Consiglio dell'Unione europea

Bruxelles, 7 luglio 2016
(OR. en)

11013/16

CYBER 83
COMPET 411
IND 158
RECH 246
TELECOM 129

NOTA DI TRASMISSIONE

Origine:	Jordi AYET PUIGARNAU, Direttore, per conto del Segretario Generale della Commissione europea
Data:	5 luglio 2016
Destinatario:	Jeppe TRANHOLM-MIKKELSEN, Segretario Generale del Consiglio dell'Unione europea
n. doc. Comm.:	COM(2016) 410 final
Oggetto:	COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI Rafforzare il sistema di resilienza informatica dell'Europa e promuovere la competitività e l'innovazione nel settore della cibersicurezza

Si trasmette in allegato, per le delegazioni, il documento COM(2016) 410 final.

All.: COM(2016) 410 final

COMMISSIONE
EUROPEA

Bruxelles, 5.7.2016
COM(2016) 410 final

COMUNICAZIONE DELLA COMMISSIONE AL PARLAMENTO EUROPEO, AL CONSIGLIO, AL COMITATO ECONOMICO E SOCIALE EUROPEO E AL COMITATO DELLE REGIONI

Rafforzare il sistema di resilienza informatica dell'Europa

e promuovere la competitività e l'innovazione nel settore della cibersicurezza

1. INTRODUZIONE/CONTESTO

Gli incidenti informatici di sicurezza, che ogni giorno causano gravi danni economici alle imprese europee e danneggiano l'economia nel suo complesso, minano la fiducia di cittadini e imprese nella società digitale. Il furto di segreti commerciali, informazioni aziendali e dati personali, l'interruzione dei servizi - anche di quelli essenziali - e la perturbazione delle infrastrutture provocano ogni anno danni economici per centinaia di miliardi di euro[1], oltre ad avere potenziali conseguenze per i diritti fondamentali dei cittadini e per la società in generale.

La strategia dell'Unione europea per la cibersicurezza del 2013[2] (strategia dell'UE per la cibersicurezza) e il suo elemento centrale, ossia la direttiva sulla sicurezza delle reti e dell'informazione[3] di prossima adozione e la direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione, costituiscono il fulcro delle misure adottate finora dall'Unione europea per rispondere a queste sfide. Inoltre, l'UE ha a sua disposizione organismi specializzati come l'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA), il Centro europeo per la lotta alla criminalità informatica (EC3) presso l'Europol e la squadra di risposta alle emergenze informatiche (CERT-UE). Recentemente sono state lanciate anche diverse iniziative settoriali (ad esempio per l'energia e i trasporti) al fine di rafforzare la cibersicurezza in diversi settori cruciali.

Nonostante questi risultati positivi, l'UE resta vulnerabile agli incidenti informatici. Tale vulnerabilità potrebbe danneggiare il mercato unico digitale e la vita economica e sociale nel suo complesso, con ripercussioni capaci di oltrepassare la sfera economica. Nel caso delle minacce ibride[4], gli attacchi informatici possono essere coordinati con altre attività per destabilizzare un paese o minare le istituzioni politiche.

In un contesto del genere, gestire un incidente informatico su vasta scala che coinvolga più Stati membri contemporaneamente pone all'UE potenziali difficoltà. Innescando sinergie con le comunicazioni sulla lotta contro le minacce ibride e sull'attuazione dell'Agenda europea sulla sicurezza[5], la Commissione sta valutando come affrontare la realtà in evoluzione della cibersicurezza e quali sono le misure aggiuntive che potrebbero essere necessarie per migliorare la resilienza dell'UE in questo ambito e la sua risposta agli incidenti informatici.

La Commissione sta inoltre affrontando la questione delle capacità industriali dell'Unione europea in materia di cibersicurezza. Anche se forse l'Europa non riuscirà ad appropriarsi dell'intera catena del valore delle tecnologie digitali, è necessario almeno mantenere e sviluppare determinate capacità essenziali. L'offerta di prodotti e servizi in grado di assicurare il massimo livello di sicurezza informatica è un'opportunità per il settore della cibersicurezza

[1] *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies; Giugno 2014.*
[2] JOIN(2013) 1.
[3] COM(2013) 48.
[4] JOIN(2016) 18.
[5] COM(2016) 230.

in Europa e potrebbe diventare un importante vantaggio competitivo. Il mercato mondiale della cibersicurezza dovrebbe collocarsi tra i comparti a più rapida espansione del settore delle TIC[6]. Perché l'UE possa svolgere un ruolo guida in questo campo sono necessarie una forte cultura di sicurezza dei dati, compresi i dati personali, e una reazione efficace agli incidenti. Tali fattori agiranno da forte incentivo agli investimenti nell'UE, contribuendo così agli ambiziosi obiettivi del mercato unico digitale in termini di crescita e occupazione.

Per raggiungere gli obiettivi sopra citati è necessario un forte impegno, volto in particolare a:

i) rafforzare la cooperazione in modo da essere più preparati agli incidenti informatici e gestirli adeguatamente

È necessario rafforzare i meccanismi di cooperazione esistenti e concordati affinché l'UE possa divenire più resiliente ed essere più preparata, anche nell'eventualità di una crisi di cibersicurezza paneuropea. Questi meccanismi di cooperazione devono essere completi, ossia coprire l'intero ciclo di vita di un incidente, dalla prevenzione alla repressione. Un'efficace cooperazione tra gli Stati membri e l'attuazione pratica delle disposizioni in materia di sicurezza per gli operatori critici richiederà inoltre all'industria delle cibersicurezza robuste soluzioni tecniche.

