AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA

UN'EUROPA AFFIDABILE E SICURA DAL PUNTO DI VISTA INFORMATICO

Strategia ENISA

Giugno 2020

UN'EUROPA AFFIDABILE E SICURA DAL PUNTO DI VISTA INFORMATICO

AGENZIA DELL'UNIONE EUROPEA PER LA CIBERSICUREZZA

PREFAZIONE

Da oltre 15 anni l'ENISA (l'Agenzia dell'Unione europea per la cibersicurezza) svolge un ruolo determinante per realizzare l'ambizione dell'UE di rafforzare la fiducia e la sicurezza digitali in tutta Europa, insieme agli Stati membri, alle istituzioni e alle agenzie dell'UE. Riunendo le comunità, l'ENISA ha contribuito positivamente a consolidare le capacità di preparazione e di risposta dell'Europa in caso di incidenti informatici.

Contestualmente, la digitalizzazione della nostra economia e della società è drasticamente aumentata, come ha dimostrato la crisi COVID-19, durante la quale si è reso fondamentale un ricorso massiccio e collettivo a soluzioni informatiche da remoto per consentire il proseguimento di molte attività. Questa crisi ha mostrato quanto gli autori di attacchi informatici approfittino della nostra dipendenza da tali tecnologie, oltre a rivelare come il panorama delle minacce informatiche si sia esteso dagli attacchi mirati a nuove forme di minacce di vasta portata, dirette a milioni di imprese e cittadini, con un numero crescente di incidenti causati da sofisticati ransomware. Il rapido sviluppo di prodotti e servizi digitali (dal Cloud e dalle videoconferenze al 5G e all'intelligenza artificiale) ha inoltre posto nuove sfide da scoprire e affrontare.

Con il suo mandato permanente e il rafforzamento dei compiti e delle capacità, l'ENISA è più che mai intesa a svolgere un ruolo di guida per aiutare l'UE e i suoi Stati membri a tenere il passo di queste sfide, mentre si apre una nuova era per la cibersicurezza in Europa.

A tal fine, l'ENISA si adopererà per anticipare le relative tendenze, acquisirà e metterà a disposizione di tutti competenze e conoscenze all'avanguardia, e sosterrà la Commissione europea e gli Stati membri nell'assistenza agli operatori pubblici e privati e ai cittadini in materia di prevenzione e gestione dei rischi connessi agli incidenti informatici. Con l'attuazione del quadro di certificazione della cibersicurezza, l'ENISA contribuirà a un cambiamento di paradigma, migliorando il livello di sicurezza delle soluzioni digitali utilizzate in Europa e aumentando in tal modo le capacità di scelta e affidamento di tutti. L'Agenzia sosterrà inoltre attivamente la comunità operativa europea della cibersicurezza cooperando strettamente e preparando una reazione comune al prossimo incidente informatico su vasta scala che colpirà l'Europa.

Quando l'ENISA assumerà la sua nuova funzione, l'apertura, l'agilità e l'affidabilità saranno gli elementi trainanti delle sue operazioni quotidiane, intensificando nel contempo la collaborazione con gli Stati membri e con la Commissione europea per armonizzare gli approcci. L'ENISA si impegnerà inoltre al fine di migliorare il suo impatto ambientale nel contesto della crisi climatica in corso e di costituire un ambiente di lavoro inclusivo e responsabile sotto il profilo sociale.

Il presente documento strategico, elaborato grazie all'impegno di tutto il personale dell'ENISA, dei membri del suo consiglio di amministrazione e del suo gruppo consultivo in un processo collaborativo e inclusivo, stabilisce i chiari obiettivi che guideranno l'attività dell'Agenzia negli anni a venire per far fronte alle sfide che la attendono.

Per conto del consiglio di amministrazione

Jean-Baptiste Demaison
Presidente del consiglio di amministrazione

Krzysztof Silicki
Vicepresidente del consiglio di amministrazione

VISIONE

Un'Europa affidabile e sicura dal punto di vista informatico

MISSIONE

La missione dell'Agenzia dell'Unione europea per la cibersicurezza (ENISA) consiste nel conseguire un elevato livello comune di cibersicurezza in tutta l'Unione, collaborando con la comunità in senso lato. A tal fine, l'Agenzia opera come centro di competenze nel campo della cibersicurezza, ricevendo e fornendo consulenza e assistenza tecnica indipendente e di elevata qualità in materia di sicurezza informatica agli Stati membri e agli organismi dell'UE, oltre a contribuire all'elaborazione e all'attuazione delle politiche informatiche dell'Unione.

Il nostro obiettivo è rafforzare la fiducia nell'economia connessa, aumentare la resilienza e l'affidabilità delle infrastrutture e dei servizi dell'UE e garantire la sicurezza digitale della nostra società e dei nostri cittadini, con l'ambizione di essere un'organizzazione agile, responsabile sotto il profilo ambientale e sociale e incentrata sulle persone.

