PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 26 - numero 5552 di Martedì 06 febbraio 2024

Cibersicurezza: la risposta dell'UE alle minacce informatiche

L'UE si sta adoperando su più fronti per promuovere la ciberresilienza, combattere la criminalità informatica e rafforzare la diplomazia informatica e la ciberdifesa. La cronistoria di quanto fatto.

Risposta dell'UE alle sfide in materia di cibersicurezza

Settori critici quali i trasporti, l'energia, la sanità e la finanza **dipendono sempre di più dalle tecnologie digitali** per la gestione delle loro attività principali. Se è vero che la digitalizzazione porta con sé enormi opportunità e offre soluzioni a molte delle sfide che l'Europa deve affrontare, non da ultimo durante la crisi COVID-19, essa espone anche l'economia e la società a minacce informatiche.

Gli attacchi informatici e la criminalità informatica stanno aumentando in tutta Europa in termini sia di quantità che di sofisticazione. Una tendenza destinata a crescere in futuro, visto che si prevede che 41 miliardi di dispositivi in tutto il mondo saranno collegati all'internet delle cose entro il 2025.

Una **risposta più forte in materia di cibersicurezza** volta alla creazione di un ciberspazio aperto e sicuro può contribuire a una maggiore fiducia dei cittadini negli strumenti e nei servizi digitali.

Nell'ottobre 2020 i leader dell'UE hanno chiesto di rafforzare la capacità dell'UE di:

- proteggersi dalle minacce informatiche
- provvedere a un ambiente di comunicazione sicuro, soprattutto attraverso la crittografia quantistica
- garantire l'accesso ai dati a fini giudiziari e di contrasto

Strategia dell'UE in materia di cibersicurezza

Nel dicembre 2020 la Commissione europea e il servizio europeo per l'azione esterna (SEAE) hanno presentato una nuova strategia dell'UE in materia di cibersicurezza. L'obiettivo di tale strategia è **rafforzare la resilienza dell'Europa** a fronte delle minacce informatiche e garantire che tutti i cittadini e le imprese possano beneficiare pienamente di servizi e strumenti digitali affidabili e attendibili. La nuova strategia include proposte concrete per l'introduzione di strumenti normativi, strategici e di investimento.

Il 22 marzo 2021 il Consiglio ha adottato conclusioni sulla strategia in materia di cibersicurezza, sottolineando che la cibersicurezza è essenziale per **costruire un'Europa resiliente, verde e digitale**. I ministri dell'UE hanno stabilito l'obiettivo fondamentale di raggiungere l'autonomia strategica mantenendo nel contempo un'economia aperta. Ciò implica anche il rafforzamento della capacità di compiere scelte autonome nel settore della cibersicurezza allo scopo di potenziare la **leadership digitale** e le capacità strategiche **dell'UE**.

Regolamento UE sulla cibersicurezza

Il regolamento UE sulla cibersicurezza è entrato in vigore nel giugno 2019 e ha introdotto:

- un sistema europeo di certificazione
- un nuovo e più forte mandato per l'Agenzia dell'UE per la cibersicurezza

Sistema europeo di certificazione della cibersicurezza

La certificazione svolge un ruolo fondamentale nel garantire elevati standard di cibersicurezza per i prodotti, servizi e processi TIC. Il fatto che attualmente diversi paesi dell'UE utilizzino sistemi di certificazione della sicurezza differenti comporta una frammentazione del mercato e ostacoli normativi.

Con il regolamento sulla cibersicurezza, l'UE ha introdotto un **quadro unico di certificazione in tutta l'UE** che:

- stimola la fiducia
- aumenta la crescita del mercato della cibersicurezza
- agevola il commercio in tutta l'UE

Il quadro fornisce un insieme completo di norme, requisiti tecnici, standard e procedure.

Agenzia dell'UE per la cibersicurezza

La nuova Agenzia dell'UE per la cibersicurezza si basa sulle strutture dell'Agenzia europea per la sicurezza delle reti e dell'informazione ? che l'ha preceduta ? ma ha un ruolo rafforzato e un mandato permanente. Ha anche adottato lo stesso acronimo (ENISA).

Sostiene gli Stati membri, le istituzioni dell'UE e altre parti interessate nella **gestione degli attacchi informatici**.

Direttiva sulla sicurezza delle reti e dei sistemi informativi

La direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS) è stata introdotta nel 2016 quale prima misura legislativa in assoluto per tutta l'UE volta ad accrescere la cooperazione tra gli Stati membri sulla questione vitale della cibersicurezza. Ha definito **obblighi di sicurezza per gli operatori di servizi essenziali** (in settori critici come l'energia, i trasporti, la sanità e la finanza) e i fornitori di servizi digitali (mercati online, motori di ricerca e servizi cloud).

