Parlamento europeo
2014-2019

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

2017/0225(COD)

30.4.2018

EMENDAMENTI
397 - 631

Progetto di relazione
Angelika Niebler
Regolamento 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")

Proposta di regolamento
(COM(2017)0477 – C8-0310/2017 – 2017/0225(COD))

Emendamento 397
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Titolo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	QUADRO PER LA SICUREZZA FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA

Or. en

Emendamento 398
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo -43 (nuovo)

Testo della Commissione	*Emendamento*
	Articolo -43
	Sicurezza fin dalla progettazione e per impostazione predefinita
	1. Tenendo conto dello stato dell'arte, i fabbricanti e i fornitori di servizi garantiscono la sicurezza fin dalla progettazione e per impostazione predefinita dei loro prodotti, processi, servizi e sistemi TIC venduti nell'Unione o esportati dalla stessa. Essi devono assicurare che il software installato sul loro prodotto, processo, servizio o sistema TIC sia sicuro e che non sia presente alcuna vulnerabilità di sicurezza nota, considerando lo stato dell'arte della tecnologia in quel momento. I prodotti, processi, servizi e sistemi TIC devono attuare le seguenti misure tecniche:
	(a) i prodotti, processi, servizi e sistemi TIC devono disporre di un software aggiornato e devono comprendere meccanismi per la ricezione periodica di aggiornamenti del software sicuri, opportunamente autenticati e attendibili;

(b) le capacità di accesso a distanza del prodotto, processo, servizio o sistema TIC devono essere documentate e protette dall'accesso non autorizzato al più tardi durante l'installazione;

(c) i prodotti TIC non devono avere le stesse password standardizzate predefinite a codifica fissa per tutti i dispositivi;

(d) i dati conservati dai prodotti, processi, servizi e sistemi TIC devono essere protetti in modo sicuro mediante i metodi più avanzati quali la cifratura;

(e) i prodotti, i processi, i servizi e i sistemi TIC devono accettare soltanto metodi di autenticazione a elevata sicurezza.

2. I fabbricanti e i fornitori di servizi devono notificare all'autorità competente qualsiasi vulnerabilità di sicurezza nota non appena essa viene riscontrata. Inoltre, devono fornire una riparazione e/o sostituzione tempestiva e gratuita per ovviare a qualsiasi nuova vulnerabilità riscontrata.

3. I prodotti, i processi, i servizi e i sistemi TIC immessi sul mercato rispettano gli obblighi di cui al paragrafo 1 durante il loro periodo di impiego prevedibile e normale.

4. Sebbene i fabbricanti siano tenuti a garantire la conformità di un prodotto, processo, servizio o sistema TIC, gli importatori devono assicurarsi che i prodotti che immettono sul mercato rispettino i requisiti applicabili e non presentino un rischio per il pubblico europeo. L'importatore deve verificare che il fabbricante al di fuori dell'UE abbia adottato le misure necessarie e che il prodotto, il processo, il servizio o il sistema sia conforme alle disposizioni dei paragrafi precedenti. I distributori di prodotti, processi, servizi e sistemi TIC devono disporre di una conoscenza di base dei requisiti giuridici e della documentazione di accompagnamento. I distributori devono essere in grado di

identificare i casi di non conformità. Essi devono inoltre poter dimostrare alle autorità nazionali di avere agito con la dovuta diligenza e di avere ricevuto conferma dal produttore o dall'importatore del fatto che sono state adottate le misure necessarie. Inoltre, un distributore deve essere in grado di assistere le autorità nazionali negli sforzi che intraprendono per ricevere la documentazione richiesta.

5. La Commissione adotta, mediante un atto di esecuzione e in cooperazione con l'ENISA, norme dettagliate sulle specificità dei requisiti di sicurezza di cui al paragrafo 1.

6. Se le autorità di vigilanza del mercato hanno motivi di ritenere che il prodotto, il processo, il servizio o il sistema TIC non rispetti i requisiti di cui al presente regolamento, esse impongono senza indugio al fabbricante o fornitore di servizi interessato di adottare le misure correttive del caso al fine di rendere il prodotto conforme ai suddetti requisiti oppure di ritirarlo dal mercato o richiamarlo entro un termine ragionevole e proporzionato alla natura del rischio, a seconda dei casi.

7. Se il fabbricante o il fornitore di servizi non adotta misure correttive adeguate nel periodo di cui al paragrafo 5, le autorità di vigilanza del mercato adottano le misure provvisorie del caso per vietare o limitare la messa a disposizione del prodotto sul mercato nazionale, per ritirarlo da tale mercato o per richiamarlo.

8. Le autorità di vigilanza del mercato organizzano controlli adeguati sulla conformità del prodotto e obbligano i fabbricanti o fornitori di servizi a richiamare dal mercato i prodotti non conformi. All'atto di individuare i prodotti che saranno oggetto del controllo di conformità, le autorità nazionali di certificazione danno la priorità ai prodotti

ad alto rischio per i consumatori, ai prodotti in cui sono integrate nuove tecnologie e/o ai prodotti con elevati tassi di vendita.

Or. en

Motivazione

Il quadro orizzontale per la definizione di un insieme di requisiti minimi in materia di sicurezza dovrebbe essere vincolante per tutti i prodotti connessi, quale condizione preliminare per la loro immissione sul mercato. L'assenza di funzionalità di sicurezza incorporate fin dalla progettazione nella maggior parte dei prodotti, dei processi, dei servizi o dei sistemi connessi presenti attualmente sul mercato dell'UE è uno dei motivi principali all'origine di vulnerabilità e del conseguente aumento degli attacchi informatici.

Emendamento 399
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo -43 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo -43 bis
	La direttiva 2014/53/UE è modificata con l'aggiunta della seguente lettera all'articolo 3, paragrafo 3:
	(f bis) le (nuove) apparecchiature radio sono sicure a livello informatico fin dalla progettazione, per impostazione predefinita e tramite attuazione;

Or. en

Emendamento 400
Olle Ludvigsson

Proposta di regolamento
Articolo 43 – comma 1

Testo della Commissione	*Emendamento*
I sistemi europei di certificazione della cibersicurezza attestano che i prodotti ***e***	***Allo scopo di garantire il corretto funzionamento del mercato interno 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.

perseguire, nel contempo, un elevato livello di cibersicurezza, ciberresilienza e fiducia all'interno dell'Unione, è introdotto un quadro europeo volontario di certificazione della cibersicurezza. Il quadro fornisce pari ed eque opportunità a tutte le imprese in Europa.

I sistemi europei di certificazione della cibersicurezza attestano che ***le procedure di sviluppo,*** i prodotti ***e/o i*** servizi TIC ***sono stati valutati con l'ausilio di una metodologia standardizzata per la valutazione della conformità, sulla base di norme di sicurezza specifiche stabilite da tali sistemi e definite al fine di tutelare*** la disponibilità, 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.

Or. en

Emendamento 401
Marisa Matias, Dan Nica, Miroslav Poche

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,	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.

processi, servizi e sistemi o accessibili tramite essi.	***I sistemi europei di certificazione della cibersicurezza stabiliscono criteri di responsabilità e propongono livelli di affidabilità per i prodotti e i servizi TIC e, se possibile, per il recupero dei dati.***

Or. en

Emendamento 402
Michał Boni, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

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 ***secondo le norme,*** per quanto riguarda la loro capacità di ***conseguire obiettivi di sicurezza***.

Or. en

Emendamento 403
Pilar del Castillo Vera

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	I sistemi europei di certificazione della cibersicurezza attestano che i prodotti***,*** ***processi*** e servizi TIC certificati nel loro ambito sono conformi a determinati requisiti ***secondo le norme,*** per quanto

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***.	riguarda la loro capacità di resistere a un determinato livello di affidabilità.

Or. en

Emendamento 404
Massimiliano Salini

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 e servizi TIC certificati nel loro ambito ***non hanno vulnerabilità note al momento della certificazione e*** sono conformi a determinati requisiti per quanto riguarda la loro capacità di resistere ***in modo dinamico***, 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.

Or. en

Emendamento 405
Csaba Molnár

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 ***stabiliti dalle norme europee o internazionali*** 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 406
Evžen Tošenovský

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 e servizi TIC certificati nel loro ambito sono conformi a determinati requisiti ***stabiliti dalle norme europee o internazionali*** 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.

Or. en

Emendamento 407
Gunnar Hökmark

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 ***le procedure di sviluppo,*** i prodotti e ***i*** servizi TIC sono ***stati valutati con l'ausilio di una metodologia standardizzata per la valutazione della conformità, sulla base di norme di sicurezza specifiche stabilite da sistemi europei di certificazione della cibersicurezza e definite al fine di tutelare*** la disponibilità, 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.

Or. en

Emendamento 408
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Clare Moody

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***,*** servizi ***e processi*** 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.

Or. en

Emendamento 409
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 43 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 43 bis
	Sicurezza fin dalla progettazione e per impostazione predefinita
	1. Tenendo conto dello stato dell'arte, i fabbricanti e i fornitori di servizi assicurano la sicurezza fin dalla progettazione e per impostazione predefinita dei loro prodotti e servizi TIC. I fabbricanti e i fornitori di servizi devono assicurare che il software installato sul loro prodotto o servizio TIC sia sicuro e non presenti alcuna vulnerabilità di sicurezza nota, considerando lo stato dell'arte della tecnologia in quel momento. I prodotti e servizi TIC devono attuare le seguenti misure tecniche:
	(a) i prodotti e servizi TIC devono disporre di software aggiornato e devono comprendere meccanismi per la ricezione periodica di aggiornamenti del software sicuri, opportunamente autenticati e attendibili;
	(b) le capacità di accesso a distanza del prodotto o servizio TIC devono essere documentate e protette dall'accesso non autorizzato al più tardi durante l'installazione;
	(c) i prodotti TIC non devono avere le stesse password standardizzate predefinite a codifica fissa per tutti i dispositivi;
	(d) i dati conservati dai prodotti e servizi TIC devono essere protetti in modo sicuro mediante i metodi più avanzati quali la cifratura;

(e) i prodotti e servizi TIC devono accettare soltanto metodi di autenticazione a elevata sicurezza.

2. I fabbricanti e i fornitori di servizi devono notificare all'autorità competente qualsiasi vulnerabilità di sicurezza nota non appena essa viene riscontrata. Inoltre, devono fornire una riparazione e/o sostituzione tempestiva per ovviare a qualsiasi nuova vulnerabilità riscontrata.

3. I prodotti e i servizi TIC immessi sul mercato rispettano gli obblighi di cui al paragrafo 1 durante il loro periodo di impiego prevedibile e normale.

4. La Commissione adotta, mediante atti di esecuzione e in cooperazione con l'ENISA, norme dettagliate sulle specificità dei requisiti di sicurezza di cui al paragrafo 1.

5. Se le autorità di vigilanza del mercato hanno motivi di ritenere che il prodotto o il servizio TIC non rispetti i requisiti di cui al presente regolamento, esse impongono senza indugio al fabbricante o fornitore di servizi interessato di adottare le misure correttive del caso al fine di rendere il prodotto conforme ai suddetti requisiti oppure di ritirarlo dal mercato o richiamarlo entro un termine ragionevole e proporzionato alla natura del rischio, a seconda dei casi.

6. Se il fabbricante o il fornitore di servizi non adotta misure correttive adeguate nel periodo di cui al paragrafo 5, le autorità di vigilanza del mercato adottano le misure provvisorie del caso per vietare o limitare la messa a disposizione del prodotto sul mercato nazionale, per ritirarlo da tale mercato o per richiamarlo.

7. Le autorità di vigilanza del mercato organizzano controlli adeguati sulla conformità del prodotto e obbligano i fabbricanti o fornitori di servizi a richiamare dal mercato i prodotti non conformi. All'atto di individuare i prodotti

che saranno oggetto del controllo di conformità, le autorità nazionali di certificazione danno la priorità ai prodotti ad alto rischio per i consumatori, ai prodotti in cui sono integrate nuove tecnologie e/o ai prodotti con elevati tassi di vendita.

Or. en

Motivazione

One of the key reasons behind the increase of cyberattacks is the lack of security functionalities incorporated in the design of the connected products and/or services. Today, most of the connected devices available in the EU's single market are designed and manufactured without the most basic security features embedded in their software. In order to trust the Internet of Things, consumers must be assured that the connected products they purchase or services they use are secure and protected from software and hardware vulnerabilities. To ensure a high-level of security by design and by default, a minimum set of requirements for security should be binding for all connected products as a condition for putting them on the market. Such a horizontal and binding framework should be established as a complement of existing and pending legislation that requires cybersecurity measures such as the General Data Protection Regulation and the proposal for a European Electronic Communication Code.

Emendamento 410
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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 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***.	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. ***La richiesta della Commissione di preparare una proposta di sistema europeo di certificazione della cibersicurezza deve essere motivata da uno o più dei seguenti motivi:*** ***(a) i sistemi di certificazione della cibersicurezza esistenti frammentano il mercato interno;***

(b) esiste l'esigenza attuale o prevista di sostenere una normativa dell'Unione;
(c) esiste una richiesta consensuale degli Stati membri***, del*** gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 ***o del gruppo permanente di portatori di interessi istituito a norma dell'articolo 20; la*** Commissione ***europea provvede affinché la richiesta proveniente da uno Stato membro rifletta la partecipazione equilibrata delle parti interessate, come le industrie, comprese le PMI, le organizzazioni sindacali, la società civile e le organizzazioni dei consumatori. In quest'ottica, gli Stati membri garantiscono misure idonee per consentire*** la ***consultazione della parti a livello nazionale riguardo al processo di*** preparazione ***e monitoraggio dei sistemi*** di certificazione.

Or. en

Emendamento 411
Evžen Tošenovský

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 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.	1. A seguito di una richiesta della Commissione ***o del gruppo europeo per la 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. Gli Stati membri o il gruppo europeo per la certificazione della 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. ***La Commissione e il gruppo europeo per la***

certificazione della cibersicurezza valutano le proposte di un sistema europeo di certificazione della cibersicurezza avanzate dalle piattaforme di consultazione dei portatori di interessi.

Or. en

Emendamento 412
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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 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.	1. 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 cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 ***propongono la preparazione di una proposta di sistema rientrante nell'ambito dell'articolo 45, paragrafo 1, lettera c), mentre il gruppo di certificazione dei portatori di interessi istituito a norma dell'articolo [20 ter] propone all'ENISA e*** alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza ***rientrante nell'ambito di applicazione dell'articolo 45, paragrafo 1, lettera a) o b)***.