VALORI

Mentalità comunitaria
L'ENISA collabora con le comunità, rispettandone le competenze e le conoscenze, e promuove le sinergie e la fiducia per assolvere nel modo migliore alla sua missione.

Eccellenza
L'ENISA mira a disporre di competenze all'avanguardia nella sua attività, mantiene i massimi livelli qualitativi di funzionamento e valuta le proprie prestazioni per cercare di migliorare continuamente attraverso l'innovazione e la previsione.

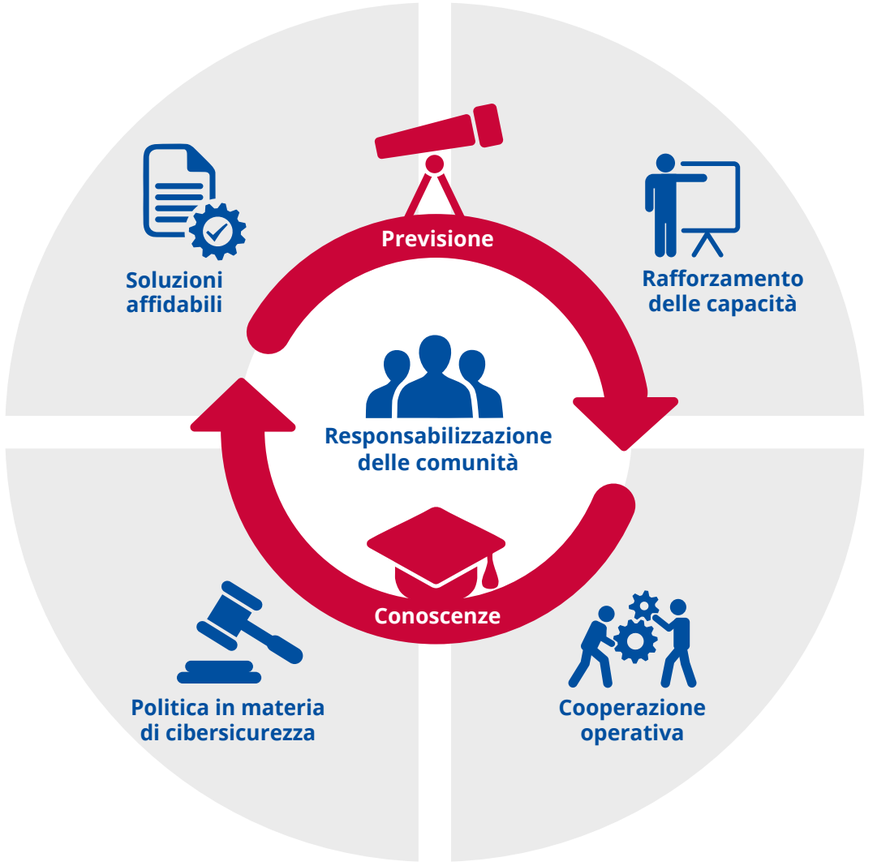
Integrità/etica
L'ENISA osserva i principi etici nonché le norme e gli obblighi pertinenti nei suoi servizi e nell'ambiente di lavoro, garantendo equità e inclusività.

Rispetto
In tutti i suoi servizi e nel suo ambiente di lavoro, l'ENISA rispetta i diritti e i valori europei fondamentali, soddisfacendo le aspettative delle sue parti interessate.

Responsabilità
L'ENISA impegna la propria responsabilità, garantendo in tal modo l'integrazione della dimensione sociale e di quella ambientale nelle pratiche e nelle procedure.

Trasparenza
L'ENISA adotta procedure, strutture e processi aperti, concreti e indipendenti, in modo da ridurre preconcetti, ambiguità, oscurità e frodi.

OBIETTIVI STRATEGICI



OS1

Obiettivo strategico

COMUNITÀ RESPONSABILIZZATE E IMPEGNATE IN TUTTO L'ECOSISTEMA DELLA CIBERSICUREZZA

Contesto

La cibersicurezza è una responsabilità condivisa. L'Europa persegue un quadro di cooperazione transettoriale e onnicomprensivo e l'ENISA svolge un ruolo chiave nel promuovere la cooperazione attiva tra le parti interessate alla cibersicurezza negli Stati membri e nelle istituzioni e agenzie dell'UE, sforzandosi di garantire la complementarità degli sforzi comuni, conferendo valore aggiunto alle parti interessate, esplorando le sinergie e avvalendosi efficacemente di competenze e risorse limitate in tema di sicurezza informatica. Le comunità devono essere responsabilizzate affinché il modello di cibersicurezza si evolva.

