Parlamento europeo
2014-2019

Commissione per l'industria, la ricerca e l'energia

2017/0225(COD)

27.3.2018

***I
PROGETTO DI RELAZIONE

sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza")
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Commissione per l'industria, la ricerca e l'energia

Relatore: Angelika Niebler

Relatore per parere (*):
Nicola Danti, commissione per il mercato interno e la protezione dei consumatori

(*) Procedura con le commissioni associate – Articolo 54 del regolamento

Significato dei simboli utilizzati

*	Procedura di consultazione
***	Procedura di approvazione
***I	Procedura legislativa ordinaria (prima lettura)
***II	Procedura legislativa ordinaria (seconda lettura)
***III	Procedura legislativa ordinaria (terza lettura)

(La procedura indicata dipende dalla base giuridica proposta nel progetto di atto.)

Emendamenti a un progetto di atto

Emendamenti del Parlamento presentati su due colonne

Le soppressioni sono evidenziate in ***corsivo grassetto*** nella colonna di sinistra. Le sostituzioni sono evidenziate in ***corsivo grassetto*** nelle due colonne. Il testo nuovo è evidenziato in ***corsivo grassetto*** nella colonna di destra.

La prima e la seconda riga del blocco d'informazione di ogni emendamento identificano la parte di testo interessata del progetto di atto in esame. Se un emendamento verte su un atto esistente che il progetto di atto intende modificare, il blocco d'informazione comprende anche una terza e una quarta riga che identificano rispettivamente l'atto esistente e la disposizione interessata di quest'ultimo.

Emendamenti del Parlamento presentati in forma di testo consolidato

Le parti di testo nuove sono evidenziate in ***corsivo grassetto***. Le parti di testo soppresse sono indicate con il simbolo ▌ o sono barrate. Le sostituzioni sono segnalate evidenziando in ***corsivo grassetto*** il testo nuovo ed eliminando o barrando il testo sostituito.
A titolo di eccezione, le modifiche di carattere strettamente tecnico apportate dai servizi in vista dell'elaborazione del testo finale non sono evidenziate.

INDICE

Pagina

PROGETTO DI RISOLUZIONE LEGISLATIVA DEL PARLAMENTO EUROPEO

sulla proposta di regolamento del Parlamento europeo e del Consiglio relativo all'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, che abroga il regolamento (UE) n. 526/2013, e relativo alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione ("regolamento sulla cibersicurezza") (COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

(Procedura legislativa ordinaria: prima lettura)

Il Parlamento europeo,

– vista la proposta della Commissione al Parlamento europeo e al Consiglio (COM(2017)0477),

– visti l'articolo 294, paragrafo 2, e l'articolo 114 del trattato sul funzionamento dell'Unione europea, a norma dei quali la proposta gli è stata presentata dalla Commissione (C8-0310/2017),

– visto l'articolo 294, paragrafo 3, del trattato sul funzionamento dell'Unione europea,

– visto il parere del Comitato economico e sociale europeo del 14 febbraio 2018[1],

– visto l'articolo 59 del suo regolamento,

– visto il parere motivato inviato dal Senato francese, nel quadro del protocollo n. 2 sull'applicazione dei principi di sussidiarietà e di proporzionalità, in cui si dichiara la mancata conformità del progetto di atto legislativo al principio di sussidiarietà,

– visti la relazione della commissione per l'industria, la ricerca e l'energia e il parere della commissione per il mercato interno e la protezione dei consumatori nonché il parere della commissione per gli affari esteri, della commissione per i bilanci e della commissione per le libertà civili, la giustizia e gli affari interni (A8-0000/2018),

1. adotta la posizione in prima lettura figurante in appresso;

2. chiede alla Commissione di presentargli nuovamente la proposta qualora la sostituisca, la modifichi sostanzialmente o intenda modificarla sostanzialmente;

3. incarica il suo Presidente di trasmettere la posizione del Parlamento al Consiglio e alla Commissione nonché ai parlamenti nazionali.

[1] GU C xx del ..., pag. xx.

Emendamento 1

Proposta di regolamento
Considerando 13

Testo della Commissione	*Emendamento*
(13) L'Agenzia dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza, anche per quanto riguarda la protezione delle infrastrutture critiche e la ciberresilienza. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza.	(13) L'Agenzia dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza, anche per quanto riguarda la protezione delle infrastrutture critiche e la ciberresilienza. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza. ***Le sue competenze saranno particolarmente necessarie in sede di elaborazione del programma di lavoro pluriennale dell'Unione europea per i sistemi europei di certificazione della cibersicurezza.***

Or. en

Emendamento 2

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi.	(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi.

Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.	Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza. ***L'Agenzia dovrebbe rispettare le competenze degli Stati membri per quanto riguarda la cibersicurezza, in particolare quelle concernenti il settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.***

Or. en

Emendamento 3

Proposta di regolamento
Considerando 25

Testo della Commissione	*Emendamento*
(25) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'Agenzia, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale.	(25) Gli Stati membri possono invitare le imprese interessate dall'incidente a collaborare fornendo le informazioni e l'assistenza necessarie all'Agenzia, fatto salvo il loro diritto di tutelare le informazioni sensibili sul piano commerciale ***e le informazioni pertinenti alla pubblica sicurezza***.

Or. en

Emendamento 4

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri	(30) Per conseguire appieno i propri

obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con ***gli organismi europei di normazione (OEN), i soggetti interessati e*** le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

Or. en

Emendamento 5

Proposta di regolamento
Considerando 33

Testo della Commissione	*Emendamento*
(33) L'Agenzia dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'UE in questo campo. Essa dovrebbe promuovere la diffusione della certificazione della cibersicurezza	(33) L'Agenzia dovrebbe sviluppare ulteriormente e mantenere le proprie competenze in materia di certificazione della cibersicurezza al fine di sostenere la politica dell'UE in questo campo. Essa dovrebbe ***basarsi sulle migliori pratiche e*** promuovere la diffusione della

nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.	certificazione della cibersicurezza nell'Unione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione a livello di Unione, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.
	Or. en

Emendamento 6

Proposta di regolamento
Considerando 35

Testo della Commissione	*Emendamento*
(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria cibersicurezza. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di cibersicurezza. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti e servizi.	(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale***, in particolare fornendo i necessari aggiornamenti,*** in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria cibersicurezza. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di cibersicurezza. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti e servizi.
	Or. en

Emendamento 7

Proposta di regolamento
Considerando 36

Testo della Commissione	*Emendamento*
(36) L'Agenzia dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, agli organi, agli uffici e alle agenzie dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca nel settore della sicurezza delle reti e dell'informazione, in particolare per quanto riguarda la cibersicurezza.	(36) L'Agenzia dovrebbe tenere pienamente conto delle attività di ricerca, sviluppo e valutazione tecnologica già in atto, in particolare quelle condotte nell'ambito delle varie iniziative di ricerca dell'Unione per fornire consulenza alle istituzioni, agli organi, agli uffici e alle agenzie dell'Unione e ove opportuno agli Stati membri, su loro richiesta, sulle esigenze in materia di ricerca nel settore della sicurezza delle reti e dell'informazione, in particolare per quanto riguarda la cibersicurezza. ***Più precisamente, dovrebbe essere instaurata una cooperazione con il Consiglio europeo della ricerca (CER) e con l'Istituto europeo di innovazione e tecnologia (EIT) e la ricerca in materia di sicurezza dovrebbe essere inclusa nell'ambito del nono programma quadro di ricerca (FP9) e di Orizzonte 2020.***

Or. en

Emendamento 8

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta

del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. ***Al fine di garantire una migliore partecipazione dei portatori di interessi nel processo di certificazione, il gruppo permanente di portatori di interessi dovrebbe avere la facoltà di proporre alla Commissione e al gruppo europeo per la certificazione della cibersicurezza (in appresso "il gruppo") l'elaborazione di una proposta di sistema europeo di certificazione della cibersicurezza e dovrebbe altresì essere consultato nelle fasi successive del processo.*** La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.