Allo stesso tempo, per garantire la resilienza degli asset informatici critici in tutta l'UE saranno necessari sforzi incessanti per trovare sinergie intersettoriali e integrare le disposizioni in materia di cibersicurezza in tutte le pertinenti politiche dell'UE. La Commissione valuterà la necessità di aggiornare, nel prossimo futuro, la strategia dell'UE per la cibersicurezza del 2013.

ii) Reagire alle sfide che il mercato unico della cibersicurezza europeo si trova ad affrontare

La strategia per il mercato unico digitale[7] ha riconosciuto che nel settore in rapido mutamento delle tecnologie e soluzioni per la sicurezza delle reti permangono lacune specifiche. Allo stesso tempo, studi di mercato indicano che il mercato interno dell'UE è ancora geograficamente frammentato per quanto riguarda l'offerta di prodotti e servizi per la cibersicurezza informatica[8]. La presente comunicazione definisce una serie di misure orientate al mercato per far fronte a queste lacune e difficoltà del mercato unico.

iii) Incoraggiare lo sviluppo di capacità industriali nel campo della cibersicurezza

Nella strategia per la cibersicurezza e nella strategia per il mercato unico digitale, la Commissione si è impegnata a promuovere un aumento dell'offerta di prodotti e servizi da parte del settore della cibersicurezza dell'UE. Di conseguenza, la Commissione adotterà una decisione che aprirà la strada a un accordo contrattuale per un partenariato pubblico-privato (PPP) sulla cibersicurezza, che avrà come obiettivo la promozione di un programma europeo

[6] Cfr. SWD(2016) 216.
[7] COM(2015) 192.
[8] Cfr. SWD(2016) 216.

di ricerca e innovazione all'avanguardia nel campo della cibersicurezza al fine di accrescere la competitività.

2. UN LIVELLO SUPERIORE DI COOPERAZIONE, CONOSCENZE E CAPACITÀ

La strategia dell'UE per la cibersicurezza, e in particolare l'imminente direttiva sulla sicurezza delle reti e dell'informazione[9], aprirà la strada a una maggiore cooperazione a livello UE tra gli Stati membri. La rapida ed efficace attuazione della direttiva sarà fondamentale alla luce della crescente digitalizzazione della vita economica e sociale (anche in considerazione del *cloud computing*, dell'internet degli oggetti e della comunicazione da macchina a macchina), della crescente interconnessione transfrontaliera e del panorama in rapida evoluzione delle minacce cibernetiche[10]. In tale contesto, l'UE deve prepararsi all'eventualità di una crisi cibernetica su vasta scala[11], compresi ad esempio gravi attacchi simultanei ai sistemi informatici critici in diversi Stati membri[12].

La cooperazione a livello di UE è pertanto essenziale per gestire sia gli incidenti informatici di minore entità ma in grado di propagarsi, sia un eventuale attacco informatico su vasta scala in più Stati membri. L'UE deve integrare gli aspetti relativi alla sicurezza informatica negli attuali meccanismi di gestione delle crisi. Deve altresì assicurare una cooperazione efficace e meccanismi rapidi di condivisione delle informazioni tra settori e Stati membri per reagire agli incidenti e contenerli. Inoltre, tali meccanismi dovrebbero operare in modo coerente, contribuendo così alla lotta contro il terrorismo, il crimine organizzato e il crimine informatico. Ciò contribuirebbe altresì a rafforzare la capacità dell'UE di coordinarsi con i partner internazionali per rispondere efficacemente alle minacce e agli incidenti su scala mondiale.

2.1. Sfruttare al massimo i meccanismi di cooperazione per la sicurezza delle reti e dell'informazione e progredire verso una nuova fase dell'ENISA

Un elemento essenziale delle capacità nazionali richieste dalla direttiva sulla sicurezza delle reti e dell'informazione è costituito dai gruppi di intervento per la sicurezza informatica in caso di incidente (CSIRT), che hanno la responsabilità di reagire rapidamente alle minacce e agli incidenti informatici. Essi formeranno una rete di CSIRT in grado di promuovere un'efficace cooperazione operativa per specifici incidenti connessi alla cibersicurezza e la condivisione delle informazioni sui rischi. Inoltre, la direttiva istituirà un gruppo di cooperazione per sostenere e facilitare la cooperazione strategica tra gli Stati membri e instaurare tra loro un clima di fiducia.

Tenuto conto della natura e della molteplicità delle minacce informatiche, la Commissione incoraggia gli Stati membri a sfruttare al massimo i meccanismi di cooperazione in materia di

[9] La direttiva sulla sicurezza delle reti e dell'informazione imporrà agli Stati membri di individuare una serie di operatori in grado di fornire servizi essenziali in settori quali energia, trasporti, finanza e sanità, di far fronte ai rischi per la cibersicurezza e di fare in modo che determinati fornitori di servizi digitali adottino misure appropriate per fronteggiare tali rischi.
[10] Cfr. SWD(2016) 216.
[11] Cfr. ad esempio la relazione dell'ENISA: Common practices of EU-level crisis management and applicability to cyber crises (aprile 2016).
[12] Cfr. SWD(2016) 216.

sicurezza delle reti e dell'informazione, come pure a rafforzare la cooperazione transfrontaliera per poter fronteggiare un indicente informatico su vasta scala. Questo rafforzamento della cooperazione in caso di incidenti informatici significativi trarrebbe vantaggio da un approccio coordinato alla cooperazione tra i vari elementi dell'ecosistema informatico nelle situazioni di crisi. Un approccio di questo tipo può essere definito in un "programma", che dovrebbe anche garantire sinergie e coerenza con i meccanismi esistenti di gestione delle crisi[13]. Bisognerebbe quindi testarlo regolarmente nel quadro di esercizi di gestione delle crisi connesse alla cibersicurezza e di altro genere. Il programma prevedrebbe un ruolo per organismi UE quali l'ENISA, il CERT-UE e il Centro europeo per la lotta alla criminalità informatica (EC3) presso l'Europol e il ricorso a strumenti sviluppati nell'ambito della rete di CSIRT. Nel primo semestre del 2017 la Commissione sottoporrà un simile programma di cooperazione all'esame del gruppo di cooperazione, della rete di CSIRT e di altre parti interessate.

