

Criminalità informatica in Europa: l'analisi Eurojust-Europol 2024



Il panorama della criminalità informatica attraversa una fase di evoluzione senza precedenti, ponendo gli investigatori europei di fronte a sfide di crescente complessità. L'ultimo report congiunto di Eurojust ed Europol *"Common Challenges in Cybercrime"* identifica sei aree critiche che necessitano di particolare attenzione: la gestione dei volumi di dati in costante crescita, la salvaguardia delle informazioni digitali cruciali, l'accessibilità ai dati, la diffusione dei servizi di anonimizzazione, le barriere alla cooperazione internazionale e le criticità nelle partnership pubblico-private.

Gli investigatori contemporanei si trovano ad affrontare una complessità che richiede competenze altamente specializzate: dall'analisi forense dei dati alla crittografia avanzata, dai sistemi blockchain all'intelligenza artificiale applicata all'analisi predittiva.

La sfida dei big data nelle indagini digitali

La gestione dei dati emerge come una delle sfide più impegnative del settore. Le indagini digitali moderne devono elaborare quantità di informazioni nell'ordine dei terabyte o petabyte, mettendo a dura prova le infrastrutture investigative tradizionali. La varietà dei formati spazia dai database SQL a strutture più sofisticate come JSON e XML, fino a contenuti non strutturati come email, post sui social media e file multimediali. Questa eterogeneità richiede sistemi di

analisi avanzati che integrino tecnologie di machine learning per il riconoscimento di pattern criminali e sistemi di Natural Language Processing per l'analisi testuale approfondita.

Conservazione dei dati e identificazione degli utenti

La conservazione dei dati digitali rappresenta un punto particolarmente critico. L'invalidazione della direttiva europea sulla *data retention* da parte della Corte di Giustizia dell'UE ha generato una situazione frammentata, dove alcuni Stati membri conservano i dati solo per pochi giorni, compromettendo le indagini transfrontaliere.

Una sfida tecnologica significativa è rappresentata dal *Carrier-Grade Network Address Translation* (CGNAT). Questa tecnologia, che consente la condivisione di un singolo indirizzo IPv4 tra migliaia di utenti, opera attraverso una sofisticata combinazione di indirizzi IP pubblici e numeri di porta, necessitando di *timestamp* estremamente precisi per l'identificazione degli utenti.

Crittografia e il caso emblematico LockBit

Il report dedica particolare attenzione alla crittografia e ai sistemi di comunicazione cifrata, con il caso LockBit come esempio paradigmatico. Il gruppo, considerato il più pericoloso al mondo nel settore ransomware fino al suo smantellamento nel febbraio 2024, ha richiesto un'operazione internazionale coordinata che ha coinvolto dieci paesi sotto la guida di Europol ed Eurojust. Gli investigatori hanno dovuto affrontare un'infrastruttura distribuita su decine di server in sette paesi, protetta da *multiple layer* di crittografia e dotata di *wallet cryptocurrency* con sofisticati

sistemi di mixing.

Guarda il video dell'intervento sulla criminalità informatica e le operazioni supportate da Europol contro i ransomware:

[embedded content]

Le risposte legislative dell'Unione Europea

Per fronteggiare questa complessità crescente, l'Unione Europea ha introdotto strumenti legislativi innovativi di ampio respiro. Il pacchetto e-Evidence, la cui piena applicazione è prevista per agosto 2026, promette di rivoluzionare l'acquisizione transfrontaliera di prove elettroniche. Parallelamente, il Digital Services Act ridefinisce le regole per le piattaforme digitali, mentre l'AI Act stabilisce un quadro normativo pionieristico per l'implementazione dell'intelligenza artificiale nelle indagini. L'efficacia di questi strumenti, tuttavia, dipenderà dalla loro integrazione armoniosa nelle pratiche investigative esistenti.

Guarda il video degli interventi su criminalità informatica e cooperazione internazionale:

[embedded content]

Criminalità informatica: l'evoluzione delle criptovalute

Il fenomeno delle criptovalute nel contesto criminale merita un'attenzione particolare. Gli investigatori si trovano ora ad affrontare scenari di crescente complessità: dall'analisi di transazioni su blockchain multiple al tracciamento attraverso sofisticati sistemi di mixing, fino alla decodifica di *smart contract* sempre più elaborati. L'ecosistema DeFi, con

protocolli come Uniswap, Aave e Compound, ha introdotto ulteriori livelli di complessità, amplificati dall'adozione di *privacy coins* e soluzioni layer-2 con implementazioni *zero-knowledge*.

Questi strumenti finanziari hanno ormai travalicato i confini della criminalità informatica tradizionale, penetrando in un ampio spettro di attività illecite. Le frodi emergono come il reato più frequentemente associato al loro utilizzo, mentre la Finanza Decentralizzata (DeFi) si afferma come nuovo territorio per il riciclaggio di denaro criminale.

