Nuova strategia dell'UE per la cibersicurezza e nuove norme per rendere più resilienti i soggetti critici fisici e digitali

Bruxelles, 16 dicembre 2020

Oggi la Commissione e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza presentano una nuova strategia dell'UE per la cibersicurezza. In quanto componente essenziale della strategia digitale dell'UE Plasmare il futuro digitale dell'Europa, del piano per la ripresa dell'Europa e della strategia dell'UE per l'Unione della sicurezza, la strategia rafforzerà la resilienza collettiva dell'Europa contro le minacce informatiche e contribuirà a garantire che tutti i cittadini e tutte le imprese possano beneficiare appieno di servizi e strumenti digitali affidabili. A prescindere da quali siano i dispositivi connessi, le reti elettriche, i servizi bancari o i trasporti aerei che i cittadini europei utilizzano o le amministrazioni pubbliche o le strutture ospedaliere che frequentano, essi devono potervi accedere con la sicurezza di essere protetti dalle minacce informatiche.

La nuova strategia per la cibersicurezza consente inoltre all'UE di rafforzare la leadership su norme e standard internazionali nel ciberspazio e di intensificare la collaborazione con i partner in tutto il mondo al fine di promuovere un ciberspazio globale, aperto, stabile e sicuro, fondato sullo Stato di diritto, sui diritti umani, sulle libertà fondamentali e sui valori della democrazia.

La Commissione sta inoltre presentando proposte per affrontare la questione della resilienza sia informatica che fisica dei soggetti critici e delle reti essenziali: una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") e una nuova direttiva sulla resilienza dei soggetti critici. Questi documenti coprono un'ampia gamma di settori e mirano ad affrontare in maniera coerente e complementare i rischi online e offline attuali e futuri, dagli attacchi informatici alla criminalità o alle catastrofi naturali.

Fiducia e sicurezza al centro del decennio digitale dell'UE

La nuova strategia per la cibersicurezza mira a salvaguardare un'Internet globale e aperto, offrendo nel contempo un meccanismo di salvaguardia, non solo per garantire la sicurezza ma anche per proteggere i valori europei e i diritti fondamentali di tutti. Sulla base dei risultati conseguiti negli ultimi mesi e anni, contiene proposte concrete di iniziative politiche, di regolamentazione e di investimento in tre aree d'azione dell'UE:

1. **resilienza, sovranità tecnologica e leadership**

In questa linea d'azione la Commissione propone di riformare le norme sulla sicurezza delle reti e dei sistemi informatici nell'ambito di una direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2") al fine di aumentare il livello di ciberresilienza dei settori pubblici e privati essenziali: strutture ospedaliere, reti energetiche, ferrovie, ma anche centri dati, amministrazioni pubbliche, laboratori di ricerca e produzione di dispositivi medici e medicinali, nonché altre infrastrutture e servizi essenziali che devono rimanere impermeabili in un contesto di minacce sempre più repentine e complesse.

La Commissione propone inoltre di avviare una rete di centri operativi per la sicurezza in tutta l'UE, alimentati dall'intelligenza artificiale (IA), che costituirà per l'UE una vera e propria barriera di cibersicurezza in grado di rilevare tempestivamente i segnali di un attacco informatico e consentire un'azione proattiva prima che si verifichino danni. Ulteriori misure comprenderanno un sostegno dedicato alle piccole e medie imprese (PMI) nel quadro dei poli dell'innovazione digitale e maggiori sforzi per migliorare le competenze della forza lavoro, attirare e trattenere i migliori talenti in materia di cibersicurezza e investire per una ricerca e un'innovazione aperta, competitiva e basata sull'eccellenza.

2. **Sviluppo della capacità operativa di prevenzione, deterrenza e risposta**

Nell'ambito di un processo progressivo e inclusivo portato avanti con gli Stati membri, la Commissione sta preparando, una nuova unità congiunta per il ciberspazio allo scopo di rafforzare la collaborazione tra gli organismi dell'UE e le autorità degli Stati membri responsabili della

prevenzione, della deterrenza e della risposta agli attacchi informatici, comprese le comunità civili, diplomatiche, di contrasto e di difesa informatica. L'alto rappresentante ha presentato proposte per rafforzare il pacchetto di strumenti della diplomazia informatica dell'UE al fine di prevenire, dissuadere e rispondere in modo efficace alle attività informatiche dolose, in particolare quelle che interessano le nostre infrastrutture, le catene di fornitura, le istituzioni e i processi democratici essenziali. L'UE mira inoltre a rafforzare ulteriormente la collaborazione in materia di ciberdifesa e a sviluppare capacità di ciberdifesa all'avanguardia, basandosi sul lavoro svolto dall'Agenzia europea per la difesa e incoraggiando gli Stati membri a sfruttare appieno la cooperazione strutturata permanente e il Fondo europeo per la difesa.