Or. en

Emendamento 9

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***dovrebbe*** essere ***considerata*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***e l'autovalutazione dovrebbero*** essere ***considerate*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo

indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. ***L'autovalutazione può essere effettuata dal fabbricante del prodotto o dal fornitore del servizio, come previsto dal nuovo quadro legislativo[1bis] e come precisato nel presente regolamento.*** La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

_____

[1bis] Regolamento (CE) n. 764/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che stabilisce procedure relative all'applicazione di determinate regole tecniche nazionali a prodotti legalmente commercializzati in un altro Stato membro (GU L 218 del 13.8.2008, pag. 21).

Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30).

Decisione n. 768/2008/CE del Parlamento europeo e del Consiglio, del 9 luglio 2008, relativa a un quadro comune per la commercializzazione dei prodotti e che abroga la decisione 93/465/CEE (GU L 218 del 13.8.2008, pag. 82).

Or. en

Emendamento 10

Proposta di regolamento
Considerando 50

Testo della Commissione	*Emendamento*
(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo.	(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo. ***È necessario un approccio basato sul rischio, pur nella consapevolezza che un unico sistema valido per tutti non è possibile.***

Or. en

Emendamento 11

Proposta di regolamento
Considerando 53

Testo della Commissione	*Emendamento*
(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di	(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di

certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.	certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo. ***L'Agenzia dovrebbe individuare e valutare i sistemi già utilizzati dall'industria o da organizzazioni private, al fine di scegliere le migliori pratiche che potrebbero diventare parte di un sistema europeo.***

Or. en

Emendamento 12

Proposta di regolamento
Considerando 56

Testo della Commissione	*Emendamento*
(56) La Commissione ***dovrebbe*** avere la facoltà di incaricare l'ENISA di preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro,	(56) La Commissione ***o il gruppo dovrebbero*** avere la facoltà di incaricare l'ENISA di preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema.

l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.	Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato. ***Il livello di affidabilità dipende dal rischio derivante dal contesto e dall'uso previsto del prodotto, processo o servizio TIC.***

Or. en

Emendamento 13

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, ***salvo disposizioni contrarie della legislazione dell'Unione o nazionale***. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario ***per i livelli di affidabilità di base e sostanziale***, ***ma non per i prodotti, processi e servizi TIC con un livello di affidabilità elevato. In una fase successiva e in funzione del livello di maturità di attuazione negli Stati membri e della criticità di un prodotto o di un servizio, è riconosciuto che i sistemi potenzialmente obbligatori per taluni prodotti e servizi TIC potranno iniziare ad evolvere in un approccio graduale***. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non

	dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

Or. en

Emendamento 14

Proposta di regolamento
Considerando 57 bis (nuovo)

Testo della Commissione	*Emendamento*
	(57 bis) L'obbligo di emettere una dichiarazione di prodotto recante informazioni strutturate in merito alla certificazione del prodotto, processo o servizio è introdotta per fornire al consumatore maggiori informazioni e per consentirgli di compiere una scelta consapevole.

Or. en

Emendamento 15

Proposta di regolamento
Considerando 58

Testo della Commissione	*Emendamento*
(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere	(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere

accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.	accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento. ***Al fine di assicurare che si applichino livelli equivalenti di qualità, conoscenze e competenze nell'Unione sono eseguiti audit, i cui risultati sono trasmessi all'ENISA e al gruppo.***

Or. en

Emendamento 16

Proposta di regolamento
Articolo 1 – comma 1 – parte introduttiva

Testo della Commissione	*Emendamento*
Allo scopo di garantire il buon funzionamento del mercato interno perseguendo nel contempo un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento:	Allo scopo di garantire il buon funzionamento del mercato interno ***evitando la frammentazione dei sistemi di certificazione nell'Unione e*** perseguendo***,*** nel contempo***,*** un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, il presente regolamento:

Or. en

Motivazione

L'emendamento sottolinea la necessità di raggiungere l'armonizzazione con il quadro di cibersicurezza e di evitare sovrapposizioni e frammentazione tra gli Stati membri.

Emendamento 17

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti e dei servizi TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria ***o*** obbligatoria in altri atti dell'Unione.	(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti***, dei processi*** e dei servizi TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria ***e, se del caso e ove opportuno,*** obbligatoria in altri atti dell'Unione.

Or. en

Motivazione

- Inclusione dei "processi" nel campo di applicazione del regolamento: con l'inclusione dei processi, l'intero ciclo di vita del prodotto è tutelato e reso sicuro.- Carattere volontario: l'emendamento sottolinea il carattere volontario del sistema; un sistema di certificazione volontario è la norma e la certificazione obbligatoria si applica solo in via eccezionale e nel rispetto di condizioni rigorose.

Emendamento 18

Proposta di regolamento
Articolo 1 – comma 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	Gli obiettivi e i compiti dell'Agenzia fanno salve le competenze degli Stati membri per quanto riguarda la cibersicurezza e, in ogni caso, fanno salve le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.

Or. en

Motivazione

Spostando questa precisazione dall'articolo 3 all'articolo 1 del regolamento, viene chiarito che le competenze degli Stati membri sono fatte salve per quanto riguarda la totalità del regolamento quadro.

Emendamento 19

Proposta di regolamento
Articolo 2 – comma 1 – punto 8

Testo della Commissione	*Emendamento*
(8) "minaccia informatica", qualsiasi circostanza o evento che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;	(8) "minaccia informatica", qualsiasi circostanza o evento che potrebbe ***danneggiare, perturbare o*** avere un impatto negativo ***di altro tipo*** sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

Or. en

Motivazione

Chiarimento della definizione.

Emendamento 20

Proposta di regolamento
Articolo 2 – comma 1 – punto 9

Testo della Commissione	*Emendamento*
(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;	(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione ***e in base alle norme internazionali ed europee approvate dall'ENISA*** che si applicano alla certificazione dei prodotti***, dei processi*** e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

Or. en

Emendamento 21

Proposta di regolamento
Articolo 2 – comma 1 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità ***oppure, ove previsto dal presente regolamento, dal fabbricante a titolo di autovalutazione,*** che attesta che un determinato prodotto***, processo*** o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

Or. en

Motivazione

L'emendamento autorizza l'autovalutazione allineandola al nuovo quadro legislativo.

Emendamento 22

Proposta di regolamento
Articolo 2 – comma 1 – punto 11 bis (nuovo)

Testo della Commissione	*Emendamento*
	(11 bis) "processo TIC", l'insieme delle attività svolte per progettare, sviluppare, mantenere e fornire un prodotto o servizio TIC;

Or. en

Emendamento 23

Proposta di regolamento
Articolo 2 – comma 1 – punto 16 bis (nuovo)

Testo della Commissione	*Emendamento*
	(16 bis) "autorità nazionale di controllo della certificazione", l'organo designato da ciascuno Stato membro a norma dell'articolo 50 del presente regolamento;

Or. en

Emendamento 24

Proposta di regolamento
Articolo 2 – comma 1 – punto 16 ter (nuovo)

Testo della Commissione	*Emendamento*
	(16 ter) "autovalutazione", la dichiarazione con la quale il fabbricante dimostra che i requisiti specifici relativi ai prodotti, ai processi e ai servizi sono stati rispettati;

Or. en

Motivazione

La definizione è necessaria per allineare l'autovalutazione al nuovo quadro legislativo.

Emendamento 25

Proposta di regolamento
Articolo 3 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di contribuire a un elevato livello di cibersicurezza nell'Unione.	1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento ***ed è potenziata*** allo scopo di contribuire a un elevato livello di cibersicurezza nell'Unione ***e di garantire la coerenza tenendo conto dei risultati ottenuti dagli Stati membri in materia di cooperazione nel quadro della direttiva sulla sicurezza delle reti e dell'informazione ("direttiva***

NIS").

Or. en

Motivazione

Emendamento volto a chiarire che il presente regolamento mira a potenziare talune strutture che sono già in vigore.

