Client-Side Scanning: l’arma a doppio taglio della cybersecurity



l Client-Side Scanning è una tecnologia di scansione lato client che promette di proteggere i bambini online, ma rischia di trasformare ogni dispositivo in uno strumento di sorveglianza di massa.

Il punto di non ritorno digitale

Nel panorama della cybersecurity del 2025, una nuova tecnologia divide profondamente esperti, legislatori e cittadini: il **Client-Side Scanning (CSS)**. Mentre l’Unione Europea si prepara a un voto decisivo entro il 14 ottobre 2025 sulla controversa proposta “Chat Control”, sotto la presidenza danese del Consiglio UE, la comunità scientifica internazionale lancia un allarme senza precedenti sui rischi che questa tecnologia comporta per la privacy e la sicurezza globali.

Il CSS nella realtà operativa del 2025

Il Client-Side Scanning rappresenta un cambio di paradigma fondamentale nell’approccio alla sicurezza digitale. Invece di indebolire la crittografia o fornire chiavi backdoor alle forze dell’ordine per decrittare le comunicazioni, il CSS consente l’analisi dei dati direttamente sui dispositivi degli utenti. La tecnologia opera scansionando il contenuto sui dispositivi prima della crittografia, aggirando di fatto le protezioni fondamentali della crittografia end-to-end.

L’architettura tecnica del CSS

Il funzionamento del CSS segue un processo strutturato:

1. Il fornitore del servizio CSS seleziona o crea un algoritmo di riconoscimento;
2. L’algoritmo viene fornito all’autorità competente che gestisce il database del materiale da identificare;
3. L’autorità competente restituisce un elenco degli hash del materiale ricercato;
4. L’elenco viene incorporato nel codice di produzione;
5. Il sistema viene installato sui dispositivi degli utenti tramite i normali aggiornamenti.

Questa architettura solleva questioni tecniche complesse. Come osserva la ricerca accademica dell’Università di Oxford, il CSS per sua natura crea seri rischi di sicurezza e privacy per tutta la società, mentre l’assistenza che può fornire alle forze dell’ordine è nel migliore dei casi problematica.

Il momento critico: ottobre 2025

Le prossime settimane sono decisive. Gli Stati membri dovrebbero finalizzare le loro posizioni nei gruppi di lavoro del Consiglio entro il 12 settembre 2025, con un possibile voto del Consiglio fissato per il 14 ottobre 2025. La presidenza danese ha fatto di questa legislazione una priorità assoluta, segnalando l’intenzione di trovare un compromesso che bilanci gli obiettivi delle forze dell’ordine con le preoccupazioni legali e tecniche sollevate dagli stati membri.

Posizioni attuali degli Stati membri:

- **Favorevoli**: Italia, Spagna e Ungheria sostengono Chat Control, anche la Francia ha dichiarato che “potrebbe sostanzialmente appoggiare la proposta”;
- **Contrari**: 8 Stati hanno espresso opposizione ufficiale: Austria, Belgio, Germania, Lussemburgo, Repubblica Ceca, Finlandia, Paesi Bassi e Polonia;
- **Indecisi**: Belgio, Estonia, Finlandia, Germania, Grecia, Slovenia, Lussemburgo e Romania risultano indecisi.

La Germania, guidata dal nuovo governo Merz insediatosi nel

maggio 2025, non si oppone più chiaramente al Chat Control, rappresentando un cambiamento politico potenzialmente decisivo per l'approvazione della normativa. Il governo tedesco guidato dal cancelliere Merz ha però confermato l'opposizione espressa con forza dal precedente esecutivo.

I rischi sistemici emergenti

Vulnerabilità di sicurezza senza precedenti

La ricerca internazionale ha identificato molteplici vettori di attacco che il CSS introduce nei sistemi digitali. Il CSS aumenta la superficie di attacco dei dispositivi degli utenti, spostandoli da un modello di sicurezza compartimentalizzato verso un approccio orientato alla raccolta di intelligence e al controllo.

