TeLex Anie
NOVITÀ LEGISLATIVE E GIURISPRUDENZIALI

Segnalazioni giuridiche a cura del Servizio Centrale Legale

N. 6 Anno XXIV
Giugno 2019

INDICE:

APPROFONDIMENTO DEL MESE:

Cybersecurity Act, di *Alessandra Toncelli*

Approfondimento del mese di Giugno 2019

CYBERSECURITY ACT

1. E' stato pubblicato sulla **GUUE n. L 151 del 7 giugno 2019**, con entrata in vigore il 27 giugno, il cosiddetto "*Cybersecurity Act*", ossia il **regolamento UE 2019/881**, relativo all'ENISA - l'Agenzia dell'Unione europea per la cibersicurezza - e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013.

Il *Cybersecurity Act,* da una parte, rafforza l'**ENISA,** la *European Network and Information Security Agency,* cui viene attribuito un mandato permanente a fornire sostegno agli Stati Membri, alle Istituzioni europee ed alle imprese, in materia di sicurezza informatica. Dall'altra, viene istituito un **quadro europeo per la certificazione della cybersecurity** di prodotti, servizi e sistemi ICT, per un approccio armonizzato dei sistemi europei di certificazione della cibersicurezza, allo scopo di creare un mercato unico digitale per tali prodotti, servizi e processi ICT.

In merito il regolamento NON introduce sistemi di certificazione già definiti, ma stabilisce un sistema comune per la creazione di specifici schemi di certificazione della cibersicurezza di prodotti/servizi/processi ICT, basati su criteri comuni a tutti gli Stati membri della UE. Gli schemi di certificazione, se rispettosi dei termini e del contenuto minimo fissati da tale quadro comune europeo, dovranno quindi ritenersi validi e riconosciuti in tutti gli Stati membri. Inoltre, una volta introdotto un sistema europeo di certificazione, eventuali sistemi nazionali già esistenti cesseranno di avere effetti e/o non ne potranno essere adottati di nuovi da parte degli Stati membri.

Il sistema europeo introdotto dal nuovo regolamento, prevede al momento una **certificazione volontaria della cibersicurezza** di prodotti, servizi e sistemi ICT; tuttavia, entro il 31 dicembre 2023 e poi ogni due anni, la Commissione europea valuterà l'eventuale necessità di rendere obbligatorio uno specifico sistema europeo di certificazione della cibersicurezza, a cominciare dai cosiddetti servizi essenziali (trasporti, energia, sanità, distribuzione acqua, settore bancario, infrastrutture digitali, infrastrutture dei mercati finanziari). Inoltre, entro il 28 giugno 2024 la Commissione valuterà se siano necessari requisiti essenziali di cibersicurezza per l'accesso al mercato interno, onde impedire l'ingresso nel mercato dell'Unione di prodotti, servizi e processi ICT, che non rispettino i requisiti di base in materia di cibersicurezza (peraltro, c'è già qualche consultazione per l'eventuale introduzione di requisiti di *cybersecurity* in alcune delle direttive di prodotto del cosiddetto *New Legal Framework*).

2. Prodotti oggetto di certificazione. La certificazione della cibersicurezza riguarderà prodotti, servizi e sistemi ICT, intesi come:

- prodotto ICT: un elemento o un gruppo di elementi di una rete o di un sistema informativo;
- servizio ICT: un servizio consistente interamente o prevalentemente nella trasmissione, conservazione, recupero o elaborazione di informazioni per mezzo della rete e dei sistemi informativi;
- processo ICT: un insieme di attività svolte per progettare, sviluppare, fornire o mantenere un prodotto ICT o servizio ICT.

