CONFERENZA DELLE REGIONI
E DELLE PROVINCE AUTONOME

21/140/CR01/C14

POSIZIONE SUL TEMA DELLA CYBERSICUREZZA

Punto 1) Odg Conferenza delle Regioni e delle Province autonome

L'impatto delle nuove tecnologie su ogni aspetto della società richiede, come dimostrato in tempo pandemico e dai recenti eventi hacker, uno sforzo aggiuntivo da parte del Governo centrale e delle Regioni e delle Province Autonome per far sì che, oltre a salvaguardare il patrimonio informativo degli enti e degli utenti in rete, si possa anche garantire la continuità dei servizi pubblici e la competitività delle imprese in un mondo digitale. La cybersecurity, infatti, rappresenta un elemento fondamentale per uno sviluppo integrato e sostenibile dell'economia e di sanità/sociale, rappresentando un fattore fondamentale per lo sviluppo e la crescita del Paese.

Le esperienze di sicurezza informatica delle Regioni devono essere messe a sistema, e fare del sistema inter-regionale un punto di forza per il Paese, che sia in grado di collaborare con la nuova Agenzia nazionale di cybersicurezza quale interlocutore unico in materia di sicurezza informatica.

In base a quanto detto, si formulano le seguenti proposte per azioni urgenti:

1. Un sistema centralizzato non può rispondere a tutte le esigenze di sicurezza informatica, che resta una problematica distribuita anche in presenza di una compiuta migrazione al cloud. Il ruolo delle Regioni deve essere forte in relazione alla tutela dei dati e dei servizi pubblici che eroga con le sue articolazioni dirette (agenzie, in house ed aziende sanitarie) ed anche a supporto degli enti locali del proprio territorio. Un unico punto centrale rischia di essere sottoposto a maggiori rischi di attacco. Serve una forte Agenzia centrale unita ad una rete regionale di nuclei di risposta alle emergenze cyber con ruolo proattivo.

   Di conseguenza, il PNRR sul tema della cybersicurezza non può prevedere unicamente investimenti a livello centrale. È essenziale ci siano finanziamenti in favore delle regioni, in particolare per il reclutamento di profili professionali informatici legati alla trasformazione digitale, alla cybersicurezza e ai dati. Vanno previsti specifici finanziamenti e specifici profili professionali insieme a semplificate modalità di reclutamento, perché non è possibile aspettare il 2024 o 2026 per contromisure che sono da attuare con urgenza sui sistemi attuali.

   Le Regioni e Province autonome hanno fatto ingenti investimenti con i fondi strutturali in infrastrutture digitali, che possono essere messe utilmente a sistema nel PSN polo/cloud nazionale, ma è urgente accrescere le competenze interne alle regioni e alle loro in house per agire subito sul fronte della sicurezza dei sistemi attuali ed anche per accompagnare il percorso verso il cloud in maniera altrettanto sicura. Serve una committenza qualificata dentro gli enti per progettare le azioni ed attivare gli investimenti giusti.

2. Accanto al potenziamento del personale informatico degli enti, occorre avviare con urgenza un piano di formazione nazionale per le competenze sui temi della sicurezza informatica e della privacy, rivolto a tutti i dipendenti delle PA di profilo non informatico che devono comunque fare la loro parte per contribuire alla sicurezza complessiva dei servizi pubblici e alla protezione dei dati personali e non.

3. Stiamo attivando una Task force inter-regionale sulla cybersicurezza, quale gruppo di lavoro tecnico permanente tra le Regioni e Province autonome, per la condivisione delle esperienze e delle buone pratiche, che possa fornire risposte immediate, dialogare con il Garante della privacy e con le strutture centrali competenti nonché formulare proposte da presentare al Governo, in particolare sulla rete dei CERT regionali. Appare evidente la necessità di arrivare a costituire nuclei operativi di risposta alle emergenze cyber su scala di aggregazione regionale.

4. Come è noto, la Conferenza Unificata ha espresso parere favorevole sul decreto-legge 14 giugno 2021, n. 82, istitutivo, tra l'altro, dell'Agenzia per la Cybersicurezza con alcune raccomandazioni che devono essere riproposte all'attenzione del Governo soprattutto alla luce di quanto accaduto e che, pertanto, si riportano in allegato**.**

5. È urgente il coinvolgimento delle Regioni per la definizione di una strategia sulla cybersicurezza dei servizi pubblici e dei relativi dati personali e non, strategia da definire sia nel breve periodo che nel medio-lungo periodo.

Roma, 4 agosto 2021