Gli esperti di cybersecurity avvertono che il Chat Control potrebbe trasformare ogni dispositivo in uno strumento di sorveglianza, compromettendo la sicurezza delle comunicazioni crittografate e violando i diritti fondamentali alla privacy dei cittadini europei.

L'inefficacia contro gli avversari

Sia i distributori che i consumatori di materiale illegale possono cercare di aggirare un sistema CSS, rendendolo inutile per l'applicazione della legge. Questo può avvenire in due modi principali:

- **Falsi negativi**: garantendo che il materiale illegale eviti la rilevazione;
- **Falsi positivi**: ingannando il sistema CSS perché segnali contenuto innocuo, inondandolo di falsi allarmi.

L'impatto economico della cybercriminalità nel 2025

Il contesto in cui si inserisce il dibattito sul CSS è

caratterizzato da una crescita esplosiva dei costi della cybercriminalità. La cybercriminalità dovrebbe costare alle aziende fino a **10,5 trilioni di dollari entro il 2025** e potrebbe raggiungere i 1**5,63 trilioni di dollari entro il 2029**.

Il costo medio globale di una violazione dei dati nel 2024 è di **4,88 milioni di dollari,** con un aumento del 10% rispetto all'anno precedente. Le organizzazioni che risolvono le violazioni in meno di 200 giorni spendono circa 3,87 milioni di dollari, mentre quelle che impiegano più di 200 giorni vedono i costi salire a 5,01 milioni di dollari.

Il paradosso della sicurezza

Le organizzazioni senza intelligenza artificiale o automazione hanno sostenuto i costi più alti (5,52 milioni di dollari), mentre quelle che utilizzano ampiamente queste tecnologie hanno ridotto i costi a 3,62 milioni di dollari. Questo dato evidenzia come l'innovazione tecnologica possa essere simultaneamente una soluzione e un rischio per la sicurezza.

Le posizioni degli stati membri

Secondo i dati resi pubblici dall'ex deputato del Partito Pirata tedesco Patrick Breyer, molti paesi che hanno respinto il Chat Control nel 2024 sono ora indecisi, "anche se il piano del 2025 è ancora più estremo". La mappa geopolitica del supporto varia tra le fonti, ma emerge un quadro di crescente divisione:

- **Danimarca**: guida il processo come presidenza di turno;
- **Germania**: posizione cruciale e attualmente indecisa;
- **Francia**: ha già abbandonato la sua opposizione secondo alcune fonti;
- **Opposizione persistente**: Olanda e Repubblica Ceca mantengono riserve significative.

Il 12 dicembre 2024, una "minoranza di blocco" di governi UE

era riuscita a fermare il piano del controllo delle chat, ma la situazione politica si è ora evoluta.

L’analisi tecnica dei fallimenti del CSS

I principi di sicurezza violati

I principi di design di Saltzer e Schroeder del 1975 per i meccanismi di protezione sono particolarmente rilevanti per i sistemi di scansione dei contenuti. Il CSS viola sistematicamente questi principi fondamentali:

1. **Economy of mechanism**: Il design dovrebbe essere il più semplice possibile, quindi facile da convalidare e testare;
2. **Separation-of-privilege**:La sicurezza dovrebbe richiedere il controllo di più soggetti indipendenti, evitando che una singola entità abbia potere assoluto;
3. **Open design**: Il design non dovrebbe essere segreto.

L’esempio Apple: un caso di studio illuminante

Nell’agosto 2021, Apple ha proposto il primo sistema CSS di produzione con il potenziale di essere distribuito su scala globale e installato su più di un miliardo di dispositivi Apple. Nonostante gli sforzi ingegneristici considerevoli e l’impiego di talenti tecnici di punta, Apple non è riuscita a produrre un design sicuro e affidabile, tanto da ritardare e possibilmente cancellare il progetto a seguito delle critiche ricevute.

Le implicazioni per l’industria della cybersecurity

Mercato e investimenti

Il mercato delle tecnologie di cybersecurity è stato valutato **185,7 miliardi di dollari nel 2024**, con in media il 12% dei budget IT destinati alla cybersecurity. Tuttavia, solo il 10% delle aziende sta aumentando le assunzioni nel campo della cybersecurity, creando un divario critico tra domanda e offerta di competenze.