Or. en

Motivazione

L'emendamento tiene conto dell'istituzione del gruppo di certificazione dei portatori di interessi.

Emendamento 413
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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 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***.	1. A seguito di una richiesta della Commissione, l'ENISA prepara un sistema europeo di certificazione della ***sicurezza informatica*** che soddisfa i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento. Gli Stati membri***,*** il gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 ***o il gruppo permanente dei portatori di interessi istituito a norma dell'articolo 20*** possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della ***sicurezza informatica***.

Or. en

Motivazione

Dovrebbe esistere un numero ragionevole di modalità per proporre la preparazione di una proposta di certificazione europea della sicurezza informatica e l'aggiunta del gruppo permanente dei portatori di interessi amplia il numero di organismi competenti abbastanza da offrire maggiori possibilità, pur garantendo una procedura informata ed equa.

Emendamento 414
Michał Boni, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark, Marian-Jean Marinescu

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	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 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.	regolamento. Gli Stati membri**,** il gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 ***o altri portatori di interessi pertinenti dell'industria*** possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza.

Or. en

Emendamento 415
Françoise Grossetête

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 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.	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**,** il gruppo europeo per la certificazione della cibersicurezza (di seguito "il gruppo") istituito a norma dell'articolo 53 ***o i rappresentanti dell'industria europea*** possono proporre alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza.

Or. fr

Emendamento 416
András Gyürk

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 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.	1. A seguito di una richiesta della Commissione, ***le organizzazioni europee di normazione (OEN) preparano*** un sistema europeo di certificazione della cibersicurezza. Gli Stati membri o il gruppo europeo per la certificazione della 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.

Or. en

Emendamento 417
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

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

Testo della Commissione	*Emendamento*
	1 bis. La Commissione adotta e pubblica, dopo avere condotto una consultazione aperta e trasparente con i portatori di interessi pertinenti, 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 soggetti a un sistema europeo di certificazione della cibersicurezza. Prima dell'adozione del programma di lavoro, la Commissione consulta l'ENISA e tiene in massima considerazione la sua opinione.

Or. en

Emendamento 418
Michał Boni, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

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, l'ENISA ***definisce gli obiettivi di sicurezza, i requisiti di sicurezza e gli elementi costitutivi della proposta di sistema***. ***Tutti gli aspetti relativi alle procedure della valutazione di conformità saranno definiti dalla Commissione, sulla base delle conclusioni dell'ENISA. In tale processo, l'ENISA coopera strettamente con i portatori di interessi dell'industria e*** 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. ***Se del caso, l'ENISA può inoltre costituire un gruppo di lavoro di portatori di interessi sulla certificazione, costituito da membri del gruppo permanente di portatori di interessi, da portatori di interessi dell'industria che garantiscano un approccio orientato all'industria e da eventuali altri portatori di interessi, al fine di fornire consulenza specialistica sugli ambiti che formano oggetto di una specifica proposta di sistema.***

Or. en

Emendamento 419
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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	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.	consulta tutti i portatori di interessi***, comprese le associazioni dei consumatori,*** e coopera strettamente con il gruppo ***e con il gruppo permanente di portatori di interessi***. Il gruppo ***e il gruppo permanente di portatori di interessi forniscono*** all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri. ***Nella preparazione di ogni proposta di sistema, l'ENISA definisce un elenco di controllo dei rischi nonché delle caratteristiche di cibersicurezza necessarie per contrastare efficacemente tali rischi.***
	Or. en

Emendamento 420
Gunnar Hökmark

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, l'ENISA consulta tutti i portatori di interessi e coopera strettamente con il gruppo***, oltre a tenere in considerazione le norme nazionali e internazionali già esistenti, compresi gli accordi informali in seno alle associazioni industriali, per evitare duplicazioni***. 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.
	Or. en

Emendamento 421
Nadine Morano

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, l'ENISA consulta ***in modo trasparente*** tutti i portatori di interessi e coopera strettamente con il gruppo***, con*** il gruppo ***permanente di portatori di interessi e, per ogni proposta di sistema, con una piattaforma di consultazione ad hoc***. ***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. fr

Motivazione

I diversi processi di consultazione possono svolgere un ruolo fondamentale nel riunire e associare strettamente gli esperti nel quadro della proposta di sistema e per mettere a disposizione dell'ENISA le loro conoscenze ed esperienze riguardo al prodotto o al servizio interessato.

Emendamento 422
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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, l'ENISA consulta tutti i portatori di interessi ***nonché, ove opportuno, le organizzazioni dei consumatori, il gruppo di lavoro dell'articolo 29 e il comitato europeo per la protezione dei dati,*** 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.

Or. en

Motivazione

Emendamento basato sul parere del GEPD. È della massima importanza creare sinergie in ambito tecnico e nel settore della governance, affinché le certificazioni rilasciate a norma del quadro europeo di certificazione della cibersicurezza e quelle rilasciate a norma del regolamento generale sulla protezione dei dati non siano percepite come contraddittorie o non correlate tra loro dalle organizzazioni che si impegnano a conformarsi agli strumenti pertinenti.

Emendamento 423
Pilar del Castillo Vera

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, l'ENISA consulta tutti i portatori di interessi ***nel quadro di una procedura formale, standardizzata e trasparente*** e coopera strettamente con il gruppo. Il gruppo ***e tutti i portatori di interessi 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

Emendamento 424
Evžen Tošenovský

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	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.	consulta tutti i portatori di interessi e coopera strettamente con il gruppo ***e con le piattaforme di consultazione dei portatori di interessi***. 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.

Or. en

Emendamento 425
Martina Werner

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, l'ENISA consulta tutti i portatori di interessi ***mediante procedure di consultazione trasparenti*** 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.

Or. en

Emendamento 426
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner

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	2. Nella preparazione delle proposte di sistemi di cui al paragrafo 1, l'ENISA consulta tutti i portatori di interessi***, come richiesto a norma dell'articolo 20 bis,*** e coopera strettamente con il gruppo. Il

consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.	gruppo fornisce all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.

Or. en

Emendamento 427
András Gyürk

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 ***del primo progetto*** di cui al paragrafo 1, l'***OEN*** consulta tutti i portatori di interessi e coopera strettamente con il gruppo. Il gruppo fornisce all'***OEN*** l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema, se necessario anche fornendo pareri.

Or. en

Emendamento 428
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

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***	2. ***Prima della*** preparazione delle proposte di sistemi di cui al paragrafo 1, ***la Commissione conduce una consultazione pubblica aperta per*** tutti i portatori di interessi***. Nella preparazione della consultazione, la Commissione*** coopera strettamente con il gruppo ***europeo per la certificazione della cibersicurezza,***

di sistema, se necessario anche fornendo pareri.	***l'***ENISA ***e il gruppo di certificazione dei portatori di interessi***.

Or. en

Motivazione

L'emendamento tiene conto dell'istituzione del gruppo di certificazione dei portatori di interessi.

Emendamento 429
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

Proposta di regolamento
Articolo 44 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Il gruppo europeo per la certificazione della cibersicurezza e il gruppo di certificazione dei portatori di interessi forniscono all'ENISA l'assistenza e la consulenza specialistica richieste in relazione alla preparazione della proposta di sistema europeo di certificazione della cibersicurezza, se necessario anche fornendo pareri.

Or. en

Motivazione

L'emendamento tiene conto dell'istituzione del gruppo di certificazione dei portatori di interessi.

Emendamento 430
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

Proposta di regolamento
Articolo 44 – paragrafo 2 ter (nuovo)

Testo della Commissione	*Emendamento*

	2 ter. Oltre che riguardo alla proposta di un sistema che rientra nell'ambito di applicazione dell'articolo 45, paragrafo 1, lettere a) e b), la Commissione consulta e richiede l'approvazione del gruppo di certificazione dei portatori di interessi prima dell'adozione finale di un sistema europeo di certificazione della cibersicurezza. Lo stesso vale per il gruppo europeo per la certificazione della cibersicurezza riguardo alla proposta di un sistema che rientra nell'ambito di applicazione dell'articolo 45, paragrafo 1, lettera c).

Or. en

Motivazione

L'emendamento tiene conto dell'istituzione del gruppo di certificazione dei portatori di interessi.

Emendamento 431
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

Proposta di regolamento
Articolo 44 – paragrafo 2 quater (nuovo)

Testo della Commissione	*Emendamento*
	2 quater. Nella preparazione di una proposta di sistema, l'ENISA, con la consulenza del gruppo europeo per la certificazione della cibersicurezza e del gruppo di certificazione dei portatori di interessi per le rispettive proposte di sistemi, definisce una scadenza entro la quale la specifica proposta di sistema diventa effettiva. Il mancato rispetto di tale scadenza comporta la nullità e la revoca della proposta di sistema.

Or. en

Motivazione

A fini di pianificazione a lungo termine degli investimenti, le parti interessate concordano congiuntamente una scadenza specifica per l'introduzione delle nuove proposte di sistemi europei di certificazione. Le disposizioni collegate alla scadenza incentiveranno la tempestiva adozione di tali sistemi.

Emendamento 432
Gunnar Hökmark

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. L'ENISA trasmette alla Commissione il sistema europeo di certificazione della cibersicurezza preparato in conformità del paragrafo 2. ***L'ENISA inserisce nelle informazioni alla Commissione eventuali osservazioni o riserve dei membri del gruppo.***

Or. en

Emendamento 433
Michał Boni, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

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. L'ENISA trasmette ***tempestivamente*** alla Commissione il sistema europeo di certificazione della cibersicurezza preparato in conformità del paragrafo 2.

Or. en

Emendamento 434
Jakop Dalunde, Reinhard Bütikofer

a nome del gruppo Verts/ALE

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 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. ***La Commissione può consultare il comitato europeo per la protezione dei dati e tenere conto del suo parere prima di adottare tali atti di esecuzione.***

Or. en

Motivazione

Emendamento basato sul parere del GEPD. Esso garantisce coerenza tra le certificazioni rilasciate a norma del quadro europeo di certificazione della cibersicurezza e quelle rilasciate a norma del regolamento generale sulla protezione dei dati.

Emendamento 435
Pilar del Castillo Vera

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 1, 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 436
Martina Werner

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 1, 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 437
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

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 1, 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 438

Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

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 ***delegati*** in conformità dell'articolo 55, paragrafo 1, prevedendo sistemi europei di certificazione della cibersicurezza per i prodotti***,*** i servizi ***e i processi*** TIC che soddisfano i requisiti di cui agli articoli 45, 46 e 47 del presente regolamento.

Or. en

Motivazione

Per garantire che i colegislatori possano esercitare i loro poteri di controllo, alla Commissione è attribuito il diritto di adottare atti delegati.

Emendamento 439
Miapetra Kumpula-Natri

Proposta di regolamento
Articolo 44 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza e li pubblicizza.	5. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza e li pubblicizza. ***L'ENISA si impegna, inoltre, a comunicare ai consumatori le informazioni pertinenti relative ai sistemi di certificazione applicabili, ad esempio fornendo orientamenti e raccomandazioni ai mercati online e offline.***

Or. en

Emendamento 440

Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 44 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'ENISA gestisce un apposito sito web che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza e li pubblicizza.	5. L'ENISA gestisce un apposito sito web***, conformemente alla direttiva (UE) 2016/2102,*** che fornisce informazioni sui sistemi europei di certificazione della cibersicurezza***, sulla revoca e la scadenza dei sistemi di certificazione e sui prodotti, processi, servizi e sistemi TIC certificati,*** e li pubblicizza.

Or. en

Emendamento 441
Gunnar Hökmark

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

Testo della Commissione	*Emendamento*
	5 bis. La Commissione può stipulare, per conto dell'Unione europea, accordi con mercati esteri o paesi terzi per il riconoscimento reciproco dei certificati. Tali accordi sono definiti conformemente alla medesima procedura di preparazione e adozione dei sistemi di cui al presente articolo, salvo indicazione contraria.

Or. en

Emendamento 442
Miapetra Kumpula-Natri

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

Testo della Commissione	*Emendamento*

5 bis. L'ENISA, tenendo nella massima considerazione l'opinione del gruppo, si assicura che le eventuali proposte di sistemi europei per la cibersicurezza non impediscano una concorrenza efficace attraverso la creazione di ostacoli all'ingresso nel mercato da parte di nuove imprese e di nuovi prodotti.

Or. en

Emendamento 443
Pavel Telička, Carolina Punset, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

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

Testo della Commissione	*Emendamento*
	5 bis. I sistemi adottati sono riesaminati e, ove necessario, aggiornati periodicamente in cooperazione con i portatori di interessi e con il gruppo nell'ambito della struttura istituita a norma del presente regolamento.

Or. en

Emendamento 444
Martina Werner

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

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

Or. en

Emendamento 445
Miapetra Kumpula-Natri

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

Testo della Commissione	*Emendamento*
	5 ter. L'ENISA fornisce i meccanismi, gli orientamenti e le procedure necessari all'adattamento e all'aggiornamento dei sistemi europei per la cibersicurezza, al fine di tenere conto dei nuovi sviluppi nella tecnologia di cibersicurezza.

Or. en

Emendamento 446
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

Proposta di regolamento
Articolo 45 – comma 1 – parte introduttiva

Testo della Commissione	*Emendamento*
I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da tener conto, se del caso, dei seguenti obiettivi di sicurezza:	I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da tener conto, se del caso, dei seguenti obiettivi di sicurezza***, al fine di garantire la disponibilità, l'integrità e la riservatezza dei servizi***:

Or. en

Emendamento 447
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 45 – comma 1 – parte introduttiva

Testo della Commissione	*Emendamento*

I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da tener conto, se del caso, ***dei*** seguenti ***obiettivi di sicurezza***:	I sistemi europei di certificazione della cibersicurezza sono progettati in modo tale da tener conto, se del caso, ***degli obiettivi collegati alle*** seguenti ***categorie***:

Or. en

Emendamento 448
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

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) ***per i prodotti corrispondenti al livello di affidabilità di base o autodichiarato, i dispositivi elettronici di consumo quali definiti all'articolo 2 [paragrafo 11 bis (nuovo)]. I sistemi europei di certificazione della cibersicurezza per questa categoria sostengono l'adozione e la commercializzazione di norme internazionali del mercato unico e da parte di tale mercato.***

Or. en

Motivazione

Per raggiungere gli obiettivi della proposta di regolamento e assicurare, in particolare, la sua adeguatezza alle esigenze future, gli obiettivi di sicurezza dovrebbero essere definiti sulla base delle applicazioni del prodotto e non delle sue funzionalità.