Allo stato attuale le conoscenze e le competenze in materia di cibersicurezza disponibili a livello dell'UE sono frammentate e non strutturate. Al fine di sostenere i meccanismi di cooperazione in materia di sicurezza delle reti e dell'informazione, le informazioni dovrebbero essere raggruppate in una "piattaforma d'informazione" affinché tutti gli Stati membri possano accedervi facilmente su richiesta. Tale piattaforma diventerebbe una risorsa centrale che permetterebbe alle istituzioni dell'UE e agli Stati membri di scambiarsi le informazioni in base alle necessità. Un accesso più agevole a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni dovrebbe aiutare gli Stati membri a rafforzare le proprie capacità e ad allineare le rispettive pratiche, rafforzando di conseguenza la resilienza complessiva agli attacchi. La Commissione, con l'appoggio dell'ENISA e del CERT-UE e grazie alle competenze del suo Centro comune di ricerca, faciliterà la creazione della piattaforma e ne assicurerà la sostenibilità.

Inoltre, dovrebbe essere costituito a livello di UE un gruppo consultivo regolare ad alto livello[14] sulla cibersicurezza, composto da esperti e responsabili decisionali dell'industria, del mondo accademico, della società civile e di altre organizzazioni interessate. Il gruppo offrirebbe alla Commissione competenze e contributi esterni, in modo aperto e trasparente, per la sua strategia in materia di cibersicurezza e per le eventuali misure normative o per altri interventi in settori specifici. Il gruppo integrerebbe altre strutture operanti nell'ambito della cibersicurezza con cui agirebbe in collegamento[15] .

Inoltre, la Commissione è tenuta a effettuare una valutazione dell'ENISA entro il 20 giugno 2018 e l'eventuale mandato dell'ENISA nuovo o modificato dovrà essere adottato entro il 19 giugno 2020[16]. In considerazione dell'attuale panorama della cibersicurezza, la

[13] In particolare, i dispositivi integrati per la risposta politica alle crisi, compresi la decisione relativa alle modalità di attuazione da parte dell'Unione della clausola di solidarietà (24 luglio 2014) e i processi decisionali della politica di sicurezza e di difesa comune.
[14] I gruppi di esperti della Commissione sono soggetti alle norme orizzontali stabilite dalla decisione della Commissione C(2016)3301.
[15] Ad esempio la piattaforma NIS (Network and Information Security), il partenariato pubblico-privato contrattuale sulla cibersicurezza e le piattaforme settoriali, come la piattaforma per la cibersicurezza degli esperti di energia (Energy Expert Cyber Security Platform, EECSP). Dovrebbe inoltre stabilire un legame con la tavola rotonda ad alto livello annunciata nella comunicazione sulla digitalizzazione dell'industria europea: COM(2016) 180.
[16] Regolamento (UE) n. 526/2013 che abroga il regolamento (CE) n. 460/2004.

Commissione intende avanzare con la valutazione e, sulla base dei risultati, presentare una proposta il prima possibile.

Nel valutare l'eventuale necessità di modificare il mandato dell'ENISA, la Commissione terrà conto delle sfide in materia di cibersicurezza sopra descritte e dello sforzo complessivo volto a intensificare la cooperazione e la condivisione delle conoscenze. Tale processo sarà l'occasione per esaminare la possibilità di rafforzare le funzioni e le capacità dell'Agenzia per aiutare gli Stati membri in modo costruttivo ad acquisire resilienza in materia di cibersicurezza. La riflessione sul mandato dell'ENISA dovrebbe inoltre considerare le nuove responsabilità dell'Agenzia previste dalla direttiva sulla sicurezza delle reti e dell'informazione, i nuovi obiettivi d'intervento per sostenere il settore della cibersicurezza (la strategia per il mercato unico digitale e in particolare il PPP contrattuale), l'evoluzione delle esigenze nella protezione dei settori critici e le nuove sfide connesse agli incidenti transfrontalieri, compresa una risposta coordinata alle crisi informatiche.

La Commissione intende:

- sottoporre ad esame, nel primo semestre del 2017, un programma di cooperazione per la gestione di incidenti informatici su vasta scala a livello di UE;
- facilitare la creazione di una "piattaforma d'informazione" per favorire lo scambio di informazioni tra gli organismi dell'UE e gli Stati membri;
- creare un gruppo consultivo ad alto livello sulla cibersicurezza;
- portare a termine la valutazione dell'ENISA entro la fine del 2017. Tale valutazione analizzerà l'esigenza di modificare o estendere il mandato dell'ENISA, nella prospettiva di un'eventuale proposta da presentare il prima possibile.

2.2 Intensificare gli sforzi nel campo dell'insegnamento, della formazione e delle esercitazioni in materia di cibersicurezza

Competenze e formazione adeguate, in relazione sia alla prevenzione degli incidenti informatici sia alla gestione e all'attenuazione del loro impatto, sono aspetti fondamentali per acquisire resilienza in materia di cibersicurezza.

Attualmente, l'ENISA, il Gruppo europeo di formazione e istruzione in materia di criminalità informatica (ECTEG) in cooperazione con il Centro europeo per la lotta alla criminalità informatica (Europol) e l'Accademia europea di polizia (CEPOL) rivestono un ruolo importante nel fornire sostegno per lo sviluppo di capacità - anche nel campo dell'informatica forense - attraverso la redazione di manuali, l'organizzazione di formazioni e le esercitazioni di cibersicurezza.

Allo stesso tempo, il ciberspazio è un ambito in rapida evoluzione in cui le capacità a duplice uso rivestono un ruolo essenziale. È pertanto necessario sviluppare la cooperazione e le sinergie tra civili e militari nel campo della formazione e delle esercitazioni per rafforzare la resilienza dell'UE e la sua capacità di reagire agli incidenti.

