



MERCATO

SICUREZZA DOCUMENTI



Gestione documentale e sicurezza: cosa fare

Studi e ricerche trattano l'importante tema della gestione dei documenti contenenti dati sensibili. I risultati denotano come ci sia ancora bisogno di consolidare le corrette pratiche di sicurezza

Un tema di cui si parla, ma non abbastanza, è quello della corretta gestione dei documenti contenenti dati sensibili. Persone e aziende sono consapevoli dei rischi, e attuano le giuste misure cautelari? Presentiamo i risultati di una ricerca condotta su singoli individui da Adiconsum e Fellowes Leonardi. Risultato: alcune buone pratiche sono già di uso comune, ma molto rimane da fare, soprattutto riguardo la sicurezza in rete.

DATI SENSIBILI E FURTO D'IDENTITÀ

Uno dei reati più gravi connessi alla cattiva gestione dei documenti e dei dati sensibili è il furto d'identità, che consiste nell'ottenere indebitamente le informazioni personali di un soggetto al fine di sostituirsi in tutto o in parte ad esso e compiere azioni illecite in suo nome, o ottenere credito tramite false credenziali.

Dai risultati di una ricerca svolta in collaborazione tra Adiconsum, l'associazione italiana difesa consumatori e ambiente promossa dalla CISL, e Fellowes Leonardi, azienda internazionale leader nella produzione di distruggidocumenti, emerge come le frodi più frequenti siano quelle derivanti da furto o smarrimento di documenti d'identità, utilizzati da chi se ne appropria indebitamente per fare acquisti o sottoscrivere contratti: la percentuale, comunque alta, è però in lieve calo (40,2% stando ai dati 2010, contro un 53,5% del 2009). Risulta in aumento la tecnica di reperire i dati fra i rifiuti di documenti personali, bancari, bollette o modelli fiscali da cui estrarre i dati necessari; pratica facilitata, tra l'altro, dall'uso della raccolta differenziata.

QUALI STRATEGIE PER DIFENDERSI?

Alcune azioni di tutela personale dei propri dati sono in aumento: distruzione dei documenti contenenti dati sensibili prima di cestinarli (si è passati da uno scarso 14% del 2009 a ben il 58,5% del 2010), custodia in luoghi sicuri di PIN e codici (69% nel 2009, 78,6% nel 2010), controllo periodico del proprio estratto conto per verificare anomalie (dal 60% del 2009 al 72,8% del 2010), la copertura della



tastiera quando si digita il PIN (57% nel 2009, 67,9% nel 2010), richiesta del servizio sms per sapere quando viene effettuata una transazione con la propria carta di credito (dal 50% del 2009 al 54,8% del 2010).

PROTEZIONE ONLINE NON SUFFICIENTE

Ancora molti passi da fare per quanto riguarda la protezione online: solo il 51,6% delle persone intervistate utilizza firewall, antivirus, antispam per proteggere il proprio computer, un dato in netto calo dal 2009 al 2010. Ancora molto scarsa la percentuale di chi usa memoria esterna per conservare documenti sensibili o riservati (comunque in leggero aumento, dal 29% del 2009 al 30,6% del 2010). Piuttosto bassa anche la percentuale

di chi ha cura di non salvare sul proprio computer password o indirizzi mail che permettano l'accesso a social network e forum ma anche a conti online: solo il 55,5% del 2010, basso anche se in leggero aumento rispetto al 51% del 2009, dichiara di cautelarsi contro questa evenienza. Mentre c'è un'alta percentuale di chi ritiene altissimo il bisogno di essere informati sul furto d'identità, rimane ancora scarso il numero di persone che se ne preoccupa: il 25% ha dichiarato di essere preoccupato poco o per niente dal furto d'identità.

Il parere di Quocirca

Louella Fernandes della società di analisi Quocirca, che nel 2011 ha condotto una ricerca sulla gestione nelle aziende della sicurezza documentale, commenta: "La nostra ricerca dimostra come l'efficienza dei processi documentali e la protezione delle informazioni siano obiettivi ancora lontani. Considerata l'importanza dei documenti all'interno delle organizzazioni, la questione della sicurezza non può più essere ignorata. Questo implica un approccio globale che si basa su tecnologie, su policy, ma anche sulla formazione degli utenti. Le aziende dovrebbero scegliere fornitori che garantiscano questo approccio e dimostrino di operare secondo elevati standard di sicurezza".