Emendamento 449
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 45 – comma 1 – lettera b

Testo della Commissione	*Emendamento*

(b) ***proteggere i dati conservati, trasmessi o altrimenti trattati dalla distribuzione accidentale o non autorizzata, dalla perdita accidentale o dall'alterazione;***	(b) ***per i prodotti corrispondenti al livello di affidabilità sostanziale, i prodotti, servizi e processi TIC relativi a un sistema di controllo industriale o utilizzati in robotica e nei veicoli autonomi, oppure il software e l'hardware di apparecchiature terminali utilizzate per la prestazione di servizi essenziali per gli operatori quali definiti nella direttiva (UE) 2016/1148. I sistemi europei di certificazione della cibersicurezza per questa categoria si basano sulle norme internazionali.***

Or. en

Motivazione

Per raggiungere gli obiettivi della proposta di regolamento e assicurare, in particolare, la sua adeguatezza alle esigenze future, gli obiettivi di sicurezza dovrebbero essere definiti sulla base delle applicazioni del prodotto e non delle sue funzionalità.

Emendamento 450
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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) ***per*** i ***prodotti corrispondenti al livello di certificazione elevato, i prodotti,*** servizi ***e processi TIC utilizzati dalla pubblica amministrazione di uno Stato membro. I sistemi europei di certificazione della cibersicurezza per questa categoria si basano sulle norme internazionali o sulle norme nazionali o multilaterali esistenti in uso negli Stati membri.***

Or. en

Motivazione

Per raggiungere gli obiettivi della proposta di regolamento e assicurare, in particolare, la sua adeguatezza alle esigenze future, gli obiettivi di sicurezza dovrebbero essere definiti sulla base delle applicazioni del prodotto e non delle sue funzionalità.

Emendamento 451
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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 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 ***e che sia predisposta una procedura per l'identificazione e la documentazione di tutte le dipendenze e le vulnerabilità presenti nei prodotti, nei processi e nei servizi TIC***;

Or. en

Motivazione

Deve esistere una procedura per l'identificazione delle vulnerabilità al fine di garantire la prevenzione degli incidenti.

Emendamento 452
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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;	***soppresso***

Or. en

Emendamento 453
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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 sfruttabili note*** e ***che resistano a un livello definito di attacco***;

Or. en

Motivazione

Dando seguito alla lettera precedente, una volta che una vulnerabilità è nota deve esistere una soluzione/patch efficace.

Emendamento 454
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

Proposta di regolamento
Articolo 45 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) 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;	***soppresso***

Or. en

Emendamento 455
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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;	***soppresso***

Or. en

Emendamento 456
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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.	***soppresso***

Or. en

Emendamento 457
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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 il software ***o l'hardware*** dei prodotti e dei servizi TIC sia aggiornato e non contenga vulnerabilità note***; accertarsi che essi siano stati progettati e attuati in modo da limitare efficacemente la loro suscettibilità alle vulnerabilità*** e che dispongano di

	meccanismi per effettuare aggiornamenti del software protetti***, compresi aggiornamenti automatici della sicurezza e la possibilità di aggiornare l'hardware***.

Or. en

Motivazione

Accertarsi dell'assenza di vulnerabilità note rappresenta un buon primo passo, ma un trattamento efficiente deve prevedere i mezzi per affrontare le vulnerabilità.

Emendamento 458
Gunnar Hökmark

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) ***agevolare l'aggiornamento del*** software ***e dell'hardware*** dei prodotti e dei servizi TIC***, la disponibilità di aggiornamenti adeguati e tempestivi per risolvere le*** vulnerabilità note e ***il fatto*** che tali prodotti e servizi dispongano di meccanismi per effettuare aggiornamenti del software ***e dell'hardware*** protetti.

Or. en

Emendamento 459
Pilar del Castillo Vera

Proposta di regolamento
Articolo 45 – comma 1 – lettera g – punto i (nuovo)

Testo della Commissione	*Emendamento*
	i) accertarsi che i prodotti e i servizi TIC siano sviluppati secondo i requisiti di sicurezza dello specifico sistema.

Or. en

Emendamento 460
Seán Kelly

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

Testo della Commissione	*Emendamento*
	(g bis) accertarsi che l'ambiente per i prodotti e servizi TIC sia diviso in sottosistemi e sottoreti più piccoli, per renderlo più gestibile ai fini della protezione e contenere i danni in caso di incidente.

Or. en

Emendamento 461
Eva Kaili, Peter Kouroumbashev

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

Testo della Commissione	*Emendamento*
	(g bis) accertarsi che l'ambiente per i prodotti e servizi TIC sia diviso in sottosistemi e sottoreti più piccoli, per renderlo più gestibile ai fini della protezione e contenere i danni in caso di incidente.

Or. en

Emendamento 462
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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

Testo della Commissione	*Emendamento*
	(g bis) accertarsi che i prodotti, processi, servizi e sistemi TIC siano sviluppati e

gestiti conformemente al principio della sicurezza fin dalla progettazione e per impostazione predefinita, nel rispetto degli obblighi definiti all'articolo -43.

Or. en

Emendamento 463
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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. ***Fatti salvi gli obblighi di sicurezza definiti all'articolo -43,*** i sistemi europei di certificazione della cibersicurezza possono specificare per i prodotti***, i processi,*** i servizi ***e i sistemi*** TIC rilasciati nel loro ambito uno o più dei seguenti livelli di affidabilità ***basati sui rischi***: ***funzionalmente sicuro, sostanzialmente e/o altamente sicuro***. ***Il livello di affidabilità si basa sull'elenco di controllo dei rischi e sulle corrispondenti funzionalità di cibersicurezza, identificate dall'ENISA ai sensi dell'articolo 44, paragrafo 2 e che sono disponibili nel prodotto, processo, servizio o sistema TIC a cui si applica il sistema di certificazione.***

Or. en

Emendamento 464
Nadine Morano

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 ***hardware e***	1. I sistemi europei di certificazione della cibersicurezza possono specificare***, a seconda del contesto e dell'uso previsto***

software TIC ***rilasciati nel loro ambito*** uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato.	***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. ***I metodi di valutazione della conformità che possono essere utilizzati devono essere specificati negli elementi di ciascun sistema europeo di certificazione della cibersicurezza, sulla base dell'analisi dei rischi***.

Or. fr

Motivazione

È preferibile che i metodi di valutazione della conformità utilizzabili non siano fissati a monte in modo generale, ma caso per caso e in funzione del tipo di prodotto o servizio, tenendo conto del contesto di utilizzo.

Emendamento 465
Clare Moody, Theresa Griffin, Peter Kouroumbashev, Arne Lietz

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 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. ***I sistemi di certificazione con diversi livelli di affidabilità sono accompagnati da informazioni che spiegano il rischio residuo corrispondente a ogni livello di affidabilità e l'esigenza per i consumatori di restare costantemente vigili e consapevoli delle minacce informatiche.***

Or. en

Motivazione

I consumatori corrono il rischio di credere che un prodotto o servizio TIC con livello di affidabilità elevato sia al riparo dalle minacce informatiche. I consumatori e le imprese dovrebbero restare costantemente vigili e consapevoli del fatto che persino prodotti o servizi

con un alto livello di affidabilità sono a rischio di incidenti informatici qualora non si seguano le migliori pratiche.

Emendamento 466
Françoise Grossetête

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 ***hardware e software*** 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, dei sistemi*** e ***dei*** servizi TIC***,*** uno o più dei seguenti livelli di affidabilità ***basati sui rischi***: di base, sostanziale e/o elevato.

Or. fr

Emendamento 467
Massimiliano Salini

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 468
Marisa Matias, Dan Nica, Miroslav Poche

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 ***specificano*** per i prodotti e i servizi TIC rilasciati nel loro ambito ***criteri di responsabilità per*** uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato.

Or. en

Emendamento 469
Michał Boni, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

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 uno o più ***requisiti*** di affidabilità ***sulla*** base ***dei rischi e delle minacce determinati dal contesto in cui dovrà operare il prodotto, il processo o il servizio***.

Or. en

Emendamento 470
Pilar del Castillo Vera

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 uno o più ***requisiti*** di affidabilità ***sulla*** base ***dei rischi e delle minacce determinati dal contesto in cui dovrà operare il prodotto, il processo o il servizio***.

Or. en

Emendamento 471
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

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 per i prodotti***,*** i servizi ***e i processi*** TIC rilasciati nel loro ambito uno o più dei seguenti livelli di affidabilità: di base, sostanziale e/o elevato.

Or. en

Motivazione

Per chiarire l'ambito di applicazione e garantire il corretto allineamento alle norme internazionali esistenti, il progetto di regolamento dovrebbe specificare che i futuri quadri di certificazione volontari si applicano ai "processi", oltre che ai "prodotti" e ai "servizi".

Emendamento 472
Evžen Tošenovský

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 per i prodotti e i servizi TIC rilasciati nel loro ambito uno o più dei seguenti livelli di affidabilità: di base, ***intermedio*** e/o elevato.

Or. en

Emendamento 473
Pilar del Castillo Vera

Proposta di regolamento
Articolo 46 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. L'ENISA identifica e sviluppa i livelli di affidabilità da specificare nei sistemi europei di certificazione della cibersicurezza in consultazione con i portatori di interessi.

Or. en

Emendamento 474
Françoise Grossetête

Proposta di regolamento
Articolo 46 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. I metodi di valutazione della conformità che possono essere utilizzati devono essere specificati negli elementi di ciascun sistema europeo di certificazione della cibersicurezza, conformemente all'articolo 47, sulla base dell'analisi dei rischi.

Or. fr

Motivazione

Per creare le condizioni necessarie a promuovere la fiducia legata al riconoscimento reciproco dei certificati e all'armonizzazione dei sistemi nazionali di certificazione, occorre una definizione comune di livelli di affidabilità, in particolare riguardo ai metodi di valutazione ad essi associati.

Emendamento 475
Pilar del Castillo Vera

Proposta di regolamento
Articolo 46 – paragrafo 2

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri:	***soppresso***
(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;	
(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;	
(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 incidenti di cibersicurezza.	

Or. en

Emendamento 476
Marisa Matias, Michał Boni, Gunnar Hökmark

Proposta di regolamento
Articolo 46 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità ***di base, sostanziale e elevato soddisfano i seguenti criteri:***	2. I livelli di affidabilità ***si riferiscono a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità corrispondente riguardo alle qualità di cibersicurezza pretese o dichiarate di un prodotto, di un processo e 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***; ***il livello di affidabilità è definito caso per caso.***

Or. en

Emendamento 477
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 46 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità ***di base, sostanziale*** e ***elevato*** soddisfano i seguenti criteri:	2. I livelli di affidabilità ***funzionalmente sicuro, sostanzialmente sicuro*** e ***altamente sicuro*** soddisfano ***rispettivamente*** i seguenti criteri:

Or. en

Emendamento 478
Edouard Martin

Proposta di regolamento
Articolo 46 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri:	2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri ***e metodi di valutazione***:

Or. fr

Emendamento 479
Françoise Grossetête

Proposta di regolamento
Articolo 46 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri:	2. I livelli di affidabilità di base, sostanziale e elevato soddisfano i seguenti criteri ***e il seguente metodo di valutazione***:

Or. fr

Emendamento 480
Evžen Tošenovský

Proposta di regolamento
Articolo 46 – paragrafo 2 – parte introduttiva

Testo della Commissione	*Emendamento*
2. I livelli di affidabilità di base, ***sostanziale*** e elevato soddisfano i seguenti criteri:	2. I livelli di affidabilità di base, ***intermedio*** e elevato soddisfano i seguenti criteri:

Or. en

Emendamento 481
Marisa Matias, Michał Boni, Gunnar Hökmark

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;	***soppresso***

Or. en

Emendamento 482
Edouard Martin

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 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; ***un certificato del livello di affidabilità di base attesta che i rischi informatici di base noti sono coperti. Il metodo di valutazione si basa sul riesame tecnico, da parte di un organismo di valutazione della conformità, della documentazione tecnica associata a un prodotto o servizio***

	nell'ambito delle tecnologie dell'informazione e della comunicazione;

Or. fr

Emendamento 483
Evžen Tošenovský

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 si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità limitato;

Or. en

Emendamento 484
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

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***	(a) il ***certificato del*** livello di affidabilità di base ***corrisponde alla valutazione effettuata da un soggetto terzo circa il fatto*** che ***i rischi di base di*** incidenti ***informatici per i processi, i prodotti o i servizi TIC sono coperti***;

tecniche e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre il rischio di incidenti ***di cibersicurezza***;

Or. en

Emendamento 485
Françoise Grossetête

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 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; ***il metodo di valutazione deve essere basato sul riesame tecnico, da parte di un organismo di valutazione della conformità, della documentazione tecnica associata a un prodotto o servizio nell'ambito delle tecnologie dell'informazione e della comunicazione;***

Or. fr

Emendamento 486
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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 ***"funzionalmente sicuro"*** si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità ***adeguato*** riguardo alle qualità di cibersicurezza pretese o dichiarate di un prodotto o di un servizio TIC ***in quanto corrisponde alla conformità degli obblighi di sicurezza di cui all'articolo [-43] secondo il principio della sicurezza fin dalla progettazione e per impostazione predefinita,*** 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;

Or. en

Emendamento 487
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

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 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 ***dispositivo elettronico di consumo*** ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche ***internazionali esistenti*** e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre il rischio di incidenti di cibersicurezza;

Or. en

Motivazione

Per creare un quadro di certificazione correttamente funzionante, è importante tenere conto dell'uso di norme esistenti e ampiamente adottate al momento della definizione dei livelli di affidabilità. Tali norme esistenti possono essere nazionali, internazionali (ISO 27XXX) o multilaterali (SOG-IS, criteri comuni).