Cosa vogliamo conseguire

- Un corpus europeo all'avanguardia di conoscenze sui concetti e sulle pratiche in materia di cibersicurezza per sviluppare la cooperazione tra gli operatori principali in tale ambito, promuovere l'esperienza acquisita e le competenze europee e creare nuove sinergie.
- Un ecosistema informatico responsabilizzato che comprenda le autorità degli Stati membri, le istituzioni, le agenzie e gli organismi dell'UE, associazioni, centri di ricerca e università, l'industria, operatori privati e cittadini, tutti impegnati a svolgere il proprio ruolo per rendere l'Europa sicura dal punto di vista informatico.

OS2

Obiettivo strategico

LA CIBERSICUREZZA COME PARTE INTEGRANTE DELLE POLITICHE DELL'UE

Contesto

La cibersicurezza è il fondamento della trasformazione digitale ed è necessaria in tutti i settori; occorre dunque tenerne conto in una vasta gamma di settori politici e iniziative. Non deve essere solo appannaggio di una comunità specializzata di esperti informatici. La cibersicurezza deve pertanto essere integrata in tutti gli ambiti della politica dell'UE. È fondamentale evitare la frammentazione e perseguire un approccio coerente, pur tenendo conto delle specificità di ciascun settore.

Cosa vogliamo conseguire

- Una consulenza e un'assistenza proattive per tutti gli operatori interessati a livello dell'UE, introducendo la dimensione della cibersicurezza nel ciclo di elaborazione delle politiche attraverso orientamenti tecnici affidabili e mirati;
- l'attuazione di quadri di gestione dei rischi per la cibersicurezza in tutti i settori e il loro monitoraggio per tutta la durata del ciclo delle politiche di sicurezza informatica.

OS3

Obiettivo strategico

UNA COOPERAZIONE EFFICACE TRA GLI ATTORI OPERATIVI ALL'INTERNO DELL'UNIONE IN CASO DI INCIDENTI INFORMATICI DI AMPIA PORTATA

Contesto

La cibersicurezza è il presupposto indispensabile per conseguire pienamente i vantaggi della società e dell'economia digitale europea. Gli attacchi informatici non conoscono confini: possono colpire tutti gli strati della società e l'Unione deve essere pronta a reagire nell'eventualità di crisi e di attacchi informatici massicci (transfrontalieri e su vasta scala). Le interdipendenze transfrontaliere hanno evidenziato la necessità di una cooperazione efficace tra gli Stati membri e le istituzioni dell'UE per una risposta più rapida e un opportuno coordinamento degli sforzi a tutti i livelli (strategico, operativo, tecnico e comunicativo).

Cosa vogliamo conseguire

- Un sostegno transfrontaliero, intersettoriale e costante alla cooperazione tra gli Stati membri e con le istituzioni dell'UE. In particolare, nell'ottica di potenziali incidenti e crisi su vasta scala, un sostegno all'ampliamento della cooperazione tecnica operativa, politica e strategica tra i principali attori operativi per consentire una reazione tempestiva, lo scambio di informazioni, la conoscenza della situazione e la comunicazione delle crisi in tutta l'Unione;
- un intervento tecnico rapido e completo, su richiesta degli Stati membri, per venire incontro alle esigenze tecniche e operative nella gestione degli incidenti e delle crisi.

OS4

Obiettivo strategico

COMPETENZE E CAPACITÀ INNOVATIVE IN MATERIA DI CIBERSICUREZZA IN TUTTA L'UNIONE

Contesto

La frequenza e la sofisticatezza degli attacchi informatici stanno aumentando rapidamente, di pari passo con l'utilizzo di infrastrutture e tecnologie dell'informazione da parte di persone, organizzazioni e industrie. Il fabbisogno di conoscenze e competenze in materia di sicurezza informatica supera l'offerta e l'UE deve investire nello sviluppo di competenze e talenti in questo ambito a tutti i livelli, dai non esperti ai professionisti altamente qualificati; gli investimenti devono puntare non solo ad ampliare il bagaglio di competenze in tema di cibersicurezza negli Stati membri, ma anche a garantire che le diverse comunità operative possiedano le capacità opportune per affrontare il panorama delle minacce informatiche.

Cosa vogliamo conseguire

- Allineamento delle competenze nell'ambito della sicurezza informatica, esperienza professionale e strutture educative per soddisfare la domanda di conoscenze e competenze in materia di cibersicurezza, in costante crescita nell'UE;
- un aumento del livello di base delle relative conoscenze e competenze in tutta l'Unione e la contestuale integrazione della cibernetica nelle nuove discipline;
- abilità ben sviluppate e collaudate, con un'adeguata capacità di far fronte efficacemente a un contesto di minacce in evoluzione in tutta l'UE.

