattere vincolante del *parere obbligatorio dell'AgID sugli elementi essenziali delle procedure di gara bandite da Consip* e dai soggetti aggregatori, concernenti l'acquisizione di beni e servizi relativi a sistemi informativi automatizzati e definiti di carattere strategico.

In quest'ottica e in coerenza con le considerazioni che precedono, nel quadro della revisione normativa del Codice dei Contratti Pubblici, **HP Inc. manifesta le raccomandazioni che seguono sui criteri di aggiudicazione**:

1. **Art. 95.4: escludere il criterio del minor prezzo a garanzia della sicurezza delle reti e dei sistemi informativi nazionali.** Alla luce delle considerazioni espresse sul rilievo della sicurezza cibernetica nel contesto storico e geopolitico attuale, il Legislatore dovrebbe escludere per via normativa la possibilità di applicazione del criterio del minor prezzo (art. 95.4) nell'ambito di

procedure di gara relativi a prodotti le cui caratteristiche tecniche rilevino ai fini della sicurezza delle infrastrutture critiche nazionali.

2. Art. 95.6: stabilire requisiti di sicurezza in materia di appalti. Le politiche di sicurezza applicate dalle aziende devono andare di pari passo con quelle adottate dal Governo e viceversa, altrimenti quest'ultime non risulterebbero pienamente efficaci. Molti attacchi *cyber* puntano agli anelli deboli della catena, rappresentati proprio da dispositivi che presentano bassi standard di sicurezza.

   Le Istituzioni nazionali devono adottare il più alto grado di sicurezza dei *device*, oltre che dei *software*, contribuendo così ad aumentare qualitativamente e quantitativamente la sicurezza del Paese. Inoltre, l'innovazione ha reso il mondo del lavoro sempre meno statico, portando i *device* ad essere maggiormente usati al di là del perimetro dell'ufficio, pertanto in questo panorama le informazioni sensibili non possono essere protette se non vengono utilizzati dispositivi "sicuri".

   Si raccomanda dunque di stabilire requisiti minimi di sicurezza obbligatori in materia di appalti, introducendo fra i criteri oggettivi e qualitativi, sui quali declinare il criterio dell'offerta economicamente vantaggiosa (OEV), la sicurezza dei prodotti *hardware* e *software* oggetto di gara quando questi rilevino ai fini della sicurezza delle reti e dei sistemi informativi del Paese.

3. Art. 95.10bis: rispettare il tetto massimo stabilito per il punteggio economico. In premessa HP raccomanda che nel processo di revisione normativa del Codice sia mantenuto un tetto massimo per il punteggio economico.

   In coerenza con le proposte di modifica sopra espresse, occorrerebbe garantire un'effettiva applicazione del criterio dell'OEV, «*al fine di assicurare l'effettiva individuazione del miglior rapporto qualità/prezzo*», e della lettera normativa.

   Nel caso in cui la natura, l'oggetto e le caratteristiche del contratto consentano l'applicazione dei criteri elencati nell'art. 95.6, HP ritiene che il soggetto appaltante non debba attribuire al punteggio economico un valore superiore al limite stabilito per via legislativa.