Emendamento 488
Massimiliano Salini

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 ***rischio*** 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 in modo significativo 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

Emendamento 489
Eva Kaili, Peter Kouroumbashev

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***	(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 ***dispositivo destinato***

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;	***all'uso da parte dei consumatori*** ed è caratterizzato in riferimento a specifiche tecniche, norme tecniche ***internazionali esistenti*** e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre il rischio di incidenti di cibersicurezza;

Or. en

Emendamento 490
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	(a bis) tale valutazione comprende un riesame della documentazione tecnica del prodotto, servizio o processo TIC;

Or. en

Emendamento 491
Marisa Matias, Michał Boni, Gunnar Hökmark

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;	***soppresso***

Or. en

Emendamento 492
Edouard Martin

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 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; ***un certificato del livello di affidabilità sostanziale attesta che i rischi noti di incidenti informatici sono coperti e che il prodotto, servizio o sistema può resistere ad attacchi effettuati con risorse limitate. Il metodo di valutazione si basa sulla verifica, da parte di un organismo di valutazione della conformità, della conformità delle funzionalità di sicurezza del prodotto o servizio;***

Or. fr

Emendamento 493
Evžen Tošenovský

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	(b) il livello di affidabilità ***intermedio*** 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***;	nell'ambito di un sistema europeo di certificazione della cibersicurezza che offre un grado di attendibilità ***intermedio***;

Or. en

Emendamento 494
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

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 ***certificato del*** livello di affidabilità sostanziale ***corrisponde alla valutazione effettuata da un soggetto terzo circa il fatto*** che ***i rischi sostanziali*** di incidenti ***informatici per i processi, i prodotti o i servizi TIC sono coperti***;

Or. en

Emendamento 495
Françoise Grossetête

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 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; ***il metodo di valutazione deve essere basato sulla verifica, da parte di un organismo di valutazione della conformità, della conformità delle funzionalità di sicurezza del prodotto o servizio.***

Or. fr

Motivazione

Per quanto riguarda i certificati relativi al livello di affidabilità elevato, i prodotti e i sistemi devono poter dimostrare la loro resistenza agli attacchi, anche a quelli più sofisticati. Il metodo di valutazione associato alla certificazione deve pertanto prevedere test di efficacia, che garantiscano che il prodotto è in grado di resistere a un dato livello di attacco.

Emendamento 496
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

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	(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**,** di un servizio ***o di un processo*** TIC ed è

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;	caratterizzato in riferimento a specifiche tecniche, norme tecniche ***internazionali esistenti*** e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di ridurre in modo significativo il rischio di incidenti di cibersicurezza;

Or. en

Motivazione

Per creare un quadro di certificazione correttamente funzionante, è importante tenere conto dell'uso di norme esistenti e ampiamente adottate al momento della definizione dei livelli di affidabilità. Tali norme esistenti possono essere nazionali, internazionali (ISO 27XXX) o multilaterali (SOG-IS, criteri comuni).

Emendamento 497
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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 ***"sostanzialmente sicuro"*** 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;

Or. en

Emendamento 498
Massimiliano Salini

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 ***rischio*** sostanziale ***corrisponde a un rischio più elevato connesso a*** un prodotto***, processo e*** servizio TIC***. Un livello di rischio maggiore sussiste se un attacco contro il prodotto, il processo e il 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

Emendamento 499
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera b bis (nuova)

Testo della Commissione	*Emendamento*
	(b bis) tale valutazione comprende il riesame della documentazione tecnica e i test delle funzionalità di sicurezza attuate, conformemente ai requisiti stabiliti nella documentazione tecnica;

Or. en

Emendamento 500
Marisa Matias, Michał Boni, Gunnar Hökmark

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	***soppresso***

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 incidenti di cibersicurezza.

Or. en

Emendamento 501
Edouard Martin

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 incidenti di cibersicurezza.	(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 incidenti di cibersicurezza. ***Un certificato del livello di affidabilità elevato attesta che i rischi noti di incidenti informatici sono coperti e che il prodotto, servizio o sistema può resistere ad attacchi sofisticati effettuati con risorse significative. Il metodo di valutazione si basa su test di efficacia, al fine di valutare la resistenza delle funzionalità di sicurezza in caso di attacco di livello elevato.***

Or. fr

Emendamento 502
Evžen Tošenovský

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 incidenti di cibersicurezza***.	(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.

Or. en

Emendamento 503
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

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***	(c) ***la*** certificazione ***dell'***affidabilità ***corrisponde alla valutazione effettuata da un soggetto terzo circa il fatto che i rischi elevati di*** incidenti ***informatici per i processi, i prodotti o i servizi TIC sono coperti***.

correlate, compresi i controlli tecnici, il cui scopo è quello di prevenire gli incidenti ***di cibersicurezza***.

Or. en

Emendamento 504
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

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 incidenti di cibersicurezza.	(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 incidenti di cibersicurezza. ***La metodologia di valutazione dovrebbe essere basata almeno su un test di efficienza che valuti la resistenza delle funzionalità di sicurezza contro aggressori che dispongono di risorse da rilevanti a illimitate.***

Or. en

Motivazione

Dato che i fattori di rischio più elevati sono determinati dalla sensibilità del prodotto o servizio, ma anche dall'intensità dei potenziali attacchi, anche quest'ultimo fattore dovrebbe essere tenuto in considerazione.

Emendamento 505

Françoise Grossetête

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 incidenti di cibersicurezza.	(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 incidenti di cibersicurezza. ***Il metodo di valutazione deve essere basato su test di efficacia, al fine di valutare la resistenza delle funzionalità di sicurezza in caso di attacco di livello elevato.***

Or. fr

Emendamento 506
Massimiliano Salini

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***	(c) il livello di ***rischio*** 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***.

correlate, compresi i controlli tecnici, il cui scopo è quello di prevenire gli incidenti di cibersicurezza.

Or. en

Emendamento 507
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

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 incidenti di cibersicurezza.	(c) il livello di affidabilità elevato si riferisce a un certificato rilasciato nell'ambito di un sistema europeo di certificazione della cibersicurezza ***basato su una norma nazionale o multilaterale in uso,*** 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 ***nazionali, internazionali e multilaterali esistenti*** e procedure correlate, compresi i controlli tecnici, il cui scopo è quello di prevenire gli incidenti di cibersicurezza.

Or. en

Motivazione

Per creare un quadro di certificazione correttamente funzionante, è importante tenere conto dell'uso di norme esistenti e ampiamente adottate al momento della definizione dei livelli di affidabilità. Tali norme esistenti possono essere nazionali, internazionali (ISO 27XXX) o multilaterali (SOG-IS, criteri comuni).

Emendamento 508
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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 incidenti di cibersicurezza.	(c) il livello di affidabilità ***"altamente sicuro"*** 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 ***"sostanzialmente sicuro"*** 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 incidenti di cibersicurezza.

Or. en

Emendamento 509
Pavel Telička, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner

Proposta di regolamento
Articolo 46 – paragrafo 2 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) tale valutazione comprende il riesame della documentazione tecnica, i test delle funzionalità di sicurezza attuate, conformemente ai requisiti stabiliti nella documentazione tecnica, e la valutazione della resistenza dei processi, dei prodotti o dei servizi TIC contro aggressori competenti che dispongono di risorse da rilevanti a illimitate, attraverso un test di penetrazione.

Or. en

Emendamento 510
Evžen Tošenovský

Proposta di regolamento
Articolo 46 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. Ove necessario, la Commissione può adottare atti di esecuzione, conformemente all'articolo 55, paragrafo 2, tenuto conto del parere dell'ENISA, del gruppo europeo per la certificazione della cibersicurezza e delle piattaforme di consultazione dei portatori di interessi, che prevedano requisiti quadro dettagliati per ogni livello di affidabilità.

Or. en

Emendamento 511
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill

Proposta di regolamento
Articolo 46 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. La metodologia che distingue tra i diversi livelli di affidabilità deve essere basata almeno su un test che valuti la resistenza delle funzionalità di sicurezza contro aggressori che dispongono di risorse da rilevanti a illimitate.

Or. en

Emendamento 512
Peter Kouroumbashev, Zigmantas Balčytis, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 46 bis (nuovo)

Testo della Commissione	*Emendamento*

Articolo 46 bis

Secondo l'analisi del rischio specifico, il metodo di valutazione idoneo della conformità, compresa l'autovalutazione, è identificato secondo le modalità di cui all'articolo 4 e all'allegato II della decisione n. 768/2008/CE;

Or. en

Motivazione

Per garantire un approccio flessibile, pragmatico e orientato al mercato riguardo alla certificazione della cibersicurezza, dovrebbe essere consentito l'uso anche di quadri e/o pratiche ampiamente adottati.

Emendamento 513
Nadine Morano

Proposta di regolamento
Articolo 46 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 46 bis
	Sulla base di un'analisi dei rischi, occorre identificare il metodo adatto di valutazione della conformità, conformemente all'articolo 47, all'articolo 4 e all'allegato II della decisione n. 768/2008/CE.

Or. fr

Motivazione

Limitare l'utilizzo di un metodo di valutazione della conformità, come l'autovalutazione, a un solo livello, senza tenere conto del prodotto interessato o del suo contesto di utilizzo, ostacola la necessaria flessibilità, che sarebbe invece utile conservare in questo ambito.

Emendamento 514
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

Proposta di regolamento

Articolo 46 ter (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 46 ter
	Fatti salvi i paragrafi 1 e 2, l'ENISA può sostituire i requisiti per il livello di affidabilità di base introducendo al loro posto un sistema informativo sulle funzionalità, come definito all'articolo 2. I criteri di tale sistema informativo sulle funzionalità sono definiti in anticipo con la partecipazione del gruppo di certificazione dei portatori di interessi.

Or. en

Motivazione

Riguardo ai livelli di affidabilità definiti nella proposta di regolamento, l'introduzione dei sistemi informativi sulle funzionalità tecniche dovrebbe essere una possibile alternativa ai livelli di affidabilità di base per i prodotti destinati ai consumatori.

Emendamento 515
Martina Werner

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;

Or. en

Emendamento 516
Pilar del Castillo Vera

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;

Or. en

Emendamento 517
Michał Boni, Massimiliano Salini, Gunnar Hökmark

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

Testo della Commissione	*Emendamento*
	(a bis) gli organismi di valutazione della conformità e di audit;

Or. en

Emendamento 518
Pilar del Castillo Vera

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(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;	(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; ***i requisiti in materia di certificazione devono essere definiti in modo tale che la certificazione possa essere integrata nei processi di sicurezza sistematici del produttore seguiti durante lo sviluppo e il ciclo di vita del prodotto o servizio in questione o basata su di essi;***

Or. en

Emendamento 519
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(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;	(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 ***e/***o a specifiche tecniche dell'Unione o internazionali***. Le norme internazionali già esistenti devono essere tenute in considerazione***;

Or. en

Emendamento 520
Olle Ludvigsson

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(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***;	(b) l'indicazione dettagliata dei requisiti di cibersicurezza rispetto ai quali i prodotti e servizi TIC sono valutati, in riferimento a norme tecniche o a specifiche tecniche***, conformemente all'articolo 2, punto 1, del regolamento (UE) n. 1025/2012***;

Or. en

Emendamento 521
Martina Werner

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(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;	(b) l'indicazione dettagliata dei requisiti 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 522
Csaba Molnár

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b

Testo della Commissione	*Emendamento*
(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;	(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 ***europee*** o internazionali;

Or. en

Emendamento 523
Pilar del Castillo Vera

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera b – punto i (nuovo)

Testo della Commissione	*Emendamento*
	i) la promozione, ove opportuno, della "sicurezza fin dalla progettazione";

Or. en

Emendamento 524
Marisa Matias, Dan Nica, Miroslav Poche

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
(c) ***se del caso,*** uno o più livelli di affidabilità;	(c) uno o più livelli di affidabilità ***circa la responsabilità dell'organismo di valutazione della conformità in caso di violazione di prodotti o servizi TIC certificati***;

Or. en

Emendamento 525
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera c

Testo della Commissione	*Emendamento*
(c) se del caso, uno o più livelli di affidabilità;	(c) se del caso, uno o più livelli di affidabilità ***che tengano conto, tra l'altro, di un approccio basato sul rischio***;

Or. en

Emendamento 526
Olle Ludvigsson

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera d

Testo della Commissione	*Emendamento*
(d) i criteri e i metodi di valutazione specifici utilizzati, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti;	(d) i criteri e i metodi di valutazione specifici utilizzati, compresi i tipi di valutazione, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti ***in riferimento a norme tecniche o a specifiche tecniche, conformemente all'articolo 2, punto 1, del regolamento (UE) n. 1025/2012***;

Or. en

Emendamento 527
Massimiliano Salini

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera d

Testo della Commissione	*Emendamento*
(d) i criteri e i metodi di valutazione specifici utilizzati, ***compresi i tipi di valutazione***, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti;	(d) ***i tipi di valutazione della conformità e*** i criteri e i metodi di valutazione specifici utilizzati, ***come stabiliti nell'articolo 4 e nell'allegato II della decisione n. 768/2008/CE***, al fine di dimostrare che gli obiettivi specifici di cui all'articolo 45 sono stati conseguiti;

Or. en

Emendamento 528
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera f

Testo della Commissione	*Emendamento*
(f) le condizioni alle quali possono essere utilizzati gli eventuali ***marchi o etichette*** previsti dal sistema;	(f) le condizioni alle quali possono essere utilizzati gli eventuali ***sistemi informativi sulle funzionalità tecniche*** previsti dal sistema;

Or. en

Emendamento 529
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera g

Testo della Commissione	*Emendamento*

(g) ***se la vigilanza rientra nel sistema,*** le norme per il controllo della conformità dei certificati ai requisiti, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;	(g) le norme per il controllo della conformità dei certificati ai requisiti, compresi i meccanismi per dimostrare il mantenimento della conformità ai requisiti di cibersicurezza specificati;

Or. en

Emendamento 530
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

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

Testo della Commissione	*Emendamento*
	(g bis) le condizioni per il rilascio, il mantenimento, la prosecuzione e l'estensione della certificazione e la riduzione del suo campo di applicazione;

Or. en

Emendamento 531
Pilar del Castillo Vera

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera h

Testo della Commissione	*Emendamento*
(h) le condizioni per il rilascio, il mantenimento, la prosecuzione e l'estensione della certificazione e la riduzione del suo campo di applicazione;	(h) le condizioni per il rilascio, il mantenimento, la prosecuzione***, il rinnovo*** e l'estensione della certificazione e la riduzione del suo campo di applicazione;

Or. en

Emendamento 532
Massimiliano Salini

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

Testo della Commissione	*Emendamento*
	(h bis) le regole per trattare le vulnerabilità che possono emergere dopo l'emissione della certificazione, attraverso la definizione di un processo organizzativo dinamico e continuo che coinvolga sia i fornitori sia gli utenti;

Or. en

Emendamento 533
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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

Testo della Commissione	*Emendamento*
	(i bis) le regole che impongono le modalità e le tempistiche secondo le quali le autorità competenti devono segnalare ai pertinenti fornitori e fabbricanti le vulnerabilità nei prodotti, processi, servizi e sistemi TIC che non sono pubblicamente note, secondo un processo coordinato di divulgazione delle vulnerabilità;

Or. en

Emendamento 534
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera j

Testo della Commissione	*Emendamento*
(j) le regole ***riguardanti il modo in cui segnalare e trattare*** le vulnerabilità ***della***	(j) le regole ***che impongono che le autorità competenti segnalino***

cibersicurezza nei prodotti e servizi TIC ***precedentemente non rilevate***;	***immediatamente ai pertinenti fornitori e fabbricanti*** le vulnerabilità nei prodotti e servizi TIC ***che non sono pubblicamente note, secondo un processo coordinato di divulgazione delle vulnerabilità***;

Or. en

Motivazione

Tali autorità legate allo Stato (come le CERT nazionali) dovrebbero condividere le informazioni sulle vulnerabilità di tutti i prodotti e servizi TIC con i fornitori e fabbricanti interessati. Tale compito dovrebbe essere svolto conformemente alle raccomandazioni e agli orientamenti definiti nelle norme internazionali ISO/IEC 29147:2014 e ISO/IEC 30111. Le autorità statali che svolgono il compito di individuare le vulnerabilità hanno profili di rischio, incentivi, obblighi e competenze molto diversi nei confronti dei fornitori e fabbricanti rispetto ai singoli ricercatori nell'ambito della sicurezza.