Per rispondere a questa necessità, e come seguito all'adozione della direttiva sulla sicurezza delle reti e dell'informazione e del quadro strategico UE in materia di ciberdifesa[17], i servizi della Commissione coopereranno con gli Stati membri, con il Servizio europeo per l'azione esterna (SEAE), con l'ENISA e con altri organismi competenti dell'UE[18] per istituire una piattaforma d'istruzione, esercitazione e formazione in materia di cibersicurezza in grado di promuovere la creazione di sinergie tra le attività di formazione del settore civile e quelle della difesa.

La Commissione intende:

- collaborare fattivamente con gli Stati membri, l'ENISA, il SEAE e altri organismi competenti dell'UE per istituire una piattaforma di formazione sulla cibersicurezza.

2.3. Gestire le interdipendenze intersettoriali e la resilienza delle infrastrutture di rete pubbliche essenziali

Un fattore importante nella valutazione del rischio e dell'impatto di un incidente informatico su vasta scala è il grado di interdipendenza transfrontaliera e intersettoriale: un incidente informatico grave in un determinato settore o Stato membro può avere ripercussioni dirette o indirette o propagarsi in altri settori o in altri Stati membri.

La cooperazione transfrontaliera e intersettoriale facilita lo scambio di informazioni e di competenze e quindi migliora la preparazione e la resilienza. La Commissione sostiene le attività intraprese in diversi settori per comprendere meglio le interdipendenze attraverso l'attuazione del programma europeo per la protezione delle infrastrutture critiche[19].

Allo stesso tempo, una condizione necessaria per far fronte ai rischi intersettoriali è la capacità di ogni singolo settore di individuare i rischi informatici, di prepararsi e di reagire. La Commissione valuterà il rischio derivante dagli incidenti informatici in settori altamente interdipendenti entro e oltre i confini nazionali, in particolare nei settori coperti dalla direttiva sulla sicurezza delle reti e dell'informazione, anche tenendo conto degli sviluppi a livello internazionale[20]. In seguito a tale valutazione, prenderà in considerazione l'eventuale necessità di ulteriori norme specifiche e/o orientamenti destinati a questi settori critici e relativi alla preparazione ai rischi informatici.

A livello europeo, i centri di condivisione e di analisi delle informazioni (ISAC, Information Sharing and Analysis Centre)[21] e i corrispondenti CSIRT possono svolgere un ruolo fondamentale nella preparazione agli incidenti informatici e nella reazione agli stessi. Al fine di assicurare flussi di informazioni efficaci sull'evoluzione delle minacce e permettere di reagire meglio agli incidenti informatici, i centri ISAC dovrebbero essere incoraggiati a collaborare con la rete di CSIRT istituita dalla direttiva sulla sicurezza delle reti e

[17] Adottato dal Consiglio Affari esteri dell'Unione europea il 18 novembre 2014 (doc. 15585/14).
[18] Quali ad esempio l'Accademia europea per la sicurezza e la difesa, l'EC3, CEPOL e l'Agenzia europea per la difesa.
[19] SWD(2013) 318.
[20] Ad esempio, una tabella di marcia per la cibersicurezza adottata dall'Agenzia europea per la sicurezza aerea e le attività dell'Organizzazione per l'aviazione civile internazionale e dell'Organizzazione marittima internazionale.
[21] Cfr. ad esempio i centri ISAC europei per l'energia (http://www.ee-isac.eu).

dell'informazione, con il Centro europeo per la lotta alla criminalità informatica (Europol), con il CERT-UE e con i competenti organismi incaricati dell'applicazione delle norme.

Lo scambio di informazioni tra le parti interessate e con le autorità durante l'intero ciclo di vita dei rischi informatici deve basarsi sul presupposto che i partecipanti possano confidare nel fatto che tale scambio non li esporrà a responsabilità. La Commissione ha constatato che una serie di preoccupazioni di questo tipo impedisce alle imprese di condividere informazioni preziose sulle minacce con i loro omologhi, tra i vari settori o con le autorità, in particolare a livello transfrontaliero. Al fine di migliorare lo scambio di informazioni sulle minacce informatiche, la Commissione cercherà di rispondere a tali preoccupazioni e di dissiparle.

Sono fondamentali anche canali di comunicazione affidabili, che assicurino la riservatezza, per incentivare le imprese a riferire in merito al furto informatico di segreti aziendali. Ciò consentirebbe di monitorare e di valutare il danno subito dall'industria europea (anche in termini di diminuzione delle vendite e perdita di posti di lavoro) e dagli istituti di ricerca, e permetterebbe di preparare un'adeguata risposta politica. Con il sostegno dell'ENISA, dell'Ufficio dell'Unione europea per la proprietà intellettuale (EUIPO) e dell'EC3 (Europol), la Commissione, dialogando con i portatori di interesse del settore privato, predisporrà canali affidabili per la segnalazione volontaria del furto informatico di segreti aziendali. Ciò dovrebbe consentire la compilazione di dati anonimizzati e aggregati a livello di UE. Tali dati possono essere condivisi con gli Stati membri per alimentare gli sforzi diplomatici e le azioni di sensibilizzazione e contribuire così a proteggere le attività immateriali dell'UE dagli attacchi informatici.

A sostegno della cibersicurezza settoriale, la Commissione europea intende inoltre promuovere l'integrazione della sicurezza informatica nello sviluppo di varie politiche settoriali dell'UE in cui questo aspetto abbia un'importanza fondamentale.

Un ultimo elemento da considerare, non meno importante, è il ruolo che spetta alle autorità pubbliche nella verifica dell'integrità delle infrastrutture essenziali di internet per individuare i problemi, informare i responsabili delle reti e, se necessario, fornire assistenza nel porre rimedio alle vulnerabilità note. Le autorità nazionali di regolamentazione potrebbero avvalersi delle capacità dei CSIRT per effettuare controlli regolari delle infrastrutture di rete pubbliche e, su tale base, incoraggiare gli operatori a porre rimedio alle lacune o alle vulnerabilità individuate dalle scansioni.

