PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4173 di Venerdì 09 febbraio 2018

Il 25 maggio 2018 è vicino, ma il 10 maggio è ancora più vicino!

Il 9 maggio 2018 il parlamento italiano deve recepire la direttiva 2016/1148 del parlamento europeo e del consiglio, recante misure per un livello comune elevato di sicurezza delle reti e di sistemi informativi dell'unione.

Questa direttiva è stata pubblicata il 6 luglio 2016 ed è composta da 75 considerando e 22 articoli.

Alla direttiva sono allegati tre documenti, che sono di estremo interesse per tutti coloro che sono coinvolti nella sicurezza delle informazioni ed anche nella sicurezza dei dati personali.

Questa direttiva nasce dal fatto che le reti ed i sistemi di servizi informativi svolgono un ruolo vitale nella società civile ed è pertanto essenziale che essi siano affidabili e sicuri nelle attività economiche sociali ed in particolare ai fini del funzionamento del mercato interno.

Questa direttiva, nata dopo una lunga elaborazione, ha visto accelerare in modo significativo il suo sviluppo, a seguito dell'aumento della portata, della frequenza e dell'impatto degli incidenti a carico della sicurezza informatica.

L'unione europea si è resa ben conto che molti servizi, pubblici e privati, possono essere compromessi in modo drammatico dal verificarsi di incidenti informatici, sia di origine accidentale, sia di origine dolosa, ed ecco la ragione per la quale solo dalla armonizzazione delle misure di sicurezza, a livello europeo, può nascere un quadro sufficientemente affidabile e protetto. In pratica, la direttiva tende a stabilire un comune minimo denominatore del livello di sicurezza, presente in tutte le nazioni europee. Si può così evitare il fatto che una debolezza informatica, in un determinato paese, possa avere drammatici riflessi sull'intera Europa.

La direttiva si rivolge agli operatori di servizi essenziali, vale a dire soggetti pubblici e privati, che rientrano in una serie di categorie dettagliate nell'allegato due.

I soggetti coinvolti sono numerosi e sono divisi in vari settori e sotto settori.

Il settore dell'energia, ad esempio, fa riferimento all'energia elettrica, petrolio, gas; il settore dei trasporti fa riferimento al trasporto aereo, al trasporto ferroviario ed al trasporto per vie d'acqua, nonché al trasporto su strada. È compreso anche il settore bancario e le infrastrutture dei mercati finanziari.

Particolare attenzione prestata al settore sanitario, alle reti di fornitura e distribuzione di acqua potabile e alle infrastrutture digitali.

Per quanto riguarda i tipi di servizi digitali, compresi in questa direttiva, sono previsti i seguenti settori:

- mercato on-line,
- motori di ricerca on-line,
- servizi di cloud computing.

La direttiva impone che tutte le autorità pubbliche e private che svolgono questi servizi, in cui anomalie funzionali potrebbe avere impatto sull'intera Europa, attuino tutta una serie di misure di sicurezza, sviluppate di concerto con organismi sovranazionali, come ad esempio ENISA.

Inoltre si fa obbligo a tutti i paesi europei di attivare delle strutture specializzate, in grado di intervenire con urgenza in caso di emergenze informatiche, conseguenti ad incidenti informatici.

Al proposito, è bene ricordare che la direttiva classifica come incidente ogni evento con un reale effetto pregiudiziale per la sicurezza della rete dei sistemi informativi.

Le squadre specializzate che debbono intervenire, in caso di incidente, vengono chiamate CSIRT computer security information response team, che a loro volta possono chiamare in causa anche le forze dell'ordine nell'ambito di una sinergia operativa, che aumenta livello di sicurezza complessivo e potenzia le capacità di reazione.

Come di consueto, la direttiva lascia gli Stati membri l'incarico di pubblicare decreti legislativi applicativi, e la data ultima concessa, come accennato in precedenza, è il 10 maggio 2018.

Ogni Stato membro deve designare un'autorità nazionale competente, che può assimilarsi alla nostra autorità garante della protezione dei dati, che assume la responsabilità di emanare provvedimenti in materia di sicurezza delle reti e dei sistemi informativi.

Inoltre ogni Stato membro deve designare un punto di contatto unico nazionale, in maniera da facilitare lo scambio di formazioni con altri paesi europei.

La squadra di pronto intervento, vale a dire lo CSIRT, è composta da rappresentanti dei CSIRT degli Stati membri e del CERT-computer Emergency response team, organismo operativo a livello europeo.

Nelle disposizioni di recepimento nazionale della direttiva europea, gli Stati membri devono impegnarsi affinché gli operatori di servizi essenziali adottino misure tecniche e organizzative adeguate e viene inoltre posto l'obbligo di notificare senza ritardo all'autorità competente ogni incidente avente un impatto rilevante sulla continuità dei servizi essenziali prestati.

Per determinare la rilevanza di impatto dell'incidente si tiene conto in particolare dei seguenti parametri:

- il numero di utenti interessati dall'incidente,
- la durata dell'incidente,
- la diffusione geografica dell'area interessata all'incidente.

Tocca alle autorità competenti degli Stati membri tenere sotto controllo la correttezza e adeguatezza dei comportamenti assunti degli operatori di servizi essenziali.

Ancora una volta, la direttiva incoraggia l'uso di norme specifiche europee, o comunque accettate a livello internazionale, relative alla sicurezza della rete e dei sistemi informativi.

I lettori che hanno già letto la direttiva sulla sicurezza delle infrastrutture critiche troveranno indubbiamente molti punti di contatto tra quella direttiva e la presente.

Restiamo tutti in impaziente attesa che l'Italia pubblichi, entro il 9 maggio 2018, il decreto legislativo di recepimento della direttiva, indicando a tutti soggetti coinvolti quali siano gli organismi di riferimento.

Nel frattempo, si potrà sviluppare l'analisi di rischio e predisporre appropriate misure di prevenzione e contenimento, che potranno essere sottoposte successivamente alla approvazione dell'autorità nazionale competente.

Adalberto Biasiotti

Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (formato pdf, 0.5 Mb)