3. **Promozione di un ciberspazio globale e aperto grazie a una maggiore cooperazione**

L'UE intensificherà la collaborazione con i partner internazionali per rafforzare l'ordine mondiale basato su regole, promuovere la sicurezza e la stabilità nel ciberspazio e proteggere i diritti umani e le libertà fondamentali online. Promuoverà norme e standard internazionali che riflettano questi valori fondamentali dell'UE cooperando con i suoi partner internazionali nell'ambito delle Nazioni Unite e in altri contesti pertinenti. L'UE rafforzerà ulteriormente il suo pacchetto di strumenti della diplomazia informatica e intensificherà gli sforzi per la creazione di capacità informatiche nei paesi terzi sviluppando un'apposita agenda esterna dell'UE. Saranno intensificati i dialoghi in materia di cibersicurezza con i paesi terzi e le organizzazioni regionali e internazionali, nonché con la comunità multipartecipativa. L'UE istituirà inoltre una rete per la diplomazia informatica in tutto il mondo per promuovere la propria visione del ciberspazio.

L'UE si è impegnata a sostenere la nuova strategia per la cibersicurezza nei prossimi sette anni con investimenti nella transizione digitale dell'UE a livelli finora mai raggiunti, attraverso il prossimo bilancio a lungo termine dell'UE, in particolare tramite il programma Europa digitale, Orizzonte Europa e il piano per la ripresa dell'Europa. Gli Stati membri sono pertanto incoraggiati a utilizzare appieno il dispositivo per la ripresa e la resilienza dell'UE per rafforzare la cibersicurezza e a fare investimenti a pari livello di quelli dell'UE. L'obiettivo è raggiungere fino a 4,5 miliardi di € di investimenti combinati da parte dell'UE, degli Stati membri e dell'industria, in particolare nell'ambito del Centro di competenza sulla cibersicurezza e della rete dei centri di coordinamento e garantire che una parte importante di questi investimenti siano effettivamente attribuiti alle PMI.

La Commissione mira inoltre a rafforzare le capacità industriali e tecnologiche dell'UE in materia di cibersicurezza, anche tramite progetti finanziati congiuntamente dall'UE e dai bilanci nazionali. L'UE ha l'opportunità unica di mettere in comune le proprie risorse per rafforzare la sua autonomia strategica e promuovere la sua leadership nel campo della cibersicurezza lungo tutta la catena di fornitura digitale (compresi dati e cloud, tecnologie per processori di prossima generazione, connettività ultrasicura e reti 6G), in linea con i suoi valori e le sue priorità.

Resilienza informatica e fisica delle reti, dei sistemi informativi e dei soggetti critici

È necessario aggiornare le misure esistenti a livello dell'UE volte a proteggere i servizi e le infrastrutture essenziali dai rischi sia informatici che fisici. I rischi per la cibersicurezza continuano a evolvere con la crescente digitalizzazione e interconnessione. Anche i rischi fisici sono diventati più complessi dall'adozione delle norme dell'UE sulle infrastrutture essenziali del 2008, che attualmente riguardano solo i settori dell'energia e dei trasporti. L'obiettivo delle revisioni è aggiornare le norme seguendo la logica della strategia dell'UE per l'Unione della sicurezza, superando la falsa dicotomia tra online e offline e mettendo da parte l'approccio a compartimenti stagni.

Per rispondere alle crescenti minacce dovute alla digitalizzazione e all'interconnessione, **la direttiva sulle misure per un elevato livello comune di cibersicurezza in tutta l'Unione (direttiva NIS rivista o "NIS 2")** proposta riguarderà le entità di medie e grandi dimensioni di diversi settori in base alla loro importanza per l'economia e la società. La direttiva NIS 2 renderà più rigidi i requisiti di sicurezza imposti alle imprese, affronterà la sicurezza delle catene di fornitura e delle relazioni con i fornitori, semplificherà gli obblighi di notifica, introdurrà misure di vigilanza più rigorose per le autorità nazionali e obblighi di esecuzione più severi e avrà l'obiettivo di armonizzare i regimi sanzionatori in tutti gli Stati membri. La direttiva NIS 2 proposta contribuirà ad aumentare la condivisione delle informazioni e la cooperazione in materia di gestione delle crisi informatiche a livello nazionale e dell'UE.

