PRIVACY INTERNATIONAL

Hackeo y vigilancia gubernamental: 10 garantías necesarias

Diciembre de 2017

Introducción

Una cantidad cada vez mayor de Gobiernos del mundo está recurriendo al hackeo para facilitar sus actividades de vigilancia. Sin embargo, muchos de ellos implementan esta capacidad de manera secreta y sin fundamentos legales claros. En los casos en que los Gobiernos buscan incluir estas facultades en sus legislaciones, suelen hacerlo sin las garantías ni los controles correspondientes para las actividades de vigilancia, como dispone el derecho internacional de los derechos humanos.

El hackeo implica singulares y graves amenazas para nuestra privacidad y nuestra seguridad. Por este motivo, incluso en los casos en que los Gobiernos emprenden actividades de vigilancia legítimas, como sucede al recoger pruebas en investigaciones penales o actividades de inteligencia, es posible que nunca puedan llegar a demostrar que el hackeo como forma de vigilancia es compatible con la legislación internacional en materia de derechos humanos. Sin embargo, hasta la fecha, ha sido insuficiente el debate público sobre el alcance y la naturaleza de esta facultad y sobre las implicancias que tiene para la privacidad y la seguridad de las personas.

Las garantías que proponemos están diseñadas para ayudar a las partes interesadas a evaluar las actividades de hackeo emprendidas por los Gobiernos, a la luz del derecho international de los derechos humanos. También tienen el objetivo de abordar las implicancias en materia de seguridad de este tipo de hackeo. En términos generales, se deben incorporar consideraciones sobre seguridad en las garantías y los mecanismos de control para las actividades de vigilancia.

Explicamos las bases conceptuales y jurídicas de las garantías que proponemos en un documento independiente llamado “Hackeo y vigilancia gubernamentales: comentario sobre las 10 garantías necesarias”.

Estas garantías forman parte de una estrategia integral emprendida por Privacy International y otras instituciones de la sociedad civil para garantizar que:

- Los Gobiernos y la industria prioricen la seguridad defensiva;
- Nuestros dispositivos, redes y servicios se diseñen de modo tal que garanticen la seguridad y protejan nuestra privacidad, y que dichas protecciones se mantengan y
- Las protecciones legales y tecnológicas se apliquen a todas las personas en todo el mundo.

¿Por qué nos preocupa tanto que los Gobiernos lleven a cabo prácticas de hackeo para vigilar?

Las actividades de hackeo que emprenden los Gobiernos son diferentes a cualquier otro tipo de técnica de vigilancia existente. El hackeo es un intento por comprender un sistema mejor de lo que el sistema se comprende a sí mismo, para luego modificarlo levemente y lograr que haga lo que el hacker desee. Fundamentalmente, se trata de hacer que las tecnologías actúen de una manera que su fabricante, propietario o usuario no había previsto ni planeado.

Los Gobiernos pueden llevar a cabo este tipo de prácticas a distancia, de manera encubierta, en diferentes jurisdicciones y a escala. Un único hackeo puede afectar a mucha gente, incluso a las personas que no son los actores principales de la investigación u operación gubernamental, o que no están relacionadas con ellas.

Es posible que en el futuro los Gobiernos recurran cada vez con mayor frecuencia a actividades de hackeo para facilitar la vigilancia. En la era digital, los datos de las personas suelen estar en manos de empresas, y estas empresas pueden tener su base en una jurisdicción extranjera. Por lo tanto, los Gobiernos han confiado generalmente en la cooperación de terceros (una empresa, un gobierno extranjero o ambos) para acceder a estos datos. Este procedimiento suele demandar demasiado tiempo y resultar infructuoso si la empresa o el gobierno extranjero no desean o no pueden proporcionar el acceso. Así, el hackeo puede ser un método más conveniente de implementar que los procedimientos legales que involucran a diversas partes.

En ocasiones, las empresas pueden mantener los datos de sus usuarios fuera de su alcance, por ejemplo si eligen no recogerlos o si los someten a cifrado. Con la excusa de no poder obtener datos digitales por motivos técnicos (fenómeno que se conoce como “going dark”), los Gobiernos presionan a las empresas para obtener acceso privilegiado a sus sistemas y rediseñar los mecanismos de seguridad. Mientras tanto, desarrollan y adquieren capacidades para hackear los productos y los servicios de esas mismas empresas, lo que puede permitirles tanto recoger datos que de otra manera serían imposibles de obtener, como eludir el cifrado y otras características de seguridad.

Mediante el hackeo, los Gobiernos pueden influir o interferir directamente en las tecnologías, que cada vez están más perfectamente integradas a nuestras vidas, economías y sociedades. Las capacidades de hackeo gubernamentales solo están restringidas por los propios recursos y capitales de los Gobiernos. Creemos que se deben priorizar los sistemas y la seguridad de los datos, y que se deben aplicar mayores restricciones para limitar y definir las facultades de hackeo de los Gobiernos.