Emendamento 26

Proposta di regolamento
Articolo 3 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Gli obiettivi e i compiti dell'Agenzia fanno salve le competenze degli Stati membri per quanto riguarda la cibersicurezza e, in ogni caso, fanno salve le attività nel settore della pubblica sicurezza, della difesa, della sicurezza nazionale e le attività dello Stato nell'ambito del diritto penale.	***soppresso***

Or. en

Motivazione

Il paragrafo in questione dovrebbe diventare il secondo comma dell'articolo 1.

Emendamento 27

Proposta di regolamento
Articolo 4 – paragrafo 3

Testo della Commissione	*Emendamento*
3. L'Agenzia sostiene lo sviluppo della capacità e la preparazione nell'Unione, assistendo ***l'***Unione, gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello sviluppo di ***abilità*** e ***competenze nel campo della***	3. L'Agenzia sostiene lo sviluppo della capacità e la preparazione nell'Unione, assistendo ***le istituzioni, le agenzie e gli organismi dell'***Unione, gli Stati membri e i portatori di interessi del settore pubblico e privato nel miglioramento della protezione delle loro reti e dei loro sistemi informativi, nello

cibersicurezza e nel ***conseguimento*** della ***ciberresilienza***.	sviluppo ***e nel miglioramento delle capacità*** di ***ciberresilienza*** e ***di risposta, nella sensibilizzazione e nello sviluppo di abilità*** e ***competenze*** nel ***campo*** della ***cibersicurezza***.

Or. en

Emendamento 28

Proposta di regolamento
Articolo 4 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'Agenzia ***rafforza*** le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.	5. L'Agenzia ***contribuisce a rafforzare*** le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.

Or. en

Emendamento 29

Proposta di regolamento
Articolo 4 – paragrafo 6

Testo della Commissione	*Emendamento*
6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.	6. L'Agenzia dovrebbe promuovere l'uso della certificazione ***con l'obiettivo di evitare la frammentazione del mercato interno e migliorare il suo funzionamento***, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel

	mercato unico digitale***, nonché di accrescere la compatibilità fra i sistemi di certificazione nazionali e internazionali esistenti***.

Or. en

Emendamento 30

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera g

Testo della Commissione	*Emendamento*
(g) gli Stati membri mediante l'organizzazione delle esercitazioni ***annuali*** di cibersicurezza su vasta scala a livello di Unione di cui all'articolo 7, paragrafo 6, e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;	(g) gli Stati membri mediante l'organizzazione delle esercitazioni ***regolari*** di cibersicurezza su vasta scala a livello di Unione di cui all'articolo 7, paragrafo 6, e la formulazione di raccomandazioni politiche basate sul processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

Or. en

Motivazione

Tenendo presente il livello di complessità, il numero di persone coinvolte nell'esercizio e la necessità di fare resoconti successivi al riguardo, una cadenza annuale non è realistica. La modifica introdurrà un esercizio completo con un valore aggiunto.

Emendamento 31

Proposta di regolamento
Articolo 6 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. L'Agenzia agevola la creazione e il lancio di un progetto europeo a lungo termine per la sicurezza dell'informazione, al fine di incentivare ulteriormente la ricerca in materia di cibersicurezza nell'Unione e negli Stati membri, in collaborazione con il Consiglio europeo della ricerca (CER) e

con l'Istituto europeo di innovazione e tecnologia (EIT) e con riferimento ai programmi di ricerca dell'Unione.

Or. en

Motivazione

La ricerca in materia di sicurezza deve essere ulteriormente sviluppata. Tale obiettivo può essere raggiunto chiedendo una stretta cooperazione con le agenzie e gli istituti competenti e instaurando un collegamento con il nono programma quadro e con il programma Orizzonte 2020.

Emendamento 32

Proposta di regolamento
Articolo 7 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia sostiene la cooperazione operativa tra gli ***enti pubblici competenti*** e tra i portatori di interessi.	1. L'Agenzia sostiene la cooperazione operativa tra gli ***Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione*** e tra i portatori di interessi ***al fine di conseguire la collaborazione, mediante l'analisi e la valutazione dei sistemi esistenti a livello nazionale, lo sviluppo e l'attuazione di un piano e l'utilizzo degli strumenti appropriati per conseguire il massimo livello di certificazione della cibersicurezza nell'Unione e negli Stati membri***.

Or. en

Motivazione

Il presente regolamento quadro dovrebbe essere considerato un punto di partenza e la scelta tra armonizzazione e riconoscimento reciproco saranno integrati in una fase successiva. L'Agenzia è il soggetto più adatto per ottenere questo effetto leva.

Emendamento 33

Proposta di regolamento
Articolo 7 – paragrafo 4 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) l'offerta, su richiesta degli Stati membri, di assistenza tecnica in caso di incidenti aventi un impatto rilevante o sostanziale;	(b) l'offerta, su richiesta degli Stati membri, di assistenza tecnica***, sotto forma di condivisione di informazioni e competenze,*** in caso di incidenti aventi un impatto rilevante o sostanziale;

Or. en

Motivazione

L'espressione "assistenza tecnica" esprime un concetto molto ampio e vago. Può essere intesa come un semplice scambio di informazioni e arrivare fino al trasferimento di dati tecnici. Occorre chiarire che non vi è ingerenza nelle competenze nazionali quando si tratta di incidenti significativi (cfr. articolo 1, paragrafo 1) e che pertanto esistono limitazioni. È chiaramente escluso il trasferimento di dati tecnici di portata eccessivamente ampia.

Emendamento 34

Proposta di regolamento
Articolo 7 – paragrafo 4 – comma 1 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	(b bis) Qualora una situazione richieda un intervento urgente, uno Stato membro può chiedere l'assistenza di esperti dell'Agenzia per valutare la situazione. La richiesta comprende una descrizione della situazione, i possibili obiettivi e le esigenze previste.

Or. en

Motivazione

È opportuno prevedere una procedura per eventi che richiedano un intervento rapido e su scala europea.

Emendamento 35

Proposta di regolamento
Articolo 7 – paragrafo 5 – comma 1

Testo della Commissione	*Emendamento*
Su richiesta di due o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di due Stati membri.	Su richiesta di due o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di due Stati membri. ***Nello svolgimento di tale indagine, l'ENISA provvede affinché non siano divulgate le azioni intraprese dagli Stati membri per salvaguardare le funzioni essenziali dello Stato, in particolare quelle riguardanti la sicurezza nazionale.***

Or. en

Emendamento 36

Proposta di regolamento
Articolo 7 – paragrafo 6

Testo della Commissione	*Emendamento*
6. L'Agenzia organizza esercitazioni ***annuali*** di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organi dell'UE nell'organizzazione di esercitazioni. Le esercitazioni annuali a livello di Unione includono gli elementi tecnici, operativi e strategici e contribuiscono a preparare la risposta cooperativa a livello di Unione agli incidenti di cibersicurezza transfrontalieri di vasta portata. L'Agenzia inoltre contribuisce e aiuta ad organizzare, se del	6. L'Agenzia organizza esercitazioni ***regolari, a cadenza almeno annuale,*** di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organi dell'UE nell'organizzazione di esercitazioni. Le esercitazioni annuali a livello di Unione includono gli elementi tecnici, operativi e strategici e contribuiscono a preparare la risposta cooperativa a livello di Unione agli incidenti di cibersicurezza transfrontalieri di vasta portata. L'Agenzia inoltre contribuisce e aiuta ad organizzare,

caso, esercitazioni di cibersicurezza settoriali insieme ai pertinenti ISAC e consente agli ISAC di partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.	se del caso, esercitazioni di cibersicurezza settoriali insieme ai pertinenti ISAC e consente agli ISAC di partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.

Or. en

Emendamento 37

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera c

Testo della Commissione	*Emendamento*
(c) fornendo assistenza nel trattamento tecnico di un incidente o di una crisi, anche agevolando la condivisione di soluzioni tecniche tra gli Stati membri;	(c) fornendo assistenza nel trattamento tecnico di un incidente o di una crisi, anche agevolando la condivisione ***volontaria*** di soluzioni tecniche tra gli Stati membri;

Or. en

Motivazione

Per assicurare la coerenza con le limitazioni introdotte all'articolo 7, paragrafo 4, lettera b).