Emendamento 535
Michał Boni, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera l

Testo della Commissione	*Emendamento*
(l) l'individuazione dei sistemi nazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti e servizi TIC;	(l) ***ove applicabile,*** l'individuazione dei sistemi nazionali di certificazione della cibersicurezza***, a norma dell'articolo 49, o di iniziative guidate dall'industria*** relativi allo stesso tipo o alle stesse categorie di prodotti***, processi*** e servizi TIC;

Or. en

Emendamento 536
Pilar del Castillo Vera

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera l

Testo della Commissione	*Emendamento*
(l) l'individuazione dei sistemi nazionali di certificazione della	(l) l'individuazione dei sistemi nazionali ***o internazionali*** di certificazione della cibersicurezza relativi allo stesso tipo

cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti e servizi TIC;	o alle stesse categorie di prodotti e servizi TIC***, requisiti di sicurezza e criteri e metodi di valutazione***;

Or. en

Emendamento 537
Pilar del Castillo Vera

Proposta di regolamento
Articolo 47 – paragrafo 1 – lettera l

Testo della Commissione	*Emendamento*
(l) l'individuazione dei sistemi nazionali di certificazione della cibersicurezza relativi allo stesso tipo o alle stesse categorie di prodotti e servizi TIC;	(l) l'individuazione dei sistemi nazionali ***o internazionali*** di certificazione della cibersicurezza ***o di iniziative guidate dall'industria*** relativi allo stesso tipo o alle stesse categorie di prodotti***, processi*** e servizi TIC;

Or. en

Emendamento 538
Pilar del Castillo Vera

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

Testo della Commissione	*Emendamento*
	(l bis) ove applicabile, il periodo di validità del certificato;

Or. en

Emendamento 539
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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

Testo della Commissione	*Emendamento*
	(m bis) le regole relative alle modalità e alle tempistiche secondo cui gli Stati membri devono informarsi reciprocamente e informare i fornitori e i fabbricanti interessati qualora vengano a conoscenza di una vulnerabilità non pubblicamente nota di un prodotto o servizio TIC certificato nel quadro del presente sistema di certificazione.

Or. en

Emendamento 540
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Fredrick Federley, Dita Charanzová, Neena Gill, Morten Løkkegaard

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

Testo della Commissione	*Emendamento*
	(m bis) le regole relative alle modalità e alle tempistiche secondo cui gli Stati membri devono informarsi reciprocamente qualora vengano a conoscenza di una vulnerabilità non pubblicamente nota di un prodotto o servizio TIC certificato nel quadro del presente sistema di certificazione.

Or. en

Emendamento 541
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

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

Testo della Commissione	*Emendamento*

(m bis) i tipi di valutazione di conformità nonché i criteri e i metodi di valutazione di cui all'articolo 4 e all'allegato II della decisione 768/2008/CE.

Or. en

Emendamento 542
Clare Moody, Theresa Griffin, Peter Kouroumbashev, Arne Lietz

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

Testo della Commissione	*Emendamento*
	(m bis) ulteriori orientamenti sulle migliori pratiche in materia di cibersicurezza e informazioni sulle minacce informatiche rimaste nonostante la certificazione.

Or. en

Motivazione

Nessun prodotto o servizio TIC è del tutto sicuro. Per evitare un atteggiamento condiscendente da parte dei consumatori o di altre organizzazioni, i sistemi di certificazione dovrebbero sottolineare l'esigenza costante di restare vigili e di rispettare le buone pratiche in materia di cibersicurezza.

Emendamento 543
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

Proposta di regolamento
Articolo 47 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Per i sistemi pertinenti, il gruppo di certificazione dei portatori di interessi o il gruppo europeo per la certificazione della cibersicurezza deve approvare, a seguito di una richiesta debitamente motivata dell'ENISA, qualsiasi proposta di aggiunta, scostamento o mancato

affidamento alle norme internazionali o dell'Unione di cui al paragrafo 1, lettera b), almeno due settimane prima della trasmissione della proposta di sistema alla Commissione a norma dell'articolo 44, paragrafo 3.

Or. en

Motivazione

I prodotti TIC che sono sviluppati, commercializzati o utilizzati nei mercati globali ed europei si affidano largamente alle norme esistenti e ampiamente adottate. Lo scostamento o il mancato ricorso a tali norme deve essere debitamente motivato.

Emendamento 544
Massimiliano Salini

Proposta di regolamento
Articolo 47 – paragrafo 3

Testo della Commissione	*Emendamento*
3. ***Se*** un atto specifico dell'Unione ***lo prevede,*** la certificazione nell'ambito di un sistema europeo di certificazione della cibersicurezza può essere utilizzata ***per dimostrare la presunzione di conformità agli obblighi imposti da tale atto***.	3. Un atto specifico dell'Unione ***può suggerire quando*** la certificazione nell'ambito di un sistema europeo di certificazione della cibersicurezza può essere utilizzata.

Or. en

Emendamento 545
Massimiliano Salini

Proposta di regolamento
Articolo 47 – paragrafo 4

Testo della Commissione	*Emendamento*
4. In assenza di una normativa armonizzata dell'Unione, anche la legislazione degli Stati membri può ***disporre che*** un sistema europeo di certificazione della cibersicurezza ***può essere utilizzato per stabilire la***	4. In assenza di una normativa armonizzata dell'Unione, anche la legislazione degli Stati membri può ***incoraggiare l'utilizzo di*** un sistema

presunzione di conformità agli obblighi di legge.	europeo di certificazione della cibersicurezza.

Or. en

Emendamento 546
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner

Proposta di regolamento
Articolo 47 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. I sistemi di certificazione possono essere creati, in particolare, per i gruppi di prodotti menzionati all'allegato I del presente regolamento.

Or. en

Emendamento 547
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 47 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 47 bis
	I sistemi creati a norma del presente regolamento non richiedono la comunicazione di modifiche, variazioni delle certificazioni o ricertificazioni, a meno che tali modifiche non abbiano effetti negativi sostanziali sulla sicurezza dei prodotti, servizi e processi TIC nonché sui dispositivi elettronici di consumo.

Or. en

Motivazione

I prodotti non sono soggetti a ricertificazione in seguito a patch/aggiornamenti software oppure per una modifica nella funzionalità del prodotto, a condizione che tali azioni non

abbiano effetti negativi sostanziali sulla sicurezza del dispositivo. L'introduzione di questo riferimento è essenziale per le imprese, in quanto gli effetti negativi della ricertificazione possono permanere per un periodo di tempo superiore all'effettivo "ciclo di vita" di un aggiornamento software, con conseguenti ripercussioni negative, in ultima istanza, sulla capacità degli utenti finali e degli operatori di migliorare le proprie capacità di cibersicurezza.

Emendamento 548
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 48 – paragrafo 1

Testo della Commissione	*Emendamento*
1. I prodotti ***e*** i servizi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.	1. I prodotti***,*** i servizi ***e i processi*** TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.

Or. en

Emendamento 549
Pilar del Castillo Vera

Proposta di regolamento
Articolo 48 – paragrafo 1

Testo della Commissione	*Emendamento*
1. I prodotti e i servizi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.	1. I prodotti***, i processi*** e i servizi TIC certificati ricorrendo a un sistema europeo di certificazione della cibersicurezza adottato a norma dell'articolo 44 sono considerati conformi ai requisiti di tale sistema.

Or. en

Emendamento 550

Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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 è obbligatoria almeno per:***
	(a) i prodotti, processi, servizi e sistemi TIC utilizzati da operatori di servizi essenziali quali definiti nella direttiva 2016/1148/UE;
	(b) i prodotti, processi, servizi e sistemi TIC destinati ai minori e a un uso domestico;
	(c) i prodotti, processi, servizi e sistemi TIC destinati a un uso medico;
	(d) i prodotti, processi, servizi e sistemi TIC utilizzati a fini di sicurezza;
	(e) i veicoli a guida autonoma.
	La Commissione può riesaminare le categorie di prodotti di cui al paragrafo 1 mediante atti di esecuzione e in cooperazione con l'ENISA.
	La certificazione è volontaria ***per tutti gli altri prodotti,*** salvo diversamente specificato nel diritto dell'Unione.

Or. en

Emendamento 551
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Clare Moody

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 è volontaria ***per i prodotti, servizi e processi TIC che rientrano nell'ambito di applicazione***

dell'articolo 45, paragrafo 1, lettere a) e b), salvo diversamente specificato nel diritto dell'Unione***, ed è obbligatoria per i prodotti, servizi e processi TIC che rientrano nell'ambito di applicazione dell'articolo 45, paragrafo 1, lettera c), salvo diversamente specificato nel diritto dell'Unione o dal gruppo europeo per la certificazione della cibersicurezza***.

Or. en

Motivazione

La distinzione tra sistemi di certificazione volontari e obbligatori è necessaria poiché gli obiettivi di sicurezza sono diversi per le due categorie di prodotti e processi TIC comprese nel presente regolamento. Nel caso della protezione di infrastrutture e informazioni governative, la certificazione è obbligatoria in quanto contribuisce a rafforzare la ciberresilienza degli Stati membri. Tale approccio, inoltre, favorirà una maggiore armonizzazione degli obblighi degli Stati membri quali definiti dalla direttiva (UE) 2016/1148.

Emendamento 552
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

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 medio ed elevato è obbligatoria. Per i livelli di affidabilità di base e sostanziale essa*** è volontaria***, ma il fabbricante deve essere obbligato a rispettare le norme di sicurezza minime***, salvo diversamente specificato nel diritto dell'Unione.

Or. en

Emendamento 553
Evžen Tošenovský

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 è ***rigorosamente*** volontaria ***e fa salve l'autovalutazione/autodichiarazione volontaria di conformità***.

Or. en

Emendamento 554
Rolandas Paksas

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 è ***obbligatoria***.

Or. en

Emendamento 555
András Gyürk

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 è volontaria, salvo diversamente specificato nel diritto ***nazionale***.

Or. en

Emendamento 556
Martina Werner

Proposta di regolamento
Articolo 48 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. 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.

Or. en

Emendamento 557
Edouard Martin

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 ***di livello di base o sostanziale*** 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.

Or. fr

Emendamento 558
Martina Werner

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	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 certificazione della cibersicurezza, adottato a norma dell'articolo 44.	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 559
Edouard Martin

Proposta di regolamento
Articolo 48 – paragrafo 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	3 bis. Un certificato europeo della cibersicurezza di livello elevato è rilasciato dalle autorità nazionali di controllo della certificazione di cui all'articolo 50 sulla base dei criteri previsti dal sistema europeo di certificazione della cibersicurezza, adottato a norma dell'articolo 44.

Or. fr

Emendamento 560
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 48 – paragrafo 4 – parte introduttiva

Testo della Commissione	*Emendamento*
4. In deroga al paragrafo 3***,*** in casi debitamente giustificati un determinato sistema europeo della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è ***uno dei seguenti:***	4. In deroga al paragrafo 3 ***e solo*** in casi debitamente giustificati un determinato sistema europeo della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è ***accreditato come organismo di valutazione della conformità a norma dell'articolo 51, paragrafo 1. La persona***

fisica o giuridica che presenta i suoi prodotti o servizi TIC al meccanismo di certificazione mette a disposizione dell'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.

Or. en

Motivazione

Chiarimento.

Emendamento 561
Françoise Grossetête

Proposta di regolamento
Articolo 48 – paragrafo 4 – parte introduttiva

Testo della Commissione	*Emendamento*
4. In deroga al paragrafo 3, in casi debitamente giustificati un determinato sistema europeo della cibersicurezza ***può*** prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è uno dei seguenti:	4. In deroga al paragrafo 3, in casi debitamente giustificati, ***come il livello di affidabilità elevato quale descritto all'articolo 46, lettera c),*** un determinato sistema europeo della cibersicurezza ***deve*** prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico ***competente in seguito a una valutazione effettuata da un organismo di valutazione della conformità indipendente e notificato***. Detto ente pubblico è uno dei seguenti:

Or. fr

Emendamento 562
Olle Ludvigsson

Proposta di regolamento
Articolo 48 – paragrafo 4 – parte introduttiva

Testo della Commissione	*Emendamento*

4. In deroga al paragrafo 3**,** in casi debitamente giustificati un determinato sistema europeo della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è ***uno dei seguenti:***	4. In deroga al paragrafo 3 ***e solo*** in casi debitamente giustificati un determinato sistema europeo della cibersicurezza può prevedere che un certificato europeo della cibersicurezza derivante da tale sistema possa essere rilasciato da un ente pubblico. Detto ente pubblico è ***accreditato come organismo di valutazione della conformità a norma dell'articolo 51, paragrafo 1.***

Or. en

Emendamento 563
Olle Ludvigsson

Proposta di regolamento
Articolo 48 – paragrafo 4 – lettera a

Testo della Commissione	*Emendamento*
(a) un'autorità nazionale di controllo della certificazione ai sensi dell'articolo 50, paragrafo 1;	***soppresso***

Or. en

Emendamento 564
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 48 – paragrafo 4 – lettera a

Testo della Commissione	*Emendamento*
(a) un'autorità nazionale di controllo della certificazione ai sensi dell'articolo 50, paragrafo 1;	***soppresso***

Or. en

Motivazione

Necessario per motivi di coerenza giuridica con le modifiche all'articolo 48, paragrafo 1.