Settori ad alto rischio

Secondo l'IBM X-Force Threat Intelligence Index 2025:

- Il **settore manifatturiero** è l'industria più colpita (26% di tutti gli attacchi);
- La **sanità** registra i costi più alti per incidente (~10 milioni di dollari);
- Il **settore finanziario** segue con circa 6 milioni di dollari;
- **Manifatturiero, energia e tecnologia** oscillano intorno ai 5-6 milioni di dollari.

Il ransomware colpisce il 59% di tutte le organizzazioni nell'ultimo anno, con costi proiettati per raggiungere circa 265 miliardi di dollari annui entro il 2031.

Prospettive future e raccomandazioni

Principi per una sicurezza responsabile

La ricerca scientifica suggerisce che qualsiasi implementazione di tecnologie di scansione dovrebbe rispettare i principi Carnegie del 2019:

1. **Utilità per le forze dell'ordine**: La proposta deve affrontare in modo significativo e prevedibile un problema legittimo e dimostrato delle forze dell'ordine;
2. **Equità**: Deve offrire garanzie significative per non

esacerbare le disparità esistenti nell'applicazione della legge;
3. **Autorizzazione**: L'uso deve essere subordinato a specifiche autorizzazioni giudiziarie e controlli legali preventivi;
4. **Specificità**: La tecnologia deve essere limitata a specifici dispositivi o casi, evitando la sorveglianza di massa indiscriminata;
5. **Focus**: Deve essere progettata per non compromettere la sicurezza informatica generale e la privacy dei cittadini.

Alternative tecnologiche

Esistono alternative più efficaci e meno invasive: indagini mirate sui sospetti, rafforzamento della cooperazione internazionale tra le forze dell'ordine, sanzioni più severe per i responsabili e maggiori investimenti nella protezione dei minori possono combattere il CSAM senza compromettere la privacy e la sicurezza digitale di tutti i cittadini.

Il bivio della privacy digitale

Il Client-Side Scanning rappresenta un momento di svolta nella storia della privacy digitale. La proposta di scansionare preventivamente tutti i dispositivi degli utenti alla ricerca di contenuti specifici è molto più invasiva delle precedenti proposte di backdoor crittografiche o accesso governativo ai dati.

Come avvertono i ricercatori internazionali:

> *"In un mondo dove le nostre informazioni personali sono conservate in dispositivi di comunicazione che portiamo nelle nostre tasche, sia la tecnologia che le leggi devono essere progettate per proteggere la nostra privacy e sicurezza, non per comprometterle".*

Il voto del 14 ottobre 2025 non determinerà solo il futuro della privacy digitale europea, ma potrebbe stabilire un precedente globale per la sorveglianza tecnologica di massa. La posta in gioco è altissima: preservare quella sottile linea che separa la sicurezza pubblica dalla sorveglianza autoritaria nell'era digitale.

Bibliografia e Fonti:

- Abelson, H., Anderson, R., Bellovin, S. M., Benaloh, J., Blaze, M., Callas, J., … & Troncoso, C. (2024). Bugs in our pockets: the risks of client-side scanning. *Journal of Cybersecurity.*
- Internet Society (2023, December 13). Client-Side Scanning – EU Case.
- World Economic Forum (2025). *Global Cybersecurity Outlook 2025*.
- IBM Security (2025). *Cost of a Data Breach Report 2025*.
- Cybersecurity Ventures (2024, November 18). Cybercrime To Cost The World $10.5 Trillion Annually By 2025.
- Coalition Inc. (2024). *Cyber Threat Index 2024: Scans, Honeypots, and CVEs*.
- Breyer, P. (2025). Chat Control: The EU's CSAM scanner proposal.
- European Parliament (2025). Parliamentary question | Proposed Chat Control law presents new blow for privacy.
- Euro News (2025). Fact check: Is the EU about to start scanning your text messages?
- Electronic Frontier Foundation (2024, June 6). EU Council Presidency's Last-Ditch Effort For Mass Scanning Must Be Rejected.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/notizie/client-side-scanning/