Parlamento europeo
2014-2019

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

2017/0225(COD)

30.4.2018

EMENDAMENTI
93 - 396

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 93
Michał Boni, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 2

Testo della Commissione	*Emendamento*
(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, imprese e amministrazioni pubbliche di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'internet degli oggetti (IoT) nel prossimo decennio dovrebbero essere disponibili in tutta l'UE milioni, se non miliardi, di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi siano connessi a internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti aziendali e individuali dispongano di informazioni insufficienti sulle caratteristiche dei prodotti e dei servizi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali.	(2) L'uso delle reti e dei sistemi informativi da parte di cittadini, imprese e amministrazioni pubbliche di tutta l'Unione è attualmente molto diffuso. La digitalizzazione e la connettività stanno diventando caratteristiche fondamentali di un numero di prodotti e servizi in costante aumento, e con l'avvento dell'internet degli oggetti (IoT) nel prossimo decennio dovrebbero essere disponibili in tutta l'UE milioni, se non miliardi, di dispositivi digitali connessi. Sebbene un numero crescente di dispositivi siano connessi a internet, la sicurezza e la resilienza non sono sufficientemente integrate nella progettazione, il che rende inadeguata la cibersicurezza. In tale contesto, l'uso limitato della certificazione fa sì che gli utenti aziendali e individuali dispongano di informazioni insufficienti sulle caratteristiche dei prodotti***, dei processi*** e dei servizi TIC in termini di cibersicurezza, il che mina la fiducia nelle soluzioni digitali. ***Tale ambizione è al centro del programma di riforma della Commissione europea per la realizzazione di un mercato unico digitale, dal momento che le reti TIC costituiscono la colonna portante dei prodotti e dei servizi digitali che sono potenzialmente in grado di aiutarci in tutti gli aspetti della nostra vita e di dare impulso alla crescita economica dell'Europa. Per far sì che gli obiettivi del mercato unico digitale siano pienamente realizzati, è necessario predisporre gli elementi tecnologici essenziali su cui si basano settori importanti come la sanità elettronica, l'IoT, l'intelligenza artificiale, le tecnologie quantistiche nonché i sistemi***

di trasporto intelligenti e le tecnologie produttive avanzate.

Or. en

Emendamento 94
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 3

Testo della Commissione	*Emendamento*
(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche).	(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la cibersicurezza nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche). ***A questo proposito, il piano d'azione per l'istruzione digitale pubblicato dalla Commissione europea il 17 gennaio 2018 è un passo nella giusta direzione, in particolare riguardo alla campagna di sensibilizzazione a livello dell'UE rivolta agli educatori, ai genitori e ai discenti per promuovere la sicurezza online, l'igiene informatica e l'alfabetizzazione mediatica, insieme all'iniziativa di insegnamento della cibersicurezza che parte dal quadro delle competenze digitali per i cittadini, per consentire alle persone di utilizzare la tecnologia con dimestichezza e responsabilità.***

Or. en

Emendamento 95
Răzvan Popa

Proposta di regolamento
Considerando 3

Testo della Commissione	*Emendamento*
(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la ***cibersicurezza*** nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche).	(3) L'incremento della digitalizzazione e della connettività comporta maggiori rischi in termini di cibersicurezza, il che rende la società in generale più vulnerabile alle minacce informatiche e aggrava i pericoli cui sono esposte le persone, comprese quelle vulnerabili come i minori. Al fine di attenuare tale rischio per la società, occorre prendere tutti i provvedimenti necessari per migliorare la ***sicurezza contro gli attacchi informatici*** nell'UE allo scopo di proteggere meglio dalle minacce informatiche le reti e i sistemi informativi, le reti di telecomunicazione, i prodotti digitali, i servizi e i dispositivi utilizzati da cittadini, amministrazioni pubbliche e imprese (dalle PMI ai gestori delle infrastrutture critiche).

Or. ro

Emendamento 96
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 3 bis (nuovo)

Testo della Commissione	*Emendamento*
	(3 bis) Gli obiettivi e i compiti dell'ENISA dovrebbero essere allineati ulteriormente alla comunicazione congiunta per quanto riguarda il suo riferimento alla promozione dell'igiene informatica e della sensibilizzazione. La ciberresilienza si può

ottenere con l'attuazione dei principi di base dell'igiene informatica.

Or. en

Emendamento 97
Massimiliano Salini

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti ***e*** dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, ***dal momento che gli incidenti informatici minano*** la fiducia ***nei fornitori di servizi digitali e*** nel mercato unico digitale ***stesso, soprattutto tra i consumatori, la fiducia*** dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti***,*** dei servizi ***e dei processi*** TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione

comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali. ***Accanto a una certificazione a livello di UE e vista la crescente disponibilità di dispositivi IoT, esiste tutta una gamma di misure volontarie che il settore privato dovrebbe adottare per rafforzare la fiducia nella sicurezza dei prodotti, dei servizi e dei processi TIC, come la cifratura e le tecnologie blockchain.***

Or. en

Emendamento 98
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per ***assicurare una risposta coordinata dell'UE e*** accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe

informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.	essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali. ***Accanto a una certificazione a livello di UE, esiste una serie di misure volontarie ampiamente accettate sul mercato, a seconda del prodotto, del servizio, dell'utilizzo o della norma; è opportuno incoraggiare tali misure, così come l'approccio dal basso verso l'alto del settore, compresi l'uso della sicurezza fin dalla progettazione, la valorizzazione delle norme internazionali e il contributo alle stesse.***

Or. en

Emendamento 99
Gunnar Hökmark

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche ***e l'aumento della portata e della precisione degli attacchi mirati***, è necessario aumentare le capacità a livello

particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala***, pur sottolineando l'importanza di mantenere e rafforzare ulteriormente le capacità nazionali di risposta alle minacce informatiche di qualsiasi dimensione***. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

Or. en

Emendamento 100
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce

informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.	informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali. ***Le sfide affrontate dovrebbero riflettersi proporzionalmente nelle risorse di bilancio destinate all'Agenzia, per garantire il funzionamento ottimale nelle circostanze attuali.***

Or. en

Emendamento 101
Martina Werner

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione ***e*** il coordinamento tra gli Stati membri e le istituzioni, le agenzie e	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la cooperazione***,*** il coordinamento ***e la condivisione delle informazioni*** tra gli

gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.	Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza***, nonché la consapevolezza di quanto sia importante condividere le informazioni e non occultarle, in quanto ciò è il principale deterrente contro gli attacchi informatici***. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

Or. en

Emendamento 102
Clare Moody, Theresa Griffin, Peter Kouroumbashev, Arne Lietz

Proposta di regolamento
Considerando 5

Testo della Commissione	*Emendamento*
(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la	(5) Tenuto conto delle maggiori sfide che l'Unione si trova ad affrontare in materia di cibersicurezza, è necessario disporre di una serie completa di misure che si basino su precedenti azioni dell'Unione e promuovano obiettivi sinergici. Tra questi obiettivi figura la necessità di rafforzare ulteriormente le capacità e la preparazione degli Stati membri e delle imprese e di migliorare la

cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.	cooperazione e il coordinamento tra gli Stati membri e le istituzioni, le agenzie e gli organismi dell'UE. Inoltre, data la natura transfrontaliera delle minacce informatiche, è necessario aumentare le capacità a livello di Unione che potrebbero integrare l'azione degli Stati membri, in particolare in caso di crisi e incidenti informatici transfrontalieri su vasta scala. Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza di cittadini e imprese circa le questioni riguardanti la cibersicurezza. Inoltre, la fiducia nel mercato unico digitale dovrebbe essere ulteriormente rafforzata fornendo informazioni trasparenti in merito al livello di sicurezza dei prodotti e dei servizi TIC ***e sottolineando che persino un livello elevato di certificazione della cibersicurezza non può garantire che un prodotto o un servizio TIC sia completamente sicuro***. Il conseguimento di questo obiettivo può essere agevolato mediante una certificazione a livello di UE che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali ***nonché la promozione dell'alfabetizzazione informatica***.

Or. en

Emendamento 103
Gunnar Hökmark

Proposta di regolamento
Considerando 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) Al fine di rafforzare le strutture di sicurezza e ciberdifesa europee, è importante mantenere e sviluppare le capacità degli Stati membri di rispondere in modo globale alle minacce informatiche, compresi gli incidenti transfrontalieri, mentre il coordinamento

a livello dell'UE da parte dell'Agenzia non dovrebbe portare a un indebolimento delle capacità o degli sforzi negli Stati membri.

Or. en

Emendamento 104
Barbara Kappel

Proposta di regolamento
Considerando 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) In ragione della specifica posizione delle piccole e medie imprese e del ruolo essenziale che esse svolgono nell'economia dell'Unione, i requisiti per una certificazione a livello dell'UE, che potrebbero far gravare oneri eccessivamente elevati su tali imprese e che non sono fondamentali per le infrastrutture critiche, devono essere valutati con cautela e/o respinti.

Or. en

Emendamento 105
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) Le imprese e i singoli consumatori dovrebbero avere informazioni precise sul livello di sicurezza dei loro prodotti TIC. Allo stesso tempo, è necessario capire che nessun prodotto garantisce la cibersicurezza e che si devono promuovere norme di base sull'igiene informatica, dando loro la priorità.

Or. en

Emendamento 106
Rolandas Paksas

Proposta di regolamento
Considerando 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) I requisiti in materia di cibersicurezza dovrebbero sempre avere l'obiettivo di raggiungere il massimo livello di sicurezza per i consumatori e, ove opportuno, istituire elementi aggiuntivi per i prodotti che devono avere standard di sicurezza più elevati in ragione dell'oggetto della protezione.

Or. en

Emendamento 107
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 7

Testo della Commissione	*Emendamento*
(7) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la strategia dell'UE per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi per la cibersicurezza. Nell'ambito dei suoi sforzi volti a proteggere maggiormente gli europei durante la navigazione online, nel 2016 l'Unione ha adottato il primo atto legislativo nel settore della cibersicurezza, la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("direttiva NIS"). La direttiva	(7) L'Unione ha già adottato importanti provvedimenti per garantire la cibersicurezza e accrescere la fiducia nelle tecnologie digitali. Nel 2013 è stata adottata la strategia dell'UE per la cibersicurezza per orientare la risposta politica dell'Unione alle minacce e ai rischi per la cibersicurezza. Nell'ambito dei suoi sforzi volti a proteggere maggiormente gli europei durante la navigazione online, nel 2016 l'Unione ha adottato il primo atto legislativo nel settore della cibersicurezza, la direttiva (UE) 2016/1148 recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione ("direttiva NIS"). La direttiva

NIS ***ha stabilito*** obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, l'acqua, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di cloud computing e mercati online). All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza.	NIS ***rispetta la strategia del mercato unico digitale e, insieme ad altri strumenti, quali la direttiva che istituisce il codice europeo delle comunicazioni elettroniche, il regolamento (UE) 2016/679 e la direttiva 2002/58/CE***, ***stabilisce*** obblighi concernenti le capacità nazionali nel campo della cibersicurezza, ha istituito i primi meccanismi volti a rafforzare la cooperazione strategica e operativa tra gli Stati membri e ha introdotto obblighi riguardanti le misure di sicurezza e le notifiche degli incidenti in tutti i settori che sono di vitale importanza per l'economia e la società, quali l'energia, i trasporti, l'acqua, i servizi bancari, le infrastrutture dei mercati finanziari, la sanità, le infrastrutture digitali e i fornitori di servizi digitali essenziali (motori di ricerca, servizi di cloud computing e mercati online). All'ENISA è stato attribuito un ruolo fondamentale nel sostegno all'attuazione di tale direttiva. Inoltre, la lotta efficace contro la cibercriminalità è una priorità importante dell'agenda europea sulla sicurezza e contribuisce al conseguimento dell'obiettivo generale di raggiungere un elevato livello di cibersicurezza.

Or. en

Emendamento 108
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 8

Testo della Commissione	*Emendamento*
(8) È noto che, dall'adozione della strategia dell'UE per la cibersicurezza del 2013 e dall'ultima revisione del mandato dell'Agenzia, il contesto politico generale è cambiato in modo significativo, anche in relazione a un contesto globale più incerto e meno sicuro. In tale contesto e nel quadro	(8) È noto che, dall'adozione della strategia dell'UE per la cibersicurezza del 2013 e dall'ultima revisione del mandato dell'Agenzia, il contesto politico generale è cambiato in modo significativo, anche in relazione a un contesto globale più incerto e meno sicuro. In tale contesto e

della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama delle minacce, per far fronte al quale l'attuale mandato non è sufficiente, come riconosciuto dalla valutazione dell'Agenzia.	***considerato il ruolo positivo che l'Agenzia ha svolto nel corso degli anni nella messa in comune delle competenze, nel coordinamento, nel rafforzamento delle capacità e*** nel quadro della nuova politica dell'Unione in materia di cibersicurezza, è necessario rivedere il mandato dell'ENISA per definirne il ruolo nel mutato ecosistema della cibersicurezza e garantire che contribuisca efficacemente alla risposta dell'Unione alle sfide poste in questo ambito dalla radicale trasformazione del panorama delle minacce, per far fronte al quale l'attuale mandato non è sufficiente, come riconosciuto dalla valutazione dell'Agenzia.

Or. en

Emendamento 109
Răzvan Popa

Proposta di regolamento
Considerando 9

Testo della Commissione	*Emendamento*
(9) L'Agenzia istituita dal presente regolamento dovrebbe succedere all'ENISA, istituita con il regolamento (UE) n. 526/2013. L'Agenzia dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli atti legislativi dell'UE nel settore della cibersicurezza, anche fornendo consulenze e pareri e fungendo da centro di informazioni e conoscenze dell'Unione. Dovrebbe promuovere lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornendo suggerimenti strategici alla Commissione europea e agli Stati membri, fungendo da punto di riferimento per iniziative politiche settoriali dell'Unione sulle questioni di cibersicurezza, promuovendo la cooperazione operativa tra gli Stati membri	(9) L'Agenzia istituita dal presente regolamento dovrebbe succedere all'ENISA, istituita con il regolamento (UE) n. 526/2013. L'Agenzia dovrebbe svolgere i compiti che le sono conferiti dal presente regolamento e dagli atti legislativi dell'UE nel settore della cibersicurezza, anche fornendo consulenze e pareri e fungendo da centro di informazioni e conoscenze dell'Unione. ***Dal momento che la maggior parte delle reti e dei sistemi informativi sono nel settore privato, l'Agenzia*** dovrebbe ***migliorare la cooperazione e*** promuovere lo scambio di buone pratiche tra gli Stati membri e i portatori di interessi del settore privato, fornendo suggerimenti strategici alla Commissione europea e agli Stati membri, fungendo da punto di riferimento per iniziative politiche settoriali dell'Unione

e tra questi ultimi e le istituzioni, le agenzie e gli organismi dell'UE.	sulle questioni di cibersicurezza, promuovendo la cooperazione operativa tra gli Stati membri e tra questi ultimi e le istituzioni, le agenzie e gli organismi dell'UE.

Or. ro

Emendamento 110
Martina Werner

Proposta di regolamento
Considerando 11

Testo della Commissione	*Emendamento*
(11) Tenuto conto delle crescenti sfide in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'Agenzia dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale europeo.	(11) Tenuto conto delle crescenti sfide in materia di cibersicurezza che l'Unione si trova ad affrontare, le risorse finanziarie e umane destinate all'Agenzia dovrebbero essere aumentate per riflettere il potenziamento del suo ruolo e dei suoi compiti, come pure la sua posizione cruciale nell'ecosistema delle organizzazioni che difendono l'ecosistema digitale europeo***, per permettere all'ENISA di svolgere efficacemente i compiti che le sono stati assegnati dal presente regolamento***.

Or. en

Emendamento 111
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 12

Testo della Commissione	*Emendamento*
(12) È opportuno che l'Agenzia sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza,	(12) È opportuno che l'Agenzia sviluppi e mantenga un elevato livello di competenza e che operi come punto di riferimento generando fiducia nel mercato interno grazie alla propria indipendenza,

alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'Agenzia dovrebbe contribuire in modo proattivo agli sforzi nazionali e dell'Unione, collaborando pienamente con istituzioni, organi, uffici e agenzie dell'Unione e con gli Stati membri. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione ***del settore*** privato e di altri portatori d'interessi. È opportuno stabilire una serie di compiti che definiscano in che modo l'Agenzia deve raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione.	alla qualità delle consulenze e delle informazioni fornite, alla trasparenza delle procedure e dei metodi operativi come pure alla diligenza nell'esecuzione dei suoi compiti. Nello svolgimento dei suoi compiti l'Agenzia dovrebbe contribuire in modo proattivo agli sforzi nazionali e dell'Unione, collaborando pienamente con istituzioni, organi, uffici e agenzie dell'Unione e con gli Stati membri. Inoltre, dovrebbe avvalersi dei contributi e della collaborazione ***dei settori*** privato ***e pubblico*** e di altri portatori d'interessi. È opportuno stabilire una serie di compiti che definiscano in che modo l'Agenzia deve raggiungere i propri obiettivi, lasciandole nel contempo una certa flessibilità di azione.

Or. en

Emendamento 112
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner

Proposta di regolamento
Considerando 12 bis (nuovo)

Testo della Commissione	*Emendamento*
	(12 bis) Il ruolo dell'Agenzia dovrebbe essere sottoposto a una valutazione continua e a un tempestivo riesame, in particolare per quanto concerne il suo ruolo di coordinamento nei confronti degli Stati membri e delle loro autorità nazionali e l'eventuale possibilità di fungere da sportello unico per gli Stati membri e gli organismi e le istituzioni dell'UE. Il ruolo dell'Agenzia nell'evitare la frammentazione del mercato interno e nella possibile introduzione di sistemi obbligatori di certificazione della cibersicurezza, qualora in futuro la situazione richieda un tale cambiamento, dovrebbe essere anch'esso valutato, insieme al ruolo dell'Agenzia riguardo alla futura

valutazione dei prodotti di paesi terzi che accedono al mercato dell'UE e alla possibile definizione di una "lista nera" delle imprese che non rispettano i criteri dell'UE.

Or. en

Emendamento 113
Martina Werner

Proposta di regolamento
Considerando 13

Testo della Commissione	*Emendamento*
(13) L'Agenzia dovrebbe assistere la Commissione tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza, anche per quanto riguarda la protezione delle infrastrutture critiche e la ciberresilienza. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza.	(13) L'Agenzia dovrebbe assistere la Commissione***, di propria iniziativa e su richiesta,*** tramite consulenze, pareri e analisi su tutte le questioni inerenti all'Unione e riguardanti l'elaborazione di politiche e normative e l'aggiornamento e la revisione nel settore della cibersicurezza, anche per quanto riguarda la protezione delle infrastrutture critiche e la ciberresilienza. L'Agenzia dovrebbe fungere da punto di riferimento per pareri e competenze sulle iniziative politiche e legislative dell'Unione in settori specifici che presentano aspetti correlati alla cibersicurezza. ***L'Agenzia dovrebbe fornire periodicamente al Parlamento aggiornamenti, analisi e revisioni nel settore della cibersicurezza e sull'evoluzione dei suoi compiti.***

Or. en

Emendamento 114
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

Proposta di regolamento
Considerando 14

Testo della Commissione	*Emendamento*
(14) Il compito di base dell'Agenzia è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva NIS, che è essenziale ai fini del rafforzamento della ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.	(14) Il compito di base dell'Agenzia è promuovere l'attuazione coerente del pertinente quadro normativo, in particolare l'effettiva attuazione della direttiva NIS***, della direttiva che istituisce il codice europeo delle comunicazioni elettroniche, del regolamento (UE) 2016/679 e della direttiva 2002/58/CE***, che è essenziale ai fini del rafforzamento della ciberresilienza. In considerazione del panorama delle minacce informatiche in rapida evoluzione, è chiaro che gli Stati membri devono essere sostenuti da un approccio trasversale più ampio allo sviluppo della ciberresilienza.

Or. en

Emendamento 115
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della	(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della

loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.	loro attuazione. ***L'Agenzia, inoltre, dovrebbe fornire assistenza e consulenza agli Stati membri e alle istituzioni dell'Unione nella definizione di politiche e pratiche trasparenti per la gestione e la divulgazione coordinata delle vulnerabilità dei prodotti, dei processi e dei servizi TIC che non sono pubblicamente note, anche instaurando una procedura di esame della divulgazione di vulnerabilità da parte dei governi e politiche di divulgazione coordinata delle vulnerabilità. Infine,*** dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.

Or. en

Emendamento 116
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi	(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi

informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.	informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, se del caso, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome. ***L'Agenzia, inoltre, dovrebbe fungere da punto di contatto per gli Stati membri e le istituzioni dell'UE, che dovrebbero poter richiedere la sua assistenza nell'ambito delle competenze e dei ruoli che le sono assegnati.***

Or. en

Emendamento 117
Martina Werner

Proposta di regolamento
Considerando 15

Testo della Commissione	*Emendamento*
(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della loro attuazione. Dovrebbe inoltre offrire formazione e materiale formativo agli enti	(15) L'Agenzia dovrebbe assistere gli Stati membri e le istituzioni, gli organi, gli uffici e le agenzie dell'Unione nei loro sforzi volti a sviluppare e consolidare le capacità e la preparazione per prevenire e individuare i problemi e gli incidenti relativi alla cibersicurezza e alla sicurezza delle reti e dei sistemi informativi e per reagirvi. In particolare, dovrebbe sostenere lo sviluppo e il potenziamento dei CSIRT nazionali perché raggiungano un livello comune elevato di maturità nell'Unione. L'Agenzia dovrebbe inoltre fornire assistenza nello sviluppo e nell'aggiornamento delle strategie dell'Unione e degli Stati membri in materia di sicurezza delle reti e dei sistemi informativi, in particolare per quanto riguarda la cibersicurezza, promuovere la loro diffusione e seguire i progressi della loro attuazione. ***Dato che gli errori umani sono uno dei rischi specifici per la***

pubblici e, ***se del caso***, "formare i formatori" al fine di assistere gli Stati membri nello sviluppo di capacità di formazione autonome.	***cibersicurezza, l'Agenzia*** dovrebbe inoltre offrire formazione e materiale formativo agli enti pubblici e, ***nella massima misura possibile***, "formare i formatori" al fine di assistere gli Stati membri ***e le istituzioni e agenzie dell'Unione*** nello sviluppo di capacità di formazione autonome.