Nel 2022 l'UE ha adottato una **direttiva NIS riveduta** (NIS2) per sostituire la direttiva del 2016. Le nuove norme garantiscono un **livello comune elevato di cibersicurezza nell'Unione**, rispondendo al panorama di minacce in evoluzione e tenendo in considerazione la trasformazione digitale, che è stata accelerata dalla pandemia di COVID-19.

La nuova normativa dell'UE:

- stabilisce nuove norme minime per un quadro normativo
- definisce meccanismi per una cooperazione efficace tra le autorità competenti di ciascun paese dell'UE
- aggiorna l'elenco dei settori e delle attività soggetti agli obblighi in materia di cibersicurezza

La direttiva NIS2 è entrata in vigore il 16 gennaio 2023.

Regolamento sulla ciberresilienza

L'UE intende introdurre **requisiti obbligatori in materia di cibersicurezza** per prodotti hardware e software con un elemento digitale connesso (come smart TV o altri elettrodomestici, baby monitor, giocattoli).

Il regolamento proposto garantisce a imprese e consumatori una protezione efficace contro le minacce informatiche.

Lotta dell'UE alla criminalità informatica

La criminalità informatica assume varie forme e molti reati comuni sono favoriti dall'informatica. Ad esempio i criminali possono:

- acquisire il controllo di dispositivi personali utilizzando malware
- sottrarre o compromettere dati personali e proprietà intellettuale per commettere frodi online
- utilizzare internet e le piattaforme dei social media per distribuire contenuti illegali
- utilizzare la "darknet" per vendere beni illeciti e servizi di pirateria informatica

Alcune forme di criminalità informatica, quali lo sfruttamento sessuale di minori online, causano gravi danni alle vittime.

5 500 miliardi di EUR
costo annuo globale della criminalità informatica

Nel quadro di Europol è stato istituito un **Centro europeo per la lotta alla criminalità informatica** specializzato che aiuta i paesi dell'UE a indagare i reati online e a smantellare le reti criminali.

La **piattaforma multidisciplinare europea di lotta alle minacce della criminalità** (EMPACT) è un'iniziativa in materia di sicurezza portata avanti dagli Stati membri e tesa a individuare, classificare in ordine di priorità e affrontare le minacce provenienti dalla criminalità organizzata internazionale. Contrastare gli attacchi informatici è una delle sue priorità.

Affrontare le frodi perpetrate con mezzi di pagamento diversi dai contanti

Le frodi e le contraffazioni perpetrate con mezzi di pagamento diversi dai contanti rappresentano una grave minaccia per la sicurezza dell'UE e sono una considerevole fonte di guadagno per la criminalità organizzata. Questo tipo di frode intacca inoltre la fiducia dei consumatori nella sicurezza delle tecnologie digitali.

Nell'aprile 2019 l'UE ha adottato **nuove norme per combattere le frodi perpetrate con mezzi di pagamento diversi dai contanti**. L'attuazione delle nuove norme da parte degli Stati membri è prevista per il 2021.

Migliorare la sicurezza dei minori online

Nel maggio 2022 la Commissione europea ha proposto una nuova legislazione per **contrastare l'abuso e lo sfruttamento sessuale dei minori online**. Le nuove norme sono attualmente oggetto di discussione in sede di Consiglio.

Nel frattempo, l'UE ha adottato norme temporanee, in deroga all'articolo 5, paragrafo 1, e all'articolo 6, paragrafo 1, della direttiva e-privacy, per far sì che i fornitori di servizi di posta elettronica basati sul web e i servizi di messaggistica possano continuare a individuare gli abusi sessuali sui minori online.

Nel maggio 2021 i negoziatori del Consiglio e del Parlamento europeo hanno raggiunto un **accordo provvisorio** sulle misure temporanee che consentono ai fornitori di servizi di comunicazione elettronica quali i servizi di posta elettronica basati sul web e i servizi di messaggistica di continuare a individuare, rimuovere e segnalare gli abusi sessuali sui minori online, anche per quanto riguarda la lotta all'adescamento, fino all'entrata in vigore della normativa permanente. Le misure sono entrate in vigore nell'agosto 2021 e saranno valide fino al 2024.

Giustizia e attività di contrasto

Le norme e politiche dell'UE affrontano anche altri aspetti della lotta alla criminalità informatica e alla criminalità in generale connessi alla giustizia e alle attività di contrasto, quali l'accesso alle prove elettroniche, la crittografia e la conservazione dei dati.