Emendamento 565
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 48 – paragrafo 4 – lettera b

Testo della Commissione	*Emendamento*
(b) un organismo accreditato come organismo di valutazione della conformità a norma dell'articolo 51, paragrafo 1, o	***soppresso***

Or. en

Motivazione

Necessario per motivi di coerenza giuridica con le modifiche all'articolo 48, paragrafo 1.

Emendamento 566
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 48 – paragrafo 4 – lettera c

Testo della Commissione	*Emendamento*
(c) un organismo istituito in virtù di leggi, disposizioni legali o altre procedure amministrative dello Stato membro interessato che soddisfa i requisiti previsti per gli organismi che certificano prodotti, processi e servizi secondo la norma ISO/IEC 17065: 2012.	***soppresso***

Or. en

Motivazione

Necessario per motivi di coerenza giuridica con le modifiche all'articolo 48, paragrafo 1.

Emendamento 567

Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Clare Moody

Proposta di regolamento
Articolo 48 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La persona fisica o giuridica che presenta i suoi prodotti ***o*** servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.	5. La persona fisica o giuridica che presenta i suoi prodotti***,*** servizi ***o processi*** TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione. ***La presentazione può essere fatta a qualsiasi organismo di valutazione della conformità di cui all'articolo 51.***

Or. en

Motivazione

Per evitare la frammentazione dei meccanismi di riconoscimento e/o conformità dei sistemi europei per la certificazione della cibersicurezza, l'articolo deve sottolineare che la presentazione può essere fatta a qualsiasi organismo di valutazione della conformità accreditato da uno Stato membro dell'UE.

Emendamento 568
Pilar del Castillo Vera

Proposta di regolamento
Articolo 48 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La persona fisica o giuridica che presenta i suoi prodotti o servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.	5. La persona fisica o giuridica che presenta i suoi prodotti***, processi*** o servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.

Or. en

Emendamento 569
Michał Boni, Seán Kelly, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 48 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La persona fisica o giuridica che presenta i suoi prodotti o servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.	5. La persona fisica o giuridica che presenta i suoi prodotti***, processi*** o servizi TIC al meccanismo di certificazione fornisce all'organismo di valutazione della conformità di cui all'articolo 51 tutte le informazioni necessarie a espletare la procedura di certificazione.

Or. en

Emendamento 570
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

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 ***minimo*** di tre anni***. Essi*** possono essere rinnovati***,*** alle stesse condizioni***,*** purché ***prorogati per ulteriori periodi senza alcun costo, previa attestazione da parte del titolare del certificato del fatto che continuano*** a essere soddisfatti i requisiti pertinenti. ***Tale attestazione deve essere fornita non prima di sei mesi e al più tardi 15 giorni prima della scadenza del periodo pertinente. Le proroghe dei certificati sono consentite per la durata dell'intero ciclo di vita del prodotto certificato.***

Or. en

Motivazione

In order to ensure market flexibility and predictability, the framework should define a minim duration of a certificate. The maximum duration of a certificate, if applicable, shall be defined on a case-by-case basis depending on the expected lifespan of the certified category of products or services. In addition, the extension of a certificate should be allowed with no extra cost, upon attestation of the certificate holder that the requirements will continue to be met. This will help contributing to a fairer Single Market as it will avoid the risk of repercussion of the extra cost incurred by re-certification to end-users.

Emendamento 571
Massimiliano Salini

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 ***il*** periodo ***definito in ciascun sistema di certificazione e sono fortemente correlati ai processi e alla capacità degli enti di organizzarsi per reagire a un attacco*** e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.

Or. en

Emendamento 572
Pilar del Castillo Vera

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 di tre anni ***definito dallo specifico sistema di certificazione*** e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.

Or. en

Emendamento 573
Michał Boni, Massimiliano Salini, Gunnar Hökmark

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 ***di tempo definito caso per caso per ciascun sistema*** e possono essere rinnovati alle stesse condizioni purché continuino a essere soddisfatti i requisiti pertinenti.

Or. en

Emendamento 574
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 48 – paragrafo 7

Testo della Commissione	*Emendamento*
7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.	7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri ***in quanto conformi ai requisiti locali in materia di cibersicurezza riguardo ai prodotti e processi TIC e ai dispositivi elettronici di consumo coperti da tale certificato, tenuto conto del livello di affidabilità specificato all'articolo 46, e non deve sussistere alcuna discriminazione tra detti certificati sulla base del fatto che siano emessi dallo Stato membro di origine o da un organismo di valutazione della conformità di cui all'articolo 51***.

Or. en

Motivazione

Per evitare la frammentazione dei meccanismi di riconoscimento e/o conformità dei sistemi europei per la certificazione della cibersicurezza, l'articolo deve sottolineare che non vi può essere discriminazione in base al luogo di emissione di un certificato.

Emendamento 575
Françoise Grossetête

Proposta di regolamento
Articolo 48 – paragrafo 7

Testo della Commissione	*Emendamento*
7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri.	7. I certificati europei della cibersicurezza rilasciati a norma del presente articolo sono riconosciuti in tutti gli Stati membri. ***Per il livello di affidabilità elevato, i certificati possono essere oggetto di reciproco riconoscimento solo se rilasciati da un organismo pubblicato quale descritto all'articolo 48, paragrafo 4, lettera a).***

Or. fr

Emendamento 576
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 48 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. La domanda di certificazione deve essere completata entro 12 mesi dalla data di presentazione, in caso contrario l'organismo di valutazione della conformità perderà il suo accreditamento.

Or. en

Motivazione

Gli organismi di valutazione della conformità elaborano tempestivamente le domande di certificazione.

Emendamento 577
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 48 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 48 bis
	Requisiti di base in materia di sicurezza informatica
	1. L'Agenzia, entro ... [due anni dalla data di entrata in vigore del presente regolamento] propone alla Commissione chiari requisiti obbligatori di base in materia di sicurezza informatica applicabili a tutti i dispositivi informatici venduti nell'Unione o esportati dalla stessa, con i quali si disponga ad esempio che:
	(a) il fabbricante rilasci una certificazione scritta attestante che il dispositivo non contiene alcun componente hardware, software o firmware con vulnerabilità note in materia di sicurezza;
	(b) il dispositivo si basi su componenti software o firmware in grado di accogliere aggiornamenti opportunamente autenticati e affidabili rilasciati dal fornitore;
	(c) le capacità documentate di accesso a distanza del dispositivo siano protette dall'accesso non autorizzato al più tardi durante l'installazione; non vi siano password standardizzate predefinite a codifica fissa per tutti i dispositivi e vi sia una possibilità documentata di aggiornamenti che indichi chiaramente le

responsabilità nel caso in cui l'utente non aggiorni il dispositivo;

(d) il fabbricante di un dispositivo connesso a Internet o di un componente software o firmware sia tenuto a notificare all'autorità competente qualsiasi vulnerabilità nota in materia di sicurezza;

(e) il fabbricante di un dispositivo connesso a Internet o di un componente software o firmware sia tenuto a provvedere alla riparazione nel caso in cui vengano scoperte nuove vulnerabilità in materia di sicurezza;

(f) il fabbricante di un dispositivo connesso a Internet o di un componente software o firmware sia tenuto a fornire informazioni sulla modalità con cui il dispositivo riceve gli aggiornamenti e sul calendario previsto per la cessazione dell'assistenza in materia di sicurezza e sia tenuto a inviare una notifica al momento della cessazione di tale sevizio di assistenza di sicurezza;

(g) il fabbricante sia tenuto a comunicare il codice sorgente e la documentazione una volta cessata l'assistenza.

2. L'Agenzia riesamina e, ove necessario, modifica i requisiti di cui al paragrafo 1 ogni due anni e presenta le eventuali modifiche sotto forma di proposte alla Commissione.

3. La Commissione può decidere, mediante atti di esecuzione, che i requisiti proposti o modificati di cui ai paragrafi 1 e 2 abbiano validità generale nell'Unione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 55, paragrafo 2.

4. La Commissione provvede a un'appropriata divulgazione dei requisiti per i quali è stata decisa la validità generale ai sensi del paragrafo 3.

5. L'Agenzia raccoglie in un registro tutti i requisiti proposti e le relative modifiche

e li rende pubblici mediante mezzi appropriati.

6. Se sta ai fabbricanti garantire la conformità di un prodotto o servizio TIC, gli importatori invece devono assicurarsi che i prodotti che immettono sul mercato rispettino i requisiti applicabili e non presentino un rischio per il pubblico europeo. L'importatore deve verificare che il fabbricante al di fuori dell'UE abbia adottato le misure necessarie e che il prodotto o il servizio sia conforme alle disposizioni del paragrafo 1. I distributori di prodotti o servizi TIC devono disporre di una conoscenza di base dei requisiti giuridici e della documentazione di accompagnamento. Essi devono poter identificare i prodotti che chiaramente non sono conformi e devono dimostrare alle autorità nazionali che hanno agito con la dovuta diligenza e che hanno ricevuto conferma dal produttore o dall'importatore del fatto che sono state adottate le misure necessarie. Inoltre, un distributore deve essere in grado di assistere le autorità nazionali negli sforzi che intraprendono per ricevere la documentazione richiesta.

7. In casi stabiliti nel sistema, in base alla natura, al ciclo di vita o al costo del prodotto, quale alternativa al processo di certificazione completo, la conformità ai requisiti obbligatori di base in materia di sicurezza informatica potrebbe essere garantita tramite un'autodichiarazione di conformità che segua la procedura applicabile per la valutazione della conformità.

Or. en

Motivazione

È importante conseguire un ambiente informatico resiliente per contrastare la criminalità informatica e tutelare i diritti fondamentali degli utenti delle tecnologie dell'informazione. È pertanto opportuno che il regolamento in esame fissi obiettivi ambiziosi a favore di parametri di riferimento obbligatori in materia di sicurezza informatica nell'Unione. Dato che la natura, il ciclo di vita o il costo del prodotto potrebbero rendere impossibile il processo di

certificazione, un'autocertificazione potrebbe offrire una via più rapida per entrare nel mercato e una tutela per le autorità e i consumatori.

Emendamento 578
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 48 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 48 bis
	Compatibilità con i sistemi internazionali di reciproco riconoscimento
	1. Nella fase preparatoria di una proposta di sistema europeo di certificazione della cibersicurezza, l'ENISA e, ove opportuno, il gruppo di certificazione dei portatori di interessi o il gruppo europeo per la certificazione della cibersicurezza valutano la pertinenza degli accordi internazionali di reciproco riconoscimento e delle certificazioni esistenti.
	2. Si deve altresì valutare se i sistemi nazionali di certificazione della cibersicurezza coperti dalla proposta di sistema sono oggetto di un accordo internazionale di reciproco riconoscimento.
	3. Qualora si accerti l'esistenza di accordi e certificazioni internazionali di reciproco riconoscimento pertinenti, l'ENISA mira a garantire la compatibilità:
	(a) basando la certificazione sulle stesse norme tecniche;
	(b) allineando l'ambito di applicazione, gli obiettivi di sicurezza, la metodologia di valutazione e i livelli di affidabilità;
	(c) avviando un dialogo con l'organo di governance equivalente ai fini dell'obiettivo di cui alle lettere a) e b).

Or. en

Motivazione

L'ambizione del regolamento è razionalizzare gli attuali sistemi di certificazione e garantirne l'ampia applicabilità in tutta l'UE. In linea con questa ambizione, il quadro di certificazione dovrebbe evitare di sostituire gli accordi internazionali di reciproco riconoscimento e cercare di sviluppare certificazioni che coprano il medesimo ambito o forniscano un ecosistema più ampio nell'ambito del quale le sensibilità europee possano essere più ampiamente riconosciute ed esportate.

Emendamento 579
Michał Boni, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

Proposta di regolamento
Articolo 49 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.	1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti***, i processi*** e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti***, processi*** e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere. ***I processi di manutenzione con aggiornamenti minori non invalidano la certificazione.***

Or. en

Emendamento 580
Pilar del Castillo Vera

Proposta di regolamento
Articolo 49 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.	1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti***, i processi*** e i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto di esecuzione adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti***, processi*** e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.

Or. en

Emendamento 581
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 49 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti ***e*** i servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto ***di esecuzione*** adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.	1. Fatto salvo il paragrafo 3, i sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti***,*** i servizi ***e i processi*** TIC coperti da un sistema europeo di certificazione della cibersicurezza cessano di produrre effetti a decorrere dalla data stabilita nell'atto ***delegato*** adottato a norma dell'articolo 44, paragrafo 4. I sistemi nazionali di certificazione della cibersicurezza e le procedure correlate per i prodotti e servizi TIC non coperti da un sistema europeo di certificazione della cibersicurezza continuano ad esistere.

Or. en

Motivazione

Per garantire che i colegislatori possano esercitare i loro poteri di controllo, alla Commissione è attribuito il diritto di adottare atti delegati.

Emendamento 582
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

Proposta di regolamento
Articolo 49 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Fatto salvo il paragrafo 3, i riferimenti contenuti nelle leggi, nelle norme, nei regolamenti o negli orientamenti applicabili a un sistema nazionale di certificazione della cibersicurezza che abbia smesso di produrre effetti giuridici ai sensi del paragrafo 1, sono considerati, invece, riferimenti al sistema europeo di certificazione della cibersicurezza (mutatis mutandis).

Or. en

Emendamento 583
Pilar del Castillo Vera

Proposta di regolamento
Articolo 49 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti e servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza in vigore.	2. Gli Stati membri non introducono nuovi sistemi nazionali di certificazione della cibersicurezza per i prodotti***, processi*** e servizi TIC coperti da un sistema europeo di certificazione della cibersicurezza in vigore.

