(4) Mettendo a disposizione del pubblico le informazioni pertinenti, l'Agenzia dell'Unione europea per la cibersicurezza (*European Union Agency for Network and Information Security* — ENISA), istituita dal regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio ([5]), contribuisce allo sviluppo del settore della cibersicurezza nell'Unione, in particolare le PMI e le start-up. L'ENISA dovrebbe puntare a una cooperazione più stretta con le università e gli istituti di ricerca al fine di contribuire alla riduzione della dipendenza da prodotti e servizi della cibersicurezza provenienti dall'esterno dell'Unione e a rinforzare le filiere all'interno dell'Unione.

(5) Gli attacchi informatici sono in aumento e la maggiore vulnerabilità alle minacce e agli attacchi informatici di un'economia e di una società connesse impone un rafforzamento delle difese. Tuttavia, mentre gli attacchi informatici avvengono spesso attraverso le frontiere, le competenze in materia di cibersicurezza e autorità incaricate dell'applicazione della legge e le relative risposte politiche sono prevalentemente nazionali. Gli incidenti su vasta scala possono ostacolare la prestazione di servizi essenziali in tutto il territorio dell'Unione. Ciò richiede capacità effettive e coordinate di risposta e di gestione delle crisi a livello di Unione, sulla base di apposite politiche e strumenti di più ampia portata per la solidarietà europea e l'assistenza reciproca. Inoltre, una valutazione periodica dello stato della cibersicurezza e della resilienza nell'Unione, che sia basata su dati affidabili a livello di Unione, e previsioni sistematiche degli sviluppi, delle sfide e delle minacce futuri, a livello di Unione e a livello mondiale, sono importanti per i responsabili delle politiche, il settore e gli utenti.

(6) 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 il rafforzamento ulteriore delle capacità e della preparazione degli Stati membri e delle imprese e il miglioramento della cooperazione, la condivisione di informazioni e il coordinamento tra gli Stati membri e le istituzioni, gli organi e gli organismi dell'Unione. 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 nei casi di crisi e incidenti transfrontalieri su vasta scala, pur tenendo conto dell'importanza di mantenere e rafforzare ulteriormente le capacità nazionali di risposta alle minacce informatiche di qualsiasi dimensione.

(7) Sono inoltre necessari ulteriori sforzi per accrescere la consapevolezza dei cittadini, delle organizzazioni e delle imprese circa le questioni riguardanti la cibersicurezza. In aggiunta, dato che gli incidenti minano la fiducia nei fornitori di servizi digitali e nel mercato unico digitale stesso, soprattutto fra i consumatori, essa dovrebbe essere ulteriormente rafforzata fornendo informazioni in maniera trasparente in merito al livello di sicurezza dei prodotti TIC, dei servizi TIC e dei processi TIC che evidenzi che persino un livello elevato di certificazione della cibersicurezza non può garantire che un prodotto TIC, un servizio TIC o un processo TIC sia completamente sicuro. Un aumento di fiducia può essere agevolato da una certificazione a livello di Unione che preveda requisiti e criteri di valutazione comuni in materia di cibersicurezza validi per tutti i settori e i mercati nazionali.

(8) La cibersicurezza non costituisce soltanto una questione relativa alla tecnologia, ma anche una in cui il comportamento umano è di pari importanza. Di conseguenza, è opportuno promuovere energicamente l'«igiene informatica», vale a dire semplici misure di routine che, se attuate e svolte regolarmente da cittadini, organizzazioni e imprese, riducono al minimo la loro esposizione a rischi derivanti da minacce informatiche.

(9) Al fine di rafforzare le strutture della cibersicurezza dell'Unione, è importante mantenere e sviluppare le capacità degli Stati membri di rispondere in modo globale alle minacce informatiche, compresi gli incidenti transfrontalieri.

(10) Le imprese e i singoli consumatori dovrebbero disporre di informazioni precise sul livello di affidabilità con cui è stata certificata la sicurezza dei loro prodotti TIC, servizi TIC e processi TIC. Allo stesso tempo, nessun prodotto TIC o servizio TIC garantisce completamente la cibersicurezza e bisogna promuovere regole basilari sull'igiene informatica, dando loro la priorità. Alla luce della crescente disponibilità di dispositivi IoT, vi è una serie di misure volontarie che il settore privato può adottare per rafforzare la fiducia nella sicurezza dei prodotti TIC, servizi TIC e processi TIC.

(11) I moderni prodotti e sistemi TIC spesso integrano e utilizzano una o più tecnologie e componenti terzi quali moduli software, biblioteche o interfacce per programmi applicativi. Tale utilizzo, detto «dipendenza», potrebbe presentare rischi supplementari connessi alla cibersicurezza in quanto le vulnerabilità riscontrate in componenti terzi potrebbero pregiudicare anche la sicurezza dei prodotti TIC, servizi TIC e processi TIC. In molti casi, l'individuazione e la documentazione di tali dipendenze consentono agli utenti finali dei prodotti TIC, servizi TIC e processi TIC di migliorare le loro attività di gestione dei rischi in materia di cibersicurezza ottimizzando, ad esempio, le procedure messe in atto per individuare le vulnerabilità e porvi rimedio.

([5]) Regolamento (UE) n. 526/2013 del Parlamento europeo e del Consiglio, del 21 maggio 2013, relativo all'Agenzia dell'Unione europea per la sicurezza delle reti e dell'informazione (ENISA) e che abroga il regolamento (CE) n. 460/2004 (GU L 165 del 18.6.2013, pag. 41).