di Lucia Ingrosso, l.ingrosso@millionaire.it

PRIVACY

PROTEZIONE DEI DATI

CYBERSECURITY

NUOVO BUSINESS

IN ARRIVO UNA NUOVA LEGGE A LIVELLO EUROPEO. MULTE PER CHI NON SI ADEGUA. OPPORTUNITÀ PER CHI OFFRE PRODOTTI E SERVIZI *AD HOC*

50% (e oltre) delle organizzazioni mondiali ha subito un cyberattacco nell'ultimo anno.

+126% l'aumento degli attacchi di cyberspionaggio.

72 le ore entro le quali bisogna riferire al Garante le violazioni dei dati.

4.530 euro, spesa media per prevenire attacchi delle imprese italiane (19mila per le imprese Ict e 44mila per le multinazionali).

UN CLIC E I DATI DI 143 MILIONI DI AMERICANI SONO FINITI IN MANO AGLI HACKER.

È successo a metà 2017, quando è stato violato il sito di Equifax, società Usa di valutazione del credito. Un caso clamoroso, ma non il primo né l'ultimo. Per non parlare del *deep web* (o *dark web*), dove tutto è in vendita al miglior offerente: foto personali, documenti riservati, dati sensibili... «Due punti fermi: la privacy non esiste e nulla in Rete può essere definito sicuro. Nel 2018 si adotterà un approccio *security-first thinking*: non si aspetterà che un attacco si verifichi, ma si farà in modo di prevenirlo» spiegano da Venustech, azienda cinese specializzata in sicurezza della Rete (www.venusense.com). America, Cina... e in Europa? *Privacy day*: la data si avvicina. Il 25 maggio sarà pienamente operativo il Regolamento generale sulla protezione dei dati (*General data protection regulation*, Gdpr) o nuovo Regolamento Ue 2016/679. Presentato dalla Commissione europea nel gennaio 2012, ha registrato oltre 4mila emendamenti.

IL PRINCIPIO BASE. È l'*accountability*: il titolare dei dati è responsabile della loro gestione e li deve custodire come fossero un bene che gli è stato affidato. Non solo, in caso di problemi dovrà dimostrare di aver fatto tutto il possibile per limitare i rischi della perdita dei dati, producendo la documentazione in grado di attestarlo. Da maggio, l'applicazione del Gdpr diventerà pienamente operativa. Tutti pronti? Pare di no, almeno secondo un'indagine condotta da NetApp (www.netapp.it). Il 70% dei manager europei ritiene che le aziende non abbiano ancora le idee chiare sui pericoli in agguato e gli interventi da fare. E chi non si adegua? Si rischiano multe fino a 20 milioni di euro o il 4% del fatturato mondiale annuo. Del resto, stare al passo con le minacce non è facile. Gli attacchi a obiettivi multipli sono cresciuti del 253% nell'ultimo anno. Il settore della cybersecurity cresce al ritmo del 12% all'anno e, secondo lo studio Pmr (www.persistencemarketresearch.com), nel 2025 avrà un valore di 205 miliardi di dollari. La corretta gestione dei dati riguarda l'aspetto della sicurezza,

45MILA
il fabbisogno di nuovi Dpo in Italia.

77MILA
dollari, stipendio annuo di un Dpo negli Usa.

360MILA
i file dannosi rilevati al giorno (+11,5% rispetto all'anno prima).

10MILA
euro al massimo, il danno subito, nella maggior parte dei casi in Italia.

200MILA
euro, il danno subito dallo 0,1% delle imprese colpite.

ma non solo. «Quello che viene richiesto alle aziende è prima di tutto un cambio di mentalità. Finora di privacy ci si occupava in modo sporadico. D'ora in poi, serviranno un nuovo modello organizzativo e una gestione più capillare e coinvolgente» spiega Paolo Balboni, fondatore di ICT Legal Consulting, studio legale internazionale specializzato nei settori della tecnologia dell'informazione, della privacy e della protezione dei dati (www.ictlegalconsulting.com). E prosegue: «Al di là degli obblighi burocratici, c'è una sfida da cogliere. L'uso che valorizza i dati in modo corretto ed etico è fondamentale, perché può produrre un vantaggio competitivo e un ritorno sull'investimento: l'esperienza insegna che, al contrario, un uso aggressivo e penalizzante per i consumatori dei dati personali può causare sfiducia da parte dei clienti e perdite di quote di mercato». Finora, il riferimento è quello del Decreto legislativo 196 del 2003. A chi è già in regola, basteranno piccoli aggiustamenti. Per gli altri? Settimane di lavoro di un professionista dedicato. E l'adozione di nuove pratiche di controllo e sicurezza.

CHE COSA FARE

«Il regolamento chiede ai gestori delle informazioni in ambito pubblico e privato di conoscere la propria realtà dal punto di vista delle risorse informative, valutare attentamente i rischi, graduare il tipo di risposte, avere un controllo indipendente al proprio interno attraverso la figura del *data protection officer*. Infine, in caso di intervento dell'autorità di garanzia e della magistratura, bisogna dimostrare gli adempimenti fatti» spiega Giovanni Buttarelli, garante europeo della privacy. Banalizzando, ogni azienda deve essere in grado di rispondere a semplici domande come: «Quando avete raccolto il mio consenso all'invio delle vostre email promozionali?», «Chi in azienda ha accesso ai miei dati?».

In pratica

- Procurarsi raccoglitori capienti.
- Fare ordine fra i dati presenti sui vari *device* e reti. Creare gruppi e sottogruppi, eliminare doppioni.
- Nominare le persone abilitate a gestire i dati.
- Compilare un registro che identifichi i dati e la finalità del loro trattamento.
- Studiare una strategia per proteggere i dati.
- Scrivere un regolamento interno per diffondere l'idea che i dati sono importanti e bisogna trattarli con cura.
- Attivare procedure periodiche di controllo per mantenere la gestione dei dati, allineata con l'innovazione tecnologica.
- Sistemi di videosorveglianza, localizzatori satellitari e call center richiedono comportamenti *ad hoc*.