Or. en

Emendamento 118
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 18

Testo della Commissione	*Emendamento*
(18) L'Agenzia dovrebbe aggregare e analizzare le relazioni nazionali dei CSIRT e della CERT-UE, definendo norme, lingua e terminologia comuni per lo scambio delle informazioni. Dovrebbe inoltre coinvolgere ***il settore*** privato, nel quadro della direttiva NIS che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo con la creazione della rete di CSIRT.	(18) L'Agenzia dovrebbe aggregare e analizzare le relazioni nazionali dei CSIRT e della CERT-UE, definendo norme, lingua e terminologia comuni per lo scambio delle informazioni. Dovrebbe inoltre coinvolgere ***i settori*** privato ***e pubblico***, nel quadro della direttiva NIS che ha gettato le basi per lo scambio volontario di informazioni tecniche a livello operativo con la creazione della rete di CSIRT.

Or. en

Emendamento 119
Barbara Kappel

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come	(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come

facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.	facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza***, rispettando le competenze nazionali degli Stati membri riguardo a questioni di specifico interesse nazionale.***
	Or. en

Emendamento 120
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.	(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe ***convocare le autorità degli Stati membri e fornire assistenza nel coordinamento della loro risposta,*** raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.
	Or. en

Emendamento 121
Martina Werner

Proposta di regolamento
Considerando 19

Testo della Commissione	*Emendamento*
(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.	(19) L'Agenzia dovrebbe contribuire a una risposta a livello di UE in caso di crisi e incidenti di cibersicurezza transfrontalieri su vasta scala. Nell'ambito di questa funzione dovrebbe raccogliere le informazioni pertinenti e agire come facilitatore tra la rete di CSIRT e la comunità tecnica e i responsabili decisionali nella gestione delle crisi. Inoltre, potrebbe sostenere la gestione degli incidenti dal punto di vista tecnico, ***ad esempio*** agevolando lo scambio di soluzioni tecniche tra gli Stati membri e contribuendo alla comunicazione pubblica. L'Agenzia dovrebbe sostenere il processo provando le modalità di tale cooperazione attraverso esercitazioni annuali di cibersicurezza.

Or. en

Emendamento 122
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

Proposta di regolamento
Considerando 26

Testo della Commissione	*Emendamento*
(26) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni dell'Unione, l'Agenzia ha bisogno di analizzare i rischi attuali ***e quelli*** emergenti. A tal fine, in cooperazione con	(26) Per comprendere meglio le sfide nel campo della cibersicurezza e al fine di fornire consulenza strategica a lungo termine agli Stati membri e alle istituzioni dell'Unione, l'Agenzia ha bisogno di analizzare i rischi***, gli incidenti, le minacce e le vulnerabilità*** attuali ***ed*** emergenti. A

gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'Agenzia dovrebbe raccogliere le informazioni pertinenti, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'Agenzia dovrebbe inoltre assistere gli Stati membri e le istituzioni, le agenzie e gli organi dell'Unione nell'individuazione delle tendenze emergenti e nella prevenzione dei problemi connessi alla cibersicurezza attraverso l'analisi di minacce ***e*** incidenti.	tal fine, in cooperazione con gli Stati membri e se del caso con gli istituti di statistica e con altri organismi, l'Agenzia dovrebbe raccogliere le informazioni pertinenti, analizzare le tecnologie emergenti e fornire valutazioni su temi specifici in relazione agli impatti previsti dal punto di vista sociale, giuridico, economico e regolamentare delle innovazioni tecnologiche sulla sicurezza delle reti e dell'informazione, in particolare sulla cibersicurezza. L'Agenzia dovrebbe inoltre assistere gli Stati membri e le istituzioni, le agenzie e gli organi dell'Unione nell'individuazione delle tendenze emergenti e nella prevenzione dei problemi connessi alla cibersicurezza attraverso l'analisi di minacce***,*** incidenti ***e vulnerabilità***.

Or. en

Emendamento 123
Răzvan Popa

Proposta di regolamento
Considerando 27

Testo della Commissione	*Emendamento*
(27) Al fine di aumentare la resilienza dell'Unione, l'Agenzia dovrebbe sviluppare l'eccellenza in materia di sicurezza delle infrastrutture di internet e delle infrastrutture critiche, fornendo consulenza, orientamenti e migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'Agenzia dovrebbe sviluppare e mantenere il "polo d'informazione" dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dalle agenzie e dagli organi dell'UE e nazionali.	(27) Al fine di aumentare la resilienza dell'Unione, l'Agenzia dovrebbe sviluppare l'eccellenza in materia di sicurezza delle infrastrutture di internet e delle infrastrutture critiche, fornendo consulenza, orientamenti e migliori pratiche. Allo scopo di agevolare l'accesso a informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle possibili soluzioni, l'Agenzia dovrebbe sviluppare e mantenere il "polo d'informazione" dell'Unione, un portale che gli utenti possano utilizzare come sportello unico per accedere alle informazioni sulla cibersicurezza provenienti dalle istituzioni, dalle agenzie e dagli organi dell'UE e nazionali. ***Facilitare l'accesso a***

informazioni meglio strutturate sui rischi connessi alla cibersicurezza e sulle potenziali misure correttive dovrebbe aiutare gli Stati membri a rafforzare le loro capacità, ad allineare le loro pratiche e a migliorare così la resilienza generale agli attacchi.

Or. ro

Emendamento 124
Seán Kelly

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni ***di igiene informatica*** a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di

protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

base in materia di autenticazione ***a più fattori, installazione di patch, criptaggio, microsegmentazione, principi del minimo privilegio*** e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi. ***Il minimo privilegio fa riferimento al caso in cui agli utenti è concesso soltanto l'accesso minimo necessario per lo svolgimento del loro lavoro e nulla di più, e ai componenti di sistema è attribuita soltanto la funzione minima necessaria a svolgere il proprio compito e nulla di più. Il principio della microsegmentazione richiede che l'intero ambiente informatico o di rete sia diviso in sottosistemi e sottoreti più piccoli, per renderlo più gestibile ai fini della protezione e contenere i danni nel caso di compromissione di un unico sottosistema o sottorete.***

Or. en

Emendamento 125
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla ***cibersicurezza*** e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla ***sicurezza informatica*** e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione ***e la pubblicazione*** di relazioni ***e guide***

a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli ***di base*** in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli in materia di autenticazione***, criptaggio, anonimizzazione*** e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi ***e l'uso sicuro dei servizi e nel diffondere, a livello di Unione, la sicurezza e la privacy fin dalla progettazione nonché la comunicazione degli incidenti e delle relative soluzioni***. ***Ai fini del raggiungimento di tale obiettivi, l'Agenzia dovrebbe utilizzare al meglio le migliori pratiche e l'esperienza disponibili, in particolare delle istituzioni universitarie e dei ricercatori che si occupano di sicurezza informatica.***

Or. en

Motivazione

Emendamento volto a specificare nel dettaglio gli obiettivi che sono in linea con il contenuto degli articoli.

Emendamento 126
Martina Werner

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini ***e*** organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui ***e*** organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini***,*** organizzazioni ***e imprese***. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui***,*** organizzazioni ***e imprese*** mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri ***e l'alfabetizzazione digitale*** e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi. ***Dato che gli errori dei singoli e la mancata conoscenza dei rischi informatici sono un fattore importante di incertezza nella cibersicurezza, all'Agenzia dovrebbero essere fornite risorse adeguate per poter esercitare tale funzione nella massima misura possibile.***

Or. en

Emendamento 127
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi ***e dei prodotti, dei processi, dei servizi e dei sistemi TIC, conformemente al principio della sicurezza fin dalla progettazione e per impostazione predefinita, fornendo allo stesso tempo agli utenti finali orientamenti in materia di migliori pratiche di igiene informatica, anche attraverso campagne di sensibilizzazione***.

Emendamento 128
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	(28) L'Agenzia dovrebbe contribuire ***attivamente*** a sensibilizzare l'opinione pubblica sui rischi***, le minacce e le vulnerabilità*** connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico***, a partire dalle scuole,*** destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

Emendamento 129
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in ***linea con il piano d'azione per l'istruzione digitale e in*** cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

Or. en

Emendamento 130
Michał Boni, Henna Virkkunen, Massimiliano Salini, Gunnar Hökmark, Marian-Jean Marinescu

Proposta di regolamento
Considerando 28

Testo della Commissione	*Emendamento*
(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.	(28) L'Agenzia dovrebbe contribuire a sensibilizzare l'opinione pubblica sui rischi connessi alla cibersicurezza e fornire orientamenti in materia di buone pratiche per i singoli utenti destinati a cittadini e organizzazioni. Dovrebbe altresì contribuire a promuovere migliori pratiche***, l'igiene informatica*** e soluzioni a livello di singoli individui e organizzazioni mediante la raccolta e l'analisi delle informazioni disponibili al pubblico relative agli incidenti di rilievo, come pure mediante l'elaborazione di relazioni finalizzate a fornire orientamenti a imprese e cittadini e a migliorare il livello complessivo di preparazione e resilienza. L'Agenzia dovrebbe inoltre organizzare regolarmente, in cooperazione con le istituzioni, gli organi, gli uffici e le agenzie degli Stati membri e dell'Unione campagne d'informazione e di sensibilizzazione del pubblico destinate agli utenti finali, allo scopo di promuovere comportamenti online individuali più sicuri e di accrescere la consapevolezza circa le potenziali minacce del ciberspazio, compresa la criminalità informatica, ad esempio phishing, botnet, frodi finanziarie e bancarie, nonché di promuovere consigli di base in materia di autenticazione e protezione dei dati. L'Agenzia dovrebbe svolgere un ruolo centrale nell'accelerare la sensibilizzazione degli utenti finali sulla sicurezza dei dispositivi.

Or. en

Emendamento 131
Martina Werner

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.	(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA), l'Agenzia del sistema globale di navigazione satellitare europeo (GSA)***, la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE), il Comitato di risoluzione unico (SRB), l'Autorità europea degli strumenti finanziari e dei mercati (ESMA), altre autorità di vigilanza europee e nazionali, ove opportuno, l'organizzazione europea di normazione (OEN), i portatori di interessi pertinenti, ove opportuno,*** e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

Emendamento 132
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella ***cibersicurezza***. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della ***cibersicurezza*** che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.	(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella ***sicurezza informatica***. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della ***sicurezza informatica*** che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti. ***È opportuno istituire partenariati con le istituzioni universitarie che hanno avviato iniziative di ricerca nei settori pertinenti, mentre il contributo delle organizzazioni dei consumatori e di altre organizzazioni***

dovrebbe giungere attraverso canali adeguati ed essere sempre oggetto di analisi.

Or. en

Motivazione

Introduzione del concetto secondo cui l'ENISA dovrebbe beneficiare dell'insieme delle conoscenze disponibili.

Emendamento 133
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi,	(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, ***le autorità di vigilanza dell'UE e le altre autorità competenti,*** le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), ***la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE), il comitato europeo per la protezione dei dati (EDPB),*** l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di

l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.	portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.
	Or. en

Emendamento 134
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un	(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, ***le autorità di vigilanza dell'UE e le altre autorità competenti,*** le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), ***la Banca centrale europea (BCE), l'Autorità bancaria europea (ABE),*** l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei

impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

Or. en

Emendamento 135
Evžen Tošenovský

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi,	(30) Per conseguire appieno i propri obiettivi, l'Agenzia dovrebbe instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), ***l'Agenzia del GNSS europeo (GSA),*** l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con gli organismi incaricati dell'applicazione delle norme su aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di questi ultimi,

l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.	l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

Or. en

Emendamento 136
Răzvan Popa

Proposta di regolamento
Considerando 30

Testo della Commissione	*Emendamento*
(30) Per conseguire appieno i propri obiettivi, l'Agenzia ***dovrebbe*** instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze e migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.	(30) Per conseguire appieno i propri obiettivi, l'Agenzia ***deve*** instaurare rapporti con le istituzioni, le agenzie e gli organismi pertinenti, compresi la CERT-UE, il Centro europeo per la lotta alla criminalità informatica (EC3) di Europol, l'Agenzia europea per la difesa (AED), l'Agenzia europea per la gestione operativa dei sistemi IT su larga scala (eu-LISA), l'Agenzia europea per la sicurezza aerea (EASA) e tutte le agenzie dell'UE coinvolte nella cibersicurezza. Dovrebbe inoltre instaurare rapporti con le autorità competenti in materia di protezione dei dati, al fine di scambiare conoscenze***,*** ***formare*** e ***scambiare*** migliori pratiche e fornire consulenza sugli aspetti della cibersicurezza che potrebbero avere un impatto sulle loro attività. I rappresentanti delle autorità di contrasto e delle autorità preposte alla protezione dei dati nazionali e dell'Unione dovrebbero poter essere rappresentati nel gruppo permanente di portatori di interessi dell'Agenzia. Nei contatti con le autorità di contrasto sugli aspetti relativi alla sicurezza delle reti e dell'informazione che possono avere un impatto sull'attività di tali autorità, l'Agenzia dovrebbe avvalersi dei canali di informazione e delle reti esistenti.

Or. ro

Emendamento 137
Evžen Tošenovský

Proposta di regolamento
Considerando 32

Testo della Commissione	*Emendamento*
(32) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti di cibersicurezza, l'Agenzia dovrebbe organizzare ***ogni anno*** esercitazioni di cibersicurezza a livello di Unione ***e***, su loro richiesta, assistere le istituzioni, le agenzie e gli organi degli Stati membri e dell'UE nell'organizzazione delle esercitazioni.	(32) Al fine di rafforzare la preparazione dell'Unione nel rispondere agli incidenti di cibersicurezza, l'Agenzia dovrebbe organizzare esercitazioni di cibersicurezza a livello di Unione***. La frequenza delle esercitazioni dovrebbe rispecchiare quella di attività simili effettuate a livello nazionale e internazionale e tenere conto, in particolare, delle esercitazioni di cibersicurezza svolte dalla NATO.*** Su loro richiesta, ***l'Agenzia dovrebbe*** assistere le istituzioni, le agenzie e gli organi degli Stati membri e dell'UE nell'organizzazione delle esercitazioni.

Or. en

Emendamento 138
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 35

Testo della Commissione	*Emendamento*
(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare ***i loro*** standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria cibersicurezza. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi ***alle norme*** in materia di cibersicurezza. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi	(35) L'Agenzia dovrebbe incoraggiare gli Stati membri***, i fabbricanti*** e i fornitori di servizi a innalzare ***gli*** standard di sicurezza generale ***dei loro prodotti, processi, servizi e sistemi TIC, che dovrebbero essere conformi agli obblighi di base in materia di sicurezza, in linea con il principio della sicurezza fin dalla progettazione e per impostazione predefinita,*** in modo che tutti gli utenti di internet possano ***essere sicuri e incentivati ad*** adottare le misure necessarie a garantire la propria cibersicurezza In particolare, i fornitori di servizi e i fabbricanti di

offerti nel mercato interno e rivolgere avvertimenti ai fornitori ***e*** ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti ***e*** servizi.

prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi ***agli obblighi di base*** in materia di cibersicurezza***, mentre gli importatori e i distributori dovrebbero garantire che i prodotti, processi, servizi e sistemi TIC che immettono sul mercato dell'UE siano conformi ai requisiti applicabili e non presentino un rischio per i consumatori europei***. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di cibersicurezza dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori ***e*** ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti***, processi,*** servizi ***e sistemi***.

Or. en

Emendamento 139
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 35

Testo della Commissione	*Emendamento*
(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria ***cibersicurezza***. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di ***cibersicurezza***. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di ***cibersicurezza*** dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza,	(35) L'Agenzia dovrebbe incoraggiare gli Stati membri e i fornitori di servizi a innalzare i loro standard di sicurezza generale in modo che tutti gli utenti di internet possano adottare le misure necessarie a garantire la propria ***sicurezza informatica e non consentire la vendita o l'uso di dispositivi che non rispettano le condizioni minime di sicurezza (ad esempio contenenti componenti hardware, software o firmware con vulnerabilità sfruttabili in materia di sicurezza, password o codici di accesso non modificabili o in chiaro, non in grado di accogliere aggiornamenti opportunamente autenticati e affidabili, privi di un'idonea gerarchia di rimedi del***

ivi inclusa la ***cibersicurezza***, dei loro prodotti e servizi.	***fabbricante o del fornitore o senza un'adeguata documentazione del ciclo di vita)***. In particolare, i fornitori di servizi e i fabbricanti di prodotti dovrebbero ritirare o riciclare i prodotti e i servizi non conformi alle norme in materia di ***sicurezza informatica***. In collaborazione con le autorità competenti, l'ENISA può diffondere informazioni sul livello di ***sicurezza informatica*** dei prodotti e dei servizi offerti nel mercato interno e rivolgere avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la ***sicurezza informatica***, dei loro prodotti e servizi.

Or. en

Motivazione

Introduzione del concetto di responsabilità per i prodotti, i servizi e la sicurezza, da delineare in termini pratici nei diversi articoli.

Emendamento 140
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 35

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

avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti e servizi.	avvertimenti ai fornitori e ai fabbricanti imponendo loro di migliorare la sicurezza, ivi inclusa la cibersicurezza, dei loro prodotti e servizi. ***L'Agenzia dovrebbe collaborare con i soggetti interessati all'elaborazione di un approccio a livello dell'UE relativo alla divulgazione responsabile delle vulnerabilità e dovrebbe promuovere le migliori pratiche in tale settore.***

Or. en

Emendamento 141
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Gunnar Hökmark, Marian-Jean Marinescu

Proposta di regolamento
Considerando 36 bis (nuovo)

Testo della Commissione	*Emendamento*
	(36 bis) Le norme sono uno strumento volontario basato sulle esigenze del mercato, che forniscono requisiti tecnici e orientamenti e sono il risultato di un processo aperto, trasparente e inclusivo. L'Agenzia dovrebbe regolarmente consultare le organizzazioni europee di normazione e cooperare strettamente con esse, in particolare nell'elaborare sistemi europei di certificazione della cibersicurezza.

Or. en

Emendamento 142
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 37

Testo della Commissione	*Emendamento*
(37) I problemi di cibersicurezza sono questioni globali. È necessaria una più stretta cooperazione internazionale per migliorare gli standard di sicurezza, anche definendo norme di comportamento comuni, condividendo le informazioni e promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'Agenzia dovrebbe sostenere una maggiore partecipazione e cooperazione dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo, se del caso, le competenze e le analisi necessarie alle istituzioni, agli organi e agli organismi dell'Unione interessati.	(37) I problemi di cibersicurezza sono questioni globali. È necessaria una più stretta cooperazione internazionale per migliorare gli standard di sicurezza, anche definendo norme di comportamento ***e codici di condotta*** comuni, ***utilizzando norme internazionali,*** condividendo le informazioni e promuovendo una più celere cooperazione internazionale nel fornire una risposta alle questioni relative alla sicurezza delle reti e dell'informazione nonché un approccio globale comune a tali questioni. A tale scopo l'Agenzia dovrebbe sostenere una maggiore partecipazione e cooperazione dell'Unione con i paesi terzi e le organizzazioni internazionali fornendo, se del caso, le competenze e le analisi necessarie alle istituzioni, agli organi e agli organismi dell'Unione interessati.

Or. en

Emendamento 143
Csaba Molnár

Proposta di regolamento
Considerando 40

Testo della Commissione	*Emendamento*
(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio	(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio

regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.	regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione. ***Alla luce dei compiti altamente tecnici e scientifici dell'Agenzia, è opportuno che il consiglio di amministrazione sia costituito da membri con un elevato livello di esperienza riguardo a questioni che rientrano nell'ambito delle missioni dell'Agenzia.***
	Or. en

Emendamento 144
Pilar del Castillo Vera

Proposta di regolamento
Considerando 40

Testo della Commissione	*Emendamento*
(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.	(40) Il consiglio di amministrazione, composto dagli Stati membri e dalla Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione. ***Tenuto conto del carattere altamente tecnico della missione dell'Agenzia, i membri del consiglio di amministrazione dovrebbero avere un'idonea esperienza riguardo a questioni che rientrano nell'ambito della missione dell'Agenzia.***

Or. en

Emendamento 145
Michał Boni, Henna Virkkunen, Massimiliano Salini

Proposta di regolamento
Considerando 40

Testo della Commissione	*Emendamento*
(40) Il consiglio di amministrazione, ***composto dagli*** Stati membri e ***dalla*** Commissione, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.	(40) Il consiglio di amministrazione, ***che rappresenta gli*** Stati membri e ***la*** Commissione ***nonché i portatori di interessi rilevanti ai fini degli obiettivi dell'Agenzia***, dovrebbe definire l'orientamento generale delle operazioni dell'Agenzia e garantire che questa svolga i propri compiti conformemente al presente regolamento. Il consiglio di amministrazione dovrebbe godere dei poteri necessari per formare il bilancio, verificarne l'esecuzione, adottare l'opportuna regolamentazione finanziaria, stabilire procedure di lavoro trasparenti per l'iter decisionale dell'Agenzia, adottare il documento unico di programmazione dell'Agenzia, adottare il proprio regolamento interno, nominare il direttore esecutivo e decidere in merito all'estensione del suo mandato e in merito alla sua conclusione.

Or. en

Emendamento 146
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 41

Testo della Commissione	*Emendamento*
(41) Per garantire il funzionamento corretto ed efficace dell'Agenzia, la Commissione e gli Stati membri	(41) Per garantire il funzionamento corretto ed efficace dell'Agenzia, la Commissione e gli Stati membri

dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze ed esperienze professionali adeguate nelle aree funzionali. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori.	dovrebbero assicurare che le persone da nominare nel consiglio di amministrazione dispongano di competenze ed esperienze professionali adeguate nelle aree funzionali. La Commissione e gli Stati membri dovrebbero inoltre sforzarsi di limitare l'avvicendamento dei loro rispettivi rappresentanti nel consiglio di amministrazione, per assicurarne la continuità dei lavori. ***Dato l'elevato valore di mercato delle competenze necessarie nel lavoro dell'Agenzia, è opportuno garantire che la retribuzione e le condizioni sociali offerte a tutti i membri del personale dell'Agenzia siano competitive e garantiscano che i migliori professionisti scelgano di lavorarvi.***

Or. en

Motivazione

Al fine di disporre di un adeguato livello di competenze, l'ENISA in quanto datore di lavoro deve essere competitiva in un mercato altamente competitivo.