La **direttiva sulla resilienza dei soggetti critici** proposta estende sia l'ambito di applicazione, sia la profondità della direttiva sulle infrastrutture critiche europee del 2008. Sono ora contemplati dieci settori: energia, trasporti, banche, infrastrutture dei mercati finanziari, sanità, acqua potabile, acque reflue, infrastrutture digitali, pubblica amministrazione e spazio. Nell'ambito della direttiva proposta ciascuno Stato membro adotterebbe una strategia nazionale per garantire la resilienza dei soggetti

critici ed effettuerebbe valutazioni periodiche dei rischi. Tali valutazioni contribuirebbero a individuare un sottoinsieme più ristretto di soggetti critici cui incomberebbero obblighi volti a rafforzarne la resilienza di fronte ai rischi non informatici, comprese le valutazioni dei rischi a livello di soggetto, l'adozione di misure tecniche e organizzative e la notifica degli incidenti. A sua volta la Commissione fornirebbe sostegno complementare agli Stati membri e ai soggetti critici, per esempio sviluppando una visione d'insieme a livello dell'UE dei rischi transfrontalieri e intersettoriali e delle migliori pratiche, metodologie e attività di formazione e di esercizio transfrontaliere per testare la resilienza dei soggetti critici.

Garantire la sicurezza delle reti di prossima generazione: 5G e oltre

Nell'ambito della nuova strategia per la cibersicurezza e con il sostegno della Commissione e dell'ENISA, l'agenzia dell'Unione europea per la cibersicurezza, gli Stati membri sono incoraggiati a portare a termine l'attuazione del pacchetto di strumenti dell'UE per le reti 5G, che definisce un approccio globale e basato sui rischi oggettivi per la sicurezza delle reti 5G e di prossima generazione.

Secondo una relazione pubblicata oggi sull'impatto della raccomandazione della Commissione sulla cibersicurezza delle reti 5G e sui progressi compiuti nell'attuazione del pacchetto di strumenti comune dell'UE comprendente misure di attenuazione, rispetto alla relazione sui progressi compiuti, pubblicata nel luglio 2020, la maggior parte degli Stati membri è già a buon punto nell'attuazione delle misure raccomandate. Ora dovrebbero mirare a completarne l'attuazione entro il secondo trimestre del 2021 e a garantire che i rischi individuati siano adeguatamente mitigati, in modo coordinato, in particolare nell'ottica di ridurre al minimo l'esposizione ed evitare la dipendenza dai fornitori ad alto rischio. La Commissione oggi delinea inoltre gli obiettivi e le azioni chiave volte a portare avanti tale sforzo coordinato a livello dell'UE.

Dichiarazioni di alcuni membri del collegio

Margrethe **Vestager**, Vicepresidente esecutiva per Un'Europa pronta per l'era digitale, ha dichiarato: *"L'Europa è determinata a portare avanti una trasformazione digitale della nostra società ed economia, che dobbiamo quindi sostenere con livelli di investimento senza precedenti. La riuscita della trasformazione digitale, che sta accelerando, si basa sulla fiducia dei cittadini e delle imprese nella sicurezza dei prodotti e dei servizi connessi che utilizzano."*

L'Alto rappresentante Josep **Borrell** ha dichiarato: *"La sicurezza e la stabilità a livello internazionale dipendono più che mai da un ciberspazio globale, aperto, stabile e sicuro in cui siano rispettati lo Stato di diritto, i diritti umani, le libertà e la democrazia. Con la strategia di oggi l'UE fa un passo avanti nella protezione dei propri governi, dei cittadini e delle imprese dalle minacce informatiche, esercitando la sua leadership nel ciberspazio, di modo che tutti possano trarre vantaggio dall'uso di Internet e delle tecnologie."*

Margaritis **Schinas**, Vicepresidente per la Promozione dello stile di vita europeo, ha affermato: *"La cibersicurezza è un elemento centrale dell'Unione della sicurezza. Non esistono più distinzioni tra minacce online e offline e la dimensione digitale è ormai indissolubilmente connessa alla dimensione reale. L'insieme di misure varate oggi dimostra che l'UE è pronta a usare tutte le risorse e le competenze a sua disposizione per prepararsi e far fronte alle minacce fisiche e informatiche con lo stesso livello di determinazione."*

