Nota di Aggiornamento

CONFINDUSTRIA

Revisione della strategia UE sulla Cybersecurity

Lente sull'UE n. 58

Ottobre 2017

Nota di Aggiornamento

1. CONTESTO

La crescente dipendenza della vita quotidiana e dell'economia globale dalle nuove tecnologie digitali ha reso la cybersecurity una questione essenziale per la prosperità e per la sicurezza dei cittadini e delle imprese.

Se da un lato, infatti, l'utilizzo sempre più ampio e pervasivo delle tecnologie digitali offre a cittadini, istituzioni e imprese nuove opportunità di connessione, favorendo la diffusione delle informazioni e lo sviluppo di nuovi modelli di business, dall'altro il ricorso all'ICT li espone a nuovi rischi, tra i quali gli attacchi da parte di "cyber criminali" che cercano spesso di sottrarre dati e compromettere il funzionamento di strutture critiche.

Solo nel 2016 si sono verificati più di 4000 attacchi con ransomware al giorno e l'80%[1] delle imprese europee ha subito almeno un incidente di cybersecurity. Negli ultimi quattro anni l'impatto economico della cibercriminalità è quintuplicato.

Alla luce del carattere sempre più transfrontaliero di tali violazioni, la Commissione europea ha deciso di presentare una strategia europea che fosse in grado di intervenire su più fronti e di adeguare alle nuove sfide la prima Strategia dell'Unione Europea per la cybersecurity del 2013.

2. ELEMENTI PRINCIPALI DELLA STRATEGIA UE SULLA CYBERSECURITY

Il 13 settembre 2017, in occasione del discorso annuale sullo stato dell'Unione del Presidente Juncker, la Commissione europea ha presentato un ampio pacchetto di misure per rafforzare la cybersecurity nell'UE.

Il Pacchetto contiene:

• La **Comunicazione** "*Resilienza, deterrenza e difesa: verso una cybersecurity forte per l'UE*", che fornisce un quadro generale di tutte le proposte;

• La **proposta di Regolamento** sull'**ENISA**, l'Agenzia dell'UE per la cybersecurity, che abroga il regolamento (UE) n. 526/2013 e che introduce un **sistema di certificazione della sicurezza informatica** per le

[1] Stato dell'Unione 2017 - Cybersecurity: la Commissione intensifica la risposta dell'UE ai ciberattacchi

tecnologie dell'informazione e della comunicazione (cd. "Cybersecurity Act");

• La **Raccomandazione** della Commissione sulla risposta coordinata degli gli Stati membri agli incidenti cyber su larga;

• La **Comunicazione** "Sfruttare al meglio la **NIS**: verso un'attuazione efficace della direttiva (UE) 2016/1148 concernente misure per un elevato livello comune di sicurezza delle reti e dell'informazione in tutta l'Unione" che mira a promuovere una piena attuazione della direttiva NIS in tutti gli Stati membri, fornendo alcuni chiarimenti e indicando le *best practices*;

• La **valutazione** del documento di lavoro dei servizi della Commissione sulla strategia UE 2013 sulla cybersecurity;

• La **Proposta di direttiva** sulla lotta contro la frode e la contraffazione di mezzi di pagamento non monetari, che sostituisce la Decisione quadro del Consiglio del 28 maggio 2001;

• La **relazione** sulla valutazione della misura in cui gli Stati membri hanno adottato le misure necessarie per conformarsi alla direttiva 2013/40/UE sugli attacchi contro i sistemi informatici.

Nelle intenzioni della Commissione, la nuova strategia mira a perseguire i seguenti **obiettivi**:

- accrescere le capacità e la preparazione degli Stati membri e delle imprese in materia di cybersecurity;
- migliorare la cooperazione e il coordinamento tra gli Stati membri e le Istituzioni, agenzie ed enti UE;
- aumentare la consapevolezza dei cittadini e delle imprese su questi temi;
- evitare la frammentazione dei sistemi di certificazione nell'UE e i correlati requisiti di sicurezza.

