PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4501 di Mercoledì 03 luglio 2019

Novità per il regolamento sulla cybersecurity

Pubblicato il regolamento europeo 2019/881 che precisa le nuove funzioni dell'ENISA e le modalità di certificazione della cybersecurity delle tecnologie dell'informazione e della comunicazione.

Non nascondo ai lettori che la approvazione di questo regolamento mi ha lasciato alquanto perplesso, soprattutto perché esso può indurre delle confusioni nei soggetti coinvolti, in quanto nello stesso documento si uccide la ormai famosa pregiata ENISA, agenzia dell'unione europea per la cyber sicurezza, e la si fa rinascere con lo stesso nome, ma con compiti ben diversi.

Con l'occasione, ricordo ai lettori che un regolamento europeo diventa immediatamente esecutivo in tutti i paesi europei e non ha bisogno di un decreto legislativo di recepimento, come invece accade per una direttiva.

Il fatto che l'Europa abbia deciso di utilizzare lo strumento del regolamento dà la prova della urgenza e dell'importanza dei temi trattati, perché la sicurezza informatica sta assumendo oggi una rilevanza enorme.

Come di consueto, il documento è composto da una serie di considerando, in particolare 110 considerando, e 69 articoli. Ancora una volta, raccomando caldamente a tutti gli operatori del settore di leggere con diligenza tutti i considerando, che spesso rappresentano un elemento esplicativo, che chiarisce il significato di alcuni successivi articoli. La traduzione in italiano lascia qua e là desiderare, in particolare per l'utilizzo di alcune forme verbali, che non dovrebbero essere mai presente in un documento legislativo di tale portata. Affermare che la nuova Elisa dovrebbe gestire un sito Web che fornisce informazioni sui siti europee di certificazione non è certo un'espressione felice, in quanto io pretendo invece che la nuova Elisa debba gestire un sito Web.

Vi è una bella differenza tra l'imporre di fare qualcosa o il raccomandare di fare qualcosa!

Ciò premesso, vediamo di analizzare come questo documento può avere un impatto significativo su tutti coloro che, per un motivo per l'altro sono coinvolti nelle tecnologie dell'informazione e della comunicazione.

Il documento si apre con una descrizione delle nuove funzioni affidate all'agenzia dell'unione europea per la cyber sicurezza, illustrandone il mandato, gli obiettivi e i compiti. L'obiettivo primario di questo documento è quello di eliminare l'attuale frammentazione degli interventi di cyber sicurezza, tra i vari paesi europei, affidando ad un unico ente, con funzioni di armonizzazione, il compito di migliorare il livello di sicurezza informatica dell'unione europea. Tale miglioramento si ottiene con vari interventi, come ad esempio, fornendo consulenza e competenze e agevolando lo scambio delle migliori pratiche fra le

autorità competenti. Anche lo sviluppo dell'attuazione di una politica dell'unione nel settore dell'identificazione elettronica e dei servizi fiduciari rappresenta un aspetto primario dei compiti affidati a questa agenzia.

Deve essere quindi chiaro che la funzione di questa agenzia è di consulenza ed assistenza, e che la responsabilità finale nella adozione di misure adeguate di sicurezza compete alle singole nazioni. Vediamo adesso come è organizzata questa agenzia:

- vi è un consiglio di amministrazione,
- un comitato esecutivo,
- un direttore esecutivo,
- un gruppo consultivo, con l'assistenza di una rete di funzionari nazionali di collegamento. In particolare, per quanto riguarda quest'ultima rete, tocca ai singoli paesi indicare quali siano i funzionari cui è affidato il collegamento tra ENISA e gli Stati nazionali.

Ruolo fondamentale è costituito dal gruppo dei portatori di interessi per la certificazione della cyber sicurezza. Questo gruppo è composto da membri selezionati fra esperti riconosciuti, e quel ruolo viene convalidato dalla commissione europea. Si tratta comunque di una rete di consulenza senza poteri decisionali.

Il funzionamento dell'agenzia è guidato da un documento unico di programmazione, che contiene le indicazioni della programmazione annuale e pluriennale, afferenti a tutte le attività pianificate.

Il bilancio e le risorse necessarie per il funzionamento dell'agenzia vengono elaborate dall'agenzia stessa e sottoposti all'approvazione della commissione, che inserisce il contributo a carico del bilancio generale dell'unione europea. Di particolare interesse il fatto che i dati personali trattati dai ENISA devono avvenire rispettando il regolamento dell'unione europea 2018 / 1725, vale a dire il regolamento applicabile all'agenzie dell'unione europea e quindi è diverso, anche se per sommi capi simile, dal regolamento 679 / 2016.

Un ruolo fondamentale affidato a ENISA è quello di sviluppare un programma di lavoro per la certificazione europea della sicurezza. Per garantire la distribuzione omogenea in tutta Europa delle attività di ENISA, deve essere allestito un sito Web dedicato ai sistemi europei di certificazione della cybersecurity, che illustra quali sono i sistemi di certificazione nazionale che sono stati sostituiti da un sistema europeo di certificazione della cybersecurity; ciò garantisce una omogeneità dei sistemi di certificazione.

I sistemi europei di certificazione della cyber sicurezza possono essere applicati a prodotti di telecomunicazioni, servizi di telecomunicazioni e processi di telecomunicazione, stabilendo il livello di affidabilità della certificazione a tre livelli: rispettivamente di base, sostanziale ed elevato.

È interessante rilevare il fatto che la certificazione può essere rilasciata da un soggetto terzo, ma anche auto valutata dal fabbricante o fornitore coinvolto. Resta inteso che in questo caso tutte le responsabilità restano in carico al soggetto coinvolto.

Come di consueto, la certificazione della cybersecurity è volontaria, salvo che sia stato diversamente specificato dal diritto dell'unione o degli Stati membri. Tocca alla commissione valutare periodicamente l'efficacia e l'utilizzo di sistemi europei di certificazione e l'eventuale necessità di rendere obbligatorio uno specifico sistema di certificazione. Ciascuno Stato membro

designa una o più autorità nazionale di certificazione, operante nel proprio territorio oppure, con l'accordo di un altro Stato membro, una stessa autorità può operare in più paesi.

La valutazione delle competenze e dell'affidabilità delle autorità nazionali possono essere verificate congiuntamente da interventi congiunti, da parte di altri paesi.

A questo proposito, è stato istituito un gruppo europeo per la certificazione della cyber sicurezza, composto da rappresentanti delle autorità nazionali, che assiste sia la commissione europea, sia ENISA, sia le autorità nazionali, nel mettere a punto incisivi programmi di protezione.

È data comunque facoltà a persone fisiche e giuridiche di presentare un reclamo nei confronti di un certificato europeo di cyber sicurezza, se si ritiene che tale certificato non sia stato correttamente rilasciato o le indicazioni non siano state correttamente attuate.

In conclusione, questo regolamento europeo non si dirige all'universo dei soggetti informatici, ma solo a particolari categorie, che lavorano nel contesto di attività sovranazionali, nel mondo delle comunicazioni.

Vedremo adesso quale sarà la tempistica per la individuazione dei componenti della nuova agenzia e per la individuazione delle autorità nazionali di certificazione.

Non mancheremo di tenere informati i lettori su ulteriori e, speriamo, rapidi sviluppi.

Adalberto Biasiotti

---

www.puntosicuro.it