Emendamento 147
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 42

Testo della Commissione	*Emendamento*
(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del	(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del

programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio***, anche di genere,*** tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

Or. en

Emendamento 148
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 42

Testo della Commissione	*Emendamento*
(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di ***cibersicurezza***, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo	(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di ***sicurezza informatica***, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo

dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.	dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio***, anche di genere,*** tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

Or. en

Motivazione

L'emendamento mira a introdurre modifiche che apportano un equilibrio di genere a taluni livelli dell'ENISA.

Emendamento 149
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 42

Testo della Commissione	*Emendamento*
(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo	(42) Il corretto funzionamento dell'Agenzia esige che il direttore esecutivo

sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.	sia nominato in base ai meriti e alla comprovata esperienza amministrativa e manageriale, nonché alla competenza e all'esperienza acquisita in materia di cibersicurezza, e che le funzioni del direttore esecutivo siano svolte in completa indipendenza. Previa consultazione della Commissione, il direttore esecutivo dovrebbe elaborare una proposta di programma di lavoro dell'Agenzia e adottare tutte le misure necessarie a garantire l'adeguata esecuzione del programma. Il direttore esecutivo dovrebbe inoltre predisporre una relazione annuale da trasmettere al consiglio di amministrazione, fornire un progetto di stato di previsione delle entrate e delle spese dell'Agenzia e dare esecuzione al bilancio. Inoltre, è opportuno che il direttore esecutivo abbia la possibilità di istituire gruppi di lavoro ad hoc per affrontare questioni specifiche, in particolare di natura tecnico-scientifica, giuridica o socio-economica. Il direttore esecutivo dovrebbe garantire che i membri dei gruppi di lavoro ad hoc siano scelti secondo i più elevati standard di competenza, tenendo in debito conto la necessità di garantire un equilibrio ***di genere*** tra le parti rappresentate, in base alle questioni specifiche, tra gli amministratori pubblici degli Stati membri, le istituzioni dell'Unione e il settore privato, compresi le imprese, gli utilizzatori e gli esperti del mondo accademico in materia di sicurezza delle reti e dell'informazione.

Or. en

Emendamento 150
Michał Boni, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia. ***Data l'importanza dei requisiti di certificazione per garantire la fiducia nell'internet degli oggetti (IoT), la Commissione dovrebbe vagliare specificamente le misure di attuazione volte a garantire l'armonizzazione degli standard di sicurezza paneuropei per i dispositivi connessi.***

Or. en

Emendamento 151
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le

organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'***adeguata*** rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	organizzazioni di consumatori***, le università*** e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia***, fornendo un contributo circa quali prodotti e servizi TIC includere in futuri sistemi europei di certificazione della sicurezza informatica***. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'***efficiente ed equa*** rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.

Or. en

Motivazione

Introduzione di principi guida per le strutture responsabili dei futuri sistemi di certificazione.

Emendamento 152
Martina Werner

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La

composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia. ***Il gruppo permanente di portatori di interessi dovrebbe avere la facoltà di suggerire l'elaborazione di proposte di sistemi di certificazione.***

Or. en

Emendamento 153
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, ***la società civile,*** le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi***, anche ricercando un equilibrio di genere,*** nell'ambito del lavoro svolto dall'Agenzia.

Or. en

Emendamento 154
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 44

Testo della Commissione	*Emendamento*
(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.	(44) È opportuno che l'Agenzia disponga di un gruppo permanente di portatori di interessi come organo consultivo, per garantire un dialogo regolare con il settore ***pubblico e*** privato, le organizzazioni di consumatori e gli altri soggetti interessati. Il gruppo permanente di portatori di interessi, istituito dal consiglio di amministrazione su proposta del direttore esecutivo, dovrebbe concentrarsi sulle questioni rilevanti per i portatori di interessi e sottoporle all'attenzione dell'Agenzia. La composizione del gruppo permanente di portatori di interessi e i compiti assegnati a tale gruppo, da consultare in particolare in merito al progetto di programma di lavoro, dovrebbero garantire un'adeguata rappresentanza dei portatori di interessi nell'ambito del lavoro svolto dall'Agenzia.

Or. en

Emendamento 155
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Gunnar Hökmark, Marian-Jean Marinescu

Proposta di regolamento
Considerando 46

Testo della Commissione	*Emendamento*
(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che l'Agenzia sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un	(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che l'Agenzia sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un

contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del mandato dell'Agenzia. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della responsabilità, la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.	contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. ***Un bilancio idoneo è essenziale per garantire che l'Agenzia disponga di capacità sufficienti ad adempiere tutti i suoi crescenti compiti e obiettivi***. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del mandato dell'Agenzia. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia. La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della responsabilità, la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.

Or. en

Emendamento 156
Răzvan Popa

Proposta di regolamento
Considerando 46

Testo della Commissione	*Emendamento*
(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che essa sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del mandato dell'Agenzia. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia.	(46) Per garantire all'Agenzia piena autonomia e indipendenza e consentirle di svolgere nuovi compiti aggiuntivi, compresi compiti urgenti imprevisti, è opportuno che essa sia dotata di un bilancio congruo e autonomo le cui entrate siano essenzialmente costituite da un contributo dell'Unione e da contributi provenienti da paesi terzi che partecipano alle attività dell'Agenzia. La maggior parte del personale dell'Agenzia dovrebbe essere impiegata nell'attuazione operativa del mandato dell'Agenzia. Allo Stato membro ospitante, o a qualsiasi altro Stato membro, dovrebbe essere consentito di contribuire volontariamente alle entrate dell'Agenzia.

La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della responsabilità, la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.	La procedura di bilancio dell'Unione dovrebbe restare applicabile a qualsiasi sovvenzione a carico del bilancio generale dell'Unione. Inoltre, ai fini della trasparenza e della responsabilità, ***nonché dell'efficacia in termini di spese,*** la revisione contabile dell'Agenzia dovrebbe essere svolta dalla Corte dei conti.
	Or. ro

Emendamento 157
Eva Kaili

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***dovrebbe*** essere ***considerata*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti ***e*** servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La ***certificazione*** non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***e l'autovalutazione dovrebbero*** essere ***considerate*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti***,*** servizi ***e processi*** TIC")***. La certificazione è*** effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. ***L'autovalutazione può essere effettuata dal fabbricante del prodotto o dall'operatore laddove la probabilità che si verifichi un incidente di cibersicurezza e/o che tale incidente provochi danni sostanziali alla società o una vasta parte di quest'ultima non è considerata elevata o sostanziale, tenuto conto dell'uso previsto del prodotto o servizio in questione da parte del fabbricante o del fornitore del servizio.*** La ***valutazione della***

conformità non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

Or. en

Emendamento 158
Martina Werner

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***dovrebbe*** essere ***considerata*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***e, ove consentito, l'autovalutazione, dovrebbero*** essere ***considerate*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC")***. La certificazione è*** effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. ***L'autovalutazione può essere effettuata dal fabbricante del prodotto o dal fornitore del servizio, come previsto dal nuovo quadro legislativo e precisato nel presente regolamento, laddove la probabilità che si verifichi un incidente di cibersicurezza o che tale incidente provochi danni sostanziali all'utente, alla società o a una parte di quest'ultima non è considerata elevata***. La certificazione

non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

Or. en

Emendamento 159
Peter Kouroumbashev, Carlos Zorrinho, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***dovrebbe*** essere ***considerata*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La ***certificazione*** non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***e l'autovalutazione, dovrebbero*** essere ***considerate*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC")***. La certificazione è*** effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. ***L'autovalutazione può essere effettuata dal fabbricante del prodotto o dall'operatore laddove la probabilità che si verifichi un incidente di cibersicurezza e/o che tale incidente provochi danni sostanziali alla società o a una vasta parte di quest'ultima non è considerata elevata, tenuto conto dell'uso previsto del prodotto o servizio in questione da parte del fabbricante o del fornitore del servizio.*** La

valutazione della conformità non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

Or. en

Emendamento 160
Marisa Matias, Clare Moody, Theresa Griffin

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***dovrebbe*** essere ***considerata*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione ***e l'autovalutazione dovrebbero*** essere ***considerate*** un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. ***L'autovalutazione può essere effettuata dalle PMI per la conformità al più basso livello di affidabilità.*** La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati ***e ciò deve essere debitamente comunicato ai consumatori e alle imprese***. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di

cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.

Or. en

Motivazione

Per ridurre i costi per le PMI dovrebbe esistere la possibilità di effettuare un'autovalutazione. Per garantire le minime conseguenze possibili sulla cibersicurezza, l'autovalutazione dovrebbe riguardare soltanto i livelli di affidabilità bassi. Considerato che neppure un alto livello di certificazione previene del tutto gli incidenti informatici, qualsiasi certificazione dovrebbe chiarire che i rischi informatici rimangono.

Emendamento 161
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche. ***Le imprese, inoltre,***

dovrebbero assicurare la sicurezza fin dalla progettazione e per impostazione predefinita dei loro prodotti e servizi TIC, tenendo conto dello stato dell'arte.

Or. en

Emendamento 162
Esther de Lange

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé la cibersicurezza dei prodotti e servizi TIC certificati. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme tecniche. ***Questi includono l'indicazione dell'eventuale capacità del prodotto e servizio TIC di svolgere le sue normali funzioni quando è disconnesso da internet.***

Or. en

Emendamento 163
Pilar del Castillo Vera

Proposta di regolamento
Considerando 47

Testo della Commissione	*Emendamento*
(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé ***la cibersicurezza dei*** prodotti e servizi ***TIC certificati***. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme ***tecniche***.	(47) La valutazione della conformità è la procedura atta a dimostrare se le prescrizioni specifiche relative a un prodotto, a un processo, a un servizio, a un sistema, a una persona o a un organismo sono state rispettate. Ai fini del presente regolamento, la certificazione dovrebbe essere considerata un tipo di valutazione della conformità concernente ***le pratiche e*** le caratteristiche di cibersicurezza di un prodotto, un processo, un servizio, un sistema o una combinazione di tali elementi ("prodotti e servizi TIC") effettuata da un soggetto terzo indipendente, diverso dal fabbricante del prodotto o dal fornitore del servizio. La certificazione non può garantire di per sé ***che i processi e i sistemi TIC certificati si traducano in*** prodotti e servizi ***sicuri dal punto di vista informatico***. Si tratta piuttosto di una procedura e di una metodologia tecnica volte ad attestare che i prodotti e i servizi TIC***, nonché i relativi sistemi e i processi,*** sono stati testati e che rispettano determinati requisiti di cibersicurezza stabiliti altrove, ad esempio specificati nelle norme ***pertinenti***.

Or. en

Emendamento 164
Pavel Telička, Carolina Punset, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 48 bis (nuovo)

Testo della Commissione	*Emendamento*
	(48 bis) Nonostante non sia possibile prevedere la futura evoluzione della tecnologia e del mercato, i fabbricanti dovrebbero tenere conto di tutte le minacce note nel momento in cui sviluppano i loro prodotti. I fabbricanti, inoltre, dovrebbero essere responsabili della qualità di un prodotto immesso sul mercato dell'UE, anche per quanto riguarda la ciberresilienza. Allo stesso tempo, i consumatori dovrebbero assumersi la propria parte di responsabilità seguendo le norme di base sull'igiene informatica, che potrebbero ridurre in modo significativo il numero di errori umani nell'ambito della cibersicurezza.

Or. en

Emendamento 165
Michał Boni, Seán Kelly, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 50

Testo della Commissione	*Emendamento*
(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non	(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non

sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo.	sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo. ***È necessario un approccio puntuale, al fine di assicurare che i servizi, i processi e i prodotti siano soggetti a opportuni sistemi di certificazione. Inoltre, è necessario un approccio basato sul rischio per un'identificazione e mitigazione efficaci dei rischi, pur riconoscendo che un unico sistema valido per tutti non è possibile.***

Or. en

Emendamento 166
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 50

Testo della Commissione	*Emendamento*
(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad	(50) Attualmente la certificazione della cibersicurezza di prodotti e servizi TIC è utilizzata solo in misura limitata. Quando esiste, è disponibile prevalentemente a livello di Stato membro o nell'ambito di sistemi promossi dall'industria. In tale contesto, un certificato rilasciato da un'autorità nazionale per la cibersicurezza non è, in linea di principio, riconosciuto dagli altri Stati membri. Le imprese pertanto potrebbero dover certificare i loro prodotti e servizi nei diversi Stati membri in cui operano, ad esempio ai fini della partecipazione a procedure nazionali di aggiudicazione degli appalti. Inoltre, stanno emergendo nuovi sistemi ma non sembra esservi un approccio coerente e olistico per quanto riguarda le questioni orizzontali relative alla cibersicurezza, ad

esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo.	esempio nel settore dell'internet degli oggetti. I sistemi esistenti presentano notevoli carenze e differenze in termini di copertura dei prodotti, livelli di affidabilità, criteri sostanziali e utilizzo effettivo. ***Il riconoscimento reciproco e la fiducia tra gli Stati membri è un elemento fondamentale in tal senso. L'ENISA ha un ruolo importante nell'aiutare gli Stati membri a sviluppare una struttura istituzionale solida e competenze in materia di protezione contro i potenziali attacchi informatici.***

Or. en

Emendamento 167
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 52

Testo della Commissione	*Emendamento*
(52) In considerazione di quanto precede, è necessario definire un quadro europeo di certificazione della ***cibersicurezza*** che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della ***cibersicurezza*** da sviluppare e che consenta di riconoscere e utilizzare i certificati per i prodotti e servizi TIC in tutti gli Stati membri. Il quadro europeo dovrebbe avere un duplice obiettivo: da un lato dovrebbe contribuire ad aumentare la fiducia nei prodotti e nei servizi TIC che sono stati certificati in base a detti sistemi. Dall'altro lato dovrebbe evitare il proliferare di certificazioni nazionali della ***cibersicurezza*** confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi dovrebbero essere non discriminatori e basati su norme tecniche ***internazionali*** e/o dell'Unione, a meno che tali norme non siano inefficaci o	(52) In considerazione di quanto precede, è necessario definire un quadro europeo di certificazione della ***sicurezza informatica*** che stabilisca i principali requisiti orizzontali per i sistemi europei di certificazione della ***sicurezza informatica*** da sviluppare e che consenta di riconoscere e utilizzare i certificati per i prodotti e servizi TIC in tutti gli Stati membri. Il quadro europeo dovrebbe avere un duplice obiettivo: da un lato dovrebbe contribuire ad aumentare la fiducia nei prodotti e nei servizi TIC che sono stati certificati in base a detti sistemi. Dall'altro lato dovrebbe evitare il proliferare di certificazioni nazionali della ***sicurezza informatica*** confliggenti o sovrapposte e ridurre così i costi per le imprese operanti nel mercato unico digitale. I sistemi dovrebbero essere ***improntati al principio della sicurezza fin dalla progettazione e ai principi di cui al regolamento (UE) 2016/679, essere*** non

inadeguate ai fini del conseguimento dei legittimi obiettivi dell'UE in tale ambito.	discriminatori e basati su norme tecniche ***ISO/IEC selezionate*** e/o dell'Unione, a meno che tali norme non siano inefficaci o inadeguate ai fini del conseguimento dei legittimi obiettivi dell'UE in tale ambito.

Or. en

Motivazione

Introduzione di principi guida per i sistemi di certificazione.

Emendamento 168
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 52 bis (nuovo)

Testo della Commissione	*Emendamento*
	(52 bis) I sistemi di certificazione dovrebbero essere basati sui sistemi già esistenti a livello nazionale e internazionale, apprendendo dai loro punti di forza attuali e analizzando e correggendo i punti deboli.

Or. en

Emendamento 169
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 52 ter (nuovo)

Testo della Commissione	*Emendamento*
	(52 ter) Occorrono soluzioni flessibili di cibersicurezza se si vuole che l'industria resti un passo avanti rispetto agli attacchi dolosi e alle minacce; pertanto, qualsiasi sistema di

certificazione dovrebbe evitare il rischio di una rapida obsolescenza.

Or. en

Emendamento 170
Gunnar Hökmark

Proposta di regolamento
Considerando 53

Testo della Commissione	*Emendamento*
(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.	(53) La Commissione dovrebbe avere la facoltà di adottare sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo. ***Gli attori dell'industria possono effettuare un'autovalutazione dei loro prodotti o servizi prima della certificazione, indicando in tal modo che il loro prodotto o servizio è pronto a iniziare il processo di certificazione, laddove ciò sia richiesto o necessario.***

Or. en

Emendamento 171
Peter Kouroumbashev, Carlos Zorrinho, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento

Considerando 53

Testo della Commissione	*Emendamento*
(53) La Commissione ***dovrebbe avere la facoltà di adottare*** sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.	(53) La Commissione***, il gruppo europeo per la certificazione della cibersicurezza e il gruppo di certificazione dei portatori di interessi dovrebbero proporre all'ENISA di preparare*** sistemi europei di certificazione della cibersicurezza relativi a gruppi specifici di prodotti e servizi TIC. Tali sistemi dovrebbero essere attuati e supervisionati dalle autorità nazionali di controllo della certificazione e i certificati rilasciati nel loro ambito dovrebbero essere validi e riconosciuti in tutta l'Unione. I sistemi di certificazione gestiti dall'industria o da altre organizzazioni private non dovrebbero rientrare nel campo di applicazione del regolamento. Tuttavia, gli organismi che li gestiscono possono proporre alla Commissione di considerarli come base per l'approvazione degli stessi come sistema europeo.

Or. en

Emendamento 172
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Considerando 53 bis (nuovo)

Testo della Commissione	*Emendamento*
	(53 bis) L'Agenzia e la Commissione dovrebbero utilizzare al meglio i sistemi di certificazione già esistenti a livello internazionale e/o dell'UE. L'ENISA dovrebbe essere in grado di valutare quali sistemi già in uso siano idonei allo scopo e possano essere integrati nella normativa europea in cooperazione con le organizzazioni di normazione dell'UE e, per quanto

possibile, riconosciuti a livello internazionale. Le buone pratiche esistenti dovrebbero essere raccolte e condivise tra gli Stati membri.

Or. en

Emendamento 173
Massimiliano Salini

Proposta di regolamento
Considerando 55

Testo della Commissione	*Emendamento*
(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti ***e*** i servizi TIC certificati nel loro ambito siano conformi ai requisiti specificati. Tali requisiti riguardano la capacità di resistere, a un determinato livello di ***affidabilità***, alle azioni che mirano a compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti e servizi TIC. I prodotti ***e*** i servizi TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei prodotti ***e*** nei servizi TIC specifici dovrebbero quindi essere	(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti***,*** i servizi ***e i processi*** TIC certificati nel loro ambito siano conformi ai requisiti specificati. Tali requisiti riguardano la capacità di resistere, a un determinato livello di ***rischio***, alle azioni che mirano a compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti***,*** servizi ***e processi*** TIC. I prodotti***,*** i servizi ***e i processi*** TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei prodotti***,*** nei servizi ***e nei***

ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche.

processi TIC specifici dovrebbero quindi essere ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche. ***Tutti gli attori coinvolti in una data filiera dovrebbero essere incoraggiati a sviluppare e adottare norme di sicurezza, norme tecniche e principi di sicurezza fin dalla progettazione in tutte le fasi del ciclo di vita del prodotto, del servizio o del processo; ogni sistema europeo di certificazione della cibersicurezza dovrebbe essere progettato per adeguarsi a tali requisiti.***

Or. en

Emendamento 174
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 55

Testo della Commissione	*Emendamento*
(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti e i servizi TIC certificati nel loro ambito siano conformi ai requisiti specificati. Tali requisiti riguardano la capacità di resistere, a un determinato livello di affidabilità, alle azioni che mirano a compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti e servizi TIC. I prodotti e i servizi TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare	(55) Lo scopo dei sistemi europei di certificazione della cibersicurezza dovrebbe essere quello di assicurare che i prodotti e i servizi TIC certificati nel loro ambito siano conformi ai requisiti specificati ***di cibersicurezza definiti in un elenco di controllo della valutazione dei rischi elaborato dall'ENISA***. Tali requisiti riguardano la capacità di resistere, a un determinato livello di affidabilità, alle azioni che mirano a compromettere la disponibilità, l'autenticità, l'integrità e la riservatezza dei dati conservati, trasmessi o trattati o le funzioni o i servizi offerti o accessibili tramite tali prodotti, processi, servizi e sistemi ai sensi del presente regolamento. Non è possibile definire dettagliatamente nel presente regolamento i requisiti di cibersicurezza per tutti i prodotti e servizi TIC. I prodotti e i servizi

requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei prodotti e nei servizi TIC specifici dovrebbero quindi essere ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche.	TIC e le relative esigenze di cibersicurezza sono talmente diversi che risulta molto difficile formulare requisiti generali in materia di cibersicurezza che siano validi in tutti i casi. È pertanto necessario adottare una nozione ampia e generale di cibersicurezza ai fini della certificazione, integrata da una serie di obiettivi di cibersicurezza specifici da prendere in considerazione al momento dell'elaborazione dei sistemi europei di certificazione della cibersicurezza. Le modalità con cui tali obiettivi saranno conseguiti nei prodotti e nei servizi TIC specifici dovrebbero quindi essere ulteriormente specificate dettagliatamente per ogni singolo sistema di certificazione adottato dalla Commissione, ad esempio facendo riferimento a norme o specifiche tecniche.

Or. en

Emendamento 175
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 56

Testo della Commissione	*Emendamento*
(56) La Commissione dovrebbe avere la facoltà di incaricare l'ENISA di preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema.	(56) La Commissione dovrebbe avere la facoltà di incaricare l'ENISA di preparare proposte di sistemi per prodotti o servizi TIC specifici***, sulla base di motivi giustificati (ovvero la frammentazione del mercato interno e l'esigenza di sostenere una normativa specifica dell'Unione o una richiesta consensuale degli Stati membri, del gruppo europeo per la certificazione della cibersicurezza e del gruppo permanente di portatori di interessi)***. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti di esecuzione.

Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.

Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.

Or. en

Emendamento 176
Evžen Tošenovský

Proposta di regolamento
Considerando 56

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

certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.

funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.