Privacidad

El hackeo permite que los Gobiernos accedan a sistemas de manera remota y, por lo tanto, potencialmente, a todos los datos almacenados en dichos sistemas. Los dispositivos digitales personales contienen cada vez mayor cantidad de información de máxima privacidad que sus propietarios guardan en cualquier otra parte. Estos dispositivos sustituyen y fusionan libretas de direcciones, correspondencia física, registros diarios, archivadores, álbumes de fotos y billeteras. De manera creciente, los Gobiernos pueden dirigir sus facultades de hackeo hacia dispositivos nuevos y emergentes, como la llamada 'Internet de las cosas' y los dispositivos corporales e incorporados, como los sensores de salud.

El hackeo también permite que los Gobiernos practiquen nuevas formas de vigilancia en tiempo real: pueden encender de manera encubierta el micrófono y la cámara, o usar la geolocalización de un dispositivo. Mediante las actividades de hackeo, los Gobiernos pueden, además, tomar continuamente capturas de pantalla del dispositivo hackeado u observar toda la información que ingresa al mismo o que sale de él, incluidos los detalles y las contraseñas de inicios de sesión, el historial de navegación en Internet y los documentos y las comunicaciones que el usuario no deseaba compartir.

Asimismo, estas actividades dan lugar a la manipulación de la información en un mundo dominado cada vez más por los datos. Controlando la funcionalidad de los sistemas, el hackeo permite a los Gobiernos eliminar o recuperar datos que habían sido borrados. También les permite dañar o implantar datos, enviar comunicaciones o informaciones falsas desde el dispositivo, agregar o editar códigos para incorporar nuevas capacidades o alterar las existentes, y eliminar cualquier rastro de la intrusión. En un mundo en el que nuestra información personal se expresa en datos cada vez con mayor frecuencia, el menor cambio que se realice en ellos –una contraseña, las coordenadas de GPS, un documento– puede tener consecuencias radicales.

Las intrusiones a la privacidad provocadas por el hackeo se amplifican enormemente cuando un Gobierno interfiere con las redes de comunicación y su infraestructura subyacente. Mediante el hackeo a un proveedor de Internet, por ejemplo, un Gobierno podría obtener acceso no solo al sistema del proveedor sino también, mediante los datos allí almacenados, a los sistemas de todos sus usuarios. Los Gobiernos también pueden interferir con diferentes tipos de redes y su infraestructura, como las que conectan a los bancos. El hackeo dirigido a las redes podría realizarse para vigilar a individuos, grupos o países específicos, o a lo largo de una gran cantidad de jurisdicciones.

El hackeo por parte de Gobiernos incluye el ataque de dispositivos que se encuentran bajo la custodia física de dichos Gobiernos. Si bien este tipo de hackeo genera el mismo tipo de preocupaciones que las mencionadas anteriormente, también presenta implicancias singulares para la privacidad. La información que contiene un dispositivo puede incluir datos que su usuario ni siquiera sabe que existen, y a los que no puede acceder. Por ejemplo, los teléfonos móviles pueden

tener información que los usuarios creen que fue eliminada, o información generada por sensores que los usuarios desconocen y a la que no pueden acceder, y que podría dar lugar a la divulgación de datos biográficos, fisiológicos o biométricos.

Seguridad

El hackeo realizado por los Gobiernos con el propósito de vigilar es también preocupante desde la perspectiva de la seguridad. Los sistemas informáticos son complejos y, casi con toda certeza, tienen vulnerabilidades. Al mismo tiempo, las interacciones de estos sistemas con sus usuarios dan lugar a vulnerabilidades que podrían aprovecharse para interferir con sus propios sistemas.

Tanto la identificación de vulnerabilidades, como su sometimiento a pruebas mediante el desarrollo de fallos aprovechables (*exploits*) y el intercambio de estos resultados son necesarios para consolidar la seguridad. Pero los Gobiernos que hackean para vigilar no buscan mejorar la seguridad de los sistemas.

En el contexto de la vigilancia, los Gobiernos no identifican vulnerabilidades para lograr que los sistemas sean seguros, mediante la realización de pruebas y una divulgación coordinada, sino para aprovechar dichas vulnerabilidades y facilitar su vigilancia del objetivo. Esta actividad puede no solo menoscabar la seguridad del sistema objetivo sino también la de otros sistemas.

Asimismo, surgen otras inquietudes relativas a la seguridad cuando los Gobiernos se aprovechan de las personas para interferir en sus propios sistemas. La suplantación de identidad (*phishing*), por ejemplo, es una técnica de ingeniería social común por medio de la que un hacker se hace pasar por una persona u organización respetable.

Los ataques de suplantación de identidad suelen adoptar la forma de correos electrónicos o mensajes de texto, que pueden incluir un enlace o archivo adjunto infectado con software malicioso (*malware*). Estas técnicas se valen de la confianza del usuario, que es crucial para mantener la seguridad de los sistemas, y de la Internet como un todo.

