Istruzioni operative

Tenuto conto dello stato dell'arte delle infrastrutture e della dotazione *hardware* e *software* delle Aziende del SSR, si dovranno prevedere interventi nei seguenti ambiti:

- **Postazioni di lavoro** - Con riferimento alla situazione del parco macchine ICT (PC, Server, periferiche) si evidenzia che una parte significativa delle Postazioni di lavoro utilizzate nelle Aziende del SSR è installato il sistema operativo *Windows Xp*, non più supportato da parte di *Microsoft* (esponendo l'ASUI di Udine a potenziali problemi di sicurezza informatica) e che pertanto è necessario predisporre un piano di sostituzione definendo le necessarie priorità. Il mercato offre oggi PC con processori compatibili solo con versioni di *Microsoft Windows 10* e non precedenti. Le Aziende, in sinergia con INSIEL S.p.A. ed in base alle azioni di rafforzamento dei software messe in atto dalla Società in house, stanno predisponendo i necessari piani di acquisizione e pianificazione di un *roll-out* del parco macchine per l'attivazione di PdL *Microsoft Windows 10* e *Internet Explorer 11*.
- ***Server*** - Azioni di adeguamento analoghe a quelle sopra descritte per le Postazioni di Lavoro si presentano anche per quanto riguarda i *Server*, per i quali si rende necessario l'adeguamento alle versioni più recenti dei Sistemi Operativi e dei software di base utilizzati.
- **Controllo degli accessi** – Un tema particolarmente importante concernente la sicurezza informatica, incluso nelle misure di sicurezza sopra citate, riguarda il controllo delle porte di accesso alla rete *LAN* e *WireLess* dell'Azienda finalizzata alla prevenzione di collegamenti con *device* non autorizzati che richiede l'implementazione di un sistema di autenticazione basato su standard *802.1x* con acquisizione e deploy di idonee tecnologie (hw e sw) e stesura di regolamenti comportamentali.
- ***Vulnerability Assessment* e *Vulnerability Scan*** – Le Aziende devono attivare delle azioni di *Vulnerability Assessment* e *Vulnerability Scan*, agendo in maniera non invasiva rispetto all'operatività *routinaria*, con l'obiettivo di identificare tutte le vulnerabilità potenziali note dei sistemi e delle applicazioni in uso. Individuate le vulnerabilità note dovranno essere mesi in atto i conseguenti piani di rimedio.
- ***Data Center*** – Ambito di indagine dei prossimi mesi da parte dell'AgID sono i *Data Center* Aziendali alla luce della circolare n. 05/2017 che prevede il censimento del patrimonio ICT delle Amministrazioni e la qualificazione dei Poli Strategici Nazionali al fine di individuare le infrastrutture candidate a ricoprire il ruolo di PSN o classificabili nelle categorie A – Data center di qualità non eleggibili a PSN, oppure con carenze strutturali o organizzative considerate minori – o B – Data center che non garantiscono requisiti minimi di affidabilità e sicurezza dal punto di vista infrastrutturale e/o organizzativo, o non garantiscono la continuità dei servizi. Allo stato dell'arte, motivi architetturali delle soluzioni in ambito SISSR, impongono alle Aziende del SSR di mantenere uno o più *Data Center* di prossimità/vani tecnici evoluti, che devono quindi essere messi in sicurezza per rispondere alle normative vigenti in ambito di sicurezza e protezione dei dati.
- **Infrastruttura** – Per ottemperare alle policy di sicurezza per il trattamento dei dati personali è necessario che le Aziende adeguino, laddove necessario, la propria infrastruttura informatica – nelle componenti attive e passive – con lo scopo di prevenire qualunque perdita, violazione e divulgazione illecita di dati sensibili. Oltre all'adozione di un appropriato sistema di controllo degli accessi, come sopra citato, è necessario adeguare gli apparati di rete e, ad esempio, intervenire con interventi di segmentazione della rete in modo che determinati oggetti siano su una sottorete separati rispetto a *host* critici, stabilire diversi livelli di criticità per i diversi segmenti di rete, mettendo in campo controlli d'accesso per passare dall'uno all'altro segmento; applicare politiche specifiche a dispositivi non autorizzati, ecc..

IL VICEPRESIDENTE

IL SEGRETARIO GENERALE