CONFINDUSTRIA

Position Paper

Cybersecurity Act

Proposta di Regolamento UE sull'ENISA e su uno schema di certificazione cybersecurity per le tecnologie dell'informazione e della comunicazione

Novembre 2017

Position Paper

CONTESTO

La crescente dipendenza della vita quotidiana e dell'economia globale dalle nuove tecnologie digitali ha reso la cybersecurity una questione di vitale importanza per cittadini e imprese.

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

Secondo l'*International Data Corporation* (IDC), entro il 2025, quasi il 90% di tutti i dati creati a livello globale richiederà un certo livello di sicurezza, ma meno della metà sarà effettivamente protetto[1]. Allo stesso tempo, il numero e l'intensità dei ciberattacchi è aumentato negli anni. Il suo impatto economico è quintuplicato nel periodo 2013-2017 e potrebbe ulteriormente aumentare di quattro volte entro il 2019[2].
Secondo la piramide sulla cybersecurity di Maslow definita dall'Agenzia europea per la cybersecurity - ENISA - , le sfide che devono affrontare le imprese, i cittadini e la società sono sempre più di cruciale importanza[3].

Con riferimento in particolare all'Italia, il nostro Paese è il settimo al mondo e il secondo in Europa più colpito dai *ransomware*[4], ossia gli attacchi che si configurano come estorsioni informatiche e che bloccano l'attività di un computer o di un qualsiasi oggetto connesso a fronte della richiesta di un riscatto economico per la sua "liberazione". Nel periodo gennaio 2016 - giugno 2017, infatti, l'Italia è stata raggiunta dal 2,53% di ransomware di tutto il mondo. Più colpiti di noi: USA (15%), Brasile (12,01%), India (9%), Vietnam (5,11%), Turchia (4,60%), Messico (4,19%). A livello europeo, invece, l'Italia è seconda (10,03%) dopo la Turchia (18,23%) e seguita da Germania (9,51%), Spagna (6,84%) e Francia (6,62%).

Alla luce del carattere sempre più transfrontaliero di tali violazioni, la Commissione europea ha deciso di adeguare alle nuove sfide la prima Strategia dell'Unione europea per la cybersecurity del 2013.

Parte di tale revisione è la proposta di Regolamento COM(2017)477 che mira al **rafforzamento dell'ENISA**, a cui viene attribuito un mandato permanente a fornire sostegno agli Stati Membri, alle Istituzioni e alle imprese in ambiti chiave tra cui quello dell'attuazione della direttiva NIS, e

[1] Data Age 2025: The Evolution of Data to Life-Critical
[2] Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, Commission Communication, 2017
[3] https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-input-to-the-css-review-b
[4] Fonte: Trend Micro "The cost of compromise", 2017

istituisce un **quadro europeo per la certificazione della cybersecurity per le tecnologie della comunicazione e dell'informazione.**

Confindustria sostiene l'iniziativa della Commissione europea di rafforzare il mandato di ENISA e di identificare sistemi di certificazione che possano soddisfare le esigenze europee.

Obiettivo ultimo dovrà essere quello di dotare l'UE di una strategia per la cybersecurity **robusta, flessibile**, **adatta alle nuove sfide**, **pro-innovazione e tecnologicamente neutrale**.

Di seguito alcune puntuali considerazioni.

1. RUOLO DELL'ENISA

Per Confindustria è **positivo che l'ENISA goda di un mandato permanente** al fine di continuare a sostenere il *capacity building* negli Stati membri in materia di cybersecurity.
La piena applicazione della direttiva NIS (Direttiva 2016/1148 per la sicurezza delle reti e delle informazioni), inoltre, richiederà un mandato più stabile per l'ENISA, ad esempio per agevolare la creazione di centri settoriali di condivisione e di analisi delle informazioni (ISAC).

Il ruolo dell'ENISA dovrà esser anche quello di **migliorare la fiducia** tra i partner pubblici e privati, la **condivisione delle conoscenze** e delle **informazioni**. Una risposta efficace agli attacchi di sicurezza informatica a livello UE richiede, infatti, un'effettiva cooperazione tra tutti gli *stakeholders* attraverso procedure e meccanismi di cooperazione che **definiscano con chiarezza i ruoli e le responsabilità dei principali attori** a livello nazionale ed europeo.