La Commissione pertanto esaminerà le condizioni giuridiche e organizzative necessarie al fine di consentire alle autorità nazionali di regolamentazione, in cooperazione con le autorità nazionali incaricate della sicurezza informatica, di richiedere ai CSIRT di effettuare regolari controlli della vulnerabilità delle infrastrutture di rete pubbliche. I CSIRT nazionali dovrebbero essere incoraggiati a cooperare, nell'ambito della rete di CSIRT, sulle migliori prassi per il monitoraggio delle reti, facilitando in tal modo la prevenzione di incidenti su vasta scala.

La Commissione intende:

- favorire l'avvio di una cooperazione europea tra i centri settoriali di condivisione e di analisi

delle informazioni, sostenere la loro collaborazione con i CSIRT e cercare di sormontare gli ostacoli che impediscono lo scambio di informazioni tra gli operatori del mercato;

- studiare il rischio strategico/sistemico derivante dagli incidenti informatici nei settori con un elevato grado di interdipendenza, entro e oltre i confini nazionali;
- valutare l'eventuale necessità di ulteriori norme e/o orientamenti sulla preparazione ai rischi informatici per i settori critici e, ove opportuno, prendere in considerazione tali norme e orientamenti;
- istituire con l'ENISA, l'EUIPO e l'EC3 canali affidabili per la segnalazione volontaria di furti informatici di segreti aziendali;
- promuovere l'integrazione di misure sulla cibersicurezza nelle politiche settoriali europee;
- esaminare le condizioni necessarie per consentire alle autorità nazionali di richiedere ai CSIRT di effettuare controlli regolari delle infrastrutture di rete fondamentali.

3. RISPONDERE ALLE SFIDE CHE IL MERCATO UNICO DELLA CIBERSICUREZZA EUROPEO SI TROVA AD AFFRONTARE

L'Europa ha bisogno di prodotti e soluzioni per la sicurezza informatica di alta qualità, alla portata di tutti e interoperabili. Tuttavia, l'offerta di prodotti e servizi per la sicurezza delle TIC nel mercato unico resta molto frammentata dal punto di vista geografico. Tale frammentazione incide negativamente sulla competitività delle imprese europee a livello nazionale, europeo e mondiale e allo stesso tempo limita la gamma di tecnologie di cibersicurezza valide e utilizzabili a cui cittadini e imprese hanno accesso[22].

In effetti, il settore della cibersicurezza in Europa si è sviluppato soprattutto in risposta alla domanda pubblica nazionale, anche nel settore della difesa. La maggior parte degli operatori europei nel settore della difesa hanno sviluppato divisioni di cibersicurezza[23]. Parallelamente, sono emerse anche innumerevoli PMI innovative, sia in mercati specializzati/di nicchia (ad esempio quello dei sistemi di crittografia) sia in mercati consolidati con nuovi modelli commerciali (ad esempio, quello dei programmi antivirus).

Le imprese tuttavia fanno fatica a crescere al di fuori del proprio mercato nazionale. L'elemento essenziale emerso chiaramente da tutte le consultazioni svolte dalla Commissione[24] è l'assenza di fiducia nelle soluzioni offerte a livello transfrontaliero. Di conseguenza, molti appalti si svolgono ancora all'interno di un determinato Stato membro e molte imprese hanno difficoltà a realizzare le economie di scala che consentirebbero loro di essere più competitive sia sul mercato interno sia a livello mondiale.

L'assenza di soluzioni interoperabili (norme tecniche), di pratiche (norme di processo) e di meccanismi UE di certificazione è un'altra delle lacune che incide sul mercato unico della

[22] Cfr. SWD(2016) 216.
[23] Cfr. SWD(2016) 216.
[24] Cfr. SWD(2016) 215.

cibersicurezza. In tale contesto, la cibersicurezza è stata identificata come una delle priorità per la normazione delle TIC per il mercato unico digitale[25].

Le prospettive di crescita limitate per le imprese operanti nel settore della cibersicurezza all'interno del mercato unico portano spesso a fusioni e acquisizioni da parte di investitori non europei[26]. Questa tendenza, sebbene dimostri la capacità di innovazione degli imprenditori europei attivi nel settore, rischia di causare la perdita di know-how e di competenze in Europa e di provocare una fuga di cervelli.

È necessario agire con urgenza per promuovere una maggiore integrazione del mercato unico per i prodotti e i servizi per la sicurezza informatica, che favorirà la diffusione di soluzioni più pratiche ed economicamente accessibili.

Gli ostacoli alla fiducia tra soggetti industriali e istituzionali europei possono essere superati promuovendo la cooperazione in una fase precoce del ciclo di vita dell'innovazione: all'interno dello stesso settore della cibersicurezza, tra fornitori e acquirenti, e in una dimensione intersettoriale che coinvolga le industrie che sono o che probabilmente diventeranno utilizzatori delle soluzioni di sicurezza informatica.

Allo stesso tempo, lo sviluppo di prodotti, servizi e tecnologie a duplice uso sta diventando sempre più importante in Europa. Sono sempre di più le soluzioni che passano dal mercato civile a quello della difesa[27]. Nell'imminente piano d'azione europeo in materia di difesa la Commissione presenterà le misure con cui intende rafforzare ulteriormente le sinergie tra settore civile e settore militare a livello europeo.

3.1 Certificazione ed etichettatura

La certificazione svolge un ruolo importante nel rafforzare la fiducia e la sicurezza di prodotti e servizi, anche per quanto riguarda i nuovi sistemi che fanno ampio uso delle tecnologie digitali e richiedono un livello elevato di sicurezza, come le automobili connesse e automatizzate, la sanità elettronica, i sistemi di controllo per l'automazione industriale e le reti elettriche intelligenti.

