

ICT: ACCRESCERE SENSIBILITÀ ALLA SICUREZZA INFORMATICA NELLA P.A.

Il CNIPA ha compiuto la radiografia con il «1° Rapporto sulla sicurezza ICT nella PAC»

Roma, 12 nov. '07 – L'informatica nella Pubblica amministrazione centrale si sta sviluppando con buoni ritmi, ma con una sensibilità ancora inadeguata al delicato tema della sicurezza. Insomma, una sorta di 'gigante dai piedi di argilla'. È quanto emerge, tra luci e ombre, dal «1° Rapporto sulla sicurezza ICT nella PAC», elaborato dal CNIPA, il Centro Nazionale per l'Informatica nella Pubblica amministrazione, che al termine di una specifica indagine (basata su 49 quesiti e su 4 indicatori chiave) presso le Pubbliche amministrazioni centrali, ha predisposto un rapporto per favorire una presa di coscienza, una riflessione e soprattutto idonei interventi.

I motivi di preoccupazione riscontrati dagli esperti del CNIPA sulla base del check-up riguardano un'insufficiente attenzione di fondo al risvolto informatico per se stesso e più in particolare la scarsa attenzione all'adeguamento organizzativo necessario per garantire la sicurezza informatica.

«Il tema dell'analisi del rischio informatico è risultato piuttosto scoperto, a dispetto della grande rilevanza che questo tema ha avuto negli ultimi anni, soprattutto nel privato». A tale proposito il dossier del CNIPA segnala che «ben 10 Amministrazioni affermano che non hanno mai effettuato un'analisi dei rischi connessi alla sicurezza informatica».

Sul fronte della *sicurezza dell'organizzazione* il rapporto afferma che «si è riscontrata una propensione molto maggiore ad attuare piani per la sicurezza fisica e logica rispetto a dedicare energie per adeguare la propria organizzazione. È evidente, infatti, che una cattiva organizzazione interna può vanificare tutti gli sforzi spesi sul piano degli strumenti adottati, rappresentando inoltre una diseconomia».

Dai quesiti posti alle Amministrazioni centrali è risultato che metà di esse non ha una voce in bilancio dedicata alla sicurezza e, «in maniera ancor più preoccupante, il 61% del campione non ha mai approntato o previsto un piano di formazione volto a stimolare negli utenti dei sistemi informativi una maggiore sensibilità al tema della sicurezza ed una maggiore capacità di affrontare consapevolmente condizioni critiche».

Il CNIPA, che si è già dotato da anni di un'unità di prevenzione e supporto alla Pubblica amministrazione centrale per le problematiche connesse alla gestione degli attacchi e degli incidenti informatici, denominata Gov-CERT, ha accertato però anche aspetti positivi. Ad esempio, sul fronte della *sicurezza logica*, ben 32 amministrazioni, ossia il 65% del campione, si collocano in una posizione più che soddisfacente, dimostrando così un «andamento ottimale».

Positivi anche gli esiti del monitoraggio della *sicurezza delle infrastrutture*, dove sono stati rilevati «risultati molto incoraggianti», soprattutto per quanto riguarda la sicurezza perimetrale, quella del controllo degli accessi fisici e le reti in genere, «investendo coerentemente sforzi e risorse». Anche se non mancano amministrazioni che hanno ammesso di «non utilizzare alcuna protezione nella connessione alla rete pubblica» e, per quanto riguarda quelle wireless, sono emerse «alcune reti protette da sistemi inadeguati».

. 2 .

Per quanto attiene alla *sicurezza dei servizi*, il check-up del CNIPA ha riscontrato «una sostanziale disomogeneità». Addirittura «i dati peggiori sono stati ottenuti sul tema della continuità operativa, evidentemente non ancora avvertito come fattore cruciale per la robustezza dell'intero impianto e per la qualità dell'intero impianto e per la qualità dei servizi offerti».

Non solo. «I risultati sono stati altrettanto scadenti per quanto attiene alla capacità delle Amministrazioni di rilevare intrusioni o attacchi, attività certamente inevitabile per qualsiasi sistema connesso ad internet per prendere le necessarie contromisure ed evitare accessi non autorizzati».

Il dossier del CNIPA pone «l'esigenza di avviare una serie di iniziative volte ad aumentare la sensibilità delle Amministrazioni su tutti gli obiettivi e ad individuare misure opportune per aumentare la robustezza e la sicurezza dei servizi erogati».

La radiografia pone una serie di esigenze e sollecita azioni per superare le criticità specifiche intervenendo sulle loro cause. Tra l'altro si rileva che «sul piano dell'organizzazione intera rimangono ancora disattese le norme emanate da tempo e che in generale la cultura della sicurezza è rimasta appannaggio degli addetti ai lavori, ma i piani di formazione e sensibilizzazione sul tema sono ancora poco diffusi, mentre è auspicio di tutti che queste iniziative possano avere la massima diffusione raggiungendo tutti gli utenti anche in periferie remote».

Un'annotazione di rilievo è relativa all'evoluzione del quadro complessivo rispetto al passato: «la tendenza sostanzialmente positiva intrapresa negli ultimi anni dalla Pubblica amministrazione rispetto al tema della sicurezza informatica» e, proprio alla luce delle criticità evidenziate dall'analisi, già 8 amministrazioni hanno reso nota la loro intenzione di dotarsi di un sistema di *disaster recovery* ed alcune di esse, tra le più importanti ai fini dei servizi a cittadini e imprese, hanno già realizzato servizi comuni di *disaster recovery*, individuando finanziamenti e strategie verso soluzioni più moderne di continuità operativa.

A tale proposito già alcuni enti previdenziali e assistenziali pubblici, che offrono fondamentali servizi ai cittadini ed alle imprese, hanno investito risorse e in collaborazione con il CNIPA hanno realizzato un Centro Unico di Back-up per assicurarsi servizi comuni di *disaster recovery* e garantirsi una continuità operativa.

Infine, è emerso che «molte Amministrazioni hanno già emesso o intendono dotarsi di un documento per le politiche di sicurezza delle infrastrutture telematiche attraverso cui diffondere norme interne relative alla sicurezza dei sistemi informativi. Su questo punto», conclude il rapporto del CNIPA, «si intuisce la necessità di individuare un blocco di norme comuni a tutte le Amministrazioni, scritte in base ad un modello condiviso e indipendente dalle dimensioni e dalle funzioni dell'Ente. Questo potrebbe da un lato ridurre gli sforzi mettendo a fattor comune le esperienze interne già disponibili; dall'altro garantirebbe una possibilità concreta di successo ad un processo così delicato». -

- Nel sito: www.cnipa.gov.it si può scaricare il testo integrale del Rapporto, in formato .pdf

Il CNIPA-Centro Nazionale per l'Informatica nella Pubblica Amministrazione opera presso la Presidenza del Consiglio dei Ministri per l'attuazione delle politiche del Ministro per le Riforme e le Innovazioni nella Pubblica Amministrazione ed ha l'obiettivo di dare supporto alla Pubblica amministrazione nell'utilizzo efficace dell'informatica per migliorare la qualità dei servizi e contenere i costi dell'azione amministrativa.