NASCE UNA NUOVA PROFESSIONE: IL *DATA PROTECTION OFFICER*

In azienda ci sono già figure dedicate alla privacy. Il titolare di trattamento dei dati si occupa delle modalità di trattamento dei dati, compreso il profilo della sicurezza. Sempre suo il compito di comunicare con gli interessati (le persone fisiche a cui si riferiscono i dati personali) e l'autorità di riferimento, cioè il Garante della privacy. A utilizzare e trattare i dati è invece il responsabile del trattamento dei dati, figura che va nominata per iscritto. Ora si affaccia la nuova figura del *data protection officer* (Dpo). I suoi compiti? Informare e fornire consulenza al titolare del trattamento, sorvegliare l'osservanza delle norme, fornire pareri e cooperare col Garante e le autorità. Per

570 MILIONI
di euro, il valore del settore della difesa cyber nelle imprese italiane con più di 20 dipendenti.

76,4 MILIARDI
di dollari, valore dell'intero settore della cybersecurity.

205 MILIARDI
di dollari, valore del settore previsto nel 2025.

Fonti: Banca d'Italia, Clusit, Federprivacy, Kaspersy Lab, Pmr.

saperne di più ci siamo rivolti a Nicola Bernardi, presidente di Federprivacy, associazione di categoria nata nel 2008, che oggi conta quasi 2.000 soci, 6.700 iscritti e 15.000 lettori della newsletter (www.federprivacy.it).

Quali sono le opportunità create dalla nuova normativa? «La presenza di un Dpo è obbligatoria in tutte le amministrazioni pubbliche, che ammontano a 20mila, in tutte le organizzazioni che trattano su larga scala dati sensibili (es. ospedali, laboratori di analisi, compagnie assicurative…), in tutte le organizzazioni che profilano il consumatore su larga scala (pensiamo ai supermercati con le carte fedeltà). Nelle altre, la presenza di un Dpo è solo consigliata. Dal nostro osservatorio, stimiamo il fabbisogno di 45mila professionisti».

Requisiti di questa nuova figura? «Non esistono né abilitazioni né un albo. Contano le competenze (giuridiche, tecniche e manageriali) e l'esperienza nel settore».

Come si diventa. Federprivacy organizza un corso intensivo da *privacy officer*, della durata di sei giornate (48 ore): un'edizione al mese, 1.500 euro, nelle sedi di Milano, Roma e Reggio Emilia. I Dpo con almeno due anni di esperienza possono poi certificarsi presso Tüv (www.tuv.it) al costo di 350 euro (dal secondo anno, quota annuale di 150).

E i guadagni? «Negli Usa i *privacy officer* guadagnano 77mila dollari all'anno (65mila euro). In Italia si parte da chi fa collezione di nomine, chiedendo 1.000 euro al mese alle aziende, in genere piccole, per cui presta il suo servizio part time».

Il rischio? Non essere all'altezza del compito, anche perché, in caso di problemi, il Garante richiede una reperibilità immediata. Di certo il Dpo non può essere l'it manager, con cui rischia di entrare in conflitto. E l'ideale sarebbe se fosse un manager, con uno stipendio da 100mila euro annui lordi» conclude Bernardi.

L'Italia è molto indietro nella gestione dei dati, tanto da essere il terzo Paese più vulnerabile d'Europa. Si stima che circa il 20% dei sistemi informatici in Italia abbia subito un attacco senza neanche saperlo

«E IO FACCIO BUSINESS CON LA CRITTOGRAFIA»

Il nuovo regolamento non è fonte solo di adempimenti, ma anche di opportunità. «È un settore che apre chance enormi. Per un Paese creativo come l'Italia c'è una straordinaria opportunità di investire risorse e diventare leader nel mondo per lo sviluppo di sistemi software e hardware che rendano più facile la vita dei gestori delle informazioni. A poterla cogliere: disegnatori, sviluppatori, produttori e distributori di queste soluzioni» ha dichiarato di recente Giovanni Buttarelli, garante europeo della protezione dei dati. Ad afferrarla al volo, ci sono molte società affermate nel settore, ma anche singoli professionisti e piccole realtà.

Andrea Ciappesoni, 42 anni, da quasi 20 lavora nel settore It. Ha cominciato a occuparsi di privacy nel 2000, leggendo, studiando e frequentando master. Oggi la cybersecurity è al centro della sua attività professionale (è un *data protection officer*, www.adeguamentiprivacy.it) e imprenditoriale. Ha infatti inventato e lanciato sul mercato Smooker, un kit basato sulla crittografia che prevede 6 barriere di sicurezza.

Come è nata l'idea? «A darmela è stato proprio il Gdpr, che in più punti segnala come la violazione dei dati personali non vada segnalata al Garante, qualora questi siano resi indecifrabili ai non autorizzati. Così ho pensato che l'uso dei sistemi di crittografia poteva essere una buona soluzione per agevolare la protezione dei dati e per limitare la responsabilità del titolare del trattamento» spiega. Il kit è composto da una card, un lettore di card Usb e una chiavetta Usb con il software (180 euro più Iva).

Come si utilizza? «Il software è di facile utilizzo, non richiede la digitazione di password e può essere realizzato come un abito su misura per ogni singolo cliente. Inoltre, oltre a proteggere i dati, permette anche di confinare le informazioni: assegnando a un team delle card con lo stesso codice, le informazioni circoleranno in sicurezza solo all'interno del gruppo». INFO: www.smooker.it