Emendamento 38

Proposta di regolamento
Articolo 7 – paragrafo 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	8 bis. L'Agenzia effettua, su richiesta, verifiche periodiche indipendenti della sicurezza informatica delle infrastrutture critiche transfrontaliere, nell'ottica di identificare eventuali rischi e di formulare raccomandazioni per rafforzarne la resilienza.

Or. en

Emendamento 39

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto -1 (nuovo)

Testo della Commissione	*Emendamento*
	(-1) definendo continuamente norme, specifiche tecniche e specifiche tecniche delle TIC;

Or. en

Motivazione

Emendamento teso a garantire che questo sia un processo continuo.

Emendamento 40

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 1

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;	(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti***, i processi*** e i servizi TIC conformemente all'articolo 44 del presente regolamento***, in cooperazione con i portatori di interessi dell'industria e le organizzazioni di normalizzazione, nel quadro di una procedura formale, standardizzata e trasparente***;

Or. en

Motivazione

È importante coinvolgere maggiormente i portatori di interessi nel processo di sviluppo di sistemi di certificazione della cibersicurezza.

Emendamento 41

Proposta di regolamento
Articolo 8 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) agevola la definizione e l'adozione di norme tecniche europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;	(b) agevola la definizione e l'adozione di norme tecniche europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri ***e l'industria***, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;

Or. en

Emendamento 42

Proposta di regolamento
Articolo 9 – comma 1 – lettera c

Testo della Commissione	*Emendamento*
(c) fornisce, in cooperazione con esperti delle autorità degli Stati membri, consulenza, orientamenti e migliori pratiche per la sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture di internet e delle infrastrutture su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148;	(c) fornisce, in cooperazione con esperti delle autorità degli Stati membri ***e i portatori di interessi dell'industria***, consulenza, orientamenti e migliori pratiche per la sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la sicurezza delle infrastrutture di internet e delle infrastrutture su cui poggiano i settori di cui all'allegato II della direttiva (UE) 2016/1148;

Or. en

Motivazione

Assicurare un miglior coinvolgimento dell'industria.

Emendamento 43

Proposta di regolamento
Articolo 9 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;	(e) sensibilizza ***costantemente*** l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;

Or. en

Emendamento 44

Proposta di regolamento
Articolo 9 – comma 1 – lettera g

Testo della Commissione	*Emendamento*
(g) organizza regolarmente, in collaborazione con gli Stati membri e con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, campagne di ***sensibilizzazione*** al fine di ***rafforzare la cibersicurezza e la sua visibilità nell'Unione***.	(g) organizza regolarmente, in collaborazione con gli Stati membri e con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, campagne di ***comunicazione*** al fine di ***suscitare un ampio dibattito pubblico***.

Or. en

Motivazione

L'emendamento è legato all'obiettivo dell'ENISA di sensibilizzare i cittadini e le imprese (articolo 4, paragrafo 7): in particolare, i consumatori, in quanto obiettivo "più debole", devono adottare un approccio diverso alla cibersicurezza.

Emendamento 45

Proposta di regolamento
Articolo 11 – comma 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) fornendo consulenza e sostegno alla Commissione, in collaborazione con il gruppo europeo per la certificazione della cibersicurezza istituito a norma dell'articolo 53, su questioni concernenti gli accordi per il riconoscimento reciproco dei certificati di cibersicurezza con i paesi terzi.

Or. en

Emendamento 46

Proposta di regolamento
Articolo 20 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.	1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti ***della sicurezza*** riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, ***gli operatori di servizi essenziali ai sensi della direttiva NIS,*** i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, ***le PMI,*** le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza***, le organizzazioni europee di normazione (OEN), gli organismi di valutazione della conformità*** e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

Or. en

Motivazione

È essenziale che l'ENISA coinvolga fortemente i pertinenti rappresentanti e operatori dell'industria dell'UE, non sovraccaricando il gruppo permanente di portatori di interessi, che dovrebbe mantenere il suo ruolo attuale di organo consultivo.

Emendamento 47

Proposta di regolamento
Articolo 20 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 20 bis
	Piattaforme di consultazione ad hoc
	Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce piattaforme di consultazione ad hoc dedicate che forniscono, caso per caso, ulteriore assistenza e consulenza all'ENISA al momento della preparazione di un sistema di certificazione conformemente al titolo III del presente regolamento. La piattaforma è aperta alla partecipazione e accompagna il processo di certificazione in stretta cooperazione con il gruppo istituito a norma dell'articolo 53. Essa approva formalmente ogni proposta di sistema di certificazione preparata dall'Agenzia prima che venga trasmessa alla Commissione per approvazione. È sciolta una volta adottato il sistema di certificazione. È composta da rappresentanti del gruppo permanente di portatori di interessi e da altri eventuali portatori di interessi, compresi rappresentanti dell'industria dell'Unione con competenze specifiche nel settore di una determinata proposta di sistema.

Or. en

Motivazione

La creazione di un sottogruppo flessibile per ciascun sistema di certificazione consente una buona rappresentanza dell'industria, specialmente delle PMI.

Emendamento 48

Proposta di regolamento
Articolo 21 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 21 bis
	Richieste all'Agenzia
	1. Le richieste di consulenza e assistenza su questioni che rientrano nell'ambito degli obiettivi e dei compiti dell'Agenzia sono inoltrate al direttore esecutivo e corredate di una documentazione informativa che illustra la questione da esaminare. Il direttore esecutivo informa il consiglio di amministrazione e il comitato esecutivo in merito alle richieste ricevute, al possibile impatto sulle risorse e, a tempo debito, al seguito dato alle richieste. Qualora respinga una richiesta, l'Agenzia motiva il proprio rifiuto.
	2. Le richieste di cui al paragrafo 1 possono provenire:
	a) dal Parlamento europeo;
	b) dal Consiglio;
	c) dalla Commissione;
	d) da qualsiasi organismo competente designato da uno Stato membro come autorità nazionale di regolamentazione ai sensi dell'articolo 2 della direttiva 2002/21/CE[1 bis].
	3. Le modalità pratiche di applicazione dei paragrafi 1 e 2, con particolare riguardo alla presentazione, alla definizione delle priorità e al seguito da dare alle richieste rivolte all'Agenzia, come pure all'informazione del consiglio di amministrazione e del comitato esecutivo in merito a esse, sono definite dal consiglio di amministrazione nel regolamento interno dell'Agenzia.

[1 bis] ***Direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002, che istituisce un quadro normativo comune per le reti ed i servizi di comunicazione elettronica (direttiva quadro) (GU L 108 del 24.4.2002, pag. 33).***

Or. en

Motivazione

L'ENISA riceve tra le 20 e le 30 richieste di consulenza e assistenza ogni anno. La procedura per tali richieste è formalizzata all'articolo 14 del regolamento n. 526/2013 sull'ENISA e deve essere inclusa nel presente regolamento nell'ambito del funzionamento dell'Agenzia.

Emendamento 49

Proposta di regolamento
Articolo 43 – comma 1

Testo della Commissione	*Emendamento*
I sistemi europei di certificazione della cibersicurezza attestano che i prodotti e servizi TIC certificati nel loro ambito sono conformi a determinati requisiti per quanto riguarda la loro capacità di resistere, a un determinato livello di affidabilità, ad azioni volte a compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, processi**,** servizi ***e sistemi*** o accessibili tramite essi.	I sistemi europei di certificazione della cibersicurezza attestano che i prodotti**,** ***processi*** e servizi TIC certificati nel loro ambito sono conformi a determinati requisiti per quanto riguarda la loro capacità di resistere, a un determinato livello di affidabilità, ad azioni volte a compromettere la disponibilità, l'autenticità, l'integrità o la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti da tali prodotti, processi ***e*** servizi o accessibili tramite essi ***durante il loro intero ciclo di vita***.

