Escaneo del lado del cliente:

Caso del Reino Unido

Diciembre de 2023

Resumen y recomendaciones

En el escrutinio actual del proyecto de ley de seguridad en línea por parte de la Cámara de los Lores, algunos debates se han centrado en el cifrado de extremo a extremo (E2EE) y el uso de tecnologías de "escaneo del lado del cliente". Internet Society busca contribuir a este debate por tres motivos: primero, el escaneo del lado del cliente socava la confianza prometida por el cifrado de extremo a extremo, poniendo en riesgo la seguridad y privacidad de las personas en el Reino Unido y más allá; segundo, el debate aún incluye argumentos engañosos que han persistido en etapas anteriores del proyecto de ley y no son una base confiable para evaluar la legislación; y tercero, el escaneo del lado del cliente no impedirá que personas motivadas compartan material ilegal sin ser detectadas.

Recomendaciones

Internet Society presenta respetuosamente las siguientes recomendaciones a los pares que examinan el proyecto de ley:

1. Apoyar la enmienda que exige que los servicios de mensajería privada queden excluidos del alcance del proyecto de ley. [Enmiendas 203 y 204]
2. Remediar las deficiencias en las salvaguardias previstas en el proyecto de ley apoyando, por ejemplo, enmiendas que exijan:
    a. Una prohibición explícita del monitoreo general, incluido el uso de escaneo del lado del cliente; [Enmienda 285]
    b. Un requisito para que los avisos de tecnología necesiten una aprobación judicial; [Enmiendas 207 y 246]
    c. Un requisito para que las intervenciones de Ofcom estén sujetas a una prueba de interés público transparente y responsable; [Enmienda 208]
    d. Un deber explícito de Ofcom de cumplir con las leyes de derechos humanos; [Enmienda 214]
    e. Un deber explícito de Ofcom de proteger la privacidad del individuo. [Enmiendas 209 y 210]

Con respecto a 2(a), el proyecto de ley de seguridad en línea debería descartar el *despliegue* masivo de tecnología que haga posible el monitoreo general, incluso si su intención declarada es que dicha tecnología solo se *habilite* de manera selectiva. Tal despliegue aún representaría una debilidad sistémica en la tecnología del mercado masivo y, por lo tanto, una amenaza significativa para la ciberseguridad y la privacidad.

El escaneo del lado del cliente viola la confidencialidad

El Gobierno continúa afirmando que las obligaciones del proyecto de ley de detectar y prevenir material ilegal "no prohíben ni debilitan el cifrado". Esto es engañoso, si dicha detección se base en la llamada puerta trasera del cifrado.[1] Si, como parece prever el Gobierno, la detección se basa en el "escaneo del lado del cliente", dicho escaneo se produce antes de que comience el proceso de cifrado. Ahora bien, esto puede hacer que la afirmación del Gobierno sea cierta de manera pedante, pero como resultado se pierde la confidencialidad. La realidad es que el escaneo anula el propósito del cifrado, crea nuevos riesgos de seguridad y priva a los ciudadanos de los medios para comunicarse de manera confidencial.

Incluso los profesionales de seguridad nacional del Reino Unido consideran que esta propuesta es insegura:

> "El escaneo del lado del cliente, a pesar de las afirmaciones de sus defensores, parece implicar algún tipo de nivel de acceso, algún tipo de capacidad para clasificar y escanear, y por lo tanto no hay manera de limitarlo al buen uso por parte de autoridades legales y creíbles, y democracias liberales".
> — Ciaran Martin, ex director ejecutivo del Centro Nacional de Seguridad Cibernética del Reino Unido.

Es legítimo cuestionar la confiabilidad de las salvaguardas reclamadas en el proyecto de ley y preguntar por qué el Gobierno ha ignorado hasta ahora el consejo de profesionales informados de la seguridad nacional.

[1] "A Backdoor is a Backdoor is a Backdoor." Internet Society, 24 de marzo de 2020, https://www.internetsociety.org/blog/2020/03/a-backdoor-is-a-backdoor-is-a-backdoor/

¿Cuáles son los riesgos del escaneo del lado del cliente?

El escaneo del lado del cliente (CSS) se refiere en términos generales a sistemas, integrados en el teléfono u otro dispositivo de un usuario, que escanean el contenido del mensaje (por ejemplo, texto, imágenes, archivos) en busca de coincidencias o similitudes con una base de datos de contenido objetable antes de enviar el mensaje.

