PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4427 di Venerdì 15 marzo 2019

Approvato il cybersecurity act, ma è solo il primo passo!

Il parlamento europeo ha portato a termine il percorso di approvazione di un piano di sicurezza informatica, applicabili all'intera Europa. Ma tra il dire e il fare passerà ancora un poco di tempo.

I mezzi di comunicazione di massa hanno dato ampio risalto al fatto che è stato recentemente approvato dal parlamento europeo il cosiddetto cyber security act, vale a dire la legge sulla sicurezza informatica, che dovrà governare, in tutti paesi dell'unione europea, le modalità con cui i vari enti gestiscono la sicurezza dei propri sistemi informativi.

Con ogni probabilità, il documento finale verrà pubblicato in Gazzetta Ufficiale nel mese di aprile 2019 ed in quell'occasione sarà nostra cura dare ai lettori il testo completo. Questa prudenza nasce dal fatto che già con il precedente regolamento europeo 679/2016 si era verificato qualche problema, a seguito della pubblicazione affrettata del testo in Gazzetta Ufficiale, tanto è vero che dopo alcuni mesi è stata pubblicata una rettifica del regolamento, correggendo parecchi errori formali ed anche un paio di errori sostanziali, dovuti in gran parte a traduzioni affrettate.

Ciò non toglie che possiamo nel frattempo vedere come questo documento potrà influenzare e, speriamo, accrescere il livello di sicurezza informatica dell'intera Europa.

Tanto per cominciare, con questo documento si conferisce un ruolo preminente ad una agenzia benemerita della unione europea, la European National Information Security Agency-ENISA, che da anni si occupa, ma solo in funzione di consulente, dei problemi di sicurezza informatica delle agenzie europee e, più in generale, dell'Europa intera.

Oggi questa agenzia fa un salto di qualità, prendendo in carico la applicazione pratica di queste disposizioni legislative, con lo specifico incarico di pubblicare delle linee guida che possano portare a certificazioni di sicurezza dei sistemi informativi.

Pubblicità
<#? QUI-PUBBLICITA-SCORM1-[EL0542] ?#>

ENISA aveva già lavorato su questo tema, pubblicando un pregevole documento, che allego a questo articoletto, concentrando la sua attenzione sulla protezione dei dati personali.

Non è detto che un'azienda, che sappia proteggere assai bene i suoi dati personali, sia anche in grado di proteggere altrettanto bene i suoi dati non personali, come ad esempio i dati relativi a brevetti, trattative commerciali, listini e sconti applicabili a specifici clienti e via dicendo. Ecco perché questa nuova formulazione del cybersecurity act permette di allargare al massimo il campo di applicazione delle misure di sicurezza informatica.

Per evitare malintesi, mi permetto di sottolineare come non toccherà a ENISA rilasciare certificazioni di sorta, ma solo stabilire delle linee guida, sulla base delle quali sarà possibile agli enti di certificazione, operanti nei vari paesi, rilasciare specifiche certificazioni di sicurezza informatica.

In Italia, già sappiamo che l'Istituto superiore delle comunicazioni e delle tecnologie dell'informazione-ISCOM, che si appoggia al ministero dello sviluppo economico, già da tempo certifica la sicurezza informatica di prodotti e sistemi ITC, secondo uno schema di certificazione sviluppato appositamente per l'Italia.

Altri schemi di certificazione esistono in altri Stati membri, ma fino ad oggi nessuno è stato in grado di garantire la omogeneità e validità dei vari schemi, presenti nei vari paesi. Se questi schemi verranno aggiornati, secondo linee guida rilasciati da ENISA, potremo avere la garanzia che vi sia armonizzazione ed omogeneizzazione di questi schemi e quindi un sistema informativo, un applicativo o un dispositivo hardware, certificato secondo i nuovi schemi in un paese europeo, potrà vedere riconosciuta la sua certificazione in tutta l'unione europea.

In altre parole, con questa disposizione legislativa ENISA, da consulente dell'Europa, diventa invece parte attiva ed addirittura promotore di procedure di sicurezza informatica, debitamente certificate.

Il carico di lavoro accresciuto per questa agenzia viene sostenuto da un apposito incremento del fondo di dotazione, anche perché il campo di intervento di ENISA è stato assai allargato da questa disposizione legislativa.

Ad esempio, in precedenza i dispositivi medici, i sistemi di controllo industriali (vi ricordate l'attacco alle centrifughe iraniane grazie un virus, che le ha distrutte, avendo superato i limiti massimi di giri al minuto?), i veicoli senza pilota e via dicendo, rientreranno nel campo delle attrezzature informatiche, per le quali occorrerà sviluppare schemi di certificazione.

Allegato documento ENISA (pdf)

Adalberto Biasiotti

Questo articolo è pubblicato sotto una Licenza Creative Commons.

---

www.puntosicuro.it