Thierry **Breton**, Commissario per il Mercato interno, ha dichiarato a sua volta: *"Le minacce informatiche evolvono rapidamente e sono sempre più complesse e adattabili. Per garantire la protezione dei nostri cittadini e delle nostre infrastrutture, dobbiamo giocare d'anticipo: uno scudo europeo per la cibersicurezza resiliente e autonomo consentirà di sfruttare le nostre competenze e conoscenze per reagire più rapidamente, limitare i danni potenziali ed essere più resilienti. Investire nella cibersicurezza significa investire nella nostra autonomia strategica e in un ambiente online sano per il futuro."*

Ylva **Johansson**, Commissaria per gli Affari interni, ha dichiarato: *"I nostri ospedali, i nostri sistemi di trattamento delle acque reflue o le nostre infrastrutture di trasporto sono forti solo quanto gli anelli più deboli della catena: vi è il rischio che le perturbazioni che si verificano in una parte dell'Unione incidano sulla fornitura di servizi essenziali altrove. Per garantire il buon funzionamento del mercato interno e i mezzi di sussistenza di coloro che vivono in Europa, le nostre infrastrutture essenziali devono essere resilienti di fronte a rischi quali catastrofi naturali, attentati terroristici, incidenti e pandemie come quella che stiamo vivendo oggi. È proprio questo l'intento della mia proposta sulle infrastrutture critiche."*

Prossime tappe

La Commissione europea e l'alto rappresentante sono determinati ad attuare la nuova strategia per la

cibersicurezza nei prossimi mesi. Entrambi riferiranno periodicamente sui progressi compiuti e informeranno e coinvolgeranno a pieno titolo in tutte le azioni pertinenti il Parlamento europeo, il Consiglio dell'Unione europea e i portatori di interessi.

Spetta ora al Parlamento europeo e al Consiglio esaminare e adottare la proposta di direttiva NIS 2 e la direttiva sulla resilienza dei soggetti critici. Una volta che le proposte saranno concordate e successivamente adottate, gli Stati membri dovranno recepirle entro 18 mesi dall'entrata in vigore.

La Commissione riesaminerà periodicamente la direttiva NIS 2 e la direttiva sulla resilienza dei soggetti critici e presenterà relazioni in merito al loro funzionamento.

Contesto

La cibersicurezza è una delle principali priorità della Commissione nonché il fondamento di un'Europa digitale e connessa. L'aumento degli attacchi informatici durante la crisi del coronavirus ha dimostrato quanto sia importante proteggere gli ospedali, i centri di ricerca e altre infrastrutture. È necessaria un'azione incisiva in questo settore affinché l'economia e la società dell'UE siano pronte per il futuro.

La nuova strategia per la cibersicurezza propone di integrare la cibersicurezza in tutti i passaggi della catena di approvvigionamento e di accorpare ulteriormente le attività e le risorse dell'UE nei quattro settori della cibersicurezza – mercato interno, attività di contrasto, diplomazia e difesa. Si basa sulla comunicazione Plasmare il futuro digitale dell'Europa e sulla strategia dell'UE per l'Unione della sicurezza, nonché su una serie di atti legislativi, iniziative e azioni che l'UE ha attuato per potenziare le capacità di cibersicurezza e garantire un'Europa più resiliente di fronte alle minacce informatiche, tra cui la strategia per la cibersicurezza del 2013, sottoposta a revisione nel 2017 e l'agenda europea sulla sicurezza 2015-2020 della Commissione. La nuova strategia riconosce inoltre la crescente interconnessione tra la sicurezza interna ed esterna, in particolare attraverso la politica estera e di sicurezza comune.

La prima normativa dell'UE sulla cibersicurezza, la direttiva NIS, entrata in vigore nel 2016, ha contribuito a conseguire un livello comune elevato di sicurezza delle reti e dei sistemi informatici in tutta l'UE. Nel febbraio di quest'anno la Commissione ha annunciato la revisione della direttiva NIS nell'ambito dell'obiettivo strategico chiave di rendere "l'Europa pronta per l'era digitale". Il regolamento dell'UE sulla cibersicurezza, in vigore dal 2019, ha dotato l'Europa di un quadro per la certificazione della cibersicurezza di prodotti, servizi e processi e ha rafforzato il mandato dell'Agenzia dell'UE per la cibersicurezza (ENISA).