Or. en

Emendamento 584
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 49 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 49 bis
	Su richiesta di qualsiasi persona fisica o giuridica, l'ENISA stabilisce se, ai fini del presente articolo, uno specifico sistema nazionale per la cibersicurezza sia coperto da un sistema europeo per la cibersicurezza, e una volta presa la propria decisione la rende pubblica entro quattro settimane dalla ricezione della richiesta.

Or. en

Motivazione

Questo processo aggiunge ulteriore chiarezza per le parti interessate e i soggetti certificati.

Emendamento 585
Olle Ludvigsson

Proposta di regolamento
Articolo 50 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Ciascuna autorità nazionale di controllo della certificazione, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila.	3. Ciascuna autorità nazionale di controllo della certificazione, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila. ***L'autorità nazionale di controllo della certificazione non può essere un organismo di certificazione o l'emittente di un certificato.***

Or. en

Emendamento 586
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 50 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Ciascuna autorità nazionale di controllo della certificazione, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila.	3. Ciascuna autorità nazionale di controllo della certificazione, per quanto riguarda la sua organizzazione, le decisioni di finanziamento, la struttura giuridica e il processo decisionale, è indipendente dai soggetti sui quali vigila. ***L'autorità nazionale di controllo della certificazione non può essere un organismo di certificazione o l'emittente di un certificato.***

Or. en

Motivazione

Necessario per garantire maggiore trasparenza e indipendenza.

Emendamento 587
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera -a (nuova)

Testo della Commissione	*Emendamento*
	(-a) organizzano controlli di mercato sui prodotti certificati e non certificati in maniera coordinata nei vari Stati membri, al fine di evitare la duplicazione dei controlli e massimizzare la verifica del mercato, per almeno il 30 % dei prodotti certificati nell'anno precedente, e obbligano il titolare del certificato a richiamare dal mercato i prodotti non conformi, a norma del paragrafo 6, lettera (e). All'atto di individuare il 30 % di prodotti che saranno oggetto del controllo

	di conformità, le autorità nazionali di certificazione danno la priorità ai prodotti ad alto rischio per i consumatori, in particolare minori, ai prodotti in cui sono integrate nuove tecnologie e/o ai prodotti con elevati tassi di vendita;

Or. en

Emendamento 588
Peter Kouroumbashev

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera a

Testo della Commissione	*Emendamento*
(a) sorvegliano e garantiscono l'applicazione delle disposizioni del presente titolo a livello nazionale e vigilano sulla conformità ***dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nei rispettivi territori ai requisiti fissati nel presente titolo e nel corrispondente sistema*** europeo ***di*** certificazione della cibersicurezza;	(a) sorvegliano e garantiscono l'applicazione delle disposizioni del presente titolo a livello nazionale e vigilano sulla conformità ***secondo le regole adottate dal gruppo*** europeo ***per la*** certificazione della cibersicurezza ***ai sensi dell'articolo 53, paragrafo 3, lettera d bis)***;

Or. en

Emendamento 589
Răzvan Popa

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera a

Testo della Commissione	*Emendamento*
(a) sorvegliano e garantiscono l'applicazione delle disposizioni del presente titolo a livello nazionale e ***vigilano sulla*** conformità dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nei rispettivi territori ai requisiti fissati nel presente	(a) sorvegliano e garantiscono l'applicazione delle disposizioni del presente titolo a livello nazionale e ***verificano la*** conformità dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nei rispettivi territori ai requisiti fissati nel presente

titolo e nel corrispondente sistema europeo di certificazione della cibersicurezza;	titolo e nel corrispondente sistema europeo di certificazione della cibersicurezza;

Or. ro

Emendamento 590
András Gyürk

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera b

Testo della Commissione	*Emendamento*
(b) monitorano e supervisionano le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;	***soppresso***

Or. en

Emendamento 591
Peter Kouroumbashev

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera b

Testo della Commissione	*Emendamento*
(b) monitorano e supervisionano le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;	(b) monitorano e supervisionano ***e, almeno ogni due anni, valutano*** le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;

Or. en

Emendamento 592

Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera b

Testo della Commissione	*Emendamento*
(b) monitorano ***e*** supervisionano le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;	(b) monitorano**,** supervisionano ***e, almeno ogni anno, valutano*** le attività degli organismi di valutazione della conformità ai fini del presente regolamento, anche in relazione alla notifica degli organismi di valutazione della conformità e ai relativi compiti stabiliti all'articolo 52 del presente regolamento;

Or. en

Emendamento 593
Peter Kouroumbashev

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera c

Testo della Commissione	*Emendamento*
(c) trattano i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio, svolgono le indagini opportune sull'oggetto del reclamo e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole.	(c) trattano i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio ***o all'autovalutazione della conformità effettuata***, svolgono le indagini opportune sull'oggetto del reclamo e informano il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole.

Or. en

Emendamento 594
Peter Kouroumbashev

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

Testo della Commissione	*Emendamento*
	(c bis) riferiscono all'ENISA e al gruppo europeo per la certificazione della cibersicurezza i risultati delle verifiche di cui alla lettera (a) e delle valutazioni di cui alla lettera (b);

Or. en

Emendamento 595
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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

Testo della Commissione	*Emendamento*
	(c bis) riferiscono all'ENISA e al gruppo europeo per la certificazione della cibersicurezza i risultati delle verifiche di cui alla lettera (a) e della valutazione di cui alla lettera (b);

Or. en

Emendamento 596
Pilar del Castillo Vera

Proposta di regolamento
Articolo 50 – paragrafo 6 – lettera d

Testo della Commissione	*Emendamento*
(d) cooperano con le altre autorità nazionali di controllo della certificazione o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi europei di certificazione della cibersicurezza;	(d) cooperano con le altre autorità nazionali di controllo della certificazione o con altre autorità pubbliche, anche mediante lo scambio di informazioni sugli eventuali prodotti***, processi*** e servizi TIC non conformi ai requisiti del presente regolamento o di specifici sistemi europei di certificazione della cibersicurezza;

Or. en

Emendamento 597
András Gyürk

Proposta di regolamento
Articolo 50 – paragrafo 7 – lettera b

Testo della Commissione	*Emendamento*
(b) condurre indagini, sotto forma di verifiche contabili, nei confronti ***degli organismi di valutazione della conformità e*** dei titolari dei certificati europei della cibersicurezza allo scopo di verificare l'osservanza delle disposizioni di cui al titolo III;	(b) condurre indagini, sotto forma di verifiche contabili, nei confronti dei titolari dei certificati europei della cibersicurezza allo scopo di verificare l'osservanza delle disposizioni di cui al titolo III;

Or. en

Emendamento 598
András Gyürk

Proposta di regolamento
Articolo 50 – paragrafo 7 – lettera c

Testo della Commissione	*Emendamento*
(c) adottare misure appropriate, nel rispetto della legislazione nazionale, al fine di accertare che ***gli organismi di valutazione della conformità o*** i titolari di certificati si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;	(c) adottare misure appropriate, nel rispetto della legislazione nazionale, al fine di accertare che i titolari di certificati si conformino al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

Or. en

Emendamento 599
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 50 – paragrafo 7 – lettera e

Testo della Commissione	*Emendamento*

(e) revocare, in conformità del diritto nazionale, i certificati non conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;	(e) revocare, in conformità del diritto nazionale, i certificati ***e i prodotti TIC destinati ai consumatori*** non conformi al presente regolamento o a un sistema europeo di certificazione della cibersicurezza;

Or. en

Emendamento 600
Pilar del Castillo Vera

Proposta di regolamento
Articolo 50 – paragrafo 8

Testo della Commissione	*Emendamento*
8. Le autorità nazionali di controllo della certificazione cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti e servizi TIC.	8. Le autorità nazionali di controllo della certificazione cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le questioni tecniche riguardanti la cibersicurezza di prodotti***, processi*** e servizi TIC.

Or. en

Emendamento 601
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 50 – paragrafo 8

Testo della Commissione	*Emendamento*
8. Le autorità nazionali di controllo della certificazione cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le	8. Le autorità nazionali di controllo della certificazione cooperano tra di loro e con la Commissione e, in particolare, si scambiano informazioni, esperienze e buone pratiche per quanto concerne la certificazione della cibersicurezza e le

questioni tecniche riguardanti la cibersicurezza di prodotti ***e*** servizi TIC.	questioni tecniche riguardanti la cibersicurezza di prodotti***,*** servizi ***e processi*** TIC.

Or. en

Emendamento 602
Cristian-Silviu Buşoi

Proposta di regolamento
Articolo 50 – paragrafo 8 – lettera a (nuova)

Testo della Commissione	*Emendamento*
	(a) ciascuna autorità nazionale di controllo della certificazione e ciascun membro e personale di tale autorità sono tenuti, conformemente al diritto dell'Unione o dello Stato membro, al segreto professionale durante e dopo la scadenza del loro mandato, riguardo a tutte le informazioni riservate di cui vengano a conoscenza nell'esercizio delle loro funzioni o dei loro poteri.

Or. en

Emendamento 603
Peter Kouroumbashev

Proposta di regolamento
Articolo 50 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 50 bis
	Revisione inter pares
	1. Le autorità nazionali di controllo della certificazione sono soggette a una revisione inter pares riguardo all'attività che svolgono a norma dell'articolo 50 del presente regolamento.
	2. La revisione inter pares comprende le valutazioni delle procedure messe in atto

dalle autorità nazionali di controllo della certificazione, in particolare le procedure di controllo della conformità dei prodotti che sono soggetti alla certificazione della cibersicurezza, la competenza del personale, la correttezza dei controlli e della metodologia di ispezione nonché la correttezza dei risultati. La revisione inter pares valuta, inoltre, se le autorità nazionali di controllo della certificazione in questione dispongano di risorse sufficienti per l'adeguato espletamento dei loro doveri, come prescritto dall'articolo 50, paragrafo 4.

3. La revisione inter pares delle autorità nazionali di controllo della certificazione è effettuata da due autorità nazionali di controllo della certificazione di altri Stati membri e dalla Commissione, almeno una volta ogni cinque anni. L'ENISA può partecipare alla revisione inter pares e decide in merito alla sua partecipazione sulla base di un'analisi della valutazione dei rischi.

4. Alla Commissione è conferito il potere, ai sensi dell'articolo 55 bis, di adottare atti delegati, al fine di stabilire un piano per la revisione inter pares durante un periodo di almeno cinque anni in cui siano definiti i criteri riguardanti la composizione del gruppo di revisione inter pares, la metodologia utilizzata per la revisione inter pares, il calendario, la periodicità e gli altri compiti relativi alla revisione inter pares. Nell'adottare tali atti delegati, la Commissione tiene debitamente conto delle considerazioni del gruppo.

5. I risultati della revisione inter pares sono esaminati dal gruppo. L'ENISA elabora e rende pubblica una sintesi dei risultati.

Or. en

Emendamento 604
Françoise Grossetête

Proposta di regolamento
Articolo 51 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Per il livello di affidabilità elevato, l'organismo di valutazione della conformità deve, oltre al proprio accreditamento, essere informato dall'autorità nazionale di controllo della certificazione riguardo alla sua competenza ed esperienza in materia di valutazione della cibersicurezza. L'autorità nazionale di controllo della certificazione deve procedere a controlli periodici sull'esperienza e le competenze degli organismi di valutazione della conformità notificati.

Or. fr

Motivazione

Per i livelli di affidabilità elevati sono richiesti test di efficacia. L'esperienza e le competenze degli organismi di valutazione della conformità che procedono ai test di efficacia devono essere anch'esse regolarmente controllate al fine di garantire, in particolare, la qualità dei test.

Emendamento 605
Edouard Martin

Proposta di regolamento
Articolo 51 – paragrafo 1 bis (nuovo)

Testo della Commissione	*Emendamento*
	1 bis. Per il livello di affidabilità elevato, gli organismi di valutazione della conformità sono autorizzati dalle autorità nazionali di controllo della certificazione soltanto quando soddisfano i requisiti in termini di competenze ed esperienza specificati, nel quadro di controlli periodici da parte di detti organismi.

Or. fr

Emendamento 606
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 51 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Gli organismi di accreditamento revocano l'accreditamento di un organismo di valutazione della conformità di cui al paragrafo 1 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.	2. L'accreditamento è rilasciato per un periodo massimo di cinque anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Gli organismi di accreditamento revocano l'accreditamento di un organismo di valutazione della conformità di cui al paragrafo 1 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. ***Gli organismi di valutazione della conformità non accettano pagamenti diretti per i loro servizi dai titolari di certificati.***

Or. en

Emendamento 607
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 51 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'accreditamento è rilasciato per un periodo massimo di ***cinque*** anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Gli organismi di accreditamento revocano l'accreditamento	2. L'accreditamento è rilasciato per un periodo massimo di ***dieci*** anni e può essere rinnovato alle stesse condizioni purché l'organismo di valutazione della conformità soddisfi i requisiti di cui al presente articolo. Gli organismi di accreditamento revocano l'accreditamento di un organismo

di un organismo di valutazione della conformità di cui al paragrafo 1 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.

di valutazione della conformità di cui al paragrafo 1 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.

Or. en

Motivazione

È necessario garantire che l'organismo di valutazione della conformità mantenga l'accreditamento fino alla scadenza del sistema di certificazione (compresa la sua proroga) rilasciato durante il suo periodo di accreditamento.

Emendamento 608
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 52 – paragrafo 5

Testo della Commissione	*Emendamento*
5. La Commissione può, mediante atti ***di esecuzione***, definire le circostanze, i formati e le procedure delle notifiche di cui al paragrafo 1. Tali atti ***di esecuzione*** sono adottati secondo la procedura d'esame di cui all'articolo 55, paragrafo 2.	5. La Commissione può, mediante atti ***delegati***, definire le circostanze, i formati e le procedure delle notifiche di cui al paragrafo 1. Tali atti ***delegati*** sono adottati secondo la procedura d'esame di cui all'articolo 55, paragrafo 2.