2.1 PROPOSTA DI REGOLAMENTO SULL'ENISA E SU UN SISTEMA DI CERTIFICAZIONE DELLA SICUREZZA INFORMATICA ("*CYBERSECURITY ACT*") (COM 2017/477)

La proposta di Regolamento mira al **rafforzamento dell'ENISA**, a cui viene attribuito un mandato permanente a fornire sostegno agli Stati Membri, alle Istituzioni europee e alle imprese in ambiti chiave tra cui quello dell'attuazione della direttiva NIS, e istituisce un **quadro europeo per la certificazione della cybersecurity di prodotti, servizi e sistemi**.

2.1.1 RAFFORZAMENTO DEL RUOLO DELL'ENISA

Al fine di supportare le Istituzioni europee, gli Stati membri e la comunità imprenditoriale nel prevenire e rispondere ai problemi di sicurezza dell'informazione e delle reti, l'ENISA svolge diverse attività nei cinque settori che le sono stati assegnati: diffusione di competenze tecniche; supporto al processo decisionale; sostegno al *capacity building* nell'Unione; potenziamento della comunità attiva nella sicurezza delle reti e dell'informazione; concessione di autorizzazioni.

La proposta di Regolamento della Commissione sulla riforma dell'ENISA riprende le conclusioni della valutazione dell'operato dell'Agenzia da parte degli stakeholder e si pone l'obiettivo di attribuire all'Agenzia un **ruolo da protagonista nel contrasto alle ciberminacce, nell'attuazione della Direttiva NIS da parte degli Stati membri e nell'elaborazione di certificazioni di cybersecurity** insieme alla Commissione.

In particolare, la proposta in questione prevede che:

- L'ENISA abbia un **mandato permanente** e che i suoi obiettivi vengano periodicamente riesaminati;
- L'ENISA assuma ufficialmente il ruolo di **agenzia europea per la cybersecurity**, oltreché da punto di riferimento nell'ecosistema europeo di cybersecurity;
- L'organizzazione dell'Agenzia tenga conto di tutti gli **stakeholder**, inclusi coloro che, come l'industria, non erano pienamente rappresentati in precedenza;
- Vengano ricompresi tra le competenze dell'Agenzia anche i nuovi settori che richiedono interventi urgenti.

Possono essere così sintetizzate invece le nuove specifiche **competenze** e **priorità d'intervento** per l'ENISA:

- Contribuire allo **sviluppo delle politiche** nel settore della sicurezza delle reti e dell'informazione e **fornire consulenza** in materia;
- Accrescere le **capacità e le competenze delle autorità pubbliche** europee e nazionali;
- Affermarsi quale **centro d'informazione europeo, di analisi, raccolta e condivisione delle *best practices*** nella cybersecurity;
- Fornire consulenza alle autorità nazionali ed europee in merito alla fissazione delle **priorità di ricerca e sviluppo**;
- Aggiornare gli **esercizi pan-europei di cybersecurity** e garantire il funzionamento delle infrastrutture IT del network dei gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT);

- Facilitare la cooperazione tra Stati membri nella **raccolta delle relazioni sulle situazioni nazionali** al fine di rispondere alle emergenze.

Il ***Management Board*** dell'ENISA sarà composto da **un rappresentante per ciascuno Stato membro** e da **due rappresentanti** nominati dalla Commissione. Tutti i rappresentanti avranno diritto di voto.

Il *Management Board*, su proposta del direttore esecutivo, istituirà un **gruppo permanente di interlocutori (*Permanent Stakeholders' Group*) composto da esperti riconosciuti che rappresentano le parti interessate, come l'industria delle TIC, i fornitori di reti o servizi di comunicazione elettronica a disposizione del pubblico**, i gruppi di consumatori, esperti accademici nella sicurezza informatica e rappresentanti delle autorità competenti nonché delle autorità di vigilanza sull'applicazione della legge e sulla protezione dei dati.