L'evoluzione della criminalità informatica in Europa: analisi comparata dei report Eurojust-Europol 2019-2024

Il confronto tra i report Eurojust-Europol del 2019 e del 2024 rivela una profonda trasformazione nel panorama della criminalità informatica europea. La complessità crescente delle minacce ha portato a un'evoluzione significativa sia nella comprensione dei fenomeni che nelle strategie di contrasto.

La prima differenza sostanziale emerge nella struttura stessa dell'analisi: se nel 2019 il focus era su cinque aree critiche, il report 2024 ne identifica sei, introducendo la gestione dei volumi di dati come sfida autonoma. Questa evoluzione riflette la crescente consapevolezza dell'importanza strategica della *data analysis* nel contrasto alle attività criminali.

Particolarmente significativo è il salto qualitativo nell'approccio alle questioni tecnologiche. Le criptovalute, che nel 2019 rappresentavano una preoccupazione marginale, sono diventate centrali nell'analisi del 2024, con

un'attenzione particolare ai protocolli DeFi e alle implementazioni degli *smart contract*. Analogamente, la trattazione della crittografia si è arricchita di considerazioni tecniche avanzate, includendo tematiche come la *quantum-resistant cryptography*.

Sul fronte legislativo, il report 2024 testimonia la maturazione del quadro normativo europeo. L'introduzione del pacchetto e-Evidence, del Digital Services Act e dell'AI Act rappresenta una risposta strutturata alle sfide identificate nel 2019, quando molte di queste iniziative erano ancora in fase di elaborazione.

La cooperazione internazionale ha subito una profonda evoluzione: dall'approccio prevalentemente procedurale del 2019 si è passati a una visione operativa integrata, esemplificata dal caso LockBit, che ha dimostrato l'efficacia delle operazioni coordinate multi-giurisdizionali.

Un elemento distintivo del report 2024 è l'enfasi posta sulle infrastrutture investigative d'avanguardia. Il focus su sistemi di *storage* distribuito e framework di *machine learning* specializzati riflette la consapevolezza che la risposta alla criminalità informatica richiede un'infrastruttura tecnologica all'altezza delle sfide contemporanee.

Le partnership pubblico-private hanno acquisito una nuova dimensione strategica. Se nel 2019 rappresentavano principalmente una sfida organizzativa, nel 2024 vengono riconosciute come elemento fondamentale nella strategia di contrasto, con un'analisi approfondita delle implicazioni per la privacy e la sicurezza dei dati.

Questa evoluzione testimonia non solo la crescente sofisticazione delle minacce informatiche, ma anche la maggiore maturità delle istituzioni europee nel contrastarle. L'approccio integrato che emerge dal report 2024, combinando strumenti legislativi, tecnologici e operativi, suggerisce una

comprensione più profonda della natura multidimensionale della criminalità informatica e della necessità di risposte altrettanto articolate.

La trasformazione osservata in questi cinque anni riflette un processo di apprendimento istituzionale significativo, dove le lezioni apprese hanno portato a strategie più sofisticate e a una maggiore consapevolezza della necessità di un approccio coordinato e tecnologicamente avanzato nella lotta alla criminalità informatica.

Infrastrutture investigative del futuro

Per rispondere a queste sfide emergenti, il report enfatizza la necessità di infrastrutture investigative d'avanguardia. Si delinea l'esigenza di sistemi di storage distribuito ad alta capacità, affiancati da cluster di calcolo per analisi forensi parallele e framework di machine learning specializzati. Gli strumenti investigativi devono evolvere per gestire l'analisi di malware avanzato, il *reverse engineering* di protocolli proprietari e tecniche sempre più sofisticate di *network traffic analysis*.

Prospettive future e considerazioni conclusive

L'orizzonte della lotta alla criminalità informatica si presenta tanto sfidante quanto ricco di opportunità. L'implementazione della *quantum-resistant cryptography* emerge come priorità imminente, mentre lo sviluppo di strumenti analitici basati su AI rappresenta una frontiera promettente. Le tecniche di de-anonimizzazione avanzata e i metodi di correlazione *cross-platform* si rivelano essenziali per tracciare attività criminali di crescente sofisticazione.

Il successo futuro dipenderà dalla capacità di orchestrare efficacemente molteplici elementi: l'integrazione dei nuovi strumenti legislativi, il potenziamento delle capacità tecnico-operative delle forze dell'ordine europee e il mantenimento di una solida cooperazione internazionale. La formazione continua del personale, l'innovazione tecnologica e il consolidamento delle partnership pubblico-private costituiscono i pilastri fondamentali di questa strategia.

Il report 2024 di Eurojust-Europol si configura quindi non solo come una fotografia dello stato attuale, ma come una bussola strategica per il futuro della cybersecurity europea. La crescente sofisticazione delle minacce informatiche richiede un approccio olistico e tecnologicamente avanzato, supportato da una formazione specialistica continua e da una cooperazione internazionale sempre più stretta.

Condividi sui Social Network:

<https://www.ictsecuritymagazine.com/notizie/criminalita-informatica-2024/>