Leonardo Scalera - Intervista al Forum ICT Security 2018

Author : Redazione

Date : 14 novembre 2018

Leonardo Scalera

Data Protection Officer presso Ministero della Giustizia

Molti purtroppo, sia nel pubblico sia nel privato, hanno considerato l'entrata in piena operativa del GDPR come un punto di inizio e non come quello di arrivo della normativa dopo due anni di preparazione. Non è stato un problema solo italiano anche se il nostro paese a maggio aveva delle percentuali di compliance nel privato sotto il 40% e nel pubblico sotto il 20%. Sia la preparazione al GDPR sia la risposta alle eventuali violazioni alle sue norme necessita grandi risorse sia economiche, sia tecnologiche sia di personale che nel caso deve essere formato ma da questo punto di vista la PA è in una situazione di assoluto ritardo.

Negli ultimi anni il cyber crime ha avuto un'impennata dettata dall'aumento dei soggetti esposti sulla rete; c'è quindi una maggiore disponibilità di dati. I settori più a rischio sono quelli i cui dati possono essere "più remunerativi" nel deep web, si pensi all'ambito sanitario, a quello farmaceutico, a quello finanziario ed alla grande industria. Nel settore privato c'è la necessità di dare un valore al dato che si tratta, fare una valutazione del rischio ed eventualmente mitigarlo per farlo rientrare in parametri accettabili, le aziende devono investire, e lo stanno, facendo, in infrastrutture tecnologiche nella sicurezza e nella formazione come dimostra l'ultimo rapporto dello IATP in collaborazione con Ernst & Young.

In alcuni casi la PA può raggiungere un livello di sicurezza accettabile, ci sono amministrazioni centrali o agenzie che ricevono ancora le opportune dotazioni, si pensi ad esempio all'Agenzia delle Entrate; ci sono parti della PA che, avendone la disponibilità economica ma non le risorse umane necessarie, ad esempio stanno cercando con appositi bandi dei DPO esterni, ma quello del personale specializzato è uno dei problemi della PA.

Esternalizzare la sicurezza comporta ovviamente dei rischi ma in quel caso bisognerebbe attuare una meticolosa sorveglianza degli appalti per trovare questi soggetti esterni che sicuramente dovrebbe poi essere costantemente monitorati tramite un'interazione pubblico/privato.

Domande:

1. A quasi 6 mesi dall'entrata in piena operatività del GDPR europeo qual è la percezione sui punti maggiormente rilevanti, nuovi obblighi, nuovi diritti, DPO, Data breach, da parte del settore sia privato che pubblico?
2. Le tendenze del cybercrime rilevate nel 2018 e la loro proiezione confermano il costante aumento degli attacchi (con conseguenti Data breach) in molti settori dell'industria privata, ma anche nel settore pubblico; alla luce della nuova normativa come (quantomeno provare) a proteggersi o come reagire in caso di attacco?
3. Considerate queste carenze e l'attuale panorama normativo (GDPR, D.lgs 196 novellato dal D.lgs 101/18, Direttiva NIS) con gli obblighi che ne derivano ritiene che la PA italiana sia in grado di raggiungere livelli accettabili di "sicurezza" con riferimento alla protezione dati, ai processi di trattamento/custodia/archiviazione, alle infrastrutture di rete?
4. Lei ha parlato di talune amministrazioni o realtà statali che potrebbero accedere ad un budget sufficiente per esternalizzare per appaltare la sicurezza. Non vede dei rischi in questo?