PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3730 di mercoledì 02 marzo 2016

In arrivo la nuova direttiva sulla sicurezza di reti e sistemi informativi

Forse pochi lettori sono al corrente del fatto che l'Europa sta per approvare la nuova direttiva sulla cybersecurity, che si applicherà a moltissime aziende, attive nel settore della informatica. Eccone i punti principali. Di Adalberto Biasiotti.

L'unione europea è giunta ormai vicina all'approvazione delle prime regole di cybersecurity, che avranno valore a livello europeo. La direttiva sulla sicurezza delle reti e dei sistemi informativi (**Direttiva NIS**) fà parte della strategia di cyber security che l'Unione Europea ha lanciato nel 2013.
L'obiettivo della direttiva è "garantire un elevato e comune livello di sicurezza delle reti e dei sistemi informativi". Per far ciò, la direttiva impone agli Stati membri dell'unione europea di attuare delle misure minime di sicurezza per tutte le aziende che operano in questi specifici settori.

In particolare, la direttiva NIS richiede che gli Stati membri dell'unione europea sviluppino ed attuino dei requisiti assai stringenti di sicurezza e di notificazione per tutti gli operatori di servizi essenziali nel mondo informatico, come ad esempio i punti di scambio Internet, e delle regole un poco più flessibili per i cosiddetti fornitori di servizi digitali, vale a dire le aziende che offrono servizi di elaborazione nel cloud, i motori di ricerca on-line e tutte le aziende che si occupano di commercio elettronico.
Ritengo importante che i lettori abbiano buona conoscenza di questo testo, perché vi sono indubbiamente delle forti connessioni tra i requisiti in materia di protezione dei dati personali tra questa direttiva e il regolamento generale europeo, ormai praticamente approvato.
Il testo concordato fra le istituzioni europee è stato approvato dai paesi membri a dicembre 2015 e dalla commissione Parlamento europeo sui diritti dei consumatori il 14 gennaio 2016.
Il prossimo passo è quello di fare approvare questa bozza di direttiva nella assemblea plenaria del Parlamento europeo. Dal momento che si tratta di una direttiva, la disposizione legislativa indica dei livelli minimi di sicurezza, che devono essere definiti in ogni paese europeo mediante disposizioni legislative nazionali.
Nulla impedisce ad ogni paese europeo di adottare delle regole anche più stringenti, se ritenute opportune.

I riflessi fra la direttiva e la protezione dei dati personali
Sotto certi aspetti, gli esperti ritengono che questa situazione sia ancora sotto osservazione ed evoluzione. Anche se il testo della direttiva richiede che vengano definite delle norme uniformi nei vari paesi, la formulazione della direttiva è abbastanza vaga e viene consentita una notevole latitudine applicativa ai paesi membri, che potrebbe portare alla attuazione delle indicazioni delle direttiva in modi diversi in paesi diversi. È il fenomeno che già si è verificato a proposito della direttiva sulla protezione dei dati personali e che ha fatto sì che, a distanza di parecchi anni, l'Unione Europea si sia resa conto che era necessario un regolamento armonizzante.

È bene sottolineare che nel testo originale della direttiva i servizi digitali non erano compresi, ma la successiva evoluzione del testo ha fatto sì che questi servizi venissero inseriti. Pertanto le aziende che forniscono servizi digitali devono conformarsi alle indicazioni della direttiva, devono attuare delle nuove misure di sicurezza e debbono attuare anche dei sistemi di notificazione, se si verificano degli incidenti che mettono a rischio la sicurezza dell'infrastruttura, secondo regole che vengono determinate in ogni singolo stato.

La inclusione dei servizi digitali negli obiettivi della direttiva ha sollevato molte perplessità tra i tutori dei dati personali. Appare infatti evidente che le aziende coinvolte possono trattare un elevatissimo numero di dati personali degli interessati, che debbono essere condivisi con le autorità nazionali, ad esempio quando le aziende devono riferire di un incidente, che coinvolga questi dati.

Per minimizzare questo rischio, la direttiva NIS giustamente non indica alcuna nuova regola afferente alla protezione dei dati personali, ma richiede che sia le infrastrutture critiche, come ad esempio i fornitori di acqua elettricità o i punti di scambio Internet, sia le aziende che forniscono servizi digitali, adottino regole conformi al regolamento generale sulla protezione dei dati, quando essi trattano dati personali.