2.1.2 QUADRO EUROPEO PER LA CERTIFICAZIONE DI CYBERSECURITYA

La Commissione propone un **sistema europeo di certificazione in materia di sicurezza informatica** che attesti che i prodotti e servizi ICT certificati conformemente a tale sistema siano "*conformi a requisiti specifici per quanto riguarda la loro capacità di resistere ad un certo livello di garanzia, 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*" (**Art. 43**).

Tale quadro **non fissa direttamente schemi di certificazione operativa**, ma **stabilisce piuttosto gli elementi fondamentali e procedurali per permettere all'ENISA**, insieme con le **autorità nazionali di vigilanza** per la certificazione riunite nell'*European Cybersecurity Certification Group*, di istituire **specifici schemi di certificazione** per determinati prodotti e servizi TIC ("***European cybersecurity certification schemes***"). Se rispettosi dei termini e del contenuto minimo fissati dal quadro europeo, gli schemi di certificazione dovranno ritenersi validi e riconosciuti in tutti gli Stati membri. La finalità di questi risiede, dunque, nell'attestare che il prodotto o il servizio TIC, sottoposto a valutazione da parte di un organismo indipendente sulla base di standard comuni, rispetta specifici requisiti di cybersecurity.

Secondo la Commissione, il sistema di certificazione unico garantirebbe una serie di benefici per le imprese e per i cittadini europei, tra cui: la fine dei costosi processi nazionali di certificazione per le imprese; il rafforzamento della conformità con i requisiti fissati dalla Direttiva NIS; la possibilità di creare schemi che offrono livelli flessibili di sicurezza (bassa,

media o alta); una maggiore rassicurazione per gli acquirenti e gli utilizzatori sulla sicurezza dei prodotti che questi ultimi acquistano e utilizzano.

La **certificazione**, che consiste nella valutazione formale di prodotti, servizi e processi da **parte di un organismo indipendente e accreditato secondo un insieme definito di criteri**, dovrebbe servire – secondo la Commissione – ad aumentare la fiducia e la sicurezza nei prodotti e nei servizi.

I diversi sistemi di certificazione attuali degli Stati membri porterebbero ad oneri elevati per le imprese attive in diversi Stati. Ad esempio, per quanto riguarda l'Italia, il 13 aprile 2017 è stato pubblicato sulla Gazzetta Ufficiale n. 87 il decreto relativo alla protezione cibernetica e alla sicurezza informatica nazionale. Tale decreto definisce i meccanismi e le procedure che le infrastrutture essenziali e i fornitori di servizi digitali dovranno seguire ai fini della riduzione delle vulnerabilità, della prevenzione dei rischi, della risposta tempestiva alle aggressioni. Con specifico riferimento alla certificazione, l'art. 11 del suddetto decreto afferma che "il Ministro dello sviluppo economico, fermo restando quanto previsto dal regolamento di cui all'art. 4, comma 3, lettera l, della legge n. 124 del 2007, promuove l'istituzione di un **centro di valutazione e certificazione nazionale** per la verifica delle condizioni di sicurezza e dell'assenza di vulnerabilità di prodotti, apparati e sistemi destinati ad essere utilizzati per il funzionamento di reti, servizi e infrastrutture critiche, di cui al comma 1, nonché di ogni altro operatore per cui sussista un interesse nazionale".

Data la mancanza di omogeneità tra i diversi strumenti di certificazione a livello nazionale, il Regolamento prevede la creazione di un quadro europeo di certificazione della sicurezza della rete per i prodotti e servizi TIC. La proposta non introduce quindi sistemi di certificazione definiti ma stabilisce un quadro per la creazione di specifici schemi di certificazione per prodotti / servizi ICT che dovranno rispettare una serie di criteri comuni a tutti gli Stati membri.

