

La fotografia dell'Osservatorio Politecnico di Milano. Pmi, Centro e Sud ancora indietro

Privacy e cyber security, metà delle imprese investe e si adegua

Pagine a cura
DI SILVANA SATURNO

Imprese italiane più attente alla protezione informatica dei dati e più consapevoli delle nuove norme sulla tutela della privacy che saranno pienamente applicabili dal prossimo 25 maggio (regolamento europeo 679/2016: cosiddetto «Gdpr», acronimo di «General data protection Regulation»).

In un anno (dal 2016 al 2017) l'attenzione delle aziende è decisamente cresciuta, se si considera che oggi almeno in un'impresa su due è in corso un progetto strutturato di adeguamento alla nuova regolamentazione europea (si tratta del 51% delle aziende, mentre l'anno scorso la percentuale era di appena il 9%) e un altro 34% delle imprese sta analizzando in dettaglio requisiti di legge e piani di attuazione.

E quanto emerge dalla ricerca realizzata dall'Osservatorio Information Security & privacy della School of management del Politecnico di Milano presentata martedì scorso in un convegno nel capoluogo lombardo.

La ricerca è stata realizzata attraverso un sondaggio rivolto a 1.107 manager (Ciso, Cso e Cio), un'indagine rivolta a risk manager e chief risk officer di 106 organizzazioni italiane e un'ulteriore indagine su 313 professionisti del settore sul tema data protection.

In base all'analisi, nel 2017 è arrivata al 58% la percentuale di aziende che ora ha un budget dedicato all'adeguamento al nuovo regolamento Gdpr sulla privacy (lo scorso anno era al 15%).

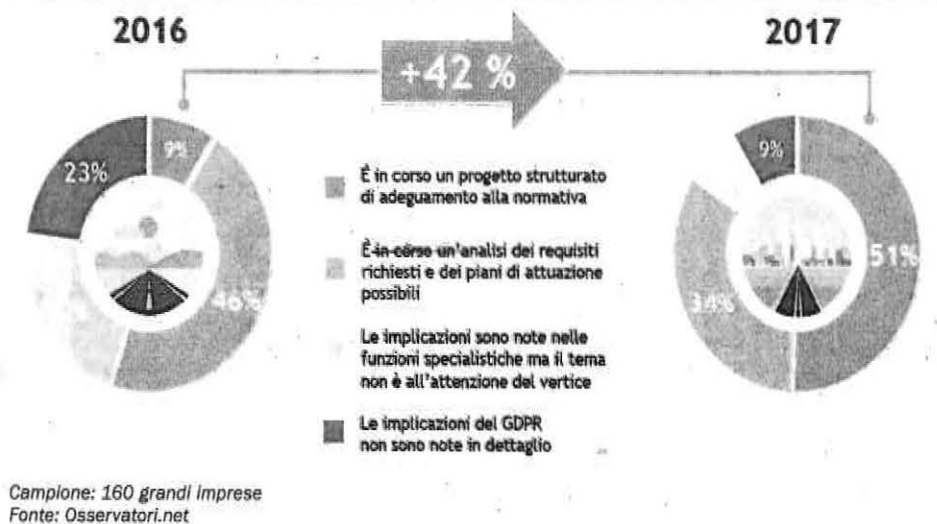
Tuttavia è ancora molto ampia la fetta di organizzazioni che non ha un budget ad hoc (il 42%). All'interno di questa fetta c'è un 23% di soggetti che prevede di stanziare le risorse nel corso dei prossimi sei mesi.

La necessità, sempre più vicina, di adeguarsi al «Gdpr» ha peraltro fatto da traino per la sicurezza informatica aziendale in generale: nel 2017 il mercato delle soluzioni di «information security» ha raggiunto il valore di 1,09 miliardi di euro, con un aumento del 12% rispetto all'anno precedente.

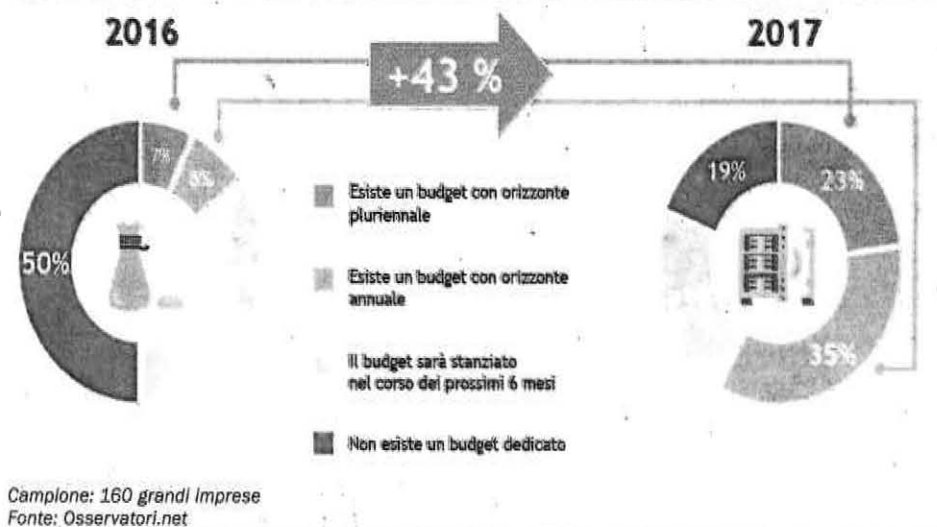
Questa accresciuta attenzione è da attribuire, comunque, prevalentemente all'azione delle grandi imprese (il 78% del totale).