Or. en

Emendamento 50

Proposta di regolamento
Articolo 44 – paragrafo -1 (nuovo)

Testo della Commissione	*Emendamento*
	-1. La Commissione adotta un programma di lavoro pluriennale dell'Unione per i sistemi europei di certificazione della cibersicurezza, che individua azioni comuni da intraprendere a livello dell'Unione e priorità strategiche. Il programma di lavoro comprende, in particolare, un elenco prioritario di prodotti, processi e servizi TIC identificati che risultano adatti ad essere soggetti a un sistema europeo di certificazione della cibersicurezza, nonché un'analisi della presenza di un livello equivalente di qualità, conoscenze e competenze tra gli organismi di valutazione della conformità e le autorità nazionali di controllo della certificazione, e, se necessario, una proposta di misure intese a conseguire tale obiettivo. Prima dell'adozione del programma di lavoro, la Commissione consulta l'ENISA e tiene in massima considerazione la sua opinione.

Or. en

Motivazione

Lo scopo del programma di lavoro è introdurre trasparenza e rendicontabilità nel processo di preparazione dei sistemi europei di certificazione della cibersicurezza.

Emendamento 51

Proposta di regolamento
Articolo 44 – paragrafo 1

Testo della Commissione	*Emendamento*
1. A seguito di una richiesta della Commissione, l'ENISA prepara un sistema europeo di certificazione della cibersicurezza che soddisfa i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento. ***Gli Stati membri o il gruppo europeo per la certificazione della***	1. ***La preparazione di una proposta di sistema europeo di certificazione della cibersicurezza può essere proposta alla Commissione o al gruppo dagli Stati membri o dal gruppo permanente di portatori di interessi.*** A seguito di una richiesta della Commissione ***o del gruppo***,

cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza.	l'ENISA prepara un sistema europeo di certificazione della cibersicurezza che soddisfa i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.

Or. en

Motivazione

Gli Stati membri e l'industria svolgono un ruolo fondamentale nella preparazione delle proposte di sistemi, poiché è dall'industria, insieme agli Stati membri, che nasce l'innovazione. Il loro parere deve essere preso debitamente in considerazione.

Emendamento 52

Proposta di regolamento
Articolo 44 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Nella preparazione delle proposte di sistemi di cui al paragrafo 1, l'ENISA consulta tutti i portatori di interessi e coopera strettamente con il gruppo***.*** Il gruppo ***fornisce*** all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.	2. Nella preparazione delle proposte di sistemi di cui al paragrafo -1 ***(nuovo)***, l'ENISA consulta tutti i portatori di interessi ***mediante procedure di consultazione trasparenti*** e coopera strettamente con il gruppo***, con*** il gruppo ***permanente di portatori di interessi e, se del caso, con le piattaforme di consultazione ad hoc conformemente all'articolo 20 bis (nuovo). Questi forniscono*** all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.

Or. en

Motivazione

Un coinvolgimento forte degli Stati membri e dell'industria richiede che essi possano contribuire allo sviluppo del sistema.

Emendamento 53

Proposta di regolamento
Articolo 44 – paragrafo 3

Testo della Commissione	*Emendamento*
3. ***L'ENISA trasmette alla Commissione il*** sistema europeo di certificazione della cibersicurezza ***preparato*** in conformità del paragrafo 2.	3. ***A seguito dell'approvazione della proposta di*** sistema europeo di certificazione della cibersicurezza ***da parte del gruppo, l'ENISA trasmette alla Commissione la proposta di sistema preparata*** in conformità del paragrafo 2. ***La Commissione valuta la conformità dei documenti elaborati dall'ENISA alla sua richiesta iniziale.***

Or. en

Emendamento 54

Proposta di regolamento
Articolo 44 – paragrafo 4

Testo della Commissione	*Emendamento*
4. La Commissione, sulla base del sistema proposto dall'ENISA, può adottare atti di esecuzione in conformità dell'articolo 55, paragrafo ***1***, prevedendo sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC che soddisfano i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.	4. La Commissione, sulla base del sistema proposto dall'ENISA, può adottare atti di esecuzione in conformità dell'articolo 55, paragrafo ***2***, prevedendo sistemi europei di certificazione della cibersicurezza per i prodotti***, i processi*** e i servizi TIC che soddisfano i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.

Or. en

Emendamento 55

Proposta di regolamento
Articolo 44 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'ENISA gestisce un apposito sito	5. L'ENISA gestisce un apposito sito

web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza e li pubblicizza.	web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza***, compresi i certificati revocati e scaduti, i certificati e le dichiarazioni di conformità,*** e li pubblicizza.

Or. en

Emendamento 56

Proposta di regolamento
Articolo 44 – paragrafo 5 – comma 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	Se un sistema europeo di certificazione della cibersicurezza soddisfa i requisiti ai quali intende conformarsi e che sono stabiliti nella corrispondente legislazione dell'Unione volta all'armonizzazione, la Commissione pubblica senza indugio un riferimento a tale riguardo nella Gazzetta ufficiale dell'Unione europea e mediante qualsiasi altro mezzo conformemente alle condizioni stabilite nell'atto corrispondente della legislazione dell'Unione volta all'armonizzazione.

Or. en

Emendamento 57

Proposta di regolamento
Articolo 44 – paragrafo 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	5 bis. L'Agenzia riesamina i sistemi adottati almeno ogni cinque anni, tenendo conto delle osservazioni ricevute dai portatori di interessi.

Or. en

Emendamento 58

Proposta di regolamento
Articolo 45 – paragrafo -1 (nuovo)

Testo della Commissione	*Emendamento*
	-1. I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da soddisfare gli obiettivi comuni di cibersicurezza in materia di integrità, riservatezza, disponibilità e tutela della vita privata. Inoltre, riducono al minimo gli altri rischi per la vita, la salute, l'ambiente e altri importanti interessi giuridici. Sono proporzionati, orientati al mercato e tengono conto dell'interesse pubblico.

Or. en

Emendamento 59

Proposta di regolamento
Articolo 45 – comma 1 – lettera a

Testo della Commissione	*Emendamento*
(a) ***proteggere i dati conservati, trasmessi o altrimenti trattati dall'archiviazione, dal trattamento, dall'accesso o dalla divulgazione accidentali o non autorizzati***;	(a) ***assicurare la riservatezza, l'integrità, la disponibilità e la privacy dei servizi, delle funzioni e dei dati***;

Or. en

Emendamento 60

Proposta di regolamento
Articolo 45 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) ***proteggere i dati conservati,***	(b) ***assicurare che soltanto le persone***

trasmessi o altrimenti trattati dalla distribuzione accidentale o non autorizzata, dalla perdita accidentale o dall'alterazione;	***autorizzate e/o i sistemi o programmi autorizzati possano accedere ai servizi, alle funzioni e ai dati e utilizzarli***;

Or. en

Emendamento 61

Proposta di regolamento
Articolo 45 – comma 1 – lettera c

Testo della Commissione	*Emendamento*
(c) assicurare che ***le persone, i programmi o le macchine autorizzati possano accedere esclusivamente ai dati, ai*** servizi ***o alle funzioni per i quali dispongono dei diritti di accesso***;	(c) assicurare che ***sia stata predisposta una procedura per l'identificazione e la documentazione di tutte le dipendenze e le vulnerabilità note presenti nei prodotti, nei processi e nei*** servizi ***TIC***;

Or. en

Emendamento 62

Proposta di regolamento
Articolo 45 – comma 1 – lettera d

Testo della Commissione	*Emendamento*
(d) ***registrare quali dati, funzioni o*** servizi ***sono stati comunicati, in quale momento e a chi***;	(d) ***assicurare che i prodotti, i processi e i*** servizi ***TIC non contengano vulnerabilità note***;

Or. en

Emendamento 63

Proposta di regolamento
Articolo 45 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) ***fare in modo*** che sia ***possibile***	(e) ***assicurare*** che sia ***stata predisposta***

verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso o che sono stati utilizzati, in quale momento e da chi;	***una procedura per trattare le vulnerabilità note di recente scoperta nei prodotti, nei processi e nei servizi TIC***;

Or. en

Emendamento 64

Proposta di regolamento
Articolo 45 – comma 1 – lettera f

Testo della Commissione	*Emendamento*
(f) ***ripristinare la disponibilità e l'accesso ai dati, ai servizi e alle funzioni in modo tempestivo in caso di incidente fisico o tecnico***;	(f) ***predisporre una procedura per monitorare, rilevare e segnalare gli incidenti di sicurezza e per rispondere a tali incidenti ed evitare che si ripetano***;