I **programmi di certificazione saranno elaborati dall'ENISA**, con l'assistenza di esperti e la stretta collaborazione del gruppo europeo di certificazione per la cybercurezza.
Il ricorso alla certificazione europea per la cybersecurity dovrebbe rimanere volontario, salvo disposizioni contrarie della legislazione dell'Unione che stabilisca requisiti di sicurezza dei prodotti e dei servizi TIC (non si esclude quindi un carattere di obbligatorietà che potrebbe emergere in futuro perché richiesto da altre legislazioni UE). I certificati sono rilasciati per un **periodo massimo di tre anni** e possono essere rinnovati, alle stesse condizioni, purché i requisiti pertinenti continuino ad essere soddisfatti.

2.2 DIRETTIVA NIS (EU 2016/1148) E COMUNICAZIONE SULLA VALORIZZAZIONE DELLA NIS (COM 2017/476)

Adottata nel luglio 2016, la Direttiva NIS è la prima normativa europea orizzontale finalizzata ad affrontare le sfide della cybersecurity. La Direttiva si pone tre obiettivi fondamentali: migliorare le capacità nazionali di cybersecurity; impostare una cooperazione in materia a livello europeo; promuovere una cultura della gestione del rischio e della comunicazione degli incidenti tra i principali attori economici, in particolare gli operatori che forniscono servizi essenziali ("OES") e i fornitori di servizi digitali ("*Digital Service Providers* – DSPs").

A tal fine, la presente Direttiva:

- Obbliga tutti gli Stati membri a identificare gli operatori dei servizi essenziali con sede nel loro territorio e a dotarsi di una strategia nazionale in materia di sicurezza della rete e dei sistemi informativi (art. 5, 7);
- Istituisce un gruppo di cooperazione per sostenere e agevolare un lavoro congiunto e lo scambio di informazioni tra gli Stati membri (art. 11);
- Crea una rete di gruppi d'intervento per la sicurezza informatica in caso di incidente ("rete CSIRT") per promuovere la fiducia e la cooperazione tra gli Stati membri (art. 12);
- Fissa obblighi di sicurezza e di notifica per gli operatori di servizi essenziali e per i fornitori di servizi digitali (art. 14, 16);
- Obbliga gli Stati membri di designare autorità nazionali competenti, punti di contatto unici e CSIRT con compiti relativi alla sicurezza della rete e dei sistemi informativi (art. 8-9, 17);

Entro il **9 novembre 2018**, gli Stati membri dovranno identificare gli **operatori di servizi essenziali con una sede nel loro territorio** per ciascun settore a cui fa riferimento la Direttiva. Per ritenersi "essenziale", è necessario che si tratti di **un servizio rilevante per il mantenimento di attività sociali o economiche fondamentali, che la fornitura di tale servizio dipenda dalla rete e dai sistemi informativi e che un eventuale incidente abbia effetti negativi rilevanti sulla fornitura del servizio**.

Secondo la Direttiva, ogni Stato membro dovrà adottare una **strategia nazionale in materia di sicurezza della rete e dei sistemi informativi**. Tale strategia dovrà tener conto di una serie di aspetti quali: obiettivi e priorità ben definite in materia di sicurezza delle reti e dei sistemi informativi; un quadro di governance adatto; l'individuazione di misure di preparazione, risposta e recupero; l'indicazione di programmi di formazione, sensibilizzazione, ricerca e sviluppo relativi alla strategia in

materia di sicurezza; un piano di valutazione dei rischi; l'indicazione degli attori coinvolti nell'attuazione della strategia nazionale.

Al fine di sostenere e agevolare la cooperazione strategica e lo scambio di informazioni tra Stati membri nell'ottica della sicurezza delle reti e dell'informazione, la Direttiva prevede l'istituzione di un **gruppo di cooperazione** composto dai rappresentanti degli Stati membri, della Commissione europea e dell'ENISA. Il gruppo si occupa principalmente di scambiare informazioni e buone pratiche tra gli Stati membri in merito alla sicurezza delle reti e dell'informazione, fornire orientamenti strategici per le attività della **rete di CSIRT** e valutare le singole strategie nazionali in materia.