Or. en

Emendamento 609
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Clare Moody

Proposta di regolamento
Articolo 53 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Il gruppo è composto dalle autorità nazionali di controllo della certificazione.	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.	Le autorità sono rappresentate dai capi o da rappresentanti ad alto livello delle autorità nazionali di controllo della certificazione. ***Su invito, i membri del gruppo di certificazione dei portatori di interessi sono autorizzati a presenziare alle riunioni del gruppo europeo per la certificazione della cibersicurezza e a partecipare alle sue attività.***

Or. en

Motivazione

Analogamente alle disposizioni relative alla partecipazione degli Stati membri alle riunioni del gruppo di certificazione dei portatori di interessi, i portatori di interessi sono autorizzati, su invito del gruppo europeo per la certificazione della cibersicurezza, a partecipare allo svolgimento delle attività.

Emendamento 610
Gunnar Hökmark

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 ***da esperti*** nazionali.

Or. en

Emendamento 611
Peter Kouroumbashev

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera d bis (nuova)

Testo della Commissione	*Emendamento*
	(d bis) adottare norme vincolanti che stabiliscano la frequenza con la quale le

autorità nazionali di controllo della certificazione devono effettuare verifiche dei certificati e autovalutazione della conformità, nonché i criteri, la portata e il campo di applicazione di tali verifiche, e adottare disposizioni e norme comuni per le relazioni, conformemente all'articolo 50, paragrafo 6;

Or. en

Emendamento 612
Pilar del Castillo Vera

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera f – punto i (nuovo)

Testo della Commissione	*Emendamento*
	i) agevolare l'allineamento dei sistemi europei di cibersicurezza con le norme riconosciute a livello internazionale, provvedendo tra l'altro a: rivedere i sistemi europei della cibersicurezza esistenti e, ove opportuno, rivolgere raccomandazioni all'ENISA affinché collabori con le pertinenti organizzazioni internazionali di normazione per ovviare a carenze o lacune nelle norme vigenti riconosciute a livello internazionale.

Or. en

Emendamento 613
Edouard Martin

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera f bis (nuova)

Testo della Commissione	*Emendamento*
	(f bis) definire un meccanismo di revisione inter pares per valutare il rispetto dei requisiti di cui al presente

regolamento da parte di ogni autorità nazionale di controllo della certificazione, in particolare la capacità di svolgere, per ogni livello di affidabilità, i compiti descritti nel presente regolamento con le competenze tecniche richieste. Ove necessario, la revisione inter pares potrà definire le misure idonee da adottare.

Or. fr

Emendamento 614
Gunnar Hökmark

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera f bis (nuova)

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

Or. en

Emendamento 615
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera g (nuova)

Testo della Commissione	*Emendamento*
	(g) istituire un processo di revisione inter pares. Tale processo tiene conto, in particolare, delle competenze tecniche richieste alle autorità nazionali di controllo della certificazione nell'adempimento dei loro compiti come

descritte all'articolo 48 e all'articolo 50 e comprende, ove necessario, la definizione di orientamenti e documenti sulle migliori pratiche, al fine di migliorare la conformità delle autorità nazionali di controllo della certificazione al presente regolamento.

Or. en

Emendamento 616
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera h (nuova)

Testo della Commissione	*Emendamento*
	(h) tenere conto dei risultati della consultazione dei portatori di interessi condotta in preparazione di una proposta di sistema, conformemente all'articolo 44 del presente regolamento.

Or. en

Motivazione

Il gruppo europeo per la certificazione della cibersicurezza tiene conto anche delle eventuali consultazioni condotte dalla Commissione in merito alla preparazione delle proposte di sistemi per la cibersicurezza.

Emendamento 617
Pavel Telička, Carolina Punset, Gesine Meissner

Proposta di regolamento
Articolo 53 – paragrafo 3 – lettera h (nuova)

Testo della Commissione	*Emendamento*
	(h) supervisionare la vigilanza e il mantenimento di un certificato.

Or. en

Emendamento 618
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 54 – comma 1

Testo della Commissione	*Emendamento*
Gli Stati membri stabiliscono le norme sulle sanzioni da irrogare in caso di violazione del ***presente*** titolo e dei sistemi europei di certificazione della cibersicurezza e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano [entro il …/senza indugio] tali norme e misure alla Commissione, nonché eventuali successive modifiche delle stesse.	Gli Stati membri stabiliscono le norme sulle sanzioni da irrogare in caso di violazione del titolo ***II bis, del titolo III*** e dei sistemi europei di certificazione della cibersicurezza e prendono tutti i provvedimenti necessari per la loro applicazione. Le sanzioni previste sono efficaci, proporzionate e dissuasive. Gli Stati membri notificano [entro il …/senza indugio] tali norme e misure alla Commissione, nonché eventuali successive modifiche delle stesse.

Or. en

Emendamento 619
Cristian-Silviu Buşoi

Proposta di regolamento
Articolo 54 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 54 bis
	Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo o dell'organismo di valutazione della conformità
	1. Fatti salvi gli eventuali altri ricorsi amministrativi o non giurisdizionali, ciascuna persona fisica o giuridica ha il diritto a un ricorso giurisdizionale effettivo:
	(a) avverso la decisione di un organismo di valutazione della conformità o di un'autorità nazionale di controllo della

certificazione nei suoi confronti, anche (ove applicabile), in relazione al rilascio (o mancato rilascio) di un certificato europeo della cibersicurezza di cui tale persona sia titolare; e

(b) laddove un'autorità nazionale di controllo della certificazione non gestisca un reclamo per cui sia competente.

2. Il ricorso avverso un organismo di valutazione della conformità o un'autorità nazionale di controllo della certificazione è presentato dinanzi ai tribunali dello Stato membro in cui è stabilito detto organismo o autorità.

Or. en

Emendamento 620
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 54 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 54 bis
	Diritto a un ricorso giurisdizionale effettivo nei confronti dell'autorità di controllo
	1. Fatti salvi gli eventuali altri ricorsi amministrativi o non giurisdizionali, ciascuna persona fisica o giuridica ha il diritto a un ricorso giurisdizionale effettivo:
	(a) avverso la decisione di un organismo di valutazione della conformità o di un'autorità nazionale di controllo della certificazione nei suoi confronti, anche in relazione al riconoscimento di un certificato europeo della cibersicurezza di cui tale persona o entità sia titolare; e

	(b) laddove un'autorità nazionale di controllo della certificazione non gestisca un reclamo per cui sia competente.
	2. Il ricorso avverso un organismo di valutazione della conformità o un'autorità nazionale di controllo della certificazione è presentato dinanzi ai tribunali dello Stato membro in cui è stabilito detto organismo o autorità.

Or. en

Motivazione

È essenziale garantire che chi richiede un certificato abbia diritto a un ricorso giurisdizionale effettivo quando richiede la certificazione nel rispettivo Stato membro. La certificazione dei prodotti o dei processi non dovrebbe essere utilizzata per favorire soggetti specifici rispetto ad altri sulla base di considerazioni viziate e di parte ovvero relative alla loro nazionalità.

Emendamento 621
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 56 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Entro ***cinque*** anni dalla data di cui all'articolo 58, e successivamente ogni ***cinque*** anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'Agenzia e delle sue prassi di lavoro, come pure l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro pervenuto all'Agenzia in relazione alle sue attività. Se ritiene che il mantenimento dell'Agenzia non sia più giustificato rispetto agli obiettivi, al mandato e ai compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'Agenzia.	1. Entro ***quattro*** anni dalla data di cui all'articolo 58, e successivamente ogni ***quattro*** anni, la Commissione valuta l'impatto, l'efficacia e l'efficienza dell'Agenzia e delle sue prassi di lavoro, come pure l'eventuale necessità di modificarne il mandato e le conseguenti implicazioni finanziarie. La valutazione tiene conto di qualsiasi riscontro pervenuto all'Agenzia in relazione alle sue attività. Se ritiene che il mantenimento dell'Agenzia non sia più giustificato rispetto agli obiettivi, al mandato e ai compiti che le sono stati assegnati, la Commissione può proporre di modificare il presente regolamento in relazione alle disposizioni che riguardano l'Agenzia.

Or. en

Emendamento 622
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 56 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti ***e*** servizi TIC nell'Unione e di migliorare il funzionamento del mercato interno.	2. La valutazione esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti***,*** servizi ***e processi*** TIC nell'Unione e di migliorare il funzionamento del mercato interno. ***La Commissione valuta, cinque anni dopo l'adozione del regolamento, un eventuale ampliamento dell'ambito di applicazione del titolo III.***

Or. en

Motivazione

Deve essere prevista la possibilità di una revisione del regolamento, in particolare riguardo al titolo III.

Emendamento 623
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 56 – paragrafo 2

Testo della Commissione	*Emendamento*
2. La ***valutazione*** esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti e servizi TIC nell'Unione e di migliorare il funzionamento del mercato interno.	2. ***Entro quattro anni dalla data di cui all'articolo 58, e successivamente ogni quattro anni,*** la ***Commissione*** esamina inoltre l'impatto, l'efficacia e l'efficienza delle disposizioni del titolo III per quanto riguarda gli obiettivi di garantire un livello adeguato di cibersicurezza dei prodotti***,*** ***processi*** e servizi TIC nell'Unione e di

migliorare il funzionamento del mercato interno.

Or. en

Emendamento 624
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 56 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. La valutazione esamina il progressivo passaggio alla certificazione obbligatoria, purché la valutazione del mercato e la consultazione dei portatori di interessi evidenzino risultati a sostegno di tale azione.

Or. en

Emendamento 625
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner

Proposta di regolamento
Titolo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	ALLEGATO 1 (nuovo)
	Al momento dell'avvio del quadro di certificazione della cibersicurezza dell'UE, è probabile che l'attenzione si concentri sul come consentire agli ambiti di interesse immediato di rispondere alle sfide poste dalle tecnologie emergenti. L'ambito dell'Internet degli oggetti (IoT) riveste un interesse particolare in quanto ha implicazioni trasversali per i requisiti applicati sia ai consumatori sia all'industria. Si propone di adottare il seguente elenco di priorità nell'ambito del quadro di certificazione:
	1) Certificazione della prestazione di

servizi cloud.
2) Certificazione dei dispositivi IoT compresi:
a) i dispositivi a livello individuale, come quelli indossabili intelligenti;
b) i dispositivi a livello di comunità, come le autovetture intelligenti, le case intelligenti, i dispositivi per la salute;
c) i dispositivi a livello sociale, come le città intelligenti e le reti intelligenti.
3) L'industria 4.0, che prevede sistemi ciberfisici intelligenti e interconnessi che automatizzano tutte le fasi delle operazioni industriali, dalla progettazione e produzione fino al funzionamento, alla catena di approvvigionamento e al mantenimento dei servizi.
4) Certificazione delle tecnologie e dei prodotti utilizzati nella vita quotidiana. Un esempio di questo tipo potrebbe essere dato dai dispositivi di messa in rete, come i router Internet domestici.

Or. en

Emendamento 626
Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	5 bis. Se un organismo di valutazione della conformità è di proprietà di un ente o un'istituzione pubblici o è gestito da questi ultimi, l'indipendenza e l'assenza di conflitti di interessi tra, da un lato, le autorità di controllo della certificazione e, dall'altro, l'organismo di valutazione della conformità, sono garantite e documentate.

Or. en

Emendamento 627

Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 8

Testo della Commissione	*Emendamento*
8. Un organismo di valutazione della conformità è in grado di effettuare tutti i compiti di valutazione della conformità ad esso assegnati dal presente regolamento, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità.	8. Un organismo di valutazione della conformità è in grado di effettuare tutti i compiti di valutazione della conformità ad esso assegnati dal presente regolamento, indipendentemente dal fatto che tali compiti siano eseguiti dall'organismo stesso o per suo conto e sotto la sua responsabilità. ***Eventuali affidamenti a terzi o consultazioni di personale esterno sono adeguatamente documentati, non prevedono alcun intermediario e sono oggetto di un accordo scritto che contempli, tra l'altro, la riservatezza e i conflitti di interessi. L'organismo di valutazione della conformità in questione si assume la piena responsabilità dei compiti svolti.***

Or. en

Emendamento 628
Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 12

Testo della Commissione	*Emendamento*
12. È garantita l'imparzialità dell'organismo di valutazione della conformità, dei suoi alti dirigenti e del personale addetto alle valutazioni.	12. È garantita l'imparzialità dell'organismo di valutazione della conformità, dei suoi alti dirigenti e del personale addetto alle valutazioni ***e dei subappaltatori***.

Or. en

Emendamento 629
Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 15

Testo della Commissione	*Emendamento*
15. Il personale di un organismo di valutazione della conformità ***è tenuto*** al segreto professionale per tutto ciò di cui ***viene*** a conoscenza nell'esercizio delle ***sue*** funzioni a norma del presente regolamento o di qualsiasi disposizione esecutiva di diritto interno, tranne nei confronti delle autorità competenti degli Stati membri in cui ***esercita*** le ***sue*** attività.	15. ***L'organismo di valutazione della conformità e*** il ***suo*** personale***, comitati, affiliate, subappaltatori e qualsiasi organismo associato o personale di organismi esterni*** di un organismo di valutazione della conformità ***sono tenuti al mantenimento della riservatezza e*** al segreto professionale per tutto ciò di cui ***vengono*** a conoscenza nell'esercizio delle ***loro*** funzioni a norma del presente regolamento o di qualsiasi disposizione esecutiva di diritto interno, tranne ***laddove la divulgazione sia richiesta dal diritto dell'UE o di uno Stato membro a cui tali persone sono soggette, salvo*** nei confronti delle autorità competenti degli Stati membri in cui ***esercitano*** le ***loro*** attività. ***I diritti di proprietà vengono tutelati. L'organismo di valutazione della conformità dispone di procedure documentate riguardo ai requisiti di cui al presente punto 15.***

Or. en

Emendamento 630
Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 15 bis (nuovo)

Testo della Commissione	*Emendamento*
	15 bis. Con l'eccezione del punto 15, i requisiti del presente allegato non precludono in alcuno modo gli scambi di informazioni tecniche e di orientamenti regolamentari tra un organismo di valutazione della conformità e una persona che richieda o stia valutando se richiedere una certificazione.

Or. en

Emendamento 631
Cristian-Silviu Buşoi

Proposta di regolamento
Allegato I – punto 15 ter (nuovo)

Testo della Commissione	*Emendamento*
	15 ter. Gli organismi di valutazione della conformità operano secondo modalità e condizioni coerenti, eque e ragionevoli, tenendo conto degli interessi delle piccole e medie imprese quali definiti nella raccomandazione 2003/361/CE in relazione alle tariffe.

Or. en