L'ENISA dovrebbe inoltre sostenere le autorità nazionali ed europee nella definizione delle priorità in materia di ricerca e sviluppo sulla sicurezza informatica ed essere di sostegno al nuovo **Centro europeo di ricerca e competenze sulla sicurezza cibernetica** e al network di ***competence center*** nei Paesi membri.

L'aumento della **cooperazione pubblico-privata è fondamentale anche in termini di risorse**. Il partenariato pubblico-privato sulla Cybersecurity del 2016 ha portato ad un aumento degli investimenti nella sicurezza delle reti di 1,8 miliardi di euro da qui al 2020. Tale risultato non può dirsi soddisfacente, basti pensare che gli Stati Uniti investiranno 17 miliardi di dollari solo nel 2017.

Con specifico riferimento, invece, al ruolo dell'ENISA nella definizione dello schema UE di certificazione di cybersecurity, nella nuova struttura di governance proposta **risulta estremamente limitato il ruolo degli**

stakeholder industriali. Infatti, a seguito di un'eventuale richiesta della Commissione di predisporre uno schema di certificazione, l'ENISA dovrà consultare solo le autorità di certificazione nazionali riunite nel nuovo "Gruppo di Certificazione sulla Cibersicurezza". A nostro avviso, è fondamentale coinvolgere sin dalle prime fasi di tale processo gli **stakeholder industriali** che hanno a cuore gli interessi strategici dell'UE. Pertanto il Gruppo di Certificazione sulla Cibersicurezza **dovrebbe essere affiancato da un gruppo di rappresentanti industriali (sia produttori che utilizzatori di ICT)** in grado di offrire quel *know-how* necessario a definire opportunamente tale schema di certificazione.

2. SCHEMA UE DI CERTIFICAZIONE CYBERSECURITY PER L'ICT

Confindustria condivide l'iniziativa della Commissione di definire un quadro europeo per la certificazione di cybersecurity che possa sostituirsi ai diversi schemi di certificazione nazionali e garantire armonizzazione a livello europeo.

Lo schema di certificazione potrà condurre ai risultati desiderati e incrementare la fiducia nei prodotti e servizi digitali se sarà **dinamico**, **adattabile** alle specifiche esigenze, definito in **stretta collaborazione con i rappresentanti industriali**, in grado di certificare la capacità di **un'organizzazione di reagire a nuove minacce e rischi** e di fornire in maniera **trasparente le informazioni necessarie** circa la capacità di rispondere a tali minacce.

In un contesto di industria connessa, è anzitutto fondamentale che tutte le parti della catena del valore svolgano responsabilmente il loro ruolo nella gestione del rischio e garantiscano "**dinamicamente**" la sicurezza dell'intero ciclo produttivo e di erogazione di servizi sin dalle prime fasi (***security-by-design***). A tal fine, riteniamo che l'**Art 45** "***Obiettivi di sicurezza dei sistemi di certificazione europea***", debba ricomprendere anche la necessità per prodotti e servizi ICT di incorporare direttamente le caratteristiche di cybersecurity **sin dalle fasi iniziali di sviluppo tecnico e progettazione e di aggiornarle dinamicamente**. Un forte impegno sulla ***security-by-design*** è, infatti, necessario per rafforzare le capacità di sicurezza dell'industria.

Non è invece condivisibile il rinnovo obbligatorio dei certificati ogni 3 anni, come richiesto dall'**art. 48, paragrafo 6**. Tale misura non premia, infatti, un intervento attivo e dinamico e rischia di portare alla mera compilazione, ogni tre anni, di un documento che attesti il livello di sicurezza accrescendo inutilmente il business delle certificazioni.
Nell'ambiente ICT, se una certificazione è "statica" (ovvero certifica la conformità in un dato momento ma non fornisce alcuna regola per l'aggiornamento continuo) non consente di attestare la capacità di un prodotto o un servizio di rispondere a nuove minacce informatiche. Dal

momento che la conformità ai requisiti di sicurezza della rete è, innanzitutto, una **questione organizzativa**, riteniamo che l'approccio più efficace per garantire la conformità dinamica è quello di introdurre nella certificazione precise procedure organizzative e tecniche che garantiscano che il fornitore di TIC abbia messo in atto un modello organizzativo in grado di reagire in modo efficace e tempestivo a nuove sfide e minacce. In questo senso riteniamo che **l'art. 46.2** debba anche fare riferimento alle procedure organizzative incluse nel certificato per garantire la conformità.