OS5

Obiettivo strategico

UN ELEVATO LIVELLO DI FIDUCIA IN SOLUZIONI DIGITALI SICURE

Contesto

I prodotti e i servizi digitali apportano vantaggi ma comportano anche rischi che devono essere individuati e attenuati. Durante la valutazione della sicurezza delle soluzioni digitali e la verifica della loro affidabilità, è fondamentale adottare un approccio comune inteso a raggiungere un equilibrio tra esigenze sociali, economiche, di mercato e in materia di cibersicurezza. Un'entità neutrale che operi in modo trasparente aumenterà la fiducia dei clienti nelle soluzioni digitali e nell'ambiente digitale nel senso più ampio del termine.

Cosa vogliamo conseguire

- Un ambiente digitale sicuro dal punto di vista informatico in tutta l'UE, in cui i cittadini possano affidarsi a prodotti, servizi e processi informatici attraverso l'attuazione di sistemi di certificazione in settori tecnologici fondamentali.

OS6

Obiettivo strategico

PREVISIONE DELLE SFIDE EMERGENTI E FUTURE IN TEMA DI CIBERSICUREZZA

Contesto

L'utilizzo dei metodi di previsione gioverebbe a numerose nuove tecnologie che sono ancora agli albori o prossime a un'adozione su vasta scala. Attraverso un processo strutturato e favorevole al dialogo tra le parti interessate, i responsabili del processo decisionale e politico potrebbero definire strategie iniziali di attenuazione in grado di migliorare la resilienza dell'UE nei confronti delle minacce alla sicurezza informatica e di trovare soluzioni per far fronte alle sfide emergenti.

Cosa vogliamo conseguire

- Comprendere le tendenze e i modelli emergenti per mezzo di scenari futuri e di previsione che contribuiscano ad attenuare le sfide informatiche delle nostre parti interessate;
- una prima valutazione delle sfide e dei rischi connessi all'adozione di opzioni emergenti future e all'adeguamento a tali opzioni, collaborando nel contempo con le parti interessate per elaborare strategie di attenuazione.

OS7

Obiettivo strategico

UNA GESTIONE EFFICIENTE ED EFFICACE DELLE INFORMAZIONI E DELLE CONOSCENZE SULLA CIBERSICUREZZA PER L'EUROPA

Contesto

L'energia che alimenta il motore della cibersicurezza è l'informazione e la conoscenza. Affinché i professionisti del settore perseguano in maniera efficiente i nostri obiettivi, lavorino in un ambiente in continua evoluzione (sia in termini di sviluppi digitali che in relazione agli operatori) e affrontino le sfide della nostra epoca, abbiamo bisogno di un processo costante di acquisizione, organizzazione, sintesi, analisi, comunicazione e conservazione delle informazioni e delle conoscenze in materia di sicurezza informatica. Tutte le fasi sono essenziali per garantire che le informazioni e le conoscenze siano condivise e ampliate nell'ambito dell'ecosistema europeo della cibersicurezza.

Cosa vogliamo conseguire

- Una gestione accessibile, personalizzata, tempestiva e applicabile delle informazioni e delle conoscenze condivise per l'ecosistema europeo della cibersicurezza, con una metodologia, infrastrutture e strumenti adeguati, abbinati a metodi di garanzia della qualità per migliorare continuamente i servizi.

INFORMAZIONI SULL'ENISA

L'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, è l'agenzia dell'Unione impegnata a conseguire un elevato livello comune di cibersicurezza in tutta Europa. Istituita nel 2004 e consolidata dal regolamento UE sulla cibersicurezza, l'Agenzia dell'Unione europea per la cibersicurezza contribuisce alla politica dell'UE in questo campo, aumenta l'affidabilità dei prodotti, dei servizi e dei processi TIC con sistemi di certificazione della cibersicurezza, coopera con gli Stati membri e gli organismi dell'UE e aiuta l'Europa a prepararsi per le sfide informatiche di domani. Attraverso lo scambio di conoscenze, lo sviluppo di capacità e la sensibilizzazione, l'Agenzia collabora con le sue principali parti interessate per rafforzare la fiducia nell'economia connessa, aumentare la resilienza delle infrastrutture dell'Unione e, in ultima analisi, garantire la sicurezza digitale della società e dei cittadini europei. Maggiori informazioni sull'ENISA e sulle sue attività sono disponibili al seguente indirizzo: www.enisa.europa.eu.

TP-02-20-759-IT-N

ENISA
Agenzia dell'Unione europea per la cibersicurezza

Sede di Atene
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Grecia

Sede di Eraklion
95 Nikolaou Plastira
700 13 Vassilika Vouton, Eraklion, Grecia

enisa.europa.eu