Per rete e sistema informativo si deve intendere invece:

a) una rete di comunicazione elettronica ai sensi dell'articolo 2, lettera a), della direttiva 2002/21/CE e, quindi, sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse (a commutazione di circuito e a commutazione di pacchetto, compresa Internet), le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica,

nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;
b) qualsiasi dispositivo o gruppo di dispositivi interconnessi o collegati, uno o più dei quali eseguono, in base ad un programma, un trattamento automatico di dati digitali; o
c) i dati digitali conservati, trattati, estratti o trasmessi per mezzo di reti o dispositivi di cui alle lettere a) e b), per il loro funzionamento, uso, protezione e manutenzione.

3. I soggetti coinvolti. Oltre all'**ENISA**, che dovrà elaborare gli schemi di certificazione, su proposta della **Commissione** Europea, gli altri attori che interverranno nell'adozione degli schemi sono:

- il Gruppo dei portatori di interessi per la certificazione della cibersicurezza (**SCCG** – *Stakeholder Cybersecurity Certification Group*), i cui membri saranno selezionati dalla Commissione tra esperti riconosciuti che rappresentino i pertinenti portatori di interessi (tra cui, quindi, anche l'industria). Il Gruppo affiancherà Commissione ed ENISA con compiti di consulenza.
- il Gruppo Europeo per la certificazione della cibersicurezza (**ECCG** – *European Cybersecurity Certification Group*) composto da rappresentanti delle autorità nazionali di certificazione della cibersicurezza o da rappresentanti di altre autorità nazionali competenti da rappresentanti di tutti gli Stati membri
- il Gruppo Consultivo ENISA (**EAG** – ENISA Advisory Group), che avrà compiti di consulenza dell'Agenzia in merito al programma di lavori della stessa, oltre che di collegamento con i vari soggetti portatori di interesse, coinvolti dai lavori;
- i **gruppi di lavoro ad hoc** che saranno istituti da ENISA in relazione ai lavori di adozione di ogni schema di certificazione e che vedranno coinvolti anche i settori industriali interessati.

4. I prossimi passi. Entro il 28 giugno 2020, la Commissione UE dovrà adottare un programma di lavoro progressivo dell'Unione (***Union rolling work programme***) con elenco dei prodotti, servizi e processi ICT per i quali verrà dato mandato all'ENISA di elaborare schemi di certificazione della cibersicurezza. L'inclusione in tale elenco dovrà essere fatta tenuto conto di diversi parametri tra cui la disponibilità e lo sviluppo di sistemi nazionali di certificazione della cibersicurezza che possono comportare un rischio di frammentazione; la domanda di mercato; eventuali sviluppi nel panorama delle minacce informatiche; una specifica richiesta da parte dell'ECCG.

Il programma dovrà essere aggiornato poi ogni tre anni, salvo specifiche esigenze di aggiornamenti più frequenti ed in linea di massima non sarà possibile adottare schemi di certificazione per prodotti non inclusi nel programma.

5. Gli schemi di certificazione. Gli schemi di certificazione dovranno attestare che i prodotti/ servizi/processi ICT, certificati in base allo schema, sono conformi a requisiti specifici per quanto riguarda la capacità di resistere ad azioni che mirano a compromettere la disponibilità, l'autenticità e l'integrità o la riservatezza dei dati memorizzati o trasmessi o elaborati o delle funzioni o dei servizi offerti o accessibili attraverso tali prodotti, processi, servizi e sistemi.

Nel dettaglio, gli schemi dovranno perseguire i seguenti **obiettivi di sicurezza informatica**:

a) proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati durante l'intero ciclo di vita del prodotto, servizio o del processo ICT;
b) proteggere i dati conservati, trasmessi o altrimenti trattati dalla distruzione, dalla perdita o dall'alterazione accidentali o non autorizzate, oppure dalla mancanza di disponibilità durante l'intero ciclo di vita del prodotto, servizio o del processo ICT;
c) le persone, i programmi o le macchine autorizzati devono poter accedere esclusivamente ai dati, ai servizi o alle funzioni per i quali dispongono dei diritti di accesso;
d) individuare e documentare le dipendenze e vulnerabilità note;
e) registrare a quali dati, servizi o funzioni è stato effettuato l'accesso e quali sono stati utilizzati o altrimenti trattati, in quale momento e da chi;
f) fare in modo che si possa verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso, che sono stati utilizzati o altrimenti trattati, in quale momento e da chi;
g) verificare che i prodotti, servizi o processi ICT non contengano vulnerabilità note;

h) ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico;
i) i prodotti, servizi o processi ICT devono essere sicuri fin dalla progettazione e per impostazione predefinita;
j) il software e l'hardware dei prodotti, servizi o processi ICT devono essere aggiornati, non contenere vulnerabilità pubblicamente note e devono disporre di meccanismi per effettuare aggiornamenti protetti.

Gli schemi dovranno comprendere i riferimenti alle **norme internazionali, europee o nazionali** applicate nella valutazione o, laddove tali norme non siano disponibili o adeguate, alle **specifiche tecniche** che rispettano le prescrizioni enunciate all'allegato II del regolamento (UE) n. 1025/2012 oppure, se tali specifiche non siano disponibili, alle specifiche tecniche o ad altri requisiti di cibersicurezza definiti nel sistema europeo di certificazione della cibersicurezza.

Gli schemi di certificazione dovranno specificare uno o più **livelli di affidabilità** in termini di sicurezza informatica tra **base, sostanziale e/o elevato** in rapporto al livello del rischio associato al previsto uso del prodotto, servizio o processo ICT, in termini di probabilità e impatto di un incidente.

Questa distinzione tra diversi livelli è funzionale anche alla possibilità, per il solo livello base, che la cibersicurezza possa essere oggetto di **autocertificazione** (volontaria) da parte del produttore o fornitore del prodotto, servizio o processo ICT, con conseguente rilascio di una **dichiarazione UE di conformità**, pur rimanendo aperta l'alternativa di richiedere invece la certificazione (sempre su base volontaria) da parte di ente accreditato, con rilascio di un **certificato europeo di cibersicurezza**. Per i livelli di affidabilità sostanziale o elevato, invece, se si vuole certificare (su base volontaria), occorrerà rivolgersi all'ente terzo.

Se nel caso del **livello base**, le attività di valutazione da intraprendere per la certificazione, dovranno comprendere almeno un **riesame della documentazione tecnica**, per il **livello sostanziale** sarà necessario anche un **test** per dimostrare che i prodotti/servizi/processi certificati attuano correttamente le necessarie funzionalità di sicurezza; per il **livello elevato,** poi, in aggiunta a riesame e test, è richiesto anche un **test di penetrazione** per valutare la resistenza agli attacchi commessi da soggetti qualificati. Sono ammesse anche attività di valutazione sostitutive di effetto equivalente.

Infine, ciascuno schema potrà prevedere **marchi** o **etichette** da riportare sui prodotti certificati, indicandone le condizioni d'uso.

6. Enti di certificazione. Tranne che per il caso di autocertificazione da parte del produttore, previsto per il livello base di cibersicurezza già esaminato, la certificazione è demandata ad organismi di valutazione della conformità che dovranno essere accreditati da organismi nazionali di accreditamento designati ai sensi del regolamento CE n. 765/2008. I requisiti per essere accreditati sono previsti in allegato allo stesso regolamento 881.
Per ciascun sistema europeo di certificazione della cibersicurezza, le autorità nazionali di certificazione della cibersicurezza dovranno notificare alla Commissione gli organismi di valutazione della conformità che sono stati accreditati e che saranno riportati in apposito elenco da pubblicarsi nella *GUUE.*

Ricordiamo infine che il nuovo regolamento 881 è direttamente applicabile in tutti gli Stati membri dal 27 giugno 2019, data della sua entrata in vigore, senza necessità di atti nazionali di trasposizione. Gli Stati membri sono però chiamati a stabilire le sanzioni applicabili per i casi di violazione sia delle norme sul quadro di certificazione della cibersicurezza sia dei sistemi europei di certificazione della cibersicurezza.

Alessandra Toncelli
Servizio Centrale Legale Federazione ANIE