Preservar la seguridad es una tarea ardua, y los Gobiernos no son los únicos actores fundamentales. Si desea obtener información más detallada sobre la interacción entre seguridad y hackeo, consulte nuestro texto, *A conflict of security: why we are so concerned about government hacking from a security perspective* (Un conflicto de seguridad: por qué nos preocupa tanto el hackeo realizado por los Gobiernos desde la perspectiva de la seguridad)

Alcance de las garantías

El término "hackeo" es difícil de definir. Para el contexto de nuestras garantías, Privacy International propone la siguiente definición:

> El hackeo es un acto o una serie de actos que interfieren con un sistema para lograr que actúe de una manera imprevista o inesperada por el fabricante, usuario o propietario de dicho sistema. "Sistema" se refiere a cualquier tipo de combinación de hardware y software, o a alguno de sus componentes.

Privacy International reconoce que es posible que existan instancias de hackeo a cargo de Gobiernos que no responden a esta definición y que, sin embargo, deben investigarse. Estamos abiertos a recibir sugerencias sobre cómo modificar esta definición para incluir esas formas diferentes de hackeo por parte de Gobiernos.

Los Gobiernos emprenden actividades de hackeo para una amplia gama de finalidades. Las garantías solo abordan las actividades de hackeo que tienen como finalidad obtener pruebas en una investigación penal o en actividades de inteligencia, o colaborar con el proceso de recogida de pruebas o en actividades de inteligencia.

Las garantías no abordan las prácticas de hackeo cuyo riesgo alcanza el nivel de una amenaza, el uso de la fuerza o un ataque armado, o que se llevan a cabo como parte de un conflicto armado activo. Por ejemplo, no incluirían las operaciones de hackeo que se llevan a cabo para clausurar una infraestructura crítica, como una red eléctrica, en un país extranjero. Sin embargo, sí contemplarían una operación para redirigir el tráfico de un proveedor de telecomunicaciones para que dicho tráfico circule por un punto de intercepción.

Las garantías se aplican a las actividades de hackeo que emprende un Gobierno tanto dentro del territorio de un Estado como fuera del mismo. Una de las garantías abarca explícitamente el hackeo llevado a cabo en territorio extranjero.

Las garantías son aplicables independientemente de que el hackeo sea llevado a cabo por funcionarios gubernamentales o personas con alguna autoridad gubernamental, bajo la dirección o el control de un Gobierno, o cuya conducta es posteriormente aceptada y adoptada como propia por un Gobierno.

Hackeo y vigilancia gubernamental: 10 garantías necesarias

1. Legalidad

Las facultades para hackear otorgadas al Gobierno deben estar descritas explícitamente en la ley y restringirse a las actividades estricta y demostrablemente necesarias para lograr un objetivo legítimo. Dicha ley debe ser accesible al público, además de ser lo suficientemente clara y precisa para permitir a las personas prever su aplicación y la extensión de la interferencia. Debe estar sujeta a revisiones periódicas mediante un proceso legislativo participativo.

2. Seguridad e integridad de sistemas

Antes de implementar medidas de hackeo, las autoridades gubernamentales deben evaluar los daños y perjuicios potenciales a la seguridad y la integridad del sistema objetivo y los sistemas en general, al igual que las de los datos del sistema objetivo y los sistemas en general, y cómo se mitigarán o corregirán dichos riesgos o perjuicios potenciales. Las autoridades gubernamentales deben incluir esta evaluación en todas las solicitudes de respaldo de las medidas de hackeo propuestas.

Los Gobiernos no deben obligar a los fabricantes de hardware o software, o a los proveedores de servicios, a facilitar las actividades de hackeo de ninguna manera, mucho menos comprometiendo la seguridad y la integridad de sus productos y servicios.

3. Necesidad y proporcionalidad

Antes de tomar alguna medida de hackeo, las autoridades gubernamentales deben, como mínimo:

(i) Establecer un alto grado de probabilidad de que:

a. Haya tenido lugar o se llevará a cabo un delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional;

b. El sistema utilizado por la persona que se sospecha cometerá un delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional, contiene evidencias relevantes y sustantivas para el presunto delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional;

c. Las evidencias relevantes y sustantivas para el presunto delito o acto de gravedad, equivalente a una amenaza específica y de gravedad para la seguridad nacional, se obtendrán hackeando el sistema objetivo;

(ii) Establecer, hasta el máximo que fuera posible, la identidad de la persona sospechada de cometer el delito o acto de gravedad equivalente a una amenaza específica y de gravedad para la seguridad nacional, y los detalles de identificación exclusivos del sistema objetivo, incluidas la localización y las configuraciones específicas;

(iii) Agotar todos los métodos menos intrusivos, o determinar que serían infructuosos, de modo que el hackeo es la opción menos intrusiva;

(iv) Establecer el método, la extensión y la duración de la medida de hackeo propuesta;

(v) Garantizar que los datos a los que se acceda y que se recojan se restringirán únicamente a la información relevante y sustantiva en relación con el delito o acto de gravedad, equivalente a la presunta amenaza específica y de gravedad a la seguridad nacional, y establecer las medidas que se tomarán para minimizar el acceso