Accesso alle prove elettroniche

I criminali sfruttano la tecnologia digitale per commettere reati e nascondere attività illecite. Le autorità di contrasto e giudiziarie fanno pertanto sempre più affidamento sulle prove elettroniche ? quali messaggi testuali, e-mail o app di messaggistica ? nelle indagini e azioni penali.

Per questo motivo l'UE sta lavorando a **nuove norme che renderanno più facile e veloce l'accesso transfrontaliero alle prove elettroniche**.

-

Per agevolare ulteriormente l'accesso transfrontaliero alle prove elettroniche nei procedimenti penali, l'UE:

- sta negoziando un **accordo con gli Stati Uniti**, il paese in cui hanno sede la maggior parte dei prestatori di servizi
- partecipa ai negoziati per il secondo protocollo addizionale alla convenzione di Budapest

Crittografia

L'UE si sta adoperando per instaurare un dibattito attivo con l'industria del settore tecnologico al fine di trovare il giusto equilibrio tra la continuità dell'utilizzo di una tecnologia crittografica forte e la **garanzia dei poteri delle autorità di contrasto e giudiziarie affinché possano operare** alle stesse condizioni del mondo offline.

Nel dicembre 2020 il Consiglio ha adottato una risoluzione sulla crittografia, sottolineando la necessità di garantire allo stesso tempo la sicurezza attraverso la crittografia e nonostante la crittografia.

-

Conservazione dei dati

Oggi per combattere in maniera efficace la criminalità è importante che i fornitori di servizi conservino determinati dati che possono essere divulgati a determinate condizioni rigorose per finalità di lotta contro la criminalità. Tuttavia, la conservazione dei dati può violare i **diritti fondamentali della persona**, in particolare i diritti alla riservatezza e alla protezione dei dati personali.

Il Consiglio ha adottato conclusioni riguardo alla **conservazione dei dati relativi a comunicazioni elettroniche** per finalità di lotta contro la criminalità. Il Consiglio ha incaricato la Commissione di raccogliere ulteriori informazioni e di organizzare consultazioni mirate nell'ambito di uno studio approfondito sulle possibili soluzioni per conservare i dati, compresa la valutazione di una futura iniziativa legislativa.

-

Rafforzare la diplomazia informatica

L'Unione europea e i suoi Stati membri promuovono fermamente un ciberspazio aperto, libero, stabile e sicuro, in cui i diritti umani, le libertà fondamentali e lo Stato di diritto siano pienamente rispettati a beneficio della stabilità sociale, della crescita economica, della prosperità e dell'integrità di società libere e democratiche.

L'UE compie considerevoli sforzi per proteggersi dalle minacce informatiche provenienti da paesi terzi, soprattutto mediante una risposta diplomatica comune chiamata "**pacchetto di strumenti della diplomazia informatica**". Tale risposta prevede **la cooperazione e il dialogo diplomatici**, misure preventive contro gli attacchi informatici e sanzioni.

La strategia dell'UE in materia di cibersicurezza adottata dalla Commissione europea e dal SEAE nel dicembre 2020 rafforza la risposta diplomatica dell'Unione agli attacchi informatici.

Sanzioni in caso di attacchi informatici

Nel maggio 2019 il Consiglio ha istituito un quadro che consente all'UE di imporre **sanzioni mirate volte a scoraggiare e contrastare gli attacchi informatici** che costituiscono una minaccia esterna per l'UE o i suoi Stati membri.

Più specificamente, per la prima volta questo quadro consente all'UE di imporre sanzioni a persone o entità responsabili di attacchi informatici o tentati attacchi informatici, che forniscono sostegno finanziario, tecnico o materiale per tali attacchi o che sono altrimenti coinvolte. Le sanzioni possono anche essere imposte ad altre persone o entità associate ad esse.

Le misure restrittive includono:

- il divieto di viaggio verso l'UE per le persone
- il congelamento dei beni di persone ed entità

Il 30 luglio 2020 sono state imposte le prime sanzioni in assoluto per attacchi informatici.

-

Cooperazione in materia di ciberdifesa

Il ciberspazio è considerato la quinta dimensione della conflittualità, essenziale per le operazioni militari quanto lo sono terra, mare, aria e spazio. Si tratta di una dimensione che comprende tutto quanto va dalle reti e infrastrutture di informazione e telecomunicazione e dai dati da esse supportati fino ai sistemi informatici, ai processori e ai dispositivi di controllo.

L'UE coopera in materia di difesa nel ciberspazio attraverso le attività dell'**Agenzia europea per la difesa** (AED), in collaborazione con l'Agenzia dell'UE per la cibersicurezza ed Europol. L'AED sostiene gli Stati membri nella creazione di una forza militare qualificata nel settore della ciberdifesa e garantisce la disponibilità di tecnologie di ciberdifesa proattive e reattive.