Or. en

Emendamento 65

Proposta di regolamento
Articolo 45 – comma 1 – lettera g

Testo della Commissione	*Emendamento*
(g) accertarsi che ***il software dei prodotti e*** dei servizi ***TIC sia aggiornato e non contenga vulnerabilità note e che tali prodotti e servizi dispongano di meccanismi per effettuare aggiornamenti del software protetti.***	(g) accertarsi che ***la disponibilità*** dei servizi***, delle funzioni e dei dati e l'accesso agli stessi siano perturbati in misura minima o siano ripristinati rapidamente in caso di incidente;***

Or. en

Emendamento 66

Proposta di regolamento
Articolo 45 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) registrare quali dati, funzioni o servizi sono stati comunicati, in quale momento e a chi;

Or. en

Emendamento 67

Proposta di regolamento
Articolo 45 – comma 1 – lettera g ter (nuova)

Testo della Commissione	*Emendamento*
	(g ter) fare in modo che sia possibile verificare quali sono i dati, i servizi o le funzioni a cui è stato effettuato l'accesso o che sono stati utilizzati, in quale momento e da chi;

Or. en

Emendamento 68

Proposta di regolamento
Articolo 45 – comma 1 – lettera g quater (nuova)

Testo della Commissione	*Emendamento*
	(g quater) assicurare che i prodotti e i servizi TIC siano elaborati secondo il principio della "sicurezza fin dalla progettazione".

Or. en

Motivazione

La formulazione degli obiettivi di sicurezza è troppo prescrittiva; deve essere più flessibile e descrittiva.

Emendamento 69

Proposta di regolamento
Articolo 46 – paragrafo 1

Testo della Commissione	*Emendamento*
1. I sistemi europei di certificazione della cibersicurezza possono specificare ***per i*** prodotti ***e i*** servizi TIC ***rilasciati nel loro ambito*** uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato.	1. I sistemi europei di certificazione della cibersicurezza possono specificare***, a seconda del contesto e dell'uso previsto dei*** prodotti***, dei processi e dei*** servizi TIC***,*** uno o più dei seguenti livelli di affidabilità ***basati sui rischi***: di base, sostanziale e/o elevato.

Or. en

Emendamento 70

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera a

Testo della Commissione	*Emendamento*
(a) il livello di affidabilità di base ***si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità limitato riguardo alle qualità di cibersicurezza pretese o dichiarate di*** un prodotto ***o di un*** servizio TIC ***ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre il rischio di incidenti di cibersicurezza;***	(a) il livello di affidabilità di base ***corrisponde a un basso rischio connesso a*** un prodotto***, processo e*** servizio TIC. ***Un basso livello di rischio sussiste se un attacco contro il prodotto, processo e servizio TIC non compromette la disponibilità, l'autenticità, l'integrità, la riservatezza o altri importanti obiettivi, quali la salute degli utenti o di terzi, l'ambiente, la tutela della vita privata, altri importanti interessi giuridici o infrastrutture critiche e i relativi sistemi o prodotti di sostegno.***

Or. en

Motivazione

È essenziale disporre di una descrizione minima dei componenti dell'affidabilità di ciascun livello di affidabilità.

Emendamento 71

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera b

Testo della Commissione	*Emendamento*
(b) il livello di affidabilità sostanziale ***si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità sostanziale riguardo alle qualità di cibersicurezza pretese o dichiarate di*** un prodotto ***o di un*** servizio TIC ***ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre in modo significativo il rischio di incidenti di cibersicurezza;***	(b) il livello di affidabilità sostanziale ***corrisponde a un rischio maggiore connesso a*** un prodotto***, processo e*** servizio TIC. ***Un livello di rischio maggiore sussiste se un attacco contro il prodotto e servizio TIC compromette la disponibilità, l'autenticità, l'integrità, la riservatezza o altri importanti obiettivi, quali la salute degli utenti o di terzi, l'ambiente, la tutela della vita privata, altri importanti interessi giuridici o infrastrutture critiche e i relativi sistemi o prodotti di sostegno.***

Or. en

Motivazione

È essenziale disporre di una descrizione minima dei componenti dell'affidabilità di ciascun livello di affidabilità.

Emendamento 72

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera c

Testo della Commissione	*Emendamento*
(c) il livello di affidabilità elevato ***si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità più*** elevato ***riguardo alle qualità di cibersicurezza pretese o dichiarate di un*** prodotto ***o di un*** servizio TIC ***rispetto ai certificati con livello di affidabilità sostanziale ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di prevenire gli***	(c) il livello di affidabilità elevato ***corrisponde a un rischio elevato connesso a un prodotto, processo e servizio TIC. Un livello di rischio*** elevato ***sussiste se un attacco contro il*** prodotto***, processo e*** servizio TIC ***compromette la disponibilità, l'autenticità, l'integrità, la riservatezza o altri importanti obiettivi ed è ragionevole presumere che metta a rischio la sovranità nazionale o la sicurezza pubblica degli Stati***.

incidenti di cibersicurezza.

Or. en

Motivazione

È essenziale disporre di una descrizione minima dei componenti dell'affidabilità di ciascun livello di affidabilità.

Emendamento 73

Proposta di regolamento
Articolo 46 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 46 bis
	Valutazione dei livelli di affidabilità dei sistemi europei di certificazione della cibersicurezza
	1. Per il livello di affidabilità di base è possibile procedere a un'autovalutazione della conformità sotto la responsabilità esclusiva del fabbricante o fornitore di prodotti, processi e servizi TIC come stabilito nell'articolo 4 e nell'allegato II della decisione n. 768/2008/CE.
	2. Per i livelli di affidabilità sostanziale ed elevato, la valutazione si fonda almeno sulla verifica della conformità delle funzionalità di sicurezza del prodotto, processo o servizio alla relativa documentazione tecnica;

Or. en

Motivazione

Consentire l'autocertificazione (detta autovalutazione) soltanto al livello più basso consentirà l'allineamento al nuovo quadro legislativo e costituirà un modo più facile ed efficiente in termini di costi per certificare i prodotti, processi e servizi che presentano un uso previsto per il mercato "di massa".

Emendamento 74

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera a

Testo della Commissione	*Emendamento*
(a) l'oggetto e l'ambito di applicazione della certificazione, compresi il tipo o le categorie di prodotti e servizi TIC coperti;	(a) l'oggetto e l'ambito di applicazione della certificazione, compresi il tipo o le categorie di prodotti***, processi*** e servizi TIC coperti***, nonché una motivazione che illustri in che modo il sistema di certificazione risponde alle esigenze del gruppo interessato previsto***;

Or. en

Emendamento 75

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	(a bis) i requisiti di cibersicurezza indicati nelle certificazioni nazionali della cibersicurezza che esso sostituisce o nella legislazione e nelle politiche che sostiene;

Or. en

Motivazione

Per facilitare la transizione, l'oggetto e l'ambito di applicazione del sistema europeo di certificazione della cibersicurezza dovrebbero essere connessi all'atto che esso sostituisce o sostiene, a seconda che l'intento sia eliminare gli ostacoli agli scambi o sostenere la legislazione e le politiche.

Emendamento 76

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(b) l'indicazione dettagliata dei requisiti	(b) l'indicazione dettagliata dei requisiti

di cibersicurezza rispetto ai quali i prodotti e servizi TIC sono valutati, ad esempio in riferimento a norme tecniche o a specifiche tecniche dell'Unione o internazionali;	di cibersicurezza rispetto ai quali i prodotti***,*** ***processi*** e servizi TIC sono valutati, ad esempio in riferimento a norme tecniche o a specifiche tecniche dell'Unione o internazionali;

Or. en

Emendamento 77

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera d bis (nuova)

Testo della Commissione	*Emendamento*
	(d bis) i tipi di valutazione della conformità, i criteri di valutazione e i metodi stabiliti nell'articolo 4 e nell'allegato II della decisione n. 768/2008/CE, al fine di assicurare che siano rispettati gli obiettivi specifici di cui all'articolo 45 del presente regolamento;

Or. en

Motivazione

L'emendamento introduce e stabilisce un collegamento con il nuovo quadro legislativo.