Nel definire il sistema di certificazione la Commissione e l'ENISA dovranno **tenere in debita considerazione un rischio marginale**, consapevoli che non esiste una sicurezza del 100%. Pertanto, sarà fondamentale il coinvolgimento del settore industriale nella definizione dei livelli minimi dei requisiti di sicurezza (**art. 46**). Le autocertificazioni da parte dei fornitori di tali requisiti di sicurezza dei dispositivi IoT rappresentano in tal senso una misura proporzionale.
Occorrerà inoltre flessibilità nel modo in cui l'adesione a un programma di certificazione sia comunicato, purché in maniera chiara e trasparente, agli utenti, tramite sito web, una casella o altri mezzi.

L'ENISA dovrebbe determinare le priorità da perseguire in stretta cooperazione con gli attori industriali (utilizzatori e fornitori di servizi ICT). Gli elementi da includere nell'**Art. 47** ***"Elementi della certificazione europea di cybersecurity"*** dovrebbero guidare e non prescrivere la definizione dello schema di certificazione.

Inoltre, il quadro europeo delle certificazioni rischia di aumentare le pratiche di etichettatura che dimostrino la richiesta conformità.
Anzitutto, occorre operare una chiara distinzione tra certificazione e etichettatura. L'etichettatura può avere un vantaggio sul mercato dei consumatori, fornendo informazioni visibili ai clienti, mentre i sistemi di certificazione svolgono un ruolo più importante nei sistemi e nei servizi delle aziende TIC. Qualsiasi discussione sull'etichettatura non deve pertanto essere direttamente collegata a schemi di certificazione senza considerare questi due strumenti separatamente. .

Qualsiasi "etichetta" sarà utile tanto quanto la sorveglianza del mercato che ne seguirà. Gli Stati membri dovranno destinare adeguate risorse al controllo del mercato e di attori *non-bona fide* che vorranno certificare tecnologie non conformi, senza che questo conduca a ulteriore sovraccarico legislativo.

L'ampia e diversificata gamma di prodotti e servizi IoT, nonché i rischi connessi, richiederà un sistema di certificazione che **risponda alle esigenze di settori diversi**. Lo schema dovrà risultare adattabile a specifiche esigenze e priorità (principio del "***no one-size-fits-all***") e garantire l'interoperabilità nel contesto europeo ed internazionale.

Tale schema dovrà inoltre trovare il **giusto equilibrio** tra la necessità di assicurare il più elevato livello di sicurezza dei prodotti/servizi e i costi che le imprese, in particolare le PMI e le start-up, saranno chiamate a sostenere. Il processo di certificazione comporterà, infatti, per le imprese dei costi di sviluppo e di *testing* (specialmente per i software), sensibilmente più alti che nel processo di sviluppo convenzionale, come dimostrato dai costi di sviluppo in quei settori che già adottano tali schemi.

Il quadro di certificazione dovrà **tenere in debita considerazione ciò che già esiste a livello europeo** (ad esempio il **GDPR** e la direttiva **NIS**). Il GDPR presto obbligherà le organizzazioni a stabilire delle misure specifiche per la sicurezza della rete, come la protezione contro la perdita, l'alterazione, la divulgazione di dati e l'accesso non autorizzato ai dati. La direttiva NIS assicura agli Stati membri di poter contare su autorità competenti in grado di reagire in caso di cyber attacchi e di notificarli.
Sarebbe importante assicurare che le procedure di segnalazione di violazione dei dati da parte delle imprese, previste sia nel GDPR che nella Direttiva NIS, vengano elaborate in modo da chiedere alle Autorità preposte di rispondere con precise informazioni alle imprese sul relativo crimine informatico.

Infine, il Regolamento non dovrebbe consentire il backdoor e dovrebbe promuovere l'uso della **crittografia**, diventata uno degli strumenti più importanti a servizio di governi, imprese e cittadini per la sicurezza nell'era digitale.