Per quanto riguarda la cibersicurezza delle reti 5G, con il sostegno della Commissione e dell'ENISA gli Stati membri hanno definito un approccio globale e basato sui rischi oggettivi con il pacchetto di strumenti dell'UE per il 5G adottato nel gennaio 2020. Dalla revisione della raccomandazione della Commissione del marzo 2019 sulla cibersicurezza delle reti 5G è emerso che la maggior parte degli Stati membri ha compiuto progressi nell'attuazione del pacchetto.

Partendo dalla strategia dell'UE per la cibersicurezza del 2013, l'UE ha sviluppato una strategia internazionale coerente e olistica in materia di cibersicurezza. In collaborazione con i suoi partner a livello bilaterale, regionale e internazionale, l'UE ha promosso un ciberspazio globale, aperto, stabile e sicuro, guidato dai valori fondamentali dell'UE e fondato sullo Stato di diritto. L'UE ha aiutato i paesi terzi a potenziare la resilienza informatica e la capacità di contrastare la criminalità informatica e ha utilizzato il suo pacchetto di strumenti della diplomazia informatica dell'UE del 2017 per contribuire ulteriormente alla sicurezza e alla stabilità internazionali nel ciberspazio, anche applicando per la prima volta il suo regime di sanzioni in campo informatico del 2019 ed inserendo 8 persone e 4 entità e organismi nell'elenco delle sanzioni. L'UE ha compiuto progressi significativi anche in termini di cooperazione in materia di ciberdifesa, comprese le capacità di ciberdifesa, in particolare nell'ambito del quadro strategico in materia di ciberdifesa (CDPF), nonché nel contesto della cooperazione strutturata permanente (PESCO) e dei lavori dell'Agenzia europea per la difesa.

La cibersicurezza è una priorità che si riflette anche nel prossimo bilancio a lungo termine dell'UE (2021-2027). Nell'ambito del programma Europa digitale, l'UE sosterrà la ricerca, l'innovazione e le infrastrutture relative alla cibersicurezza, nonché la ciberdifesa e il settore della cibersicurezza dell'UE. Inoltre in risposta alla crisi del coronavirus, che ha fatto registrare un aumento degli attacchi informatici durante il lockdown, il piano per la ripresa dell'Europa garantisce ulteriori investimenti in materia di cibersicurezza.

L'UE riconosce da tempo la necessità di garantire la resilienza delle infrastrutture critiche che forniscono servizi essenziali per il buon funzionamento del mercato interno e per la vita e i mezzi di sussistenza dei cittadini europei. Per questo motivo nel 2006 l'UE ha istituito il programma europeo per la protezione delle infrastrutture critiche (PEPIC) e nel 2008 ha adottato la direttiva sulle infrastrutture critiche europee, che si applica ai settori dell'energia e dei trasporti. Tali misure sono

state integrate negli anni successivi da varie misure settoriali e intersettoriali su aspetti specifici quali la capacità di reagire ai cambiamenti climatici, la protezione civile o gli investimenti esteri diretti.

Per ulteriori informazioni

Scheda informativa sulla nuova strategia dell'UE per la cibersicurezza

Scheda informativa sulla proposta di direttiva recante misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione (revisione della direttiva NIS)

Scheda informativa sulla cibersicurezza: azione esterna dell'UE

Domande e risposte: la nuova strategia dell'UE per la cibersicurezza e le nuove norme per rendere i soggetti fisici e digitali critici più resilienti

Proposta di direttiva recante misure volte a garantire un livello comune elevato di cibersicurezza nell'Unione (revisione della direttiva NIS o "NIS 2")

Proposta di direttiva sulla resilienza dei soggetti critici (cfr. anche l'Allegato 1 della proposta, nonché lavalutazione d'impatto e la relativa sintesi)

Unione europea della sicurezza

Valutazione d'impatto sulla revisione della direttiva NIS ("NIS 2")

Per saperne di più sulla cibersicurezza

Per saperne di più sulla direttiva NIS

IP/20/2391

Contatti per la stampa:

Johannes BAHRKE (+32 2 295 86 15)
Adalbert JAHNZ (+ 32 2 295 31 56)
Nabila MASSRALI (+32 2 298 80 93)
Marietta GRAMMENOU (+32 2 298 35 83)
Laura BERARD (+32 2 295 57 21)
Xavier CIFRE QUATRESOLS (+32 2 297 35 82)

Informazioni al pubblico: contattare Europe Direct telefonicamente allo 00 800 67 89 10 11 o per e-mail