Emendamento 78

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera m bis (nuova)

Testo della Commissione	*Emendamento*
	(m bis) le condizioni per il riconoscimento reciproco dei sistemi di certificazione con i paesi terzi;

Or. en

Motivazione

L'obiettivo è conseguire l'armonizzazione in tutta l'UE.

Emendamento 79

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera m ter (nuova)

Testo della Commissione	*Emendamento*
	(m ter) il periodo massimo di validità del certificato.

Or. en

Emendamento 80

Proposta di regolamento
Articolo 47 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 47 bis
	Dichiarazione di prodotto
	1. Il fabbricante o fornitore di prodotti, processi e servizi TIC rilascia una dichiarazione di prodotto che fornisce, tra l'altro, le seguenti informazioni pertinenti riguardo alla certificazione di tale prodotto, processo e servizio:
	- il rispetto dei requisiti indicati nel sistema;
	- l'interoperabilità del prodotto, del processo e del servizio;
	- la possibilità di aggiornamenti del prodotto, del processo e del servizio e il periodo per il quale sono forniti tali aggiornamenti.
	Rilasciando tale dichiarazione, il fabbricante o fornitore di prodotti, processi e servizi TIC si assume la responsabilità della conformità del prodotto o servizio TIC ai requisiti stabiliti nel sistema.

	2. Il produttore o fornitore di prodotti e servizi TIC mantiene a disposizione dell'autorità nazionale di controllo della certificazione di cui all'articolo 50, paragrafo 1, per un periodo di 10 anni, la dichiarazione di prodotto e la pertinente documentazione tecnica relativa alla conformità dei prodotti o servizi TIC a un sistema. Una copia della dichiarazione è trasmessa all'autorità nazionale di controllo della certificazione e all'ENISA.

Or. en

Motivazione

È nell'interesse dei consumatori e dell'industria conoscere le specifiche del prodotto, processo e servizio TIC. Per questo motivo, l'articolo 47 bis (nuovo) prevede l'obbligo per i fabbricanti o i fornitori di rilasciare una dichiarazione di prodotto contenente le pertinenti informazioni. Il consumatore sarà quindi in grado di prendere una decisione informata.

Emendamento 81

Proposta di regolamento
Articolo 48 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La certificazione è volontaria, salvo diversamente specificato nel diritto dell'Unione.	2. La certificazione ***per il livello di affidabilità elevato è obbligatoria. Per i livelli di affidabilità di base e sostanziale essa*** è volontaria, salvo diversamente specificato nel diritto dell'Unione.

Or. en

Motivazione

I prodotti, processi e servizi TIC a rischio più elevato dovrebbero essere soggetti a una valutazione obbligatoria per rafforzare la fiducia.

Emendamento 82

Proposta di regolamento
Articolo 48 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Un certificato europeo della cibersicurezza ai sensi del presente articolo è rilasciato dagli organismi di valutazione della conformità di cui all'articolo 51 sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza, adottato a norma dell'articolo 44.	3. Un certificato europeo della cibersicurezza ai sensi del presente articolo è rilasciato ***a seguito di un'autovalutazione oppure*** dagli organismi di valutazione della conformità di cui all'articolo 51 sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza, adottato a norma dell'articolo 44.

Or. en

Emendamento 83

Proposta di regolamento
Articolo 48 – paragrafo 6

Testo della Commissione	*Emendamento*
6. I certificati sono rilasciati per un periodo massimo ***di tre anni*** e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.	6. I certificati sono rilasciati per un periodo massimo ***determinato dalle norme del sistema e tenendo conto di un ciclo di vita ragionevole*** e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.

Or. en

Motivazione

Ciò garantisce la flessibilità di adeguare il periodo di validità all'uso previsto.

Emendamento 84

Proposta di regolamento
Articolo 48 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 48 bis
	Obiezioni formali ai sistemi europei di certificazione della cibersicurezza

1. Se uno Stato membro ritiene che un sistema europeo di certificazione della cibersicurezza non soddisfi completamente i requisiti ai quali intende conformarsi e che sono stabiliti nella corrispondente legislazione dell'Unione volta all'armonizzazione, informa la Commissione e fornisce una spiegazione dettagliata. La Commissione decide, previa consultazione del comitato istituito conformemente alla pertinente legislazione dell'Unione volta all'armonizzazione, se del caso, o a seguito di altre forme di consultazione di esperti del settore:

(a) di pubblicare, non pubblicare o pubblicare con limitazioni i riferimenti al sistema europeo di cibersicurezza in questione nella Gazzetta ufficiale dell'Unione europea;

(b) di mantenere o mantenere con limitazioni i riferimenti del sistema europeo di cibersicurezza in questione nella Gazzetta ufficiale dell'Unione europea, o di ritirarli dalla stessa.

2. La Commissione pubblica sul proprio sito web le informazioni relative ai sistemi europei di cibersicurezza che sono stati oggetto della decisione di cui al paragrafo 1.

3. La Commissione informa l'ENISA della decisione di cui al paragrafo 1 e, se necessario, richiede la revisione del sistema europeo di cibersicurezza in questione.

4. La decisione di cui al paragrafo 1, lettera a), è adottata secondo la procedura consultiva di cui all'articolo 55, paragrafo 2.

5. La decisione di cui al paragrafo 1, lettera b), è adottata secondo la procedura d'esame di cui all'articolo 55, paragrafo 2 bis (nuovo).

Or. en

Emendamento 85

Proposta di regolamento
Articolo 49 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. Gli Stati membri comunicano alla Commissione tutte le richieste di elaborazione di sistemi nazionali di certificazione della cibersicurezza ed espongono le ragioni per la loro adozione.

Or. en

Emendamento 86

Proposta di regolamento
Articolo 49 – paragrafo 3 ter (nuovo)

Testo della Commissione	*Emendamento*
	3 ter. Su richiesta, gli Stati membri inviano almeno in forma elettronica qualsiasi progetto di sistema nazionale di certificazione della cibersicurezza agli altri Stati membri, all'ENISA o alla Commissione.

Or. en

Emendamento 87

Proposta di regolamento
Articolo 49 – paragrafo 3 quater (nuovo)

Testo della Commissione	*Emendamento*
	3 quater. Entro tre mesi, ciascuno Stato membro risponde alle osservazioni ricevute da qualsiasi altro Stato membro, dall'ENISA o dalla Commissione riguardo a qualsiasi progetto di cui al paragrafo 3 ter, e tiene debitamente conto

di tali osservazioni.

Or. en

Emendamento 88

Proposta di regolamento
Articolo 49 – paragrafo 3 quinquies (nuovo)

Testo della Commissione	*Emendamento*
	3 quinquies. Se uno Stato membro riceve osservazioni secondo le quali il progetto di sistema nazionale di certificazione della cibersicurezza avrebbe un effetto negativo sul mercato interno, consulta l'ENISA e la Commissione prima di adottarlo.

Or. en

Motivazione

L'introduzione di un sistema di notifica mira a prevenire la creazione di ostacoli nel mercato interno prima che essi si concretizzino e costituisce una prassi comune in materia di norme e regolamentazioni tecniche.

Emendamento 89

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	(b bis) eseguono audit per assicurare che si applichino standard equivalenti nell'Unione e riferire in merito ai risultati all'ENISA e al gruppo;

Or. en

Motivazione

Ciò contribuisce a garantire l'applicazione di un livello uniforme di servizio e di qualità in tutta l'UE e a prevenire la possibilità di ricercare la certificazione più vantaggiosa.

Emendamento 90

Proposta di regolamento
Articolo 51 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Al fine di assicurare che si applichino standard equivalenti nell'Unione vengono eseguiti audit, i cui risultati sono trasmessi all'ENISA e al gruppo.