3. FURTO DI DATI INDUSTRIALI E SEGRETI COMMERCIALI

Confindustria rileva come la proposta **non affronti il problema dei ciberattacchi alle imprese sotto forma di furto di tecnologie, di segreti commerciali e di altre informazioni industriali confidenziali**. Le imprese innovative sono sempre più esposte a pratiche disoneste finalizzate all'appropriazione indebita di segreti commerciali e proprietà intellettuale (PI). Il furto industriale di PI e segreti commerciali è in continuo aumento: tali attacchi rappresentano il 25% di tutti gli attacchi informatici in tutti i settori, e fino al 94% di tutti i cyber attacchi nel settore manifatturiero nel 2016[5]. Si prevede che il costo dei furti di PI industriale e dei segreti commerciali dovrebbe essere circa dell'1-2% del PIL[6] e provocherà una perdita di competitività, riduzione degli investimenti in R&S e posti di lavoro. Nell'interesse dell'innovazione, è opportuno prendere in considerazione risposte ex-ante efficaci in tutte le politiche dell'UE e incoraggiare l'uso di innovazioni tecnologiche (es. *blockchain*) che consentano di prepararsi a questi attacchi.

[5] Net Losses: Estimating the Global Cost of Cybercrime, Economic impact of cybercrime II, Center for Strategic and International Studies June 2014, https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf
[6] https://create.org/resource/economic-impact-of-trade-secret-theft/

La Commissione dovrebbe lanciare uno studio per determinare quali opzioni legali esistono per scoraggiare gli Stati nel supportare, autorizzare, tollerare o trascurare la prevenzione di ciberattacchi o ciberintrusioni.

4. STANDARDIZZAZIONE

I sistemi di certificazione UE per la sicurezza informatica dovrebbero utilizzare gli standard esistenti in relazione ai requisiti tecnici e alle procedure di valutazione che i prodotti dovranno rispettare.
Sarà anzitutto necessario, pertanto, portare a termine l'identificazione degli standard preesistenti o mancanti per determinati prodotti e servizi prima che vengano adottati nuovi schemi. Inoltre, è fondamentale assicurare un ruolo di **primo piano** alle **organizzazioni di standardizzazione europee** (es. CEN/CENELEC e ETSI) nel processo di sviluppo degli schemi di certificazione data la loro esperienza nello sviluppo di regolamenti tecnici.

Gli standard a cui dovranno rifarsi gli schemi dovranno facilitare **l'interoperabilità, evitare le duplicazioni, essere rilevanti per l'industria** e definiti in modo **aperto e trasparente**.

5. CONSAPEVOLEZZA

Dal momento che il 95% di tutti gli incidenti di cybersecurity è dovuto a errori umani, sono soprattutto gli utenti i più vulnerabili del ciberspazio. È pertanto necessario istruirli e renderli consapevoli di quanto sia importante l'"igiene informatica" dei dispositivi connessi.

Qualsiasi **iniziativa e supporto** da parte della Commissione e degli Stati membri a questo proposito può davvero fare la differenza e sostenere gli sforzi delle imprese che investono continuamente nella sicurezza della rete.

Gli utenti delle tecnologie IoT dovrebbero essere incoraggiati a mantenere aggiornati i propri dispositivi a beneficio dell'intero cyberspazio. Ciò richiederà sforzi da parte dell'industria nel diffondere le *best practice* e dell'UE nel sostenere tale impegno attraverso finanziamenti adeguati a valere su Horizon 2020, Fondi strutturali ed EFSI.

Inoltre il *gap* di competenze in materia di cybersecurity per i professionisti che lavorano nel settore privato è destinato a crescere a 1,8 milioni a livello mondiale e a 350 mila a livello europeo entro il 2022[7]. Riteniamo

[7] https://iamcybersafe.org/gisws/

fondamentale **aggiornare i sistemi educativi nazionali** in modo che ingegneri, programmatori, sviluppatori e altre occupazioni che saranno create dall'esplosione di dispositivi IoT in vari settori delle nostre società, saranno in grado di comprendere l'importanza della sicurezza della rete.