Or. en

Emendamento 177
Peter Kouroumbashev, Edouard Martin, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 56

Testo della Commissione	*Emendamento*
(56) ***La*** Commissione dovrebbe avere la facoltà di ***incaricare l'ENISA di*** preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti ***di esecuzione***. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e	(56) ***Dopo il completamento di un'idonea consultazione dei portatori di interessi da parte della*** Commissione***, l'ENISA*** dovrebbe avere la facoltà di preparare proposte di sistemi per prodotti o servizi TIC specifici. La Commissione, sulla base dei sistemi proposti dall'ENISA, dovrebbe quindi essere autorizzata ad adottare il sistema europeo di certificazione della cibersicurezza mediante atti ***delegati***. Tenendo conto dell'obiettivo generale e degli obiettivi di sicurezza individuati nel presente regolamento, i sistemi europei di certificazione della cibersicurezza adottati dalla Commissione dovrebbero specificare una serie minima di elementi riguardanti l'oggetto, l'ambito di applicazione e il funzionamento di ogni singolo sistema. Questi dovrebbero includere, tra l'altro, l'ambito di applicazione e l'oggetto della certificazione della cibersicurezza, compresi le categorie di prodotti e servizi TIC, l'indicazione particolareggiata dei requisiti di cibersicurezza, ad esempio con

il livello di affidabilità desiderato: di base, sostanziale e/o elevato.	riferimenti a norme o specifiche tecniche, i criteri e i metodi di valutazione specifici e il livello di affidabilità desiderato: di base, sostanziale e/o elevato.
	Or. en

Emendamento 178
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, ***poiché l'esistenza di requisiti di base in materia di sicurezza informatica riveste la massima importanza per i consumatori e per la sicurezza delle reti, alcune situazioni devono essere trattate obbligatoriamente e in modo armonizzato. Devono essere applicate soluzioni a tutti i servizi e dispositivi dei consumatori per far fronte alle sfide di un mondo sempre più connesso. Tali requisiti minimi potrebbero includere l'autenticazione, la sicurezza dei collegamenti e patch per le vulnerabilità individuate.*** Al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di

prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

Or. en

Motivazione

L'aggiunta intende risolvere rapidamente l'attuale mancanza di requisiti di base armonizzati in materia di sicurezza informatica e prevenire il rischio che i dispositivi dei consumatori siano trasformati in partecipanti botnet.

Emendamento 179
Michał Boni, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. ***Dopo questa fase iniziale e in funzione del livello di maturità di attuazione negli Stati membri e della criticità di un prodotto o di un servizio, è riconosciuto che, in futuro, potranno iniziare gradualmente a evolversi sistemi potenzialmente obbligatori per taluni prodotti, processi e servizi TIC, per le future generazioni di tecnologie e in risposta agli obiettivi strategici di domani.*** Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la

certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

Or. en

Emendamento 180
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione ***o*** nazionale. ***Tuttavia,*** al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie ***del presente regolamento o*** della legislazione dell'Unione ***e*** nazionale. ***La certificazione europea della cibersicurezza dovrebbe essere obbligatoria, ad esempio, per i prodotti, i processi, i servizi e i sistemi TIC con un rischio intrinseco elevato, destinati all'uso, tra l'altro, da parte di operatori di servizi essenziali, di minori, a casa, in autovetture connesse e su dispositivi medici.*** Al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

Or. en

Emendamento 181
Gunnar Hökmark

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente. ***Tuttavia, il presente regolamento dovrebbe lasciare impregiudicati i sistemi nazionali sui quali gli Stati membri mantengono la sovranità per la gestione di prodotti e servizi TIC utilizzati per soddisfare le esigenze del settore sovrano di tali Stati.***

Or. en

Emendamento 182
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe ***restare*** volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. ***Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.***	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe ***essere*** volontario ***per i livelli di affidabilità considerati di base o sostanziali, ma obbligatorio per i livelli di affidabilità considerati medi o elevati***, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione.

Or. en

Emendamento 183
Esther de Lange

Proposta di regolamento
Considerando 57

Testo della Commissione	*Emendamento*
(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data	(57) Il ricorso alla certificazione europea della cibersicurezza dovrebbe ***diventare obbligatorio nel lungo periodo, ma come punto di partenza può*** restare volontario, salvo disposizioni contrarie della legislazione dell'Unione o nazionale. Tuttavia, al fine di conseguire gli obiettivi del presente regolamento e di evitare la frammentazione del mercato interno, i sistemi e le procedure nazionali di certificazione della cibersicurezza per i prodotti e i servizi TIC contemplati da un sistema europeo di certificazione della

stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.	cibersicurezza dovrebbero cessare di produrre effetti a decorrere dalla data stabilita dalla Commissione mediante un atto di esecuzione. Inoltre, gli Stati membri non dovrebbero introdurre nuovi sistemi nazionali di certificazione per la certificazione della cibersicurezza di prodotti e servizi TIC già contemplati da un sistema europeo di certificazione della cibersicurezza esistente.

Or. en

Emendamento 184
Miapetra Kumpula-Natri

Proposta di regolamento
Considerando 57 bis (nuovo)

Testo della Commissione	*Emendamento*
	(57 bis) Quando propongono nuovi sistemi europei di cibersicurezza, l'ENISA e gli altri organi competenti dovrebbero prestare attenzione alle dinamiche competitive della proposta, assicurandosi specificamente che laddove il settore interessato abbia numerose piccole e medie imprese, come nel caso dello sviluppo software, i sistemi di certificazione non rappresentino un ostacolo all'accesso al mercato per le nuove imprese e le innovazioni.

Or. en

Emendamento 185
Csaba Molnár

Proposta di regolamento
Considerando 57 bis (nuovo)

Testo della Commissione	*Emendamento*

	(57 bis) L'obbligo di emettere una dichiarazione di prodotto recante informazioni strutturate in merito alla certificazione del prodotto, processo o servizio è introdotto per fornire al consumatore maggiori informazioni e per consentirgli di compiere una scelta consapevole, rafforzando in tal modo la fiducia nel mercato unico digitale.

Or. en

Emendamento 186
Miapetra Kumpula-Natri

Proposta di regolamento
Considerando 57 ter (nuovo)

Testo della Commissione	*Emendamento*
	(57 ter) I sistemi europei di cibersicurezza contribuiranno ad armonizzare e unificare le pratiche in tale settore nell'UE. Essi, tuttavia, non devono diventare il livello minimo di cibersicurezza. La progettazione di sistemi europei di cibersicurezza dovrebbe tenere conto delle innovazioni nel settore della cibersicurezza e consentirne l'ulteriore sviluppo.

Or. en

Emendamento 187
Martina Werner

Proposta di regolamento
Considerando 58

Testo della Commissione	*Emendamento*
(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero	(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero

essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.	essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento. ***L'Agenzia dovrebbe effettuare audit per garantire un livello di qualità e diligenza equivalente a quello degli organismi di valutazione della conformità, al fine di evitare un arbitraggio normativo. I risultati dovrebbero essere comunicati all'Agenzia, alla Commissione e al Parlamento e resi disponibili al pubblico.***

Or. en

Emendamento 188
Peter Kouroumbashev, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 58

Testo della Commissione	*Emendamento*
(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi	(58) In seguito all'adozione di un sistema europeo di certificazione della cibersicurezza, i fabbricanti di prodotti TIC o i fornitori di servizi TIC dovrebbero essere in grado di presentare una domanda di certificazione dei loro prodotti o servizi

a un organismo di valutazione della conformità di propria scelta. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.	a un organismo di valutazione della conformità di propria scelta***, ovunque nell'Unione***. Se soddisfano determinati requisiti stabiliti nel presente regolamento, gli organismi di valutazione della conformità dovrebbero essere accreditati da un organismo di accreditamento. L'accreditamento dovrebbe essere concesso per un periodo massimo di cinque anni, con la possibilità di rinnovarlo alle stesse condizioni, purché l'organismo di valutazione della conformità soddisfi i requisiti. Gli organismi di accreditamento dovrebbero revocare l'accreditamento di un organismo di valutazione della conformità se le condizioni per l'accreditamento non sono, o non sono più, soddisfatte o se le azioni intraprese da un organismo di valutazione della conformità sono contrarie alle disposizioni del presente regolamento.

Or. en

Emendamento 189
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Considerando 58 bis (nuovo)

Testo della Commissione	*Emendamento*
	(58 bis) L'Agenzia dovrebbe formulare chiari requisiti obbligatori di base in materia di sicurezza informatica, i quali dovrebbero essere proposti alla Commissione affinché ne promuova l'adozione sotto forma di atti vincolanti, per tutti i dispositivi informatici venduti nell'Unione o esportati dalla stessa. Tali requisiti dovrebbero essere sviluppati entro due anni dalla data di entrata in vigore del presente regolamento e in seguito dovrebbero essere rivisti ogni due anni al fine di garantire miglioramenti costanti e dinamici. I suddetti requisiti di base in materia di sicurezza informatica

dovrebbero prevedere, tra l'altro, che il dispositivo non contenga alcuna vulnerabilità nota della sicurezza e che sia in grado di accogliere aggiornamenti di sicurezza affidabili, che il fornitore notifichi alle autorità competenti le vulnerabilità note e ripari o sostituisca il dispositivo interessato, o che il fornitore riferisca quando terminerà l'assistenza di sicurezza per tale dispositivo.

Or. en

Motivazione

È importante creare un ambiente informatico resiliente per tutelare i diritti fondamentali degli utenti delle tecnologie dell'informazione dell'UE. 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.

Emendamento 190
Gunnar Hökmark

Proposta di regolamento
Considerando 58 bis (nuovo)

Testo della Commissione	*Emendamento*
	(58 bis) Le norme nazionali e internazionali già esistenti sviluppate sul mercato nonché gli accordi informali delle associazioni internazionali, in particolare la Internet Engineering Taskforce e il Consorzio mondiale del Web, dovrebbero essere tenuti in considerazione all'atto della preparazione delle proposte di sistemi.

Or. en

Emendamento 191
Peter Kouroumbashev, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento

Considerando 59

Testo della Commissione	*Emendamento*
(59) È necessario imporre a tutti gli Stati membri di designare un'autorità di controllo della certificazione della cibersicurezza per vigilare sulla conformità degli organismi di valutazione della conformità e dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio ai requisiti del presente regolamento e dei pertinenti sistemi di certificazione della cibersicurezza. Le autorità nazionali di controllo della certificazione dovrebbero trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio, svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Esse dovrebbero inoltre cooperare 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 di cibersicurezza.	(59) È necessario imporre a tutti gli Stati membri di designare un'autorità di controllo della certificazione della cibersicurezza per vigilare sulla conformità degli organismi di valutazione della conformità e dei certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio ai requisiti del presente regolamento e dei pertinenti sistemi di certificazione della cibersicurezza***, e garantire che i certificati europei di cibersicurezza siano riconosciuti nel loro territorio***. Le autorità nazionali di controllo della certificazione dovrebbero trattare i reclami presentati dalle persone fisiche o giuridiche in relazione ai certificati rilasciati dagli organismi di valutazione della conformità stabiliti nel loro territorio ***o in relazione al presunto mancato riconoscimento dei certificati nel loro territorio***, svolgere le indagini opportune sull'oggetto del reclamo e informare il reclamante dello stato e dell'esito delle indagini entro un termine ragionevole. Esse dovrebbero inoltre cooperare 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 di cibersicurezza ***o sul mancato riconoscimento dei certificati europei di cibersicurezza***.

Or. en

Emendamento 192
Peter Kouroumbashev, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 60 bis (nuovo)

Testo della Commissione	*Emendamento*
	(60 bis) Al fine di garantire un'applicazione coerente e adeguata alle esigenze future del quadro europeo di certificazione della cibersicurezza, è opportuno istituire un gruppo di certificazione dei portatori di interessi in seno all'ENISA. Tale gruppo dovrebbe essere costituito da esperti riconosciuti che rappresentano il mondo universitario, gli organismi di normazione, le organizzazioni dei consumatori, il settore delle TIC e gli operatori non pubblici di servizi essenziali quali definiti nell'allegato II della direttiva (UE) 2016/1148, che consiglieranno e assisteranno l'ENISA al fine di garantire un'attuazione e un'applicazione coerenti del quadro europeo di certificazione della cibersicurezza; assistere e cooperare strettamente con l'Agenzia nella preparazione e adozione delle proposte di sistemi di certificazione della cibersicurezza; raccomandare proposte di sistemi europei di certificazione della cibersicurezza e adottare pareri indirizzati alla Commissione relativi al mantenimento e alla revisione degli attuali sistemi europei di certificazione della cibersicurezza. Il gruppo di certificazione dei portatori di interessi dovrebbe essere istituito con l'obiettivo di apportare il contributo di esperti dei portatori di interessi pertinenti al quadro europeo di certificazione della cibersicurezza. La struttura del gruppo di certificazione dei portatori di interessi dovrebbe consentire di invitare membri ad hoc che contribuiscano all'attività di elaborazione, sviluppo o adozione di nuove proposte di sistemi.

Or. en

Emendamento 193

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

Proposta di regolamento
Considerando 63

Testo della Commissione	*Emendamento*
(63) Al fine di specificare ulteriori criteri per l'accreditamento degli organismi di valutazione della conformità, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. Durante i lavori preparatori la Commissione dovrebbe svolgere adeguate consultazioni, anche a livello di esperti. Tali consultazioni dovrebbero essere condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016. In particolare, per assicurare pari opportunità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti in concomitanza con gli esperti degli Stati membri e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione che si occupano della preparazione degli atti delegati.	(63) Al fine di specificare ulteriori criteri per l'accreditamento degli organismi di valutazione della conformità ***e garantire condizioni uniformi di attuazione del presente regolamento***, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. Durante i lavori preparatori la Commissione dovrebbe svolgere adeguate consultazioni, anche a livello di esperti ***e con tutti i portatori di interessi, compresi quelli che non partecipano ai gruppi summenzionati***. Tali consultazioni dovrebbero essere condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016. In particolare, per assicurare pari opportunità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti in concomitanza con gli esperti degli Stati membri e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione che si occupano della preparazione degli atti delegati.

Or. en

Emendamento 194
Martina Werner

Proposta di regolamento
Considerando 63

Testo della Commissione	*Emendamento*

(63) Al fine di specificare ulteriori criteri per l'accreditamento degli organismi di valutazione della conformità, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. Durante i lavori preparatori la Commissione dovrebbe svolgere adeguate consultazioni, anche a livello di esperti. Tali consultazioni dovrebbero essere condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016. In particolare, per assicurare pari opportunità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti in concomitanza con gli esperti degli Stati membri e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione che si occupano della preparazione degli atti delegati.	(63) Al fine di specificare ulteriori criteri per l'accreditamento degli organismi di valutazione della conformità, è opportuno delegare alla Commissione il potere di adottare atti conformemente all'articolo 290 del trattato sul funzionamento dell'Unione europea. Durante i lavori preparatori la Commissione dovrebbe svolgere adeguate consultazioni, anche a livello di esperti ***e con i portatori di interessi pertinenti, ove opportuno***. Tali consultazioni dovrebbero essere condotte nel rispetto dei principi stabiliti nell'accordo interistituzionale "Legiferare meglio" del 13 aprile 2016. In particolare, per assicurare pari opportunità di partecipazione alla preparazione degli atti delegati, il Parlamento europeo e il Consiglio dovrebbero ricevere tutti i documenti in concomitanza con gli esperti degli Stati membri e i loro esperti dovrebbero avere sistematicamente accesso alle riunioni dei gruppi di esperti della Commissione che si occupano della preparazione degli atti delegati.

Or. en

Emendamento 195
Peter Kouroumbashev, Edouard Martin, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 64

Testo della Commissione	*Emendamento*
(64) Al fine di garantire condizioni uniformi di esecuzione del presente regolamento, dovrebbero essere attribuite alla Commissione competenze di esecuzione ove previsto dal presente regolamento. È altresì opportuno che tali competenze siano esercitate conformemente al regolamento (UE) n. 182/2011.	***soppresso***

Or. en

Emendamento 196
Peter Kouroumbashev, Edouard Martin, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Considerando 65

Testo della Commissione	*Emendamento*
(65) ***La procedura d'esame dovrebbe essere utilizzata per l'adozione degli*** atti ***di esecuzione*** sui sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC; sulle modalità di conduzione delle indagini da parte dell'Agenzia; sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di controllo della certificazione alla Commissione.	(65) ***Si potrebbero adottare, inoltre,*** atti ***delegati*** sui sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC; sulle modalità di conduzione delle indagini da parte dell'Agenzia; sulle circostanze, sui formati e sulle procedure delle notifiche degli organismi di valutazione della conformità accreditati da parte delle autorità nazionali di controllo della certificazione alla Commissione.

Or. en

Emendamento 197
Barbara Kappel

Proposta di regolamento
Considerando 68 bis (nuovo)

Testo della Commissione	*Emendamento*
	(68 bis) I prodotti e i servizi TIC costituiscono prodotti di consumo per la comunicazione elettronica, così come altri prodotti di consumo e prodotti orientati al consumatore che sono connessi, come i prodotti per le case intelligenti e i contatori intelligenti, che registrano e trasmettono informazioni per via digitale.

Or. de

Emendamento 198
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 1 – comma 1 – parte introduttiva

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

Or. en

Emendamento 199
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 1 – comma 1 – lettera a

Testo della Commissione	*Emendamento*
(a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, l'Agenzia dell'UE per la ***cibersicurezza***, di seguito denominata "l'Agenzia" e	(a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA, l'Agenzia dell'UE per la ***ciberresilienza***, di seguito denominata "l'Agenzia" e *(La modifica si applica all'intero testo e l'approvazione dell'emendamento implica adeguamenti in tutto il testo).*

Or. en

Emendamento 200
Barbara Kappel

Proposta di regolamento
Articolo 1 – comma 1 – lettera a

Testo della Commissione	*Emendamento*
(a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA,	(a) stabilisce gli obiettivi, i compiti e gli aspetti organizzativi dell'ENISA,

l'Agenzia dell'UE per la cibersicurezza, di seguito denominata "l'Agenzia" ***e***	l'Agenzia dell'UE per la ***cibersicurezza***, di seguito denominata "l'Agenzia"

Or. en

Emendamento 201
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti ***e*** dei servizi TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione.	(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti***, dei processi,*** dei servizi ***e dei sistemi*** TIC nell'Unione. Tale quadro si applica fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione. *(La modifica si applica all'intero testo e l'approvazione dell'emendamento implica adeguamenti in tutto il testo).*

Or. en

Emendamento 202
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti ***e*** dei servizi TIC nell'Unione. Tale quadro si applica	(b) stabilisce un quadro per l'introduzione di sistemi europei di certificazione della cibersicurezza al fine di garantire un livello adeguato di cibersicurezza dei prodotti***,*** dei servizi ***e dei processi*** TIC nell'Unione. Tale quadro si

fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione.	applica fatte salve le disposizioni specifiche in materia di certificazione volontaria o obbligatoria in altri atti dell'Unione.

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". In questo modo si contribuirà a evitare la creazione di un processo orizzontale onnicomprensivo di certificazione di terzi per tutte le soluzioni di cibersicurezza.

Emendamento 203
Pilar del Castillo Vera

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

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

Or. en

Emendamento 204
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 1 – comma 1 – lettera b

Testo della Commissione	*Emendamento*

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

Or. en

Motivazione

La modifica si applica all'intero testo. L'approvazione dell'emendamento implica adeguamenti in tutto il testo.

Emendamento 205
Barbara Kappel

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

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

Or. en

Emendamento 206
Michał Boni, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 1 – comma 1 – lettera b

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

Or. en

Emendamento 207
Gunnar Hökmark

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

Testo della Commissione	*Emendamento*
	(b bis) tutte le azioni previste dal presente regolamento, in particolare per quanto concerne la preparazione, l'adozione e l'applicazione delle norme e delle specifiche tecniche che definiscono i requisiti tecnici e/o la metodologia di valutazione della sicurezza associata a un sistema di cibersicurezza, tengono conto dei principi della libera circolazione dei beni e dei servizi e della non discriminazione.

Or. en

Emendamento 208
Barbara Kappel

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

Testo della Commissione	*Emendamento*

(b bis) tutela gli interessi nazionali e la sicurezza degli Stati membri rispettando le loro competenze riguardo a questioni di specifico interesse nazionale.

Or. en

Emendamento 209
Olle Ludvigsson

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

Testo della Commissione	*Emendamento*
	Tutte le misure da adottare ai sensi del presente regolamento tengono in considerazione i principi della libera circolazione dei beni e dei servizi sanciti dal trattato sul funzionamento dell'Unione europea e sono non discriminatorie. Ciò riguarda, in particolare, la preparazione, l'adozione e l'applicazione delle norme e delle specifiche tecniche che definiscono i requisiti tecnici e/o la metodologia di valutazione della sicurezza associata a un sistema di cibersicurezza.

Or. en

Emendamento 210
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 2 – punto 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	(5 bis) "autorità nazionale di controllo della certificazione", un'autorità di uno Stato membro incaricata di svolgere sul suo territorio attività di monitoraggio, contrasto e supervisione connesse alla certificazione di sicurezza informatica;

Or. en

Emendamento 211
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 2 – punto 8

Testo della Commissione	*Emendamento*
(8) "minaccia informatica", qualsiasi circostanza o evento che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;	(8) "minaccia informatica", qualsiasi ***azione, compreso un comando automatizzato,*** circostanza o evento che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

Or. en

Emendamento 212
Peter Kouroumbashev, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 8

Testo della Commissione	*Emendamento*
(8) "minaccia informatica", qualsiasi ***circostanza o evento*** che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;	(8) "minaccia informatica", qualsiasi ***azione intenzionale, compreso un comando automatizzato,*** circostanza o evento che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

Or. en

Emendamento 213
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 2 – punto 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	(8 bis) "igiene informatica", istituzione di semplici misure di routine, come l'autenticazione a più fattori, l'installazione di patch, il criptaggio, la microsegmentazione e il privilegio minimo, che gli utenti e le imprese possono adottare per minimizzare i rischi derivanti da minacce informatiche e per meglio proteggersi online;

Or. en

Emendamento 214
Seán Kelly

Proposta di regolamento
Articolo 2 – punto 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	(8 bis) "igiene informatica", istituzione di semplici misure di routine, come l'autenticazione a più fattori, l'installazione di patch, il criptaggio, la microsegmentazione e il privilegio minimo, che gli utenti finali possono adottare per minimizzare i rischi derivanti da minacce informatiche e per meglio proteggersi online;

Or. en

Emendamento 215
Peter Kouroumbashev, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 8 bis (nuovo)

Testo della Commissione	*Emendamento*
	(8 bis) "incidente informatico", qualsiasi azione o evento intenzionale o non

intenzionale che potrebbe avere un impatto negativo sulla rete e sui sistemi informativi, sui loro utenti e sulle persone interessate;

Or. en

Emendamento 216
Pilar del Castillo Vera

Proposta di regolamento
Articolo 2 – punto 9

Testo della Commissione	*Emendamento*
(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici***, norme tecniche*** e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;	(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici e procedure definiti a livello di Unione ***e conformi alle norme o alle specifiche tecniche TIC come definite nel regolamento (UE) n. 1025/2012,*** che si applicano alla certificazione dei prodotti***, dei processi*** e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

Or. en

Emendamento 217
Marisa Matias, Henna Virkkunen, Michał Boni

Proposta di regolamento
Articolo 2 – punto 9

Testo della Commissione	*Emendamento*
(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione	(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche ***che tengono conto delle norme nazionali e internazionali già esistenti,*** e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti***, dei processi***

(TIC) che rientrano nell'ambito di applicazione del sistema;	e dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

Or. en

Emendamento 218
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 2 – punto 9

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

Or. en

Motivazione

L'ENISA può basare i propri sistemi sulle norme approvate dalle organizzazioni europee o internazionali ISO/IEC di normazione, inserendole ove opportuno nella certificazione, previa idonea selezione. Tale inclusione non dovrebbe sostituire l'esigenza di rispettare la norma; invece, la certificazione potrebbe essere facilitata da una prova pre-esistente della conformità alla norma.