Con l'obiettivo più specifico di stimolare la collaborazione e la fiducia fra gli Stati membri, è stata istituita anche una rete di CSIRT. Composta dai CSIRT dei vari Stati membri, ossia i gruppi di intervento designati a livello nazionale per trattare gli incidenti e i rischi secondo procedure definite, la rete ha la funzione di scambiare informazioni sulle attività dei singoli CSIRT, oltreché informazioni relative a singoli incidenti, e fornire sostegno agli Stati membri che hanno subito incidenti transfrontalieri.

La Direttiva richiede, inoltre, che gli operatori e i fornitori di servizi essenziali e digitali adottino **misure organizzative per la gestione dei rischi per la sicurezza delle reti e dei sistemi informativi**, nonché strumenti per prevenire e notificare eventuali incidenti occorsi.

Infine, ogni Stato membro dovrà designare una o più **autorità nazionali competenti in materia di sicurezza delle reti e dei sistemi informativi** che dovrà occuparsi dell'applicazione della Direttiva a livello nazionale. A meno che non venga ricompreso nel ruolo dell'autorità nazionale, andrà designato anche un **punto di contatto unico** per ogni Stato membro, che svolgerà una funzione di collegamento per garantire la cooperazione transfrontaliera delle autorità degli Stati membri con le autorità competenti negli altri Stati membri, con il gruppo di cooperazione e con la rete di CSIRT.

2.3 PROPOSTA DI DIRETTIVA RELATIVA ALLA LOTTA CONTRO LE FRODI E LE FALSIFICAZIONI DI MEZZI DI PAGAMENTO DIVERSI DAI CONTANTI (COM 2017/489)

Attualmente, la decisione quadro 2001/413/GAI stabilisce norme minime comuni per punire penalmente le frodi ai mezzi di pagamento diversi dai contanti. L'agenda europea sulla sicurezza ha riconosciuto, tuttavia, che tale decisione quadro non riflette più la realtà odierna e non è più in grado di far fronte alle nuove sfide e alle nuove tecnologie operanti nelle transazioni economiche attuali. La Commissione ha ritenuto quindi di

dover prevedere nuovi strumenti di contrasto alle frodi con mezzi di pagamento diversi dai contanti. Oltre che fonti importanti d'entrata per la criminalità organizzata, tali tipi di frodi rappresentano un ostacolo allo sviluppo del mercato unico digitale, in termini di perdita economica diretta e di riduzione della fiducia dei consumatori.

Alla luce delle principali vulnerabilità individuate dalla Commissione, attinenti all'**incompletezza del quadro giuridico attuale e alle lacune nella prevenzione delle frodi**, la presente proposta di Direttiva persegue **tre obiettivi specifici**: istituire un quadro politico e giuridico chiaro e tecnologicamente neutro; eliminare gli ostacoli operativi alle indagini e alle azioni penali; migliorare l'intero sistema della prevenzione.

Per far ciò, la proposta di Direttiva chiede agli Stati membri di adottare una serie di misure per rendere punibili atti commessi intenzionalmente. Tra questi si segnalano: l'utilizzo fraudolento di mezzi di pagamento rubato o contraffatto; furto o altra appropriazione indebita di strumenti di pagamento; ottenimento ai fini di utilizzo, vendita o distribuzione di un mezzo di pagamento rubato o indebitamente appropriato; effettuare o indurre un trasferimento di denaro per procurare un ingiusto profitto all'autore del reato intervenendo su dati informatici, ostacolando o interrompendo un sistema di informazione. Dal punto di vista sanzionatorio, inoltre, la proposta richiede la previsione da parte degli Stati di **apposite sanzioni detentive e interdittorie**, rispettivamente per le persone fisiche e giuridiche che commettono i reati considerati nel testo normativo.

Per quanto riguarda le indagini e la cooperazione interstatale, infine, la Commissione ha richiesto la creazione di appositi strumenti d'indagine, simili a quelli utilizzati contro la criminalità organizzata, e ha previsto l'istituzione da parte degli Stati membri di un apposito punto di contatto operativo a livello nazionale. Ogni centro, disponibile 24h su 24 e 7 giorni su 7, dovrà occuparsi di gestire le richieste di assistenza e provvedere ad un efficace scambio di informazioni relative ai reati previsti dalla proposta di Direttiva.