Ciò significa che quando le aziende devono notificare all'autorità il verificarsi di un incidente afferente alla sicurezza, la notificazione deve essere elaborata in modo tale da essere conforme con le regole di sicurezza sui dati personali, che sono specificamente illustrate nel regolamento generale sulla protezione dei dati. Se un incidente di sicurezza comporta una violazione di dati personali, che potrebbero mettere a rischio la tutela di questi dati, le aziende devono notificare le autorità garanti in ogni paese, in modo che gli utenti possono essere coinvolti e protetti.
La direttiva tuttavia non fà alcun riferimento alle garanzie che devono offrire i governi nazionali, che vengono a conoscenza di informazioni afferenti alla rivelazione dei dati, né vengono date indicazioni su come i governi dovrebbero proteggere questi dati, né come si possono usare per una analisi dell'evento. Ciò significa che l'intervento delle autorità garanti nazionali, incaricate di proteggere i dati dei cittadini, diventa un passo essenziale per assicurare che il trattamento di questi dati sia sufficientemente garantistico.

Si pensi ad esempio ad una violazione di dati che riguarda un settore critico, come ad esempio la distribuzione dell'energia elettrica. Le aziende che eroga energia elettrica sono in possesso di una straordinaria quantità di dati personali degli utenti, che potrebbero essere usate in maniera non appropriata per una moltitudine di finalità, anche se non appropriate.
Quali garanzie vi sono che, quando il governo manterrà in possesso di questi dati, trasmessi in relazione una possibile violazione, essi non verranno trattati con le dovute garanzie?

Verranno introdotte nuove norme di sicurezza per le aziende coinvolte?
È interessante rilevare che, nelle fasi finali della negoziazione tra le varie autorità europee, che ha portato alla elaborazione della versione quasi finale della direttiva, sono stati inseriti dei vincoli circa la capacità degli Stati membri di imporre norme di sicurezza o requisiti di notificazione ai fornitori di servizi digitali, che vadano oltre quelli già indicati nel testo della direttiva. Tuttavia, se le norme di sicurezza sono veramente armonizzate, si potrebbe manifestare il rischio che delle pratiche di sicurezza non idonee potrebbero diffondersi in tutta l'Europa.

Gli esperti rilevano, infatti, che le norme legislative possono essere senz'altro importanti, ma la natura completamente evolutiva delle sfide della sicurezza può far sì che queste norme possano presto diventare obsolete. A questo punto gli Stati membri avrebbero emesso delle regole minime, che potrebbero essere non idonee a fronteggiare le nuove sfide tecnologiche, poste dai criminali.

Tuttavia, il limite per inserire regole aggiuntive di sicurezza, applicabili alle aziende digitali, non è assoluto. I paesi europei possono ancora inserire ulteriori requisiti di sicurezza, sulla base di esigenze di "sicurezza nazionale" o per mantenere "la legge e l'ordine". Ciò significa che, alla fin fine, le aziende digitali probabilmente dovranno conformarsi a tutta una serie di misure di sicurezza, nell'unione europea, che potrebbero cambiare da paese a paese.

I prossimi passi
Nei prossimi mesi, il testo concordato della direttiva disse sarà votato nella assemblea plenaria del Parlamento europeo. Una volta ratificato, gli Stati membri avranno 21 mesi per dare contenuto pratico a questa direttiva, grazie all'emissione di provvedimenti legislativi nazionali.
L'esperienza passata mostra che molti paesi europei, che cercavano di evitare o limitare i loro obblighi nei confronti della **protezione dei dati personali**, hanno manifestato una tendenza a stabilire tutt'una serie di eccezioni, spesso non molto chiare, per ragioni di "sicurezza nazionale".
Questo è un errore.
Gli esperti ritengono che gli Stati membri dell'Unione Europea non dovranno usare queste eccezioni per limitare i loro obblighi nei confronti di altre disposizioni europee, incluso l'impegno a rispettare i dettati della carta europea sui diritti fondamentali e gli obblighi imposti dal regolamento generale sulla protezione dei dati.
Ci auguriamo che i corpi legislativi nazionali prenderanno buona nota di questi obblighi di rispetto dei diritti umani, quando

pubblicheranno i provvedimenti legislativi che daranno attuazione alla direttiva.

Nota di AB: Ringrazio la collega Lucia Krahulcova per il suo prezioso contributo.

Allegato testo direttiva (245 kB).

Adalberto Biasiotti

---

www.puntosicuro.it