Emendamento 219
Françoise Grossetête

Proposta di regolamento
Articolo 2 – punto 9

Testo della Commissione	*Emendamento*

(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti ***e*** dei servizi nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;	(9) "sistema europeo di certificazione della cibersicurezza", la serie completa di norme, requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano alla certificazione dei prodotti***, dei processi,*** dei servizi ***e dei sistemi*** nell'ambito delle tecnologie dell'informazione e della comunicazione (TIC) che rientrano nell'ambito di applicazione del sistema;

Or. fr

Motivazione

Occorre adottare un approccio sistemico che tenga conto dell'intero ciclo di vita di un sistema. La modifica dovrebbe essere estesa alle altre parti del testo che vi vanno riferimento.

Emendamento 220
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 9

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

Or. en

Emendamento 221
Pilar del Castillo Vera

Proposta di regolamento
Articolo 2 – punto 9

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

Or. en

Emendamento 222
Peter Kouroumbashev, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 9 bis (nuovo)

Testo della Commissione	*Emendamento*
	(9 bis) "sistema europeo di autocertificazione della cibersicurezza", la serie completa di norme, specifiche o requisiti tecnici, norme tecniche e procedure definiti a livello di Unione che si applicano all'autocertificazione dei prodotti, dei servizi e dei processi TIC che rientrano nell'ambito di applicazione del sistema;

Or. en

Motivazione

L'emendamento intende garantire che il progetto di regolamento riconosca l'autovalutazione come un'opzione praticabile. Il concetto di autovalutazione è ampiamente utilizzato in alcuni settori industriali e dovrebbe svolgere un ruolo nel futuro quadro dell'UE. Il requisito che tutti i futuri sistemi di certificazione siano valutati da terze parti per l'intera gamma dei prodotti TIC è eccessivamente oneroso.

Emendamento 223

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

Proposta di regolamento
Articolo 2 – punto 9 bis (nuovo)

Testo della Commissione	*Emendamento*
	(9 bis) "igiene informatica", l'autenticazione a più fattori, l'installazione di patch, il criptaggio e la microsegmentazione che riducono al minimo i rischi derivanti da minacce informatiche e applicano il principio del privilegio minimo;

Or. en

Emendamento 224
Peter Kouroumbashev, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 9 ter (nuovo)

Testo della Commissione	*Emendamento*
	(9 ter) "sistema europeo di cibersicurezza", un sistema europeo di certificazione o autocertificazione della cibersicurezza;

Or. en

Motivazione

L'emendamento intende anche garantire che il progetto di regolamento riconosca l'autovalutazione come un'opzione praticabile. Il concetto di autovalutazione è ampiamente utilizzato in alcuni settori industriali e dovrebbe svolgere un ruolo nel futuro quadro dell'UE. Il requisito che tutti i futuri sistemi di certificazione siano valutati da terze parti per l'intera gamma dei prodotti TIC è eccessivamente oneroso.

Emendamento 225
Gunnar Hökmark

Proposta di regolamento

Articolo 2 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un ***documento*** rilasciato ***da*** un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC ***soddisfa i requisiti specifici stabiliti*** da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un ***attestato*** rilasciato ***in seguito ad autovalutazione o tramite*** un organismo di valutazione della conformità ***accreditato*** che attesta che ***una determinata procedura di sviluppo o*** un determinato prodotto o servizio TIC ***è stato valutato con una metodologia standardizzata per la valutazione della conformità sulla base di norme di sicurezza specifiche stabilite*** da un sistema europeo di certificazione della cibersicurezza;

Or. en

Emendamento 226
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 2 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un ***documento*** rilasciato ***da*** un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un ***attestato*** rilasciato ***in seguito ad autovalutazione o tramite*** un organismo di valutazione della conformità ***accreditato*** che attesta che un determinato ***processo,*** prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

Or. en

Motivazione

In base alla complessità e al rischio, la certificazione tramite autovalutazione può essere una possibilità.

Emendamento 227
Martina Werner

Proposta di regolamento
Articolo 2 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità oppure ***in seguito ad autovalutazione, ove consentito,*** che attesta che un determinato prodotto***, processo*** o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

Or. en

Emendamento 228
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 2 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto***, processo*** o servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

Or. en

Motivazione

La modifica si applica all'intero testo. L'approvazione dell'emendamento implica adeguamenti in tutto il testo.

Emendamento 229
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 10

Testo della Commissione	*Emendamento*
(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto ***o*** servizio TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;	(10) "certificato europeo di cibersicurezza", un documento rilasciato da un organismo di valutazione della conformità che attesta che un determinato prodotto***,*** servizio ***o processo*** TIC soddisfa i requisiti specifici stabiliti da un sistema europeo di certificazione della cibersicurezza;

Or. en

Emendamento 230
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 2 – punto 11

Testo della Commissione	*Emendamento*
(11) "prodotto ***e*** servizio TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;	(11) "prodotto***, processo,*** servizio ***e sistema*** TIC", qualsiasi ***prodotto, servizio, processo, sistema o loro combinazione che costituisca un*** elemento o gruppo di elementi della rete e dei sistemi informativi; *(La modifica si applica all'intero testo e l'approvazione dell'emendamento implica adeguamenti in tutto il testo).*

Or. en

Emendamento 231
Pilar del Castillo Vera

Proposta di regolamento

Articolo 2 – punto 11

Testo della Commissione	*Emendamento*
(11) "prodotto e servizio TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;	(11) "prodotto e servizio TIC", qualsiasi ***prodotto, processo o servizi che costituisca un*** elemento o gruppo di elementi della rete e dei sistemi informativi;

Or. en

Emendamento 232
Peter Kouroumbashev, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 2 – punto 11

Testo della Commissione	*Emendamento*
(11) "prodotto ***e*** servizio TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;	(11) "prodotto**,** servizio ***e processo*** TIC", qualsiasi elemento o gruppo di elementi della rete e dei sistemi informativi;

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", al fine di evitare la creazione di un processo orizzontale onnicomprensivo di certificazione di terzi per tutte le soluzioni di cibersicurezza.

Emendamento 233
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody

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

Testo della Commissione	*Emendamento*
	(11 bis) "dispositivo elettronico di consumo", un dispositivo costituito da

componenti hardware e software che effettuano il trattamento di dati personali o si collegano a internet per il funzionamento di elettrodomestici domotici e di controllo domestico, sistemi per l'ufficio, apparecchiature e dispositivi di instradamento che collegano a una rete, come le TV intelligenti, i giocattoli e le console di gioco, assistenti virtuali o personali, dispositivi di streaming connessi, dispositivi indossabili nonché sistemi a comando vocale e di realtà virtuale;

Or. en

Motivazione

Per una maggiore efficienza nella definizione della governance del quadro di riferimento, il livello di affidabilità di base mira a certificare i prodotti o i processi TIC che rientrano nella categoria dei dispositivi IoT di consumo, come quelli elencati sopra. L'ambito di applicazione comprende dispositivi che non ricevono automaticamente aggiornamenti di sicurezza periodici e/o che non sono dotati di solide funzionalità di autenticazione; pertanto dovrebbe escludere dispositivi endpoint come i telefoni cellulari, i PC, i computer portatili e i tablet.

Emendamento 234
Olle Ludvigsson

Proposta di regolamento
Articolo 2 – punto 14

Testo della Commissione	*Emendamento*
(14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008;	(14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008***, definita mediante una norma***;

Or. en

Emendamento 235
Gunnar Hökmark

Proposta di regolamento

Articolo 2 – punto 14

Testo della Commissione	*Emendamento*
(14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008;	(14) "valutazione della conformità", la valutazione della conformità ai sensi dell'articolo 2, punto 12, del regolamento (CE) n. 765/2008***, definita mediante una norma;***

Or. en

Emendamento 236
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody

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

Testo della Commissione	*Emendamento*
	(16 bis) "sistema informativo sulle funzionalità", indicazione visiva dei dati sotto forma di etichetta finalizzata a fornire informazioni all'utente finale sulla funzionalità, la connettività e le caratteristiche sensoriali, cinetiche o di sicurezza di un dispositivo elettronico di consumo.

Or. en

Motivazione

L'introduzione di una definizione del concetto di "sistema informativo sulle funzionalità" è necessaria in quanto tali sistemi potrebbero fornire informazioni utili all'operatore e/o all'utente finale riguardo a specifiche funzionalità di sicurezza dei prodotti TIC che sono commercializzati.

Emendamento 237
Pavel Telička, Caroline Nagtegaal, Gesine Meissner

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

Testo della Commissione	*Emendamento*
	(16 bis) "autovalutazione", come definita sulla base del regolamento (CE) n. 768/2008, modulo H.

Or. en

(768/2008/CE, modulo H http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:218:0082:0128:it:PDF)

Emendamento 238
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Titolo 2

Testo della Commissione	*Emendamento*
ENISA – l'Agenzia dell'UE per la ***cibersicurezza***	ENISA – l'Agenzia dell'UE per la ***ciberresilienza***

Or. en

Emendamento 239
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 3 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di ***contribuire a*** un elevato livello di cibersicurezza nell'Unione.	1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di ***conseguire*** un elevato livello di ***ciberresilienza e, in particolare, di*** cibersicurezza nell'Unione.

Or. en

Emendamento 240
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 3 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di ***contribuire a*** un elevato livello di ***cibersicurezza*** nell'Unione.	1. L'Agenzia svolge i compiti che le sono attribuiti dal presente regolamento allo scopo di ***conseguire*** un elevato livello di ***sicurezza informatica*** nell'Unione.

Or. en

Motivazione

La modifica consiste nell'alzare il livello di ambizione, in linea con l'ambito di applicazione della proposta.

Emendamento 241
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 3 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. L'Agenzia assiste gli Stati membri e le istituzioni dell'Unione nella definizione di politiche e pratiche per una gestione responsabile e una divulgazione coordinata delle vulnerabilità dei prodotti e dei servizi TIC che non sono pubblicamente note.

Or. en

Motivazione

Tali politiche dovrebbero essere coerenti con le raccomandazioni e gli orientamenti definiti nelle norme internazionali ISO/IEC 29147:2014 e ISO/IEC 30111.

Emendamento 242
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 3 – paragrafo 3

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

Or. en

Motivazione

Non è opportuno estendere le limitazioni derivanti dai trattati.

Emendamento 243
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

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

Testo della Commissione	*Emendamento*
	3 bis. L'Agenzia assiste gli Stati membri e le istituzioni dell'Unione nella definizione di politiche e pratiche trasparenti per una gestione responsabile e una divulgazione coordinata delle vulnerabilità dei prodotti, dei processi, dei servizi e dei sistemi TIC che non sono pubblicamente note.

Or. en

Motivazione

I governi vengono a conoscenza delle vulnerabilità attraverso diversi canali e si trovano di fronte a interessi in competizione riguardo a quando e in che modo comunicare le vulnerabilità che hanno individuato. Per affrontare la questione occorre una politica solida, trasparente e responsabile da parte dei governi per gestire le procedure di esame della divulgazione di vulnerabilità. Sono pochi gli Stati membri che dispongono di tale politica e alla luce della realizzazione di una strategia per il mercato unico digitale dell'UE ciberresiliente e cibersicura, è opportuno ampliare il mandato dell'ENISA, per aiutare gli

Stati membri a definire la propria politica e a sviluppare un approccio coordinato e coerente a livello dell'UE.

Emendamento 244
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 4 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia opera come centro di competenze nel settore della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.	1. L'Agenzia opera come centro di competenze ***teoriche e pratiche*** nel settore della cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.

Or. en

Emendamento 245
Răzvan Popa

Proposta di regolamento
Articolo 4 – paragrafo 1

Testo della Commissione	*Emendamento*
1. L'Agenzia opera come centro di competenze ***nel settore della*** cibersicurezza grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.	1. L'Agenzia opera come centro di competenze ***per la*** cibersicurezza ***in Europa*** grazie alla sua indipendenza, alla qualità scientifica e tecnica delle consulenze e dell'assistenza fornite e delle informazioni che mette a disposizione, alla trasparenza delle procedure e dei metodi operativi utilizzati e alla diligenza nell'esecuzione dei suoi compiti.

Or. ro

Emendamento 246
Edouard Martin

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza.	2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza***, tra cui le politiche settoriali in tale ambito, al fine di aumentare la pertinenza delle politiche e della normativa dell'UE con una dimensione di cibersicurezza e di favorire la coerenza nella loro attuazione a livello nazionale***.

Or. fr

Emendamento 247
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza.	2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza ***e nell'accrescimento della consapevolezza tra i cittadini e le imprese***.

Or. en

Emendamento 248
Răzvan Popa

Proposta di regolamento
Articolo 4 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia assiste le istituzioni, le agenzie e gli organismi dell'Unione, come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza.	2. L'Agenzia ***fornisce consulenza e*** assiste le istituzioni, le agenzie e gli organismi dell'Unione, ***la Commissione,*** come pure gli Stati membri, nell'elaborazione e nell'attuazione di politiche relative alla cibersicurezza.

Or. ro

Emendamento 249
Martina Werner

Proposta di regolamento
Articolo 4 – paragrafo 3

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

Or. en

Emendamento 250
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 4 – paragrafo 4

Testo della Commissione	*Emendamento*

4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, su questioni relative alla cibersicurezza.	4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, ***comprese le organizzazioni della società civile, tra cui le organizzazioni dei consumatori e*** il settore privato, su questioni relative alla cibersicurezza.

Or. en

Emendamento 251
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 4 – paragrafo 4

Testo della Commissione	*Emendamento*
4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, su questioni relative alla ***cibersicurezza***.	4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, ***le organizzazioni di consumatori e altre organizzazioni della società civile***, su questioni relative alla ***sicurezza informatica***.

Or. en

Motivazione

Il riferimento al settore privato va adeguatamente esteso ad altre importanti parti interessate, soprattutto dal momento che il maggiore impatto è sui consumatori.

Emendamento 252
Răzvan Popa

Proposta di regolamento
Articolo 4 – paragrafo 4

Testo della Commissione	*Emendamento*
4. L'Agenzia promuove la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, ***su questioni relative alla*** cibersicurezza.	4. L'Agenzia promuove ***e consolida*** la cooperazione e il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, ***al fine di raggiungere un livello elevato di*** cibersicurezza ***negli Stati membri***.

Or. ro

Emendamento 253
Martina Werner

Proposta di regolamento
Articolo 4 – paragrafo 4

Testo della Commissione	*Emendamento*
4. L'Agenzia promuove la cooperazione ***e*** il coordinamento a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, su questioni relative alla cibersicurezza.	4. L'Agenzia promuove la cooperazione***,*** il coordinamento ***e la condivisione delle informazioni*** a livello di Unione tra gli Stati membri, le istituzioni, le agenzie e gli organismi dell'Unione e i portatori di interessi, compreso il settore privato, su questioni relative alla cibersicurezza.

Or. en

Emendamento 254
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 4 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'Agenzia rafforza le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella	5. L'Agenzia rafforza le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella

prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.	prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri***, e per svolgere i propri compiti di assistenza alle istituzioni dell'Unione nello sviluppo delle politiche in materia di cibersicurezza***.

Or. en

Emendamento 255
Edouard Martin

Proposta di regolamento
Articolo 4 – paragrafo 5

Testo della Commissione	*Emendamento*
5. L'Agenzia rafforza le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri.	5. L'Agenzia rafforza le capacità di cibersicurezza a livello di Unione per integrare l'azione degli Stati membri nella prevenzione delle minacce informatiche e nella reazione alle stesse, in particolare in caso di incidenti transfrontalieri***, conformemente alle disposizioni della direttiva (UE) 2016/1148***.

Or. fr

Emendamento 256
Răzvan Popa

Proposta di regolamento
Articolo 4 – paragrafo 5

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

Or. ro

Emendamento 257
Gunnar Hökmark

Proposta di regolamento
Articolo 4 – paragrafo 5

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

Or. en

Emendamento 258
Olle Ludvigsson

Proposta di regolamento
Articolo 4 – paragrafo 5

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

Or. en

Emendamento 259
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 4 – paragrafo 5 bis (nuovo)

Testo della Commissione	*Emendamento*

	5 bis. L'Agenzia ha le capacità per convocare le autorità degli Stati membri e fornire assistenza nel coordinamento della loro risposta, in particolare in caso di incidenti transfrontalieri.

Or. en

Emendamento 260
Barbara Kappel

Proposta di regolamento
Articolo 4 – paragrafo 6

Testo della Commissione	*Emendamento*
6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.	6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale***, senza trascurare gli specifici aspetti sensibili che riguardano le piccole e medie imprese***.

Or. en

Emendamento 261
Pavel Telička, Carolina Punset, Morten Løkkegaard, Caroline Nagtegaal, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 4 – paragrafo 6

Testo della Commissione	*Emendamento*
6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di	6. L'Agenzia dovrebbe promuovere l'uso della certificazione, anche contribuendo all'istituzione e al mantenimento di un apposito quadro di

certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza e di rafforzare in tal modo la fiducia nel mercato unico digitale.	certificazione della cibersicurezza a livello di Unione, conformemente al titolo III del presente regolamento, al fine di aumentare la trasparenza dell'affidabilità dei prodotti e dei servizi TIC in termini di cibersicurezza***, di ridurre la frammentazione del mercato interno*** e di rafforzare in tal modo la fiducia nel mercato unico digitale.

Or. en

Emendamento 262
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 4 – paragrafo 6

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

Or. en

Emendamento 263
Michał Boni, Henna Virkkunen, Massimiliano Salini

Proposta di regolamento
Articolo 4 – paragrafo 6 bis (nuovo)

Testo della Commissione	*Emendamento*
	6 bis. L'Agenzia promuove i principi dell'igiene informatica.

Or. en

Emendamento 264
Clare Moody, Theresa Griffin, Peter Kouroumbashev, Arne Lietz

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza ***dei*** cittadini e ***delle*** imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove ***e sostiene progetti che contribuiscono a*** un elevato livello di consapevolezza ***e di alfabetizzazione informatica tra i*** cittadini e ***le*** imprese sulle questioni relative alla cibersicurezza.

Or. en

Motivazione

Sebbene l'ENISA debba contribuire al rafforzamento della fiducia nei confronti del mercato unico digitale tramite la certificazione, ciò non dovrebbe portare a un atteggiamento compiacente. Un alto livello di alfabetizzazione informatica è essenziale affinché i consumatori comprendano, ad esempio, le differenze tra i vari livelli di affidabilità previsti dall'atto in esame.

Emendamento 265
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza ***e fornisce indicazioni su come migliorare la ciberresilienza***.

Or. en

Emendamento 266

Martina Werner

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove un elevato livello di consapevolezza ***e alfabetizzazione digitale*** dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

Or. en

Emendamento 267
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove un elevato livello di ***igiene informatica e*** consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

Or. en

Emendamento 268
Seán Kelly

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove un elevato livello di ***igiene informatica e*** consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

Or. en

Emendamento 269
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 4 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia promuove un elevato livello di consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.	7. L'Agenzia promuove un elevato livello di ***igiene informatica e*** consapevolezza dei cittadini e delle imprese sulle questioni relative alla cibersicurezza.

Or. en

Emendamento 270
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 4 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. L'Agenzia fornisce consulenza e assistenza agli Stati membri e alle istituzioni dell'Unione nella definizione di politiche e pratiche per una gestione responsabile e una divulgazione coordinata delle vulnerabilità dei prodotti, dei processi, dei servizi e dei sistemi TIC che non sono pubblicamente note, anche instaurando, in particolare, procedure di esame della divulgazione di vulnerabilità da parte dei governi e politiche di divulgazione coordinata delle vulnerabilità.

Or. en

Emendamento 271
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 4 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. L'Agenzia fornisce assistenza e consulenza gli Stati membri e alle istituzioni dell'Unione nella definizione di politiche e pratiche per una gestione responsabile e una divulgazione coordinata delle vulnerabilità dei prodotti e dei servizi TIC che non sono pubblicamente note, anche instaurando procedure di esame della divulgazione di vulnerabilità da parte dei governi e politiche di divulgazione coordinata delle vulnerabilità.

Or. en

Motivazione

Tale compito dovrebbe essere svolto conformemente alle raccomandazioni e agli orientamenti definiti nelle norme internazionali ISO/IEC 29147:2014 e ISO/IEC 30111.