Cuanto más dependen nuestras vidas y economías de los servicios en línea y la comunicación digital, más vital es para las personas, las familias, las empresas y los gobiernos comunicarse de forma segura y con la confianza de que sus conversaciones y transacciones son confidenciales. Los proveedores de servicios de comunicación en línea han implementado cada vez más E2EE para sus usuarios, para mejorar la seguridad, la privacidad y la confianza incluso cuando la comunicación, inevitablemente, pasa a través de uno o más intermediarios. Al mismo tiempo, los gobiernos y los organismos encargados de hacer cumplir la ley continúan buscando acceso a las comunicaciones para detectar y prevenir delitos.

Los defensores de las tecnologías CSS las posicionan como la solución. Sin embargo:

> Si romper el cifrado es como abrir una carta al vapor mientras pasa por una oficina de clasificación, el escaneo del lado del cliente es como leer la carta mientras se escribe. El resultado es el mismo: la privacidad de la comunicación del individuo está muerta.

Como explica una reciente opinión conjunta[2] del Consejo Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos, el CSS "puede eludirse fácilmente cifrando el contenido con la ayuda de una aplicación independiente". El CSS abre así la puerta a medidas desproporcionadas, que ponen en riesgo a los ciudadanos y no resolverán el problema de detectar material ilegal procedente de delincuentes incluso ligeramente decididos.

Conclusión

La comunicación confidencial es esencial para una sociedad digital y una economía basada en datos, y E2EE es esencial para la comunicación confidencial. El escaneo del lado del cliente frustra el propósito de E2EE, violando fundamentalmente la confidencialidad que los usuarios esperan y necesitan cuando se comunican en línea. Es más, el CSS debe ser ubicuo y omnipresente para ser eficaz, creando un círculo vicioso que el proyecto de ley de seguridad en línea no puede cuadrar: si el CSS se puede eludir fácilmente, no tiene sentido; si es omnipresente, es desproporcionado.

---

[2] "CEPD-SEPD Dictamen conjunto 4/2022 sobre la propuesta de Reglamento del Parlamento Europeo y el Consejo por el que se establecen normas para prevenir y combatir el abuso sexual de los menores" 28 de julio de 2022, https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-042022-proposal_en

Ya sabemos que el Gobierno quiere que todas las grandes plataformas de comunicaciones estén sujetas a este requisito. Es engañoso que el Gobierno afirme, al mismo tiempo, que esto no equivale a una obligación general de monitoreo.

El escaneo del lado del cliente, en productos y servicios de consumo masivo:

- **Reduce la confianza en el ecosistema de Internet.** La pérdida de confianza en la comunicación en línea dañará la economía del Reino Unido en un momento de extrema fragilidad.
- **Presenta un grave riesgo para los derechos fundamentales,** tal y como se expresa en el dictamen conjunto EDPB-EDPS.
- **Impone una seguridad deficiente a los usuarios, incluidos aquellos que corren mayor riesgo,** con pocas posibilidades de prevenir las acciones de delincuentes o gobiernos hostiles.

Las facultades del Proyecto de Ley de Seguridad en Línea incorporan la obligación de detectar contenidos ilegales en las comunicaciones privadas. Esto es desproporcionado y su eficacia está en duda. El Gobierno debería eliminar esta obligación del proyecto de ley y centrarse en otras formas más efectivas de detener el crimen en la red y mantener seguros a los usuarios.

Para obtener más información:

Los defensores del escaneo del lado del cliente señalan esta tecnología como una solución para identificar contenido objetable en entornos E2EE. En este documento, hemos expuesto algunas de las formas en que el CSS incumple el acuerdo de confianza de E2EE y los peligros que presenta.

Para obtener información adicional sobre cómo funciona el CSS y sus fallas inherentes, la hoja informativa de Internet Society sobre escaneo del lado del cliente puede servir como recurso para discusiones detalladas sobre políticas.[3] Nuestros otros recursos[4] sobre cifrado, seguridad y privacidad también pueden ser útiles para los formuladores de políticas que están preocupados pero no están familiarizados con el tema.

Información sobre Internet Society

Internet Society es una organización benéfica global fundada en 1992 por algunos de los primeros pioneros de Internet. Creemos que Internet es una fuerza para el bien y estamos trabajando para lograr una Internet abierta, conectada globalmente, segura y confiable que beneficie a todos. Con 110

[3] "Hoja informativa: Escaneo del lado del cliente.", 26 de septiembre de 2022, https://www.internetsociety.org/es/resources/doc/2020/escaneo-del-lado-del-cliente/

[4] "¿Qué es el cifrado?" Internet Society, 14 de julio de 2022, https://www.internetsociety.org/issues/encryption/what-is/

capítulos activos en seis continentes, de los cuales 28 están en Europa, y más de 100 000 usuarios individuales que apoyan nuestras actividades, Internet Society es un actor importante y un interlocutor confiable y técnicamente informado de la sociedad civil para cuestiones de gobernanza de Internet.