Perdita di dati: nel 43% dei casi la colpa è dei dipendenti

By **Redazione LineaEDP**

Nonostante le aziende investano in tecnologie avanzate, non mettono a disposizione budget per assumere o formare personale competente

Quando il sistema informatico aziendale va improvvisamente in tilt o certi dati risultano inspiegabilmente spariti dai server, il primo pensiero va ad un attacco hacker o a un virus. Ma non è sempre colpa dei pirati informatici, anzi molte volte per trovare la causa del problema non c'è bisogno di cercare troppo lontano, e spesso il guaio è provocato da manovre maldestre degli stessi dipendenti che dovrebbero proteggere il patrimonio dei dati.

Secondo un recente studio di Intel Security il **43% dei furti di dati è da imputarsi ai dipendenti**, e nella metà dei casi le cause sono addirittura fortuite. A spiegarlo, è il Generale **Umberto Rapetto**, già comandante del Nucleo Speciale Frodi Telematiche della Guardia di Finanza, che affronterà questa tematica al 6° Privacy Day Forum il 13 ottobre a Roma: "*Volontarietà e accidentalità vanno a fondersi in una sostanziale inaffidabilità del personale impiegato, imponendo anche ai più scettici di adottare iniziative organizzative, regolamentari e tecniche per arginare un rischio che può rivelarsi addirittura catastrofico. Spesso si affronta l'argomento solo a cose fatte, quando un evento nocivo ha avuto luogo e si rende necessario individuarne il responsabile, quando è tardi e si perde ancor più tempo per capire cosa fare e a chi rivolgersi per farlo*".

Oltre alle ripercussioni che un incidente informatico può avere all'interno dell'azienda, impiegare personale inadeguato per gestire i dati personali può produrre effetti devastanti anche sul piano normativo ed economico, come afferma il presidente di Federprivacy, **Nicola Bernardi**: "*Anche se le aziende investono in tecnologie avanzate, paradossalmente non mettono poi a disposizione sufficienti budget per assumere o formare personale competente in grado di gestire in modo efficiente e sicuro gli enormi flussi di dati personali che trattano con le proprie infrastrutture, esponendosi a pericoli di data breach da cui possono derivare paralisi delle attività, danni reputazionali, e pesantissime sanzioni del Garante della Privacy. Con il nuovo Regolamento UE, le imprese dovranno infatti notificare le violazioni all'Authority, che potrà comminare multe fino a 20 milioni di euro o al 4% del fatturato, e nei casi più gravi dovranno essere informati anche gli stessi interessati, con l'inevitabile esposizione alla gogna mediatica*".

Le aziende che si dotano di tecnologie avanzate, devono quindi correre ai ripari avvalendosi anche di adeguate misure tecniche ed organizzative per prevenire veri e propri disastri informatici, investendo in risorse umane qualificate e nella loro formazione, ricorrendo inoltre a strumenti efficaci come ad esempio la certificazione ISO/IEC 27001:2013, norma che fornisce una serie di requisiti e standard sulla sicurezza delle informazioni, utile anche ai fini della compliance al nuovo Regolamento Privacy UE, a cui le imprese devono adeguarsi entro il 25 maggio 2018.