Emendamento 272
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 5 – comma 1 – punto 1

Testo della Commissione	*Emendamento*
1. fornendo assistenza e consulenza, in particolare fornendo un parere ***indipendente*** e lavori preparatori, per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel settore della cibersicurezza, nonché delle iniziative legislative e politiche settoriali che	1. fornendo assistenza e consulenza, in particolare fornendo un parere ***e un'analisi indipendenti delle pertinenti attività nel ciberspazio*** e lavori preparatori, per lo sviluppo e la revisione delle politiche e della normativa dell'Unione nel settore della cibersicurezza, nonché delle iniziative legislative e politiche settoriali

presentano una correlazione con le questioni relative alla cibersicurezza;	che presentano una correlazione con le questioni relative alla cibersicurezza;

Or. en

Emendamento 273
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 5 – comma 1 – punto 2

Testo della Commissione	*Emendamento*
2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;	2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali ***lo sviluppo di software e sistemi sicuri,*** la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni ***nonché misure tecniche e organizzative, in particolare l'istituzione di programmi di divulgazione coordinata delle vulnerabilità***, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

Or. en

Motivazione

The NIS-Directive leaves open the range of measures a company can take in order to ensure compliance as part of the "technical and organisational measures" prescribed in Article 14 of Directive (EU) 2016/1148. These measures can include the establishment of a coordinated vulnerability programme, and Member states may explicitly consider parameters regarding the establishment of such a programme in transposing the NIS Directive. ENISA can provide guidelines on how to create such a CVD-programme in order to create a consistent European approach to coordinated vulnerability disclosure that is consistent with the guidelines and recommendations defined in international standards ISO/IEC 29147:2014 and ISO/IEC 30111.

Emendamento 274
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

Proposta di regolamento
Articolo 5 – comma 1 – punto 2

Testo della Commissione	*Emendamento*
2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;	2. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di cibersicurezza, in particolare in relazione alla direttiva (UE) 2016/1148, ***alla direttiva che istituisce il codice europeo delle comunicazioni elettroniche, al regolamento (UE) 2016/679 e alla direttiva 2002/58/CE***, anche mediante pareri, orientamenti, consigli e migliori pratiche su questioni quali la gestione del rischio, la segnalazione degli incidenti e la condivisione delle informazioni, e agevolando lo scambio di migliori pratiche tra le autorità competenti in materia;

Or. en

Emendamento 275
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. assistendo il comitato europeo per la protezione dei dati istituito dal regolamento (UE) 2016/679 nell'elaborazione di linee guida volte a precisare a livello tecnico le condizioni che consentono l'uso lecito dei dati personali da parte dei titolari del trattamento a fini di sicurezza informatica, nell'ottica di tutelare la loro infrastruttura individuando e bloccando

attacchi ai danni dei loro sistemi informativi nel quadro:

i) del regolamento (UE) 2016/679[1 bis];

ii) della direttiva (UE) 2016/1148[1 ter] e

iii) della direttiva 2002/58/CE[1 quater];

[1 bis] Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1). [1 ter] Direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (GU L 194 del 19.7.2016, pag. 1). [1 quater] Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

Or. en

Motivazione

L'emendamento è volto a istituire adeguati meccanismi di cooperazione.

Emendamento 276
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*

2 bis. assistendo gli Stati membri nell'attuazione uniforme delle politiche e della normativa dell'Unione in materia di protezione dei dati, in particolare in relazione al regolamento (UE) 2016/679, e assistendo il comitato europeo per la protezione dei dati (EDPB) nell'elaborazione di linee guida relative all'attuazione del regolamento (UE) 2016/679 a fini di cibersicurezza. L'EDPB deve essere tenuto a consultare l'ENISA ogni volta che formula un parere o adotta una decisione riguardo all'attuazione del regolamento generale sulla protezione dei dati e alla cibersicurezza, in particolare, a titolo esemplificativo, per questioni relative alle valutazioni d'impatto sulla tutela della vita privata, alla notifica delle violazioni dei dati, al trattamento in sicurezza, ai requisiti di sicurezza e alla privacy fin dalla progettazione;

Or. en

Motivazione

Nel contesto del rafforzamento del mandato dell'ENISA, è importante che l'Agenzia sia anche adeguatamente consultata dagli organismi regolamentari dell'UE in merito a questioni di protezione dei dati a fini di cibersicurezza. L'Agenzia ha facoltà di attivarsi in merito a questioni relative alla politica di cibersicurezza dell'UE analogamente a quanto fa il Garante europeo della protezione dei dati nell'ambito della protezione dei dati.

Emendamento 277
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 5 – comma 1 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. proponendo un piano che definisca il ruolo, le responsabilità e i diritti e gli obblighi di natura giuridica di fornitori, fabbricanti, come pure dei CERT e dei CSIRT e che chiarisca

ulteriormente i diritti e le tutele giuridici dei ricercatori nel settore della sicurezza informatica, nell'ambito di un programma di divulgazione coordinata delle vulnerabilità, in particolare nei casi di divulgazioni multiple di vulnerabilità che coinvolgono molteplici ricercatori e fornitori riguardo a vulnerabilità rilevate in diversi Stati membri;

Or. en

Motivazione

Il caso delle vulnerabilità Meltdown e Spectre ha dimostrato la necessità di programmi di divulgazione coordinata delle vulnerabilità a livello dell'UE che siano di portata più ampia rispetto a quelli dei gestori di servizi essenziali. Tale piano deve essere coerente con le raccomandazioni e gli orientamenti definiti nelle norme internazionali ISO/IEC 29147:2014 e ISO/IEC 30111.

Emendamento 278
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. fornendo assistenza e consulenza agli Stati membri e alle istituzioni dell'Unione nella definizione di politiche e pratiche per una gestione responsabile e una divulgazione coordinata delle vulnerabilità dei prodotti, dei processi, dei servizi e dei sistemi TIC che non sono pubblicamente note, anche instaurando, in particolare, procedure di esame della divulgazione di vulnerabilità da parte dei governi e politiche di divulgazione coordinata delle vulnerabilità;

Or. en

Emendamento 279
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 ter (nuovo)

Testo della Commissione	*Emendamento*
	2 ter. proponendo politiche con l'obiettivo di garantire che i fabbricanti, i fornitori di servizi, gli importatori e i distributori di TIC agiscano con la dovuta diligenza per quanto concerne la tempestiva correzione delle vulnerabilità in materia di sicurezza informatica nei loro prodotti, processi e servizi, per evitare di esporre indebitamente i loro utenti alla criminalità informatica;

Or. en

Emendamento 280
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 ter (nuovo)

Testo della Commissione	*Emendamento*
	2 ter. proponendo politiche con l'obiettivo di garantire che i fabbricanti di TIC agiscano con la dovuta diligenza per quanto concerne la tempestiva correzione delle vulnerabilità in materia di sicurezza informatica nei loro prodotti e servizi, per evitare di esporre indebitamente i loro utenti alla criminalità informatica;

Or. en

Motivazione

Stabilire una corretta ripartizione delle responsabilità è essenziale per incentivare tutte le parti interessate ad agire con la dovuta diligenza.

Emendamento 281
Jakop Dalunde, Reinhard Bütikofer

a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 quater (nuovo)

Testo della Commissione	*Emendamento*
	2 quater. proponendo politiche che stabiliscano un solido quadro di responsabilità per tutte le parti interessate che partecipano agli ecosistemi basati sulle TIC;

Or. en

Motivazione

L'emendamento è volto a incoraggiare tutte le parti interessate ad agire con la dovuta diligenza.

Emendamento 282
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 quinquies (nuovo)

Testo della Commissione	*Emendamento*
	2 quinquies. proponendo politiche che rafforzano la regolamentazione delle responsabilità degli operatori delle infrastrutture di rete critiche nel caso di un attacco ai danni dei loro sistemi informativi che si ripercuote sui loro utenti a causa del mancato uso della dovuta diligenza da parte di alcuni utenti o dell'operatore stesso, laddove questi ha omesso di adottare misure ragionevoli per prevenire l'incidente o per mitigarne gli effetti su tutti gli utenti;

Or. en

Motivazione

Gli operatori delle infrastrutture critiche dovrebbero avere la responsabilità di ottenere garanzie del fatto che solo utenti/partecipanti sicuri e affidabili utilizzano la loro

infrastruttura e, se necessario, dovrebbero isolare quelli non sicuri in modo da evitare incidenti.

Emendamento 283
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 sexies (nuovo)

Testo della Commissione	*Emendamento*
	2 sexies. proponendo politiche che limitano l'acquisto e l'uso degli "zero-day" da parte delle autorità pubbliche allo scopo di attaccare sistemi informativi; promuovendo verifiche dei software e finanziando personale esperto;

Or. en

Motivazione

Sviluppando, acquistando e sfruttando "accessi secondari" (le cosiddette backdoor) ai sistemi informatici servendosi del denaro dei contribuenti, gli enti governativi mettono a repentaglio la sicurezza dei cittadini. Per proteggere le altre parti interessate che gestiscono con responsabilità simili vulnerabilità, l'Agenzia dovrebbe proporre politiche che favoriscono lo scambio responsabile di informazioni sugli "zero-day" e altri tipi di vulnerabilità della sicurezza che non sono ancora pubblicamente note e che ne agevolano la correzione.

Emendamento 284
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 2 septies (nuovo)

Testo della Commissione	*Emendamento*
	2 septies. proponendo politiche che prevedono che le autorità pubbliche, le imprese private, i ricercatori, le università e le altre parti interessate pubblichino tutte le vulnerabilità critiche riguardanti la sicurezza che non sono ancora

pubblicamente note nel quadro di una divulgazione responsabile;

Or. en

Motivazione

Sono necessarie opportune politiche dell'UE per attuare un processo coerente di divulgazione responsabile in tutta l'Unione.

Emendamento 285
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 5 – comma 1 – punto 7 octies (nuovo)

Testo della Commissione	*Emendamento*
	7 octies. proponendo politiche che promuovono l'estensione dell'uso del "codice sorgente aperto verificabile" alle soluzioni informatiche nel settore pubblico e l'uso correlato di strumenti automatizzati allo scopo di agevolare la verifica del codice sorgente e controllare facilmente che non vi siano "backdoor" e altre eventuali vulnerabilità riguardanti la sicurezza;

Or. en

Motivazione

È opportuno incoraggiare l'uso di software con codice sorgente aperto nelle pubbliche amministrazioni, le quali dovrebbero anche accettare le responsabilità correlate di verificare il codice sorgente delle applicazioni di cui fanno uso (per accertare la presenza/assenza di gravi vulnerabilità in materia di sicurezza informatica).

Emendamento 286
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

Proposta di regolamento
Articolo 5 – comma 1 – punto 4 – punto 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	(2 bis) lo sviluppo e la promozione di politiche volte a sostenere la disponibilità o integrità generale del nucleo pubblico di una rete internet aperta, che consente la funzionalità essenziale di internet nel suo complesso e che supporta il suo funzionamento normale, ivi comprese, solo a titolo di esempio, la sicurezza e la stabilità dei protocolli chiave (in particolare DNS, BGP e IPv6), il funzionamento del sistema dei nomi di dominio (compresi quelli di tutti i domini di primo livello), nonché il funzionamento della zona root;

Or. en

Motivazione

La tutela del nucleo pubblico di internet è una norma emergente che è sostenuta dalla Commissione mondiale per la stabilità del ciberspazio, la quale ha ricevuto il proprio mandato dalle conclusioni della 4ª conferenza mondiale sul ciberspazio svoltasi nel 2015 all'Aia, come pure dalla 5ª relazione del gruppo di esperti governativi delle Nazioni Unite.

Emendamento 287
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 5 – comma 1 – punto 5 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) lo stato di attuazione della procedura coordinata di esame della divulgazione di vulnerabilità da parte degli Stati membri e delle istituzioni dell'Unione.

Or. en

Emendamento 288

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

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	(a bis) gli Stati membri e le istituzioni dell'Unione nell'elaborazione e nell'attuazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi, le cui pratiche e conclusioni devono essere trasparenti e soggette a un controllo indipendente;

Or. en

Motivazione

Una procedura di esame della divulgazione di vulnerabilità da parte di un governo implica la gestione di vulnerabilità scoperte da agenzie governative e definisce una procedura che consente di determinare quando e in che modo l'agenzia governativa deve divulgare la vulnerabilità di cui è a conoscenza. Provvedere affinché i governi e le rispettive agenzie dispongano di solide politiche per gestire l'esame e il coordinamento della divulgazione di vulnerabilità è una norma di importanza critica, che dovrebbe essere promossa all'interno dell'UE.

Emendamento 289
Evžen Tošenovský

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera g

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

processo di valutazione delle esercitazioni e sugli insegnamenti tratti da queste ultime;

Or. en

Emendamento 290
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera g

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

Or. en

Emendamento 291
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 6 – paragrafo 1 – lettera i bis (nuova)

Testo della Commissione	*Emendamento*
	(i bis) gli Stati membri e le istituzioni dell'Unione nell'elaborazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi che siano trasparenti e soggette a una valutazione indipendente.

Or. en

Emendamento 292
Seán Kelly

Proposta di regolamento
Articolo 6 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.	2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire***, su principi di igiene informatica e*** su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Or. en

Emendamento 293
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 6 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.	2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire***, su principi di igiene informatica e*** su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Or. en

Emendamento 294
Michał Boni, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 6 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire e su come affrontare le questioni regolamentari connesse allo scambio di informazioni.	2. L'Agenzia agevola l'istituzione di centri di condivisione e di analisi delle informazioni (ISAC) settoriali e fornisce loro un sostegno costante, in particolare nei settori che figurano nell'allegato II della direttiva (UE) 2016/1148, fornendo migliori pratiche e orientamenti sugli strumenti disponibili, sulla procedura da seguire***, su principi di igiene informatica e*** su come affrontare le questioni regolamentari connesse allo scambio di informazioni.

Or. en

Emendamento 295
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 6 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. L'Agenzia agevola la creazione e l'avvio di un progetto europeo a lungo termine in materia di sicurezza informatica volto a sostenere la crescita di un'industria della sicurezza informatica dell'UE indipendente e a integrare la sicurezza informatica in tutti gli sviluppi delle tecnologie dell'informazione nell'Unione.

Or. en

Motivazione

L'ENISA dovrebbe fornire consulenza ai legislatori in merito all'elaborazione di politiche che consentano all'UE di rimettersi in pari con le industrie della sicurezza informatica nei paesi terzi. Il progetto dovrebbe avere una portata paragonabile a quanto realizzato in precedenza a favore del settore del trasporto aereo (esempio di Airbus). Ciò è necessario per sviluppare un'industria delle TIC dell'UE che sia più solida, sovrana e affidabile (cfr. studio dell'unità Prospettiva scientifica, STOA, PE 614.531).

Emendamento 296
Françoise Grossetête

Proposta di regolamento
Articolo 7 – titolo

Testo della Commissione	*Emendamento*
Compiti relativi alla cooperazione operativa a livello di Unione	Compiti relativi ***al sostegno*** alla cooperazione operativa a livello di Unione

Or. fr

Emendamento 297
Françoise Grossetête

Proposta di regolamento
Articolo 7 – paragrafo 4 – comma 1 – parte introduttiva

Testo della Commissione	*Emendamento*
L'Agenzia ***contribuisce alla*** cooperazione operativa nell'ambito della rete di CSIRT fornendo sostegno agli Stati membri mediante:	L'Agenzia ***sostiene la*** cooperazione operativa nell'ambito della rete di CSIRT ***conformemente alle disposizioni dell'articolo 12, paragrafo 2, della direttiva (UE) 2016/1148,*** fornendo sostegno agli Stati membri mediante:

Or. fr

Motivazione

Il ruolo dell'ENISA nel quadro della rete di CSIRT è già definito dalla direttiva NIS (direttiva (UE) 2016/1148).

Emendamento 298
Gunnar Hökmark

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

Testo della Commissione	*Emendamento*
(b) ***l'offerta,*** su richiesta degli Stati membri, ***di assistenza tecnica*** in caso di incidenti aventi un impatto rilevante o sostanziale;	(b) ***il sostegno,*** su richiesta degli Stati membri, in caso di incidenti aventi un impatto rilevante o sostanziale;

Or. en

Emendamento 299
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 5 – comma 1

Testo della Commissione	*Emendamento*
Su richiesta di ***due*** o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di ***due Stati membri***.	Su richiesta di ***uno*** o più Stati membri interessati, e al solo fine di fornire ***assistenza sotto forma di*** consulenza per la prevenzione di futuri incidenti ***o sotto forma di assistenza nella risposta a incidenti di vasta scala***, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. ***L'Agenzia svolge le suddette attività ricevendo le informazioni pertinenti dagli Stati membri interessati e utilizzando risorse proprie di analisi delle minacce nonché risorse per la risposta agli incidenti messe a disposizione dalla CERT UE a tale scopo***. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli

	incidenti interessino più di ***uno Stato membro***.

Or. en

Emendamento 300
Martina Werner

Proposta di regolamento
Articolo 7 – paragrafo 5 – comma 1

Testo della Commissione	*Emendamento*
Su richiesta di ***due o più Stati membri interessati,*** e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di ***due Stati membri***.	Su richiesta di ***uno Stato membro interessato*** e al solo fine di fornire ***assistenza sotto forma di*** consulenza per la prevenzione di futuri incidenti ***o sotto forma di assistenza nella risposta a incidenti di vasta scala***, l'Agenzia fornisce assistenza alle imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale indagine anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di ***uno Stato membro***.

Or. en

Emendamento 301
Françoise Grossetête

Proposta di regolamento
Articolo 7 – paragrafo 5 – comma 1

Testo della Commissione	*Emendamento*
Su richiesta di due o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza ***alle***	Su richiesta di due o più Stati membri interessati, e al solo fine di fornire consulenza per la prevenzione di futuri incidenti, l'Agenzia fornisce assistenza

imprese interessate o effettua un'indagine tecnica ex post a seguito della notifica da parte delle imprese interessate di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale ***indagine*** anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di due Stati membri.	***nell'analisi*** di incidenti aventi un impatto significativo o rilevante ai sensi della direttiva (UE) 2016/1148. L'Agenzia svolge tale ***analisi*** anche su richiesta debitamente motivata della Commissione di concerto con gli Stati membri interessati nel caso in cui gli incidenti interessino più di due Stati membri.

Or. fr

Motivazione

L'ENISA dovrebbe effettuare analisi degli incidenti accompagnate da proposte di soluzioni, invece di svolgere indagini lunghe e complesse. L'ENISA deve concentrarsi sulle proprie missioni di sostegno alla cooperazione e alla condivisione di soluzioni tecniche tra gli Stati membri: è in questo che risiede il suo valore aggiunto a livello europeo.

Emendamento 302
Françoise Grossetête

Proposta di regolamento
Articolo 7 – paragrafo 5 – comma 2

Testo della Commissione	*Emendamento*
L'ambito dell'***indagine e la procedura da seguire nel suo svolgimento sono concordati*** dagli Stati membri interessati e dall'Agenzia ***e non pregiudicano eventuali indagini penali in corso relative allo stesso incidente***. L'***indagine*** si conclude con una relazione tecnica finale redatta dall'Agenzia, in particolare sulla base delle informazioni e dei commenti forniti dagli Stati membri e dalla o dalle imprese interessati, e concordata con gli Stati membri interessati. Una sintesi della relazione, incentrata sulle raccomandazioni per la prevenzione di futuri incidenti, è condivisa con la rete di CSIRT.	L'ambito dell'***analisi è concordato*** dagli Stati membri interessati e dall'Agenzia. L'***analisi*** si conclude con una relazione tecnica finale redatta dall'Agenzia, in particolare sulla base delle informazioni e dei commenti forniti dagli Stati membri e dalla o dalle imprese interessati, e concordata con gli Stati membri interessati. Una sintesi della relazione, incentrata sulle raccomandazioni per la prevenzione di futuri incidenti, è condivisa con la rete di CSIRT.

Or. fr

Emendamento 303
Evžen Tošenovský

Proposta di regolamento
Articolo 7 – paragrafo 6

Testo della Commissione	*Emendamento*
6. L'Agenzia organizza esercitazioni ***annuali*** di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organi dell'UE nell'organizzazione di esercitazioni. Le esercitazioni annuali a livello di Unione includono gli elementi tecnici, operativi e strategici e contribuiscono a preparare la risposta cooperativa a livello di Unione agli incidenti di cibersicurezza transfrontalieri di vasta portata. L'Agenzia inoltre contribuisce e aiuta ad organizzare, se del caso, esercitazioni di cibersicurezza settoriali insieme ai pertinenti ISAC e consente agli ISAC di partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.	6. L'Agenzia organizza esercitazioni ***biennali*** di cibersicurezza a livello di Unione e, su loro richiesta, sostiene gli Stati membri e le istituzioni, le agenzie e gli organi dell'UE nell'organizzazione di esercitazioni. Le esercitazioni annuali a livello di Unione includono gli elementi tecnici, operativi e strategici e contribuiscono a preparare la risposta cooperativa a livello di Unione agli incidenti di cibersicurezza transfrontalieri di vasta portata. L'Agenzia inoltre contribuisce e aiuta ad organizzare, se del caso, esercitazioni di cibersicurezza settoriali insieme ai pertinenti ISAC e consente agli ISAC di partecipare anche alle esercitazioni di cibersicurezza a livello di Unione.

Or. en

Emendamento 304
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 7

Testo della Commissione	*Emendamento*
7. L'Agenzia elabora periodicamente una relazione sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro: dai CSIRT degli Stati membri (su base volontaria) o dai punti di	7. L'Agenzia elabora periodicamente una relazione ***approfondita*** sulla situazione tecnica della cibersicurezza nell'UE in merito agli incidenti e alle minacce, sulla base delle informazioni pubblicamente disponibili, della propria analisi e delle relazioni condivise, tra l'altro: dai CSIRT degli Stati membri (su base volontaria) o

contatto unici istituiti dalla direttiva NIS (conformemente all'articolo 14, paragrafo 5, della direttiva NIS), dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol e dalla CERT-UE.	dai punti di contatto unici istituiti dalla direttiva NIS (conformemente all'articolo 14, paragrafo 5, della direttiva NIS), dal Centro europeo per la lotta alla criminalità informatica (EC3) presso Europol e dalla CERT-UE. ***Il direttore esecutivo presenta le conclusioni pubbliche al Parlamento europeo.***

Or. en

Emendamento 305
Clare Moody, Theresa Griffin, Peter Kouroumbashev, Arne Lietz

Proposta di regolamento
Articolo 7 – paragrafo 7 – comma 1 (nuovo)

Testo della Commissione	*Emendamento*
	L'Agenzia contribuisce, ove opportuno e previa approvazione da parte della Commissione, alla cooperazione informatica transfrontaliera con il Centro di eccellenza per la ciberdifesa cooperativa della NATO e l'Accademia NATO per la comunicazione e l'informazione (NCI).