La **strategia dell'UE in materia di cibersicurezza** adottata dalla Commissione e dal SEAE nel dicembre 2020 rafforza:

- il coordinamento della ciberdifesa
- la cooperazione e lo sviluppo di capacità in materia di ciberdifesa

La **politica dell'UE in materia di ciberdifesa**, adottata nel novembre 2022 dalla Commissione e dal SEAE, mira a potenziare le capacità di ciberdifesa dell'UE e a rafforzare il coordinamento e la cooperazione tra le cibercomunità militari e civili.

Il 23 maggio 2023 il Consiglio ha adottato **conclusioni sulla politica di ciberdifesa dell'UE** in cui si sottolinea l'importanza di rafforzare ulteriormente la resilienza dell'UE per far fronte alle minacce informatiche.

-

Finanziamento e ricerca

Piano per la ripresa

La cibersicurezza è una delle **priorità dell'UE nella risposta alla pandemia di COVID-19**, durante la quale si è registrato un aumento degli attacchi informatici. Il piano prevede investimenti aggiuntivi in questo settore.

-

Orizzonte Europa

È essenziale trovare soluzioni innovative che possano proteggerci dalle più recenti e più avanzate minacce informatiche. Per questo motivo la cibersicurezza è un aspetto importante dei **programmi quadro di finanziamento dell'UE in materia di ricerca e innovazione** Orizzonte 2020 e il suo successore Orizzonte Europa. Nel maggio 2020 l'UE ha impegnato **49 milioni**

di EUR per promuovere l'innovazione nei sistemi di cibersicurezza e privacy.

-

Europa digitale

Nel quadro del programma Europa digitale per il periodo 2021-2027, l'UE si è impegnata a investire **1,6 miliardi di EUR** in capacità di cibersicurezza e nell'ampia diffusione di infrastrutture e strumenti per la cibersicurezza in tutta l'UE a favore di pubbliche amministrazioni, imprese e singoli cittadini.

Centro di competenza per la cibersicurezza

Nel dicembre 2020 il Consiglio e il Parlamento europeo hanno raggiunto un accordo informale sulla proposta di istituire il **Centro europeo di competenza per la cibersicurezza nell'ambito industriale, tecnologico e della ricerca**, sostenuto da una rete di centri nazionali di coordinamento.

Nell'aprile 2021 il Consiglio ha adottato il regolamento che istituisce il centro e la rete.

-

Il nuovo centro mira a:

- migliorare ulteriormente la ciberresilienza
- contribuire alla diffusione delle tecnologie più recenti nel settore della cibersicurezza
- sostenere le start-up e le PMI del settore della cibersicurezza
- rafforzare la ricerca e l'innovazione in materia di cibersicurezza
- contribuire a colmare il divario di competenze in materia di cibersicurezza

Bucarest è stata selezionata dagli Stati membri dell'UE come sede del nuovo centro.

-

Cibersicurezza delle infrastrutture critiche

Dispositivi connessi sicuri

I dispositivi connessi ? compresi i macchinari, i sensori e le reti che costituiscono l'internet delle cose ? e la loro sicurezza svolgeranno un ruolo chiave nel plasmare ulteriormente il futuro digitale dell'Europa.

Nel dicembre 2020 il Consiglio ha adottato **conclusioni** in cui si riconoscono l'utilizzo crescente di prodotti di largo consumo e dispositivi industriali connessi a internet e i relativi **nuovi rischi per la vita privata, la sicurezza delle informazioni e la cibersicurezza**. Le conclusioni definiscono le priorità per affrontare tale questione cruciale e per rafforzare la competitività globale del settore dell'internet delle cose dell'UE garantendo i più elevati standard di resilienza, protezione e sicurezza.

-

Proteggere le reti 5G

Le reti 5G sono essenziali non solo per la comunicazione digitale, ma anche per settori critici quali l'energia, i trasporti, il settore bancario e la sanità. Garantire la resilienza delle reti 5G è quindi fondamentale per la nostra società.

Viste le stime di entrate mondiali nel settore del 5G pari a 225 miliardi di EUR per il 2025, il 5G è una risorsa chiave perché l'Europa sia competitiva sul mercato globale e la sua cibersicurezza è cruciale per garantire l'autonomia strategica dell'Unione.

Nel gennaio 2020 l'UE ha concordato un **pacchetto di strumenti** per individuare possibili misure comuni tese ad **attenuare i principali rischi per la cibersicurezza** delle reti 5G e per fornire orientamenti.

La cronistoria completa

Fonte: Consilio Europeo

www.puntosicuro.it