Solo il 22% delle aziende che hanno investito in sicurezza informatica, infatti, è rappresentato da piccole e medie imprese (pmi), che restano ferme, in particolare le piccole, a strumenti basic di protezione e

Gdpr, cresce la consapevolezza delle aziende



Le risorse dedicate al Gdpr



per la gran parte sono prive di una figura ad hoc responsabile della cyber security in azienda (il 70% ancora non ce l'ha; per chi ce l'ha, nella maggior parte dei casi si tratta dell'imprenditore stesso o del direttore generale).

E se la sicurezza informatica è ancora «roba da grandi», purtroppo è anche roba, fin qui, prevalentemente da imprese del Nord Italia: a utilizzare soluzioni di «information security» è stato infatti il 40% delle imprese del Nordovest e il 30% di quelle del Nordest, contro il 19% delle aziende del Centro, e appena il 15% di quelle del Sud.

«Nonostante le minacce aumentino, l'evoluzione del mercato restituisce un quadro tutto sommato ottimistico», ha commentato **Gabriele Faggioli**, responsabile scientifico dell'Osservatorio Information Security & Privacy del Politecnico di Milano, «nelle aziende

italiane cresce la consapevolezza dell'importanza della gestione della sicurezza e della privacy, mentre aumentano i budget stanziati. La figura del chief information security officer (manager responsabile

Nel 2017 è arrivata al 58% la percentuale di aziende che hanno un budget dedicato all'adeguamento al nuovo regolamento Gdpr sulla privacy. Tuttavia è ancora molto ampia la fetta di organizzazioni che non ha un budget ad hoc (il 42%)

della sicurezza informatica, ndr) sta acquisendo maggior rilevanza rispetto al passato e si assiste a una progressiva strutturazione delle funzioni preposte alla gestione della sicurezza».

«Il 2017 si è rivelato un anno di svolta per la gestione della sicurezza e della privacy in Italia», ha sottolineato

Alessandro Piva, direttore dell'Osservatorio Information Security & Privacy, «gli investimenti aumentano in modo consistente, grazie anche alla spinta del Gdpr».

Le nuove regole Ue per la privacy (Gdpr). Mancano poco più di tre mesi alla piena operatività del regolamento 679/2016 (il regolamento è entrato in vigore il 24 maggio 2016 e diventerà direttamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018); provvedimento che, come si legge sulla Guida pratica messa a disposizione dal Garante della privacy sul proprio sito, porterà significative innovazioni per cittadini, aziende, enti, associazioni e liberi professionisti.

Sinteticamente, il regolamento contiene nuovi diritti e garanzie per le persone fisiche

e maggiori responsabilità per chi «tratta» i dati personali (enti, imprese). In particolare si prevedono: una maggiore chiarezza su informativa e consenso al trattamento dei dati, criteri più rigidi per il trasferimento dei dati al di fuori dell'Ue e per i casi di violazione di dati personali («data breach»), limiti al trattamento automatizzato dei dati e alla profilazione, l'introduzione del diritto all'oblio (diritto a ottenere la cancellazione dei propri dati personali anche on line da parte del titolare del trattamento), il diritto alla portabilità dei dati.

Imprese ed enti, come accennato, avranno, dal 25 maggio, corrispondenti nuovi oneri e responsabilità; in caso di violazioni di legge, scatteranno sanzioni salate. Sono previste semplificazioni degli adempimenti, con particolare riguardo ai soggetti più responsabili e collaborativi anche in termini di autoregolamentazione.

Secondo la ricerca dell'Osservatorio del Politecnico di Milano, oggi soltanto l'8% delle imprese, contro il 23% di un anno fa, ha una «scarsa conoscenza» delle implicazioni nelle nuove regole Ue sulla privacy.

«Sull'adeguamento al Gdpr emerge un sostanziale cambio di marcia», spiega Faggioli, «con buona parte delle imprese che ha avviato da tempo importanti progetti di adeguamento al Gdpr. Il fatto che 3/4 delle aziende abbiano iniziato a stendere politiche di sicurezza e valutazione dei rischi», prosegue, «significa aver coinvolto le giuste competenze e aver preso coscienza della problematica. Nei prossimi mesi è probabile che gli investimenti aumentino e si spostino dai progetti di adeguamento al Gdpr a iniziative di mantenimento dell'adattamento normativo, come l'analisi dei rischi su nuovi trattamenti e la verifica dell'impatto della protezione dei dati».

Le principali azioni in corso o già realizzate dalle aziende per adeguarsi al «Gdpr» riguardano la valutazione dell'adeguamento (87%), l'individuazione di ruoli e responsabilità (80%), la stesura o la modifica della documentazione (77%), la definizione delle politiche di sicurezza e valutazione dei rischi (77%), la creazione e l'aggiornamento del registro dei trattamenti (74%), la valutazione di impatto sulla protezione dei dati personali (57%), la procedura di infiltrazione dei dati (53%) e il servizio di Data protection officer (50%).