Or. en

Emendamento 306
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 7 – paragrafo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	7 bis. L'Agenzia prepara, insieme al SEAE, una relazione periodica sulla situazione globale della cibersicurezza relativa agli incidenti e alle minacce per gli individui, compresi gli utenti

vulnerabili al di fuori dell'UE come avvocati, giornalisti o difensori dei diritti umani, al fine di aiutare le istituzioni dell'Unione a far fronte a esigenze esterne e ad adempiere, all'estero, alle sue responsabilità in materia di diritti umani.

Or. en

Emendamento 307
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera a

Testo della Commissione	*Emendamento*
(a) aggregando le relazioni delle fonti nazionali al fine di contribuire a creare una conoscenza situazionale comune;	(a) ***analizzando e*** aggregando le relazioni delle fonti nazionali al fine di contribuire a creare una conoscenza situazionale comune;

Or. en

Emendamento 308
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Edouard Martin, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera c

Testo della Commissione	*Emendamento*
(c) fornendo assistenza nel trattamento tecnico di un incidente o di una crisi, anche agevolando la condivisione di soluzioni tecniche tra gli Stati membri;	(c) fornendo assistenza nel trattamento tecnico di un incidente o di una crisi, ***sulla base delle proprie competenze e di risorse indipendenti,*** anche agevolando la condivisione di soluzioni tecniche tra gli Stati membri;

Or. en

Emendamento 309
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) mettendo a punto sistemi di certificazione che disincentivano i fabbricanti e i fornitori di servizi TIC dal creare "backdoor" segrete che indeboliscono intenzionalmente la sicurezza informatica di prodotti e servizi commerciali e hanno un impatto negativo sulla sicurezza globale di internet;

Or. en

Motivazione

Questo dovrebbe essere riconosciuto come uno degli obiettivi principali dei sistemi di certificazione.

Emendamento 310
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera e bis (nuova)

Testo della Commissione	*Emendamento*
	(e bis) fornendo assistenza agli Stati membri e alle istituzioni dell'Unione in merito alla definizione e all'istituzione di un quadro dell'UE per la risposta alle crisi in materia di cibersicurezza che integri gli obiettivi e le modalità di cooperazione suggeriti nella [raccomandazione della Commissione relativa alla risposta coordinata agli

incidenti e alle crisi di cibersicurezza del 13.9.2017].

Or. en

Emendamento 311
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera e bis (nuova)

Testo della Commissione	*Emendamento*
	(e bis) fornendo assistenza e consulenza agli Stati membri in merito alla definizione e all'attuazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi.

Or. en

Motivazione

Tale compito dovrebbe essere svolto conformemente alle raccomandazioni e agli orientamenti definiti nelle norme ISO/IEC 29147:2014 e ISO/IEC 30111.

Emendamento 312
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera e bis (nuova)

Testo della Commissione	*Emendamento*
	(e bis) fornendo assistenza agli Stati membri in merito alla definizione e all'attuazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi.

Or. en

Emendamento 313
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Kathleen Van Brempt, Dan Nica, Clare Moody

Proposta di regolamento
Articolo 7 – paragrafo 8 – lettera e ter (nuova)

Testo della Commissione	*Emendamento*
	(e ter) fornendo assistenza agli Stati membri e alle istituzioni dell'Unione in merito allo sviluppo e all'adozione di una tassonomia e di un modello comuni per le relazioni sulla situazione, al fine di descrivere le cause tecniche e le conseguenze degli incidenti di cibersicurezza e migliorare ulteriormente la cooperazione tecnica e operativa durante la crisi.

Or. en

Motivazione

Tale suggerimento è stato avanzato anche dalla Commissione nella sua raccomandazione relativa alla riposta coordinata agli incidenti e alle crisi di cibersicurezza su larga scala del 13.9.2017

Emendamento 314
Eva Kaili, Peter Kouroumbashev

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

Testo della Commissione	*Emendamento*
	8 bis. convocando le autorità degli Stati membri e fornendo assistenza in merito al coordinamento della loro risposta, conformemente ai principi di sussidiarietà e proporzionalità.

Or. en

Emendamento 315
Evžen Tošenovský

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

Testo della Commissione	*Emendamento*
	8 bis. L'Agenzia sostiene e promuove la cooperazione tra gli Stati membri nella conduzione di audit sulla sicurezza informatica delle infrastrutture critiche transfrontaliere.

Or. en

Emendamento 316
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 7 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 7 bis
	Capacità tecniche dell'Agenzia
	Per raggiungere gli obiettivi di cui agli articoli 5, 6 e 7, l'Agenzia sviluppa, tra l'altro, le seguenti capacità e competenze tecniche:
	1. La capacità di analizzare dati informativi sulle minacce su vasta scala.
	2. La capacità di effettuare un'analisi forense su dispositivi e apparecchiature terminali.
	3. La capacità di analizzare malware, indicatori di compromissione e altre informazioni relative a una minaccia o a un incidente di cibersicurezza.

	4. La capacità di raccogliere informazioni sulle minacce di cibersicurezza da fonti pubblicamente disponibili e commerciali.
	5. La capacità di rendere disponibili attrezzature tecniche, strumenti e competenze in remoto e in locale su richiesta di uno Stato membro, nei casi contemplati dall'articolo 7, paragrafi 5 e 8.
	Per fornire le capacità tecniche descritte nel presente articolo l'Agenzia provvede affinché le sue procedure di assunzione riflettano le diverse competenze tecniche richieste.
	Per fornire le capacità tecniche descritte nel presente articolo e sviluppare le competenze pertinenti, l'Agenzia coopera con la CERT UE ed Europol a norma dell'articolo 7, paragrafo 2.

Or. en

Emendamento 317
Gunnar Hökmark

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – parte introduttiva

Testo della Commissione	*Emendamento*
(a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti e dei servizi TIC, come stabilito al titolo III del presente regolamento:	(a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza ***delle procedure di sviluppo,*** dei prodotti e dei servizi TIC, come stabilito al titolo III del presente regolamento:

Or. en

Emendamento 318
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – parte introduttiva

Testo della Commissione	*Emendamento*
(a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti ***e*** dei servizi TIC, come stabilito al titolo III del presente regolamento:	(a) sostiene e promuove lo sviluppo e l'attuazione della politica dell'Unione in materia di certificazione della cibersicurezza dei prodotti***,*** dei servizi ***e dei processi*** TIC, come stabilito al titolo III del presente regolamento:

Or. en

Emendamento 319
András Gyürk

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

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;	***soppresso***

Or. en

Motivazione

Il relatore non è favorevole al nuovo compito di certificazione dell'ENISA. La certificazione dovrebbe essere effettuata da un soggetto diverso, dato che richiede conoscenze e competenze specifiche.

Emendamento 320
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

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

Testo della Commissione	*Emendamento*

(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;	(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti, i processi e i servizi TIC conformemente all'articolo 44 del presente regolamento***, in cooperazione con l'industria, le PMI, i portatori di interessi nell'ambito della ricerca e dell'università e le organizzazioni a tutela dei consumatori, nel quadro di una procedura chiara e trasparente***;

Or. en

Emendamento 321
Martina Werner

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

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

Or. en

Emendamento 322
Pilar del Castillo Vera

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

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC	(1) identificando e preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente

conformemente all'articolo 44 del presente regolamento;	regolamento***, in cooperazione con i portatori di interessi dell'industria, nel quadro di una procedura formale, standardizzata e trasparente***;

Or. en

Emendamento 323
Massimiliano Salini

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

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;	(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC, in cooperazione con ***il gruppo permanente di portatori di interessi e il gruppo di certificazione dei portatori di interessi*** conformemente all'articolo 44 del presente regolamento;

Or. en

Emendamento 324
Michał Boni, Massimiliano Salini, Krišjānis Kariņš, Gunnar Hökmark

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

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti e i servizi TIC conformemente all'articolo 44 del presente regolamento;	(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti***, i processi*** e i servizi TIC***, in cooperazione con il gruppo di lavoro di portatori di interessi e*** conformemente all'articolo 44***, paragrafo 2,*** del presente regolamento;

Or. en

Emendamento 325
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

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

Testo della Commissione	*Emendamento*
(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti ***e*** i servizi TIC conformemente all'articolo 44 del presente regolamento;	(1) preparando proposte di sistemi europei di certificazione della cibersicurezza per i prodotti***,*** i servizi ***e i processi*** TIC conformemente all'articolo 44 del presente regolamento;

Or. en

Emendamento 326
Peter Kouroumbashev

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

Testo della Commissione	*Emendamento*
	(1 bis) effettuando, in cooperazione con il gruppo europeo per la certificazione della cibersicurezza, valutazioni delle procedure per l'emissione di certificati europei di cibersicurezza messe in atto dagli organismi di valutazione della conformità di cui all'articolo 51, finalizzate ad assicurare l'applicazione uniforme del presente regolamento da parte degli organismi di valutazione della conformità all'atto dell'emissione dei certificati;

Or. en

Emendamento 327
Peter Kouroumbashev

Proposta di regolamento

Articolo 8 – comma 1 – lettera a – punto 1 ter (nuovo)

Testo della Commissione	*Emendamento*
	(1 ter) svolgendo verifiche ex post periodiche e indipendenti sulla conformità dei prodotti e dei servizi TIC certificati rispetto ai sistemi europei di certificazione della cibersicurezza;

Or. en

Emendamento 328
András Gyürk

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 2

Testo della Commissione	*Emendamento*
(2) assistendo la Commissione nel provvedere alle funzioni di segretariato del gruppo europeo per la certificazione della cibersicurezza a norma dell'articolo 53 del presente regolamento;	***soppresso***

Or. en

Emendamento 329
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione ***e*** con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione***,*** con l'industria, ***con le PMI, con i portatori di interessi pertinenti nell'ambito della ricerca e dell'università***

	e con le organizzazioni a tutela dei consumatori;

Or. en

Emendamento 330
Pilar del Castillo Vera

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria***, nel quadro di una procedura formale, standardizzata e trasparente***;

Or. en

Emendamento 331
Barbara Kappel

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) ***fornendo assistenza alle piccole e medie imprese*** elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

Or. en

Emendamento 332

Seán Kelly

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche***, anche riguardo ai principi dell'igiene informatica,*** in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

Or. en

Emendamento 333
Eva Kaili, Peter Kouroumbashev

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche***, anche riguardo ai principi dell'igiene informatica,*** in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

Or. en

Emendamento 334
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti ***e*** dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche ***e principi di igiene informatica*** in merito ai requisiti di cibersicurezza dei prodotti***,*** dei servizi ***e dei processi*** TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

Or. en

Emendamento 335
Gunnar Hökmark

Proposta di regolamento
Articolo 8 – comma 1 – lettera a – punto 3

Testo della Commissione	*Emendamento*
(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;	(3) elaborando e pubblicando orientamenti e sviluppando buone pratiche in merito ai requisiti di cibersicurezza ***delle procedure di sviluppo*** dei prodotti e dei servizi TIC, in cooperazione con le autorità nazionali di controllo della certificazione e con l'industria;

Or. en

Emendamento 336
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 8 – comma 1 – lettera a bis (nuova)

Testo della Commissione	*Emendamento*
	(a bis) sostiene e promuove la definizione e l'attuazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi, anche riguardo alle vulnerabilità dei prodotti,

dei processi, dei servizi e dei sistemi TIC certificati di cui al titolo II del presente regolamento;

Or. en

Emendamento 337
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 8 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) agevola la definizione e l'adozione di norme tecniche europee e ***internazionali*** in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;	(b) ***consulta le organizzazioni internazionali di normazione ISO/IEC e le organizzazioni di normazione europee riguardo allo sviluppo di norme, per assicurare che le norme utilizzate nei sistemi europei di certificazione della cibersicurezza siano adeguate e*** agevola la definizione e l'adozione di norme tecniche europee e ***ISO/IEC*** in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;

Or. en

Motivazione

Le norme possono essere elementi costitutivi delle certificazioni e, pertanto, una buona cooperazione con le organizzazioni di normazione può garantire la definizione di norme idonee allo scopo e l'inserimento delle norme migliori nei sistemi.

Emendamento 338

Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 8 – comma 1 – lettera b

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

Or. en

Emendamento 339
Gunnar Hökmark

Proposta di regolamento
Articolo 8 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) agevola la definizione e l'adozione di norme tecniche europee e internazionali in materia di gestione dei rischi e di sicurezza dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, comprese le norme tecniche nazionali degli Stati membri, a norma	(b) agevola la definizione e l'adozione di norme tecniche europee e internazionali in materia di gestione dei rischi e di sicurezza ***delle procedure di sviluppo,*** dei prodotti e dei servizi TIC e, in collaborazione con gli Stati membri, redige pareri e linee guida riguardanti i settori tecnici relativi ai requisiti di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali e concernenti altresì le norme tecniche già esistenti, ***le norme internazionali e gli accordi***

dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;	***internazionali informali,*** comprese le norme tecniche nazionali degli Stati membri, a norma dell'articolo 19, paragrafo 2, della direttiva (UE) 2016/1148;

Or. en

Emendamento 340
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 8 – comma 1 – lettera b

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

Or. en

Emendamento 341
Pilar del Castillo Vera

Proposta di regolamento
Articolo 8 – comma 1 – lettera b – punto i (nuovo)

Testo della Commissione	*Emendamento*
	(i) promuove, in base al livello di rischio, l'uso di mezzi aggiuntivi per la

certificazione della conformità alle norme in materia di cibersicurezza;

Or. en

Emendamento 342
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 8 – comma 1 – lettera c

Testo della Commissione	*Emendamento*
(c) effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze del mercato della cibersicurezza sul versante della domanda e dell'offerta, al fine di promuovere ***tale mercato*** nell'Unione.	(c) effettua regolarmente, diffondendone poi i risultati, analisi delle principali tendenze ***e vulnerabilità*** del mercato della cibersicurezza sul versante della domanda e dell'offerta, al fine di promuovere ***la cibersicurezza*** nell'Unione.

Or. en

Emendamento 343
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 8 – comma 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) mette a punto sistemi di certificazione che disincentivano i fabbricanti e i fornitori di servizi TIC dal creare "backdoor" segrete che indeboliscono intenzionalmente la sicurezza informatica di prodotti e servizi commerciali e hanno un impatto negativo sulla sicurezza globale di internet;

Or. en

Motivazione

Questo dovrebbe essere riconosciuto come uno degli obiettivi principali dei sistemi di certificazione.

Emendamento 344
Marietje Schaake, Matthijs van Miltenburg, Gerben-Jan Gerbrandy, Jan Philipp Albrecht, Julia Reda, Urmas Paet, Kaja Kallas, Pavel Telička, Dita Charanzová, Neena Gill, Morten Løkkegaard

Proposta di regolamento
Articolo 8 – comma 1 – lettera c bis (nuova)

Testo della Commissione	*Emendamento*
	(c bis) sostiene e promuove la definizione e l'attuazione di politiche di divulgazione coordinata delle vulnerabilità e di procedure di esame della divulgazione di vulnerabilità da parte dei governi.

Or. en

Emendamento 345
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 8 – comma 1 – lettera c ter (nuova)

Testo della Commissione	*Emendamento*
	(c ter) redige linee guida relative alle modalità e alle tempistiche secondo cui gli Stati membri sono tenuti a 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 conformemente al titolo III del presente regolamento, comprese linee guida sul coordinamento delle politiche di divulgazione coordinata;

Or. en

Motivazione

L'identificazione e la divulgazione responsabile delle vulnerabilità è un modo per realizzare l'obiettivo dell'ENISA, pertanto occorre aggiungere un compito specifico.

Emendamento 346
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 8 – comma 1 – lettera c quater (nuova)

Testo della Commissione	*Emendamento*
	(c quater) redige linee guida e raccomandazioni sui requisiti minimi di sicurezza per i dispositivi informatici immessi sul mercato dell'UE o esportati dall'Unione, sostenendo in tal modo il rapido processo legislativo necessario in questo specifico caso.

Or. en

Motivazione

L'esigenza urgente di garantire la sicurezza dei dispositivi dei consumatori connessi e dei futuri dispositivi IoT può essere sostenuta dalla Commissione attraverso atti vincolanti, ma l'ENISA deve gettare le basi a tale scopo.

Emendamento 347
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 9 – comma 1 – lettera b

Testo della Commissione	*Emendamento*
(b) effettua analisi strategiche a lungo termine delle minacce e degli incidenti di cibersicurezza al fine di individuare le tendenze emergenti e contribuire a prevenire i problemi connessi alla cibersicurezza;	(b) effettua analisi strategiche a lungo termine delle minacce***, delle vulnerabilità*** e degli incidenti di cibersicurezza al fine di individuare le tendenze emergenti e contribuire a prevenire i problemi connessi alla cibersicurezza;

Or. en

Emendamento 348
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 9 – comma 1 – lettera c

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

Or. en

Emendamento 349
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 9 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per ***i singoli*** utenti destinate a cittadini e organizzazioni;	(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per ***gli*** utenti destinate a cittadini e organizzazioni***, e promuove l'adozione di valide misure preventive in materia di sicurezza informatica e di protezione dei dati e di tutela della vita privata affidabili***;

Or. en

Motivazione

In questo modo si chiarisce l'ambito delle attività di sensibilizzazione, sottolineando l'importanza di intervenire in un'ottica di prevenzione.

Emendamento 350
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 9 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) ***sensibilizza*** l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;	(e) ***sviluppa vaste campagne strategiche finalizzate a sensibilizzare*** l'opinione pubblica sui rischi connessi alla cibersicurezza ***e alle vulnerabilità*** e fornisce orientamenti ***e formazione*** in materia di buone pratiche per i singoli utenti destinate a cittadini e organizzazioni;

Or. en

Emendamento 351
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 9 – comma 1 – lettera e

Testo della Commissione	*Emendamento*
(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e fornisce orientamenti in materia di buone pratiche per ***i singoli*** utenti destinate a cittadini e organizzazioni;	(e) sensibilizza l'opinione pubblica sui rischi connessi alla cibersicurezza e ***sulle pratiche di igiene informatica e*** fornisce orientamenti in materia di buone pratiche per ***gli*** utenti destinate a cittadini e organizzazioni***, al fine di migliorare la loro ciberresilienza***;

Or. en

Emendamento 352
Martina Werner

Proposta di regolamento
Articolo 9 – comma 1 – lettera e

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

Or. en

Emendamento 353
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 9 – comma 1 – lettera g

Testo della Commissione	*Emendamento*
(g) organizza regolarmente, in collaborazione con gli Stati membri e con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, campagne di sensibilizzazione al fine di rafforzare la cibersicurezza e la sua visibilità nell'Unione.	(g) organizza regolarmente, in collaborazione con gli Stati membri e con le istituzioni, gli organi, gli uffici e le agenzie dell'Unione, campagne di sensibilizzazione al fine di rafforzare la ***consapevolezza riguardo alla*** cibersicurezza ***e ai suoi possibili rischi e minacce per la vita dei cittadini*** e la sua visibilità nell'Unione.

Or. en

Emendamento 354
Seán Kelly

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) sostiene un più stretto coordinamento e lo scambio di migliori pratiche tra gli Stati membri in materia di educazione, igiene informatica e sensibilizzazione sulla cibersicurezza,

agevolando la creazione e il mantenimento di una rete di punti di contatto educativi nazionali.

Or. en

Emendamento 355
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) promuove la diffusa adozione da parte di tutti gli attori sul mercato unico digitale di valide misure preventive in materia di sicurezza informatica e di affidabili tecnologie di protezione dei dati e di rafforzamento della tutela della vita privata come prima linea di difesa dagli attacchi ai sistemi informativi.

Or. en

Motivazione

Emendamento basato sul parere del GEPD (sulle tecnologie di rafforzamento della tutela della vita privata). Il ruolo dell'ENISA dovrebbe estendersi chiaramente oltre il sostegno agli Stati membri, alla Commissione e alle agenzie dell'UE, e dovrebbe essere inoltre più visibile al settore e al pubblico in generale.

Emendamento 356
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) promuove l'adozione da parte di tutti gli attori sul mercato unico digitale di valide misure preventive in materia di sicurezza informatica e di protezione dei dati e di tutela della vita privata affidabili,

ai sensi del regolamento (UE) 2016/679 e del [regolamento 2017/0003/COD].

Or. en

Emendamento 357
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Martina Werner, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) sostiene un più stretto coordinamento e lo scambio di migliori pratiche tra gli Stati membri in materia di educazione, formazione e sviluppo delle competenze in materia di cibersicurezza, igiene informatica e sensibilizzazione.

Or. en

Emendamento 358
Michał Boni, Henna Virkkunen, Massimiliano Salini, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) sostiene un più stretto coordinamento e lo scambio di migliori pratiche tra gli Stati membri in materia di alfabetizzazione sulla cibersicurezza, igiene informatica e sensibilizzazione.

Or. en

Emendamento 359
Evžen Tošenovský

Proposta di regolamento
Articolo 9 – comma 1 – lettera g bis (nuova)

Testo della Commissione	*Emendamento*
	(g bis) agevola la creazione e il mantenimento di una rete di punti di contatto educativi nazionali.

Or. en

Emendamento 360
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 10 – comma 1 – lettera a

Testo della Commissione	*Emendamento*
(a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi ***e*** alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;	(a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi***,*** alle minacce ***e alle vulnerabilità*** attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le ***più avanzate*** tecnologie per la prevenzione dei rischi ***senza mettere a repentaglio la tutela della vita privata e i diritti di libertà dei cittadini***;

Or. en

Emendamento 361
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 10 – comma 1 – lettera a

Testo della Commissione	*Emendamento*

(a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca ***nel settore*** della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;	(a) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca ***nei settori*** della cibersicurezza, ***della protezione dei dati e della tutela della vita privata,*** al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

Or. en

Motivazione

Emendamento basato sul parere del GEPD. I compiti dell'ENISA in materia di ricerca nel settore della protezione dei dati e della tutela della vita privata erano sanciti dal precedente regolamento (UE) n. 526/2013, ma non sono più presenti nella proposta della Commissione. È probabile che la scomparsa di tali compiti in materia di ricerca e consulenza comporti l'interruzione del lavoro dell'ENISA sulle tecnologie di rafforzamento della tutela della vita privata e della protezione dei dati e, più in generale, sulla protezione dei dati sin dalla progettazione e per impostazione predefinita.