Stanno prendendo forma iniziative nazionali per definire requisiti di cibersicurezza di alto livello, ivi inclusi requisiti di certificazione, per i componenti informatici di infrastrutture tradizionali. Sebbene si tratti di iniziative importanti, c'è il rischio che provochino la frammentazione del mercato unico e problemi di interoperabilità. Solo in pochi Stati membri esistono sistemi efficaci di certificazione della sicurezza per i prodotti TIC[28]. Pertanto, per poter vendere i suoi prodotti in più Stati membri, un fornitore di TIC potrebbe essere costretto a sottoporsi a diversi processi di certificazione. Nella peggiore delle ipotesi, un prodotto o un

[25] COM(2016) 176/2.
[26] Cfr. SWD(2016) 216.
[27] Nel 2013 i prodotti a duplice uso hanno rappresentato circa il 20% delle esportazioni totali dell'UE (in termini di valore). I dati si riferiscono anche al commercio interno all'UE.
[28] Cfr. il documento SWD(2016) 216 per l'accordo SOGIS (Senior Officers Group for Information Systems) (decisione 92/242/CEE del Consiglio del 31 marzo 1992) e altri sistemi esistenti, ad esempio *Commercial Product Assurance* nel Regno Unito e *Certification Sécuritaire de Premier Niveau* in Francia.

servizio TIC concepito per soddisfare requisiti di sicurezza informatica in un determinato Stato membro non può essere immesso sul mercato in un altro Stato membro.

Per un mercato unico funzionante nel settore della sicurezza informatica, un eventuale quadro per la certificazione della sicurezza di prodotti e servizi TIC dovrebbe tendere a conseguire i seguenti obiettivi: i) coprire un'ampia gamma di sistemi, prodotti e servizi TIC; ii) assicurare l'applicazione in tutti e 28 gli Stati membri; iii) riguardare qualsiasi livello di sicurezza informatica, tenendo conto nel contempo degli sviluppi a livello internazionale.

A tal fine, la Commissione istituirà un gruppo di lavoro specifico sulla certificazione della sicurezza di prodotti e servizi TIC, costituito da esperti degli Stati membri e dell'industria. Il suo scopo sarà sviluppare entro la fine del 2016, in cooperazione con l'ENISA e con il Centro comune di ricerca, una tabella di marcia che valuti la possibilità di elaborare una proposta relativa a un quadro europeo di certificazione della sicurezza delle TIC entro la fine del 2017. In tale contesto, la Commissione valuterà anche il regolamento (CE) n. 2008/765 e le disposizioni relative alla certificazione previste dal regolamento generale sulla protezione dei dati 2016/679[29].

Il processo comprenderà un'ampia consultazione e una valutazione d'impatto, che permetteranno alla Commissione di prendere in considerazione varie opzioni per la creazione del quadro di certificazione per i prodotti e i servizi TIC. La Commissione valuterà inoltre la possibilità di integrare la certificazione della sicurezza delle TIC nei settori delle infrastrutture (ad esempio aviazione, settore ferroviario, industria automobilistica), nonché in specifici meccanismi di certificazione e validazione delle tecnologie pronte all'impiego (ad esempio, la cibersicurezza dei sistemi di controllo per l'automazione industriale[30], l'internet degli oggetti, il *cloud computing*). La Commissione affronterà inoltre le carenze individuate nel sistema europeo di certificazione della sicurezza delle TIC sopra citato.

Nella misura del possibile, le attività di certificazione si baseranno su norme tecniche riconosciute a livello internazionale e saranno sviluppate con i partner internazionali.

La Commissione esaminerà anche le opzioni concernenti il modo migliore per integrare la certificazione della sicurezza delle TIC nella futura legislazione relativa a settori specifici, anche in relazione agli aspetti che riguardano la sicurezza.

Oltre a eventuali opzioni normative, la Commissione valuterà anche la possibilità di istituire un sistema europeo di etichettatura per la sicurezza dei prodotti TIC che sia improntato a una logica commerciale, su base volontaria e poco oneroso. Il sistema, che sarà complementare alla certificazione, intende migliorare la visibilità della cibersicurezza nei prodotti

[29] Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, prevede due codici di condotta destinati a contribuire alla corretta applicazione delle norme in materia di protezione dei dati, e meccanismi di certificazione che coprano tutti i principi di protezione dei dati, compresa in particolare la sicurezza dei dati nel trattamento dei dati personali.

[30] Cfr. il gruppo tematico della rete di riferimento dell'UE per le infrastrutture critiche (ERNCIP) sulla cibersicurezza dei sistemi di controllo industriale, all'indirizzo https://erncip-project.jrc.ec.europa.eu/download-area/category/16-case-studies-for-industrial-automation-and-control-systems.

commerciali, in modo da rafforzarne la competitività nel mercato unico e a livello mondiale. Si terranno in debita considerazione iniziative settoriali e orizzontali in corso avviate dall'industria, sia sul fronte dell'offerta che della domanda.

Le amministrazioni pubbliche saranno fortemente coinvolte per consentire l'uso di specifiche comuni e i riferimenti alla certificazione negli appalti pubblici. La Commissione provvederà inoltre a monitorare e riferire in merito all'uso dei requisiti di certificazione pertinenti negli appalti pubblici, a livello nazionale, in particolare per i sistemi relativi a settori specifici (energia, trasporti, sanità, pubblica amministrazione, ecc.).