2.4 RACCOMANDAZIONE DELLA COMMISSIONE RELATIVA ALLA RISPOSTA COORDINATA AGLI INCIDENTI E ALLE CRISI DI CYBERSECURITY SU VASTA SCALA (C 2017/6100)

La Commissione europea ha stabilito che un incidente di cybersecurity può essere considerato una "crisi" a livello dell'Unione quando le perturbazioni da esso conseguenti sono così ampie **da non poter essere garantite autonomamente da uno o più Stati membri pregiudicati e il cui impatto sia così vasto da richiedere una risposta tempestiva da parte dell'Unione**.

Sin dal 2016, la Commissione incoraggia gli Stati membri a sfruttare gli strumenti di risposta coordinata offerti dalla Direttiva NIS. Tuttavia, quest'ultima non ha previsto un quadro di cooperazione dell'Unione in caso di incidenti e crisi di cybersecurity di vasta scala. Per tale ragione, la Commissione ha avviato una consultazione in materia ad aprile 2017, i cui contributi sono stati ricompresi nella raccomandazione presa in considerazione e nel relativo allegato.

Nella sua raccomandazione, la Commissione ha chiesto agli Stati membri di **istituire un quadro di risposta alle crisi di cybersecurity dell'UE** che delinei i soggetti interessati e le procedure operative standard per favorire la cooperazione delle varie parti. In linea con il suddetto programma, gli Stati membri dovrebbero stabilire, in collaborazione con i servizi della Commissione e il SEAE, una serie di orientamenti per l'attuazione pratica delle procedure in modo condiviso e secondo i vigenti meccanismi dell'UE di gestione delle crisi, ossia l'IPCR e il CRM del SEAE.

Tra le misure presenti nell'Allegato della Raccomandazione, si segnala in particolare la proposta di rendere operativo e funzionale il c.d. "**Fondo di risposta alle emergenze cibernetiche**". Seguendo l'esempio di altri meccanismi di crisi che operano in diversi settori normativi dell'UE, il Fondo consentirebbe agli Stati membri di chiedere aiuto a livello dell'UE durante o dopo incidenti gravi, sempre che lo Stato membro vittima si sia dotato, prima dell'incidente, di un sistema nazionale di vigilanza e di un sistema di cybersecurity coerente con i termini della Direttiva NIS. La sua funzione di integrazione dei preesistenti meccanismi di gestione delle crisi a livello UE consentirebbe sia una risposta rapida nell'interesse della solidarietà, sia un finanziamento delle azioni specifiche di risposta alle emergenze.

LINK AI DOCUMENTI

Proposta di Regolamento sull'ENISA e sulla certificazione di cybersecurity delle tecnologie d'informazione e comunicazione (COM 2017/477)

Decreto del Presidente del Consiglio dei Ministri del 17 febbraio 2017 relativo alla protezione cibernetica e alla sicurezza informatica nazionale Direttiva NIS (EU 2016/1148)

Comunicazione sulla valorizzazione della NIS (COM 2017/476)

Proposta di Direttiva relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti (COM 2017/489)

Raccomandazione della Commissione relativa alla risposta coordinata agli incidenti e alle crisi di cybersecurity su vasta scala (C 2017/6100)

Comunicazione congiunta al Parlamento europeo e al Consiglio – Resilienza, deterrenza e difesa: verso una cybersecurity forte per l'UE (JOIN 450/2017)

Comunicato stampa: Stato dell'Unione 2017 - Cybersecurity: la Commissione intensifica la sua risposta ai ciberattacchi

Stato dell'Unione 2017: Cybersecurity: la Commissione intensifica la sua risposta ai ciberattacchi – Domande e risposte

Strategia Europea di Cybersecurity

Per maggiori informazioni: Cinzia Guido, c.guido@confindustria.eu