Emendamento 362
Răzvan Popa

Proposta di regolamento
Articolo 10 – comma 1 – lettera t

Testo della Commissione	*Emendamento*
(t) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;	(t) fornisce consulenza all'Unione e agli Stati membri sulle esigenze e le priorità in materia di ricerca nel settore della cibersicurezza ***e della protezione dei dati***, al fine di consentire di reagire in maniera efficace ai rischi e alle minacce attuali ed emergenti, anche per quanto riguarda le tecnologie dell'informazione e della comunicazione nuove ed emergenti, e di utilizzare efficacemente le tecnologie per la prevenzione dei rischi;

Or. ro

Emendamento 363
Olle Ludvigsson

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

Testo della Commissione	*Emendamento*
	(c bis) fornendo 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, in collaborazione con il gruppo europeo per la certificazione della cibersicurezza (il "gruppo") istituito a norma dell'articolo 53.

Or. en

Emendamento 364
Clare Moody, Theresa Griffin, Peter Kouroumbashev

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

Testo della Commissione	*Emendamento*
	(c bis) fornendo alle organizzazioni internazionali, ove opportuno, i dati raccolti dall'Agenzia nell'esecuzione del suo mandato, a condizione che ciò non comporti una violazione della normativa dell'Unione sulla protezione dei dati.

Or. en

Motivazione

L'attribuzione di un attacco informatico si basa sui dati raccolti sia dall'industria sia da organismi pubblici. Viste le difficoltà di attribuzione degli attacchi informatici e l'importanza di tale attribuzione, l'Agenzia dovrebbe poter condividere i dati sulle violazioni informatiche con paesi terzi e organizzazioni internazionali come la NATO, al fine di contribuire allo sforzo mondiale per contrastare la criminalità informatica e gli attacchi informatici.

Emendamento 365
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 13 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro ***e*** due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.	1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro**,** due rappresentanti nominati dalla Commissione ***e dal Parlamento europeo e, dopo la sua istituzione a norma dell'articolo 20, tre rappresentanti del gruppo permanente di portatori di interessi, uno dei quali rappresenta gli interessi dei consumatori***. Tutti i rappresentanti hanno diritto di voto.

Or. en

Emendamento 366
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 13 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.	1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro***, tre rappresentanti del gruppo permanente dei portatori di interessi, uno dei quali deve rappresentare gli interessi dei consumatori,*** e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.

Or. en

Motivazione

La proposta dovrebbe garantire che tutti i portatori di interessi siano adeguatamente rappresentati nella struttura di governance dell'ENISA.

Emendamento 367
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 13 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno diritto di voto.	1. Il consiglio di amministrazione è composto da un rappresentante per ciascuno Stato membro e due rappresentanti nominati dalla Commissione. Tutti i rappresentanti hanno ***pari*** diritto di voto.

Or. en

Emendamento 368
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 13 – paragrafo 3

Testo della Commissione	*Emendamento*
3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata ***tra uomini e donne*** nel consiglio di amministrazione.	3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza ***di genere*** equilibrata nel consiglio di amministrazione.

Or. en

Emendamento 369
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 13 – paragrafo 3

Testo della Commissione	*Emendamento*
3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata ***tra uomini e donne*** nel consiglio di amministrazione.	3. I membri del consiglio di amministrazione e i loro supplenti sono nominati in base alle loro conoscenze in materia di cibersicurezza, tenendo conto delle pertinenti competenze gestionali, amministrative e di bilancio. La Commissione e gli Stati membri si sforzano di limitare l'avvicendamento dei loro rappresentanti nel consiglio di amministrazione, al fine di assicurarne la continuità dei lavori. La Commissione e gli Stati membri mirano a conseguire una rappresentanza equilibrata ***in termini di genere*** nel consiglio di amministrazione.

Or. en

Emendamento 370
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 13 – paragrafo 4

Testo della Commissione	*Emendamento*
4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di ***quattro*** anni. Il mandato è rinnovabile.	4. La durata del mandato dei membri del consiglio di amministrazione e dei loro supplenti è di ***cinque*** anni. Il mandato è rinnovabile.

Or. en

Emendamento 371

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

Proposta di regolamento
Articolo 15 – comma 1

Testo della Commissione	*Emendamento*
Il consiglio di amministrazione elegge tra i propri membri, a maggioranza dei due terzi dei membri, un presidente e un vicepresidente con un mandato di ***quattro*** anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.	Il consiglio di amministrazione elegge tra i propri membri, a maggioranza dei due terzi dei membri, un presidente e un vicepresidente con un mandato di ***cinque*** anni, rinnovabile una sola volta. Tuttavia, qualora il presidente o il vicepresidente cessino di far parte del consiglio di amministrazione in un qualsiasi momento in corso di mandato, questo giunge automaticamente a termine alla stessa data. Il vicepresidente sostituisce ex officio il presidente nel caso in cui quest'ultimo non sia in grado di svolgere i propri compiti.

Or. en

Motivazione

Per favorire la coerenza e la prevedibilità del lavoro dell'ENISA, il mandato del consiglio di amministrazione (compresi il suo presidente e vicepresidente) è allineato a quello del direttore esecutivo. È allineato, inoltre, al mandato del gruppo permanente di portatori di interessi, che dura la metà di quello del consiglio di amministrazione (due anni e mezzo).

Emendamento 372
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 18 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il	3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il

direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.	direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto. ***Le nomine mirano a conseguire una rappresentanza di genere equilibrata nel comitato esecutivo.***

Or. en

Motivazione

Le nomine al comitato esecutivo devono anche essere finalizzate all'equilibrio di genere, rispecchiando le disposizioni relative al consiglio di amministrazione all'articolo 13, paragrafo 3.

Emendamento 373
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 18 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.	3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale può anche presiedere il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto. ***La composizione del comitato esecutivo deve mirare a conseguire una rappresentanza di genere equilibrata.***

Or. en

Emendamento 374
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 18 – paragrafo 3

Testo della Commissione	*Emendamento*
3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale ***può anche presiedere*** il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.	3. Il comitato esecutivo consta di cinque membri designati tra i membri del consiglio di amministrazione, tra cui figurano il presidente del consiglio di amministrazione, il quale ***non presiede*** il comitato esecutivo, e un rappresentante della Commissione. Il direttore esecutivo partecipa alle riunioni del comitato esecutivo senza diritto di voto.

Or. en

Emendamento 375
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 18 – paragrafo 4

Testo della Commissione	*Emendamento*
4. La durata del mandato dei membri del ***consiglio di amministrazione*** è di ***quattro*** anni. Il mandato è rinnovabile.	4. La durata del mandato dei membri del ***comitato esecutivo*** è di ***cinque*** anni. Il mandato è rinnovabile.

Or. en

Motivazione

Allineamento alla formulazione suggerita per il consiglio di amministrazione.

Emendamento 376
Peter Kouroumbashev, Zigmantas Balčytis, Edouard Martin, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 19 – paragrafo 5 bis (nuovo)

Testo della Commissione	*Emendamento*
	5 bis. Il direttore esecutivo è tenuto a presentare alle commissioni competenti

del Parlamento europeo, due volte all'anno, una relazione sullo stato della cibersicurezza in Europa. Il direttore esecutivo deve essere invitato dal Parlamento, inoltre, a fornire un contributo dell'ENISA riguardo a un eventuale strumento legislativo dell'UE che imponga obblighi in materia di cibersicurezza.

Or. en

Motivazione

Il Parlamento dovrebbe avere il diritto di esercitare una funzione di sorveglianza sulla politica in materia di cibersicurezza, mentre l'Agenzia dovrebbe essere adeguatamente consultata per ogni progetto legislativo riguardante la cibersicurezza.

Emendamento 377
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, José Blanco López, Theresa Griffin, Miapetra Kumpula-Natri, Eva Kaili, Dan Nica, Clare Moody, Kathleen Van Brempt

Proposta di regolamento
Articolo 19 – paragrafo 5 ter (nuovo)

Testo della Commissione	*Emendamento*
	5 ter. Il direttore esecutivo ha facoltà, inoltre, di agire in veste di consulente speciale istituzionale sulla politica in materia di cibersicurezza per il presidente della Commissione europea, secondo il mandato definito nella decisione della Commissione C(2014) 541 del 6 febbraio 2014.

Or. en

Emendamento 378
Massimiliano Salini

Proposta di regolamento
Articolo 20 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione***, su proposta del direttore esecutivo,*** istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali ***il settore*** delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.	1. Il consiglio di amministrazione istituisce un gruppo permanente di portatori di interessi ***per ogni sistema*** composto da esperti riconosciuti che rappresentano i portatori di interessi, quali ***gli utenti e i fornitori*** delle TIC, ***le associazioni di piccole e medie imprese,*** i fornitori ***e gli utenti*** delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni ***e associazioni*** dei consumatori, gli esperti universitari in materia di cibersicurezza***, le organizzazioni europee di normazione, quali definite all'articolo 2, paragrafo 8, del regolamento (UE) n. 1025/2012, le agenzie e gli organismi settoriali pertinenti dell'Unione*** e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

Or. en

Emendamento 379
Martina Werner

Proposta di regolamento
Articolo 20 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti	1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, ***compresi i gruppi delle PMI,*** i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza, ***le organizzazioni***

notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.	***europee di normazione e gli organi di valutazione della conformità*** e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati. ***Il consiglio di amministrazione garantisce un idoneo equilibrio tra i diversi gruppi di portatori di interessi.***

Or. en

Emendamento 380
Michał Boni, Seán Kelly, Henna Virkkunen, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 20 – paragrafo 1

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

Or. en

Emendamento 381

Gunnar Hökmark

Proposta di regolamento
Articolo 20 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali ***il settore*** delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.	1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali ***i settori europeo e internazionale*** delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico ***e le relative associazioni***, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

Or. en

Emendamento 382
Marisa Matias, Xabier Benito Ziluaga, Sofia Sakorafa

Proposta di regolamento
Articolo 20 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni dei consumatori, gli esperti universitari in materia di cibersicurezza e i rappresentanti delle autorità competenti notificati a norma della [direttiva che	1. Il consiglio di amministrazione, su proposta del direttore esecutivo, istituisce un gruppo permanente di portatori di interessi composto da esperti riconosciuti che rappresentano i portatori di interessi, quali il settore delle TIC, ***le PMI,*** i fornitori delle reti o dei servizi di comunicazione elettronica accessibili al pubblico, le organizzazioni ***di tutela*** dei consumatori, ***le università e*** gli esperti universitari in materia di cibersicurezza ***e protezione dei dati*** e i rappresentanti delle

istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.	autorità competenti notificati a norma della [direttiva che istituisce il codice europeo delle comunicazioni elettroniche], nonché le autorità di contrasto e le autorità di controllo preposte alla protezione dei dati.

Or. en

Emendamento 383
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 20 – paragrafo 1

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

Or. en

Emendamento 384
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 20 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici.	2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici. ***Le procedure seguono le migliori pratiche atte ad assicurare un'equa rappresentanza e la parità dei diritti per tutti i portatori di interessi e mirano a garantire una rappresentanza di genere equilibrata.***

Or. en

Motivazione

È necessaria una rappresentanza equa e giusta per conseguire i migliori risultati. Inoltre, l'obiettivo dell'equilibrio di genere, che rispecchia le disposizioni dell'articolo 13, punto 3, e dell'articolo 18, punto 3, deve essere anch'esso perseguito in questo caso.

Emendamento 385
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 20 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici.	2. Le procedure per il gruppo permanente di portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del consiglio di amministrazione, la proposta del direttore esecutivo e il funzionamento del gruppo sono specificati nel regolamento interno dell'Agenzia e resi pubblici. ***Le procedure seguono le migliori pratiche per un'equa rappresentanza e la parità dei diritti per tutti i portatori di interessi e perseguono un approccio equilibrato in termini di genere.***

Or. en

Emendamento 386
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 20 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. La composizione del gruppo permanente dei portatori di interessi comprende un minimo di cinque organizzazioni di consumatori e organizzazioni della società civile.

Or. en

Motivazione

La composizione attuale del gruppo permanente dei portatori di interessi comprende un solo esperto, su trenta membri del gruppo, in rappresentanza della posizione dei consumatori, il che non è sufficiente.

Emendamento 387
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 20 – paragrafo 2 bis (nuovo)

Testo della Commissione	*Emendamento*
	2 bis. La composizione del gruppo permanente dei portatori di interessi comprende un minimo di cinque organizzazioni in rappresentanza dei consumatori e/o della società civile.

Or. en

Emendamento 388
Michał Boni, Massimiliano Salini, Krišjānis Kariņš, Marian-Jean Marinescu, Gunnar Hökmark

Proposta di regolamento
Articolo 20 – paragrafo 4 bis (nuovo)

Testo della Commissione	*Emendamento*
	4 bis. Il gruppo permanente dei portatori di interessi fornisce aggiornamenti periodici sulla sua pianificazione durante l'anno e stabilisce gli obiettivi nel suo programma di lavoro, che viene pubblicato ogni sei mesi al fine di garantire la trasparenza.

Or. en

Emendamento 389
Peter Kouroumbashev, Zigmantas Balčytis, Carlos Zorrinho, Theresa Griffin, Miroslav Poche, Miapetra Kumpula-Natri, Clare Moody

Proposta di regolamento
Articolo 20 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 20 bis
	Gruppo di certificazione dei portatori di interessi
	1. Il direttore esecutivo istituisce un gruppo di certificazione dei portatori di interessi, composto da esperti riconosciuti che rappresentano i gruppi dei consumatori, le università, gli organismi di normazione, gli operatori di servizi essenziali quali definiti nell'allegato II della direttiva (UE) 2016/1148, e il settore delle TIC, comprese le PMI.
	2. Le procedure per il gruppo di certificazione dei portatori di interessi, in particolare per quanto riguarda il numero, la composizione e la nomina dei membri da parte del direttore esecutivo e il funzionamento del gruppo, sono specificati nel regolamento interno dell'Agenzia e resi pubblici.

3. Il mandato dei membri del gruppo di certificazione dei portatori di interessi è di due anni e mezzo. Il mandato è rinnovabile. I membri del consiglio di amministrazione non possono essere membri del gruppo di certificazione dei portatori di interessi. I membri del gruppo permanente di portatori di interessi possono essere membri anche del gruppo di certificazione dei portatori di interessi. Gli esperti della Commissione e degli Stati membri sono autorizzati a presenziare, dietro invito, alle riunioni del gruppo di certificazione dei portatori di interessi. I rappresentanti di altri organismi considerati pertinenti dal direttore esecutivo che non sono membri del gruppo di certificazione dei portatori di interessi possono essere invitati a partecipare alle riunioni di tale gruppo e alle sue attività.

4. Il gruppo di certificazione dei portatori di interessi fornisce consulenza all'Agenzia relativamente allo svolgimento delle sue attività riguardo al titolo III del presente regolamento. In particolare ha facoltà di proporre all'ENISA, agli Stati membri e alla Commissione la preparazione di una proposta di sistema europeo di certificazione della cibersicurezza, come previsto all'articolo 44 del presente regolamento, e di partecipare alle procedure descritte agli articoli da 43 a 48 e all'articolo 53 del presente regolamento per ottenere l'approvazione di tali sistemi.

5. Per garantire che il gruppo di certificazione dei portatori di interessi possieda le necessarie competenze, il direttore esecutivo o i membri di tale gruppo nominano membri ad hoc per l'elaborazione, la definizione o l'adozione di una nuova proposta di sistema. Tali membri ad hoc hanno gli stessi diritti e obblighi dei membri nominati e hanno facoltà di fornire le loro competenze in qualsiasi fase della definizione e/o dell'approvazione della rispettiva proposta

di sistema. Un membro ad hoc può contribuire alle attività del gruppo di certificazione dei portatori di interessi relativamente a più di una proposta di sistema.

Or. en

Motivazione

Per garantire un'idonea partecipazione dei portatori di interessi alla proposta, elaborazione e approvazione dei sistemi europei di certificazione della cibersicurezza, come definiti dal titolo III del presente regolamento, l'ENISA è incaricata di istituire un gruppo di certificazione dei portatori di interessi, che partecipa a pieno titolo a tali processi. Il gruppo di certificazione dei portatori di interessi è composto da esperti riconosciuti che rappresentano i gruppi dei consumatori, le università, gli organismi di normazione, gli operatori di servizi essenziali quali definiti nell'allegato II della direttiva (UE) 2016/1148, e il settore delle TIC, comprese le PMI.

Emendamento 390
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 20 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 20 bis
	Forum consultivo
	La Commissione, insieme all'Agenzia, provvede affinché nello svolgimento delle sue attività rispetti, per quanto riguarda ciascuna misura di esecuzione, una partecipazione equilibrata di rappresentanti degli Stati membri e di tutte le pertinenti parti interessate da tale prodotto o gruppo di prodotti come l'industria, compresi PMI, artigiani, sindacati, commercianti, dettaglianti, importatori, gruppi per la tutela ambientale e organizzazioni dei consumatori. Tali parti si riuniscono in un forum consultivo. L'esito di tale forum può dare impulso alla proposta di un

sistema. Il regolamento interno del forum è stabilito dalla Commissione.

Or. en

Emendamento 391
Pavel Telička, Carolina Punset, Morten Løkkegaard, Gesine Meissner, Morten Helveg Petersen

Proposta di regolamento
Articolo 21 bis (nuovo)

Testo della Commissione	*Emendamento*
	Articolo 21 bis
	Richieste all'Agenzia
	1. L'Agenzia deve istituire e gestire uno sportello unico attraverso il quale possano essere presentate richieste di consulenza e assistenza che rientrano nell'ambito degli obiettivi e dei compiti dell'Agenzia. Tali richieste devono essere corredate di una documentazione informativa che spieghi la questione da trattare. L'Agenzia deve valutare il possibile impatto sulle risorse e, a tempo debito, dare un seguito alle richieste. Qualora respinga una richiesta, l'Agenzia motiva il proprio rifiuto.
	2. Le richieste di cui al paragrafo 1 possono provenire:
	(a) dal Parlamento europeo
	(b) dal Consiglio
	(c) dalla Commissione
	(d) da un qualsiasi organismo competente designato da uno Stato membro quale autorità nazionale di regolamentazione definita all'articolo 2 della direttiva 2002/21/CE.
	3. Le modalità pratiche di applicazione dei paragrafi 1 e 2, con particolare riguardo alla presentazione, alla definizione delle priorità e al seguito da dare alle richieste come pure all'informazione, sono definite

	dal consiglio di amministrazione nel regolamento interno dell'Agenzia.

Or. en

Emendamento 392
Dario Tamburrano, Marco Zullo, Fabio Massimo Castaldo

Proposta di regolamento
Articolo 23 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.	2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare ***sul programma di lavoro e i relativi progressi*** e sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.

Or. en

Emendamento 393
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 23 – paragrafo 2

Testo della Commissione	*Emendamento*
2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.	2. L'Agenzia provvede a che il pubblico e le parti interessate dispongano di informazioni appropriate, obiettive, affidabili e facilmente accessibili, in particolare ***sulle discussioni e*** sui risultati del suo lavoro. Inoltre, rende pubbliche le dichiarazioni di interessi rese a norma dell'articolo 22.

Or. en

Motivazione

La trasparenza deve poter essere attuata, tenendo conto dell'applicazione dell'articolo 24.

Emendamento 394
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 34 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Il consiglio di amministrazione adotta una decisione che stabilisce le norme relative al distacco di esperti nazionali presso l'Agenzia.	2. Il consiglio di amministrazione adotta una decisione che stabilisce le norme relative al distacco di esperti nazionali presso l'Agenzia***, tra l'altro vietando le pratiche a titolo gratuito e promuovendo la remunerazione equa***.

Or. en

Motivazione

Parità di retribuzione a parità di lavoro: per ottenere il personale migliore è inaccettabile che l'UE imponga agli esperti di vari Stati membri di lavorare agli stessi compiti con differenti livelli di retribuzione nazionali.

Emendamento 395
Marisa Matias, Clare Moody, Theresa Griffin

Proposta di regolamento
Articolo 39 – paragrafo 1

Testo della Commissione	*Emendamento*
1. Se necessario ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'Agenzia può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'Agenzia può, previa approvazione da parte della Commissione, istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali. Detti	1. Se necessario ai fini del conseguimento degli obiettivi stabiliti nel presente regolamento, l'Agenzia può cooperare con le autorità competenti di paesi terzi, con le organizzazioni internazionali o con entrambi. A tal fine l'Agenzia può, previa approvazione da parte della Commissione, istituire accordi di lavoro con le autorità dei paesi terzi e con le organizzazioni internazionali. ***La***

accordi non creano obblighi giuridici per l'Unione e gli Stati membri.	***cooperazione con la NATO, laddove presente, può comprendere esercitazioni congiunte sulla cibersicurezza e il coordinamento congiunto per la risposta agli incidenti informatici.*** Detti accordi non creano obblighi giuridici per l'Unione e gli Stati membri.

Or. en

Motivazione

Data la natura transfrontaliera degli incidenti informatici, l'ENISA dovrebbe intervenire, ove opportuno, insieme ad attori della cibersicurezza in Europa, tra cui la NATO. Ciò è particolarmente importante considerato che la NATO potrebbe avere capacità informatiche di cui l'ENISA non dispone, e viceversa. In un contesto di intensificazione globale degli attacchi informatici contro gli Stati, è essenziale per la sicurezza dell'Europa che l'ENISA cooperi con organizzazioni internazionali come la NATO a livello internazionale.

Emendamento 396
Jakop Dalunde, Reinhard Bütikofer
a nome del gruppo Verts/ALE

Proposta di regolamento
Articolo 41 – paragrafo 2

Testo della Commissione	*Emendamento*
2. Lo Stato membro che ospita l'Agenzia fornisce le migliori condizioni possibili al fine di garantire il corretto funzionamento dell'Agenzia, compresi l'accessibilità della sede, l'esistenza di strutture scolastiche adeguate per i figli del personale, un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi.	2. Lo Stato membro che ospita l'Agenzia fornisce le migliori condizioni possibili al fine di garantire il corretto funzionamento dell'Agenzia, compresi l'accessibilità della sede ***centrale e degli altri uffici tramite un aeroporto internazionale***, l'esistenza di strutture scolastiche adeguate per i figli del personale, un accesso adeguato al mercato del lavoro, alla sicurezza sociale e alle cure mediche per i figli e i coniugi.

Or. en

Motivazione

Sebbene lo Stato ospitante sia una questione che esula dal presente regolamento, garantire le migliori condizioni per il funzionamento dell'Agenzia rientra nel suo campo di applicazione, e nel presente emendamento si forniscono orientamenti a tal fine.