La Commissione intende:

- definire entro la fine del 2016 una tabella di marcia per l'elaborazione di un'eventuale proposta relativa a un quadro europeo per la certificazione della sicurezza delle TIC, da presentare entro la fine del 2017, e valutare la fattibilità e l'impatto di un quadro europeo poco oneroso per l'etichettatura relativa alla cibersicurezza;
- valutare la necessità di una certificazione della sicurezza delle TIC nei meccanismi settoriali di certificazione/validazione e, se del caso, ovviare alle carenze;
- prevedere, ove opportuno, l'integrazione della certificazione della sicurezza dei prodotti TIC nelle future proposte legislative destinate a settori specifici;
- promuovere il coinvolgimento delle amministrazioni pubbliche al fine di facilitare l'uso della certificazione e di specifiche comuni negli appalti pubblici;
- monitorare l'uso dei pertinenti requisiti di certificazione negli appalti pubblici e nell'acquisizione di contratti e riferire sullo stato del mercato tra tre anni.

3.2. Far crescere gli investimenti nella cibersicurezza in Europa e sostenere le PMI

Sebbene l'innovazione nel settore della cibersicurezza sia in piena espansione in Europa, nell'UE ancora non esiste una vera cultura degli investimenti nella sicurezza informatica. Le PMI innovative in questo campo sono numerose, ma spesso non sono in grado di espandere la propria attività, anche a causa della mancanza di investimenti facilmente accessibili che possano sostenerle nelle prime fasi di sviluppo. Le imprese lamentano inoltre un accesso limitato al capitale di rischio in Europa e non dispongono di mezzi economici sufficienti per accrescere la propria visibilità con attività di marketing o per gestire la varietà dei requisiti di normazione e conformità.

Allo stesso tempo, la cooperazione tra i diversi soggetti coinvolti nella cibersicurezza è piuttosto frammentaria e sono necessari ulteriori sforzi per aumentare la concentrazione economica e sviluppare nuove catene del valore[31].

[31] Cfr. SWD(2016) 216.

Per aumentare gli investimenti nella cibersicurezza in Europa e sostenere le PMI, è necessario agevolare l'accesso ai finanziamenti. È necessario sostenere anche lo sviluppo di cluster di cibersicurezza che siano competitivi a livello mondiale e di centri di eccellenza in ecosistemi regionali favorevoli alla crescita digitale. Tale sostegno deve essere collegato a strategie di specializzazione intelligente e ad altri strumenti dell'UE, affinché il settore della cibersicurezza in Europa possa avvalersene meglio.

La Commissione intende fare in modo che la comunità della cibersicurezza sia pienamente informata sulle opportunità di finanziamento disponibili a livello europeo, nazionale e regionale (sia di quelle connesse agli strumenti orizzontali sia di quelle correlate a bandi specifici[32]) utilizzando gli strumenti e i canali esistenti, ad esempio la rete Enterprise Europe.

La Commissione integrerà queste iniziative valutando insieme alla Banca europea per gli investimenti (BEI) e al Fondo europeo per gli investimenti (FEI) le modalità per agevolare l'accesso ai finanziamenti. Tali agevolazioni potranno assumere la forma di investimenti in equity e quasi-equity, prestiti, garanzie a favore di progetti o controgaranzie per gli intermediari, ad esempio mediante la creazione di una piattaforma per gli investimenti nella cibersicurezza e il Fondo europeo per gli investimenti strategici[33].

Inoltre, la Commissione intende anche esaminare la possibilità di sviluppare, insieme agli Stati membri e alle regioni interessati, una piattaforma di specializzazione intelligente per la cibersicurezza[34]. Tale piattaforma permetterebbe di coordinare e pianificare le strategie per la cibersicurezza e di instaurare una collaborazione strategica tra le parti interessate negli ecosistemi regionali. Un approccio di questo tipo dovrebbe contribuire anche a sbloccare il potenziale dei fondi strutturali e di investimento europei esistenti a favore del settore della cibersicurezza.

Più in generale, la Commissione intende promuovere un approccio basato sul concetto della sicurezza sin dalla progettazione. Cercherà di fare in modo che tutti i grandi investimenti in infrastrutture che abbiano una componente digitale e che siano cofinanziati dai fondi europei tengano regolarmente conto dei requisiti di sicurezza informatica. A tal fine, introdurrà progressivamente i requisiti pertinenti nelle norme sui programmi e sugli appalti pubblici.

La Commissione intende:

- utilizzare gli strumenti esistenti di sostegno alle PMI per far sì che la comunità della

[32] Cfr. ad esempio il bando multisettoriale 2016 nell'ambito del Meccanismo per collegare l'Europa e i bandi COSMO 2016 correlati al programma di internazionalizzazione dei cluster.
[33] Nel quadro del Fondo europeo per gli investimenti strategici i singoli progetti possono essere finanziati direttamente o indirettamente tramite piattaforme di investimento. Le piattaforme di investimento possono contribuire a finanziare progetti più piccoli e a riunire fondi di varia provenienza per consentire investimenti diversificati aventi un rilievo geografico o tematico.
[34] Cfr. gli strumenti di specializzazione intelligente (RIS3): http://s3platform.jrc.ec.europa.eu/.

cibersicurezza sia meglio informata sui meccanismi di finanziamento esistenti;

- fare maggiore ricorso agli strumenti e ai meccanismi dell'UE per sostenere le PMI innovative nella ricerca di sinergie tra il mercato della cibersicurezza del settore civile e di quello della difesa[35];

- valutare, insieme alla BEI e al FEI, la possibilità di agevolare l'accesso agli investimenti, ad esempio attraverso una piattaforma specifica per gli investimenti nella cibersicurezza o altri strumenti;

- sviluppare una piattaforma di specializzazione intelligente per aiutare gli Stati membri e le regioni interessati a investire nel settore della cibersicurezza (RIS3);

- promuovere un approccio basato sul concetto della sicurezza sin dalla progettazione nei grandi investimenti in infrastrutture che abbiano una componente digitale e siano cofinanziati dai fondi dell'UE.