Or. en

Emendamento 91

Proposta di regolamento
Articolo 53 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Il gruppo è composto dalle autorità nazionali di controllo della certificazione. Le autorità sono rappresentate dai capi o da rappresentanti ad alto livello delle autorità nazionali di controllo della certificazione.	2. Il gruppo è composto dalle autorità nazionali di controllo della certificazione ***di tutti gli Stati membri***. Le autorità sono rappresentate dai capi o da rappresentanti ad alto livello delle autorità nazionali di controllo della certificazione.

Or. en

Motivazione

Ciò renderà più aperti e trasparenti i lavori del gruppo.

Emendamento 92

Proposta di regolamento
Articolo 55 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo

5 del regolamento (UE) n. 182/2011.

Or. en

MOTIVAZIONE

È un dato di fatto che la rivoluzione digitale mondiale stia prendendo sempre più piede e si stia diffondendo nelle nostre economie, nelle nostre società e a livello dei governi, rendendo vulnerabili tutti i nostri dati. I consumatori, le industrie, le istituzioni e le democrazie a livello locale, nazionale, europeo e mondiale hanno subito ciberattacchi, atti di ciberspionaggio o di sabotaggio informatico e vi è una diffusa consapevolezza del fatto che tali eventi aumenteranno in maniera consistente negli anni a venire.

Miliardi di dispositivi sono collegati a Internet e interagiscono su un nuovo livello e su una nuova scala: insieme ai servizi correlati, possono migliorare la vita dei cittadini e le nostre economie. Tuttavia, gli individui e le organizzazioni potranno divenire pienamente parte del mondo digitale solo avendo fiducia nelle tecnologie digitali. Tale fiducia implica che i dispositivi IoT, i processi e i servizi siano sicuri.

Al fine di conseguire detti obiettivi, la Commissione ha proposto il "regolamento sulla cibersicurezza", che costituisce una parte importante, nonché uno strumento essenziale, della nuova strategia dell'UE per la cibersicurezza, che mira a fornire all'Europa una visione di lungo termine a riguardo e a rafforzare la fiducia nelle tecnologie digitali. Occorre contestualizzare tale aspetto nel quadro legislativo già in vigore. L'UE ha già istituito l'Agenzia europea per la sicurezza delle reti e dell'informazione (ENISA) e ha adottato una direttiva sulla sicurezza delle reti e dell'informazione (la direttiva SRI), attualmente in fase di recepimento negli ordinamenti nazionali degli Stati membri.

Il regolamento sulla cibersicurezza si compone di due parti: nella prima vengono specificati il ruolo e il mandato dell'ENISA al fine di rafforzare l'Agenzia, mentre nella seconda è introdotto un sistema di certificazione della cibersicurezza sotto forma di quadro volontario volto a migliorare la sicurezza dei dispositivi connessi e dei prodotti e servizi digitali.

Il relatore, in generale, si compiace della proposta formulata dalla Commissione in merito al regolamento sulla cibersicurezza in quanto è fondamentale per ridurre al minimo i rischi e le minacce alla sicurezza delle informazioni e alle reti, nonché per consentire ai consumatori di avere fiducia nelle soluzioni informatiche, segnatamente a riguardo dell'Internet degli oggetti. Il relatore ritiene fortemente che l'Europa possa divenire un attore imprescindibile della cibersicurezza. L'Europa presenta una solida base industriale e, pertanto, è nell'interesse sia dei consumatori che dell'industria lavorare sul miglioramento della cibersicurezza in relazione ai beni di consumo, le applicazioni industriali e le infrastrutture critiche.

È opportuno modificare la proposta della Commissione a riguardo sia della parte concernente l'ENISA che della parte relativa alla certificazione.

Per quanto riguarda la prima, il relatore ritiene sia fondamentale stabilire il quadro adeguato per garantire la solidità e il funzionamento dell'Agenzia. Il relatore accoglie con favore il rafforzamento del ruolo dell'ENISA, compresi il suo mandato permanente e l'incremento del bilancio e dell'organico, ma sottolinea la necessità di adottare un approccio realistico considerando il numero ancora esiguo di esperti impiegati dall'ENISA rispetto alle dimensioni dell'organico di talune autorità nazionali di controllo della certificazione. L'ENISA dovrebbe continuare a coordinare la cooperazione operativa, basandosi sull'esperienza maturata

nell'ambito della direttiva SRI, continuare a sostenere le attività di rafforzamento delle capacità svolte dagli Stati membri nonché fungere da fonte di informazioni. L'ENISA è inoltre chiamata a svolgere un ruolo preminente nella definizione dei sistemi di cibersicurezza europei, insieme agli Stati membri e alle parti interessate.

Per quanto riguarda la certificazione, il relatore è a favore di una maggiore chiarezza circa l'ambito di applicazione della proposta. Da un lato, il regolamento dovrebbe concernere non solo i prodotti e i servizi, ma il loro intero ciclo di vita. I processi devono pertanto essere inclusi nel campo di applicazione. Dall'altro, alcune delle competenze degli Stati membri dovrebbero essere chiaramente escluse, ovvero quelle riguardanti il settore della pubblica sicurezza, la difesa, la sicurezza nazionale e il diritto penale.

Per quanto riguarda il sistema di certificazione della cibersicurezza, il relatore propone di specificare più in dettaglio un approccio basato sul rischio, contrapposto a un sistema di certificazione "universale". Il relatore è altresì favorevole a un sistema volontario, ma solo per i livelli base e di garanzia sostanziale. Per i prodotti, i processi o i servizi che rientrano nel livello di garanzia più elevato, è preferibile a suo avviso un sistema obbligatorio. Per quanto riguarda la valutazione delle tecnologie digitali appartenenti al livello di garanzia base, il relatore suggerisce inoltre un collegamento all'approccio al nuovo quadro legislativo, il che consentirà un esercizio di valutazione, nonché il conseguimento di un sistema più economico e meno oneroso che ha dimostrato la sua validità in vari settori.

Il relatore ritiene che i produttori o fornitori di prodotti, processi e servizi TIC debbano essere obbligati a rilasciare una dichiarazione sul prodotto recante informazioni strutturate relative alla certificazioni e che indichi, ad esempio, la disponibilità di aggiornamenti o l'interoperabilità di prodotti, processi o servizi certificati. In questo modo il consumatore potrebbe disporre di informazioni utili al momento della scelta di un dispositivo. Il relatore esprime la propria preferenza per una dichiarazione di prodotto di questo tipo rispetto a un'etichetta o un marchio che potrebbero essere fuorvianti per i consumatori.

Il relatore è fermamente convinto che la struttura di governance proposta dalla Commissione debba essere migliorata per garantire maggiore trasparenza a tutti gli attori coinvolti. Suggerisce pertanto l'adozione di un programma di lavoro pluriennale dell'Unione che identifichi le azioni comuni da intraprendere a livello unionale e che indichi i settori in cui devono essere introdotti i sistemi di certificazione europea in via prioritaria, nonché il livello di equivalenza della conoscenze e delle competenze degli organi di valutazione e di controllo negli Stati membri. Il rafforzamento della governance implica anche una maggiore partecipazione degli Stati membri e del settore dell'industria al processo di certificazione. Il ruolo degli Stati membri può essere rafforzato qualora il "gruppo" introdotto dall'articolo 53 della proposta, e composto dalle autorità nazionali di controllo della certificazione, sia posto su un piano di parità con la Commissione nell'ambito del processo di elaborazione del sistema di certificazione. Il gruppo dovrà altresì approvare una proposta di sistema europeo. Infine, è opportuno rafforzare anche la partecipazione dell'industria al processo di certificazione, chiarendo ad esempio la composizione del gruppo permanente di portatori di interesse e creando gruppi consultivi ad-hoc dell'ENISA al fine di acquisire ulteriori competenze e conoscenze dal settore industriale e altre parti interessate nell'ambito dei processi di certificazione. Il relatore ritiene che tutte queste misure consentiranno alle PMI di prendere parte più attivamente al processo.

Il sistema di certificazione europea necessita, in fase di elaborazione, di un maggiore coinvolgimento degli organismi europei di normalizzazione, quali il Comitato europeo di normalizzazione e il Comitato europeo di normalizzazione elettrotecnica. In tal modo sarebbe possibile garantire che a prevalere siano le norme internazionali già esistenti e globalmente accettate.