4. STIMOLARE E FAVORIRE LO SVILUPPO DELL'INDUSTRIA EUROPEA DELLA SICUREZZA INFORMATICA ATTRAVERSO L'INNOVAZIONE - ISTITUZIONE DEL PPP CONTRATTUALE SULLA CIBERSICUREZZA

Per stimolare la competitività e l'innovazione dell'industria europea della cibersicurezza sarà firmato un partenariato pubblico-privato contrattuale (PPP contrattuale). Il PPP contrattuale consentirà di mettere insieme le risorse delle imprese e del settore pubblico per raggiungere l'eccellenza nella ricerca e nell'innovazione.

Scopo del partenariato è costruire la fiducia tra gli Stati membri e l'industria, promuovendo la cooperazione nelle fasi iniziali del processo di ricerca e innovazione. Un altro obiettivo è allineare la domanda all'offerta, per consentire all'industria di comprendere le esigenze future degli utenti finali e dei settori che sono importanti utilizzatori delle soluzioni di cibersicurezza (ad es. energia, sanità, trasporti, finanza). Essi dovrebbero essere così maggiormente invogliati a definire esigenze comuni in materia di sicurezza digitale, tutela della vita privata e protezione dei dati per le rispettive attività.

Il PPP contrattuale sulla cibersicurezza contribuirà inoltre a massimizzare l'uso dei fondi disponibili, in primo luogo attraverso un maggiore coordinamento con gli Stati membri. In secondo luogo, verrà data maggiore attenzione a poche priorità tecniche per aiutare il settore della sicurezza informatica a fare importanti progressi tecnologici e a padroneggiare le tecnologie essenziali del futuro. In tale contesto, lo sviluppo di software *open source* e di norme tecniche aperte può contribuire a promuovere la fiducia, la trasparenza e l'innovazione dirompente e dovrebbe pertanto essere parte dell'investimento realizzato con il PPP contrattuale.

[35] Ad esempio, la rete Enterprise Europe e la rete europea di regioni connesse con il settore della difesa offriranno alla regioni nuove opportunità per esplorare la possibilità di una cooperazione transfrontaliera nel settore dei prodotti a duplice uso, anche per quanto riguarda la cibersicurezza, e alle PMI nuove opportunità per partecipare ad attività di *matchmaking*.

Il lavoro svolto nell'ambito del PPP contrattuale sulla cibersicurezza si avvarrà anche delle sinergie con altri progetti europei, in particolare quelli che affrontano aspetti relativi alla sicurezza. Fra questi figurano l'iniziativa Fabbriche del futuro, l'iniziativa Edilizia ad alta efficienza energetica, i PPP sul 5G e sui *big data*[36] e altri PPP settoriali[37], nonché l'iniziativa sull'internet delle cose[38]. Inoltre, verrà promosso uno stretto allineamento con il cloud europeo per la scienza aperta e l'iniziativa europea per il supercalcolo per le tecnologie quantistiche (ad esempio, l'innovazione nella distribuzione quantistica delle chiavi (QKD) e la ricerca nell'informatica quantistica).

Il PPP contrattuale sulla cibersicurezza, lanciato nell'ambito del programma quadro di ricerca e innovazione dell'UE Orizzonte 2020[39] per il periodo 2014-2020, mobiliterà fondi a partire da due pilastri del programma: Leadership nelle tecnologie abilitanti e industriali (LEIT-ICT) e Sfida per la società - Società sicure (SC7). Il bilancio complessivo del PPP contrattuale potrà arrivare a 450 milioni di EUR, con un triplice effetto leva sul fronte dell'industria. La sicurezza informatica dovrebbe essere affrontata e coordinata con le altre parti pertinenti di Orizzonte 2020 (ad esempio con le sfide per la società riguardanti l'energia, i trasporti e la sanità e con la sezione "Eccellenza"). Ciò contribuirà agli obiettivi del PPP contrattuale sulla cibersicurezza. Tale coordinamento dovrebbe avvenire anche a uno stadio iniziale, durante la fase di progettazione delle strategie settoriali.

Il PPP contrattuale sarà attuato in modo trasparente, con una governance aperta e flessibile adattata al contesto in rapida evoluzione della cibersicurezza. Esso terrà conto della necessità degli Stati membri di discutere in che modo l'evoluzione tecnologica influisce sul funzionamento sicuro delle infrastrutture nazionali e transfrontaliere. Analogamente, i risultati ottenuti con il partenariato devono essere sostenibili nell'arco di diversi anni perché i suoi obiettivi possano essere raggiunti.

Il PPP contrattuale potrà contare sull'appoggio dell'organizzazione europea per la cibersicurezza (European Cyber Security Organisation, ECSO), i cui membri rispecchieranno l'eterogeneità del mercato della sicurezza informatica in Europa e includeranno anche le amministrazione pubbliche nazionali, regionali e locali, i centri di ricerca, le università e altre parti interessate.

La Commissione intende:

- concludere con l'industria un accordo di partenariato pubblico-privato contrattuale sulla cibersicurezza che diventi operativo nel terzo trimestre del 2016;

- lanciare inviti a presentare proposte nell'ambito di Orizzonte 2020 correlati al PPP contrattuale sulla cibersicurezza nel primo trimestre del 2017;

[36] Il partenariato pubblico-privato per l'infrastruttura 5G e il partenariato pubblico-privato con Big Data Value.
[37] Ad esempio il SESAR o il partenariato pubblico-privato Shift2Rail.
[38] Alliance for Internet of Things Innovation (AIOTI).
[39] http://ec.europa.eu/programmes/horizon2020/en/official-documents.

- assicurare il coordinamento del PPP contrattuale sulla cibersicurezza con le pertinenti strategie settoriali, gli strumenti di Orizzonte 2020 e i PPP settoriali.

5. CONCLUSIONE

La presente comunicazione presenta misure volte a rafforzare la resilienza dell'Europa in materia di sicurezza informatica e a promuovere un settore della cibersicurezza competitivo e innovativo in Europa, come annunciato nella strategia dell'UE per la cibersicurezza e nella strategia per il mercato unico digitale. La Commissione invita il Parlamento europeo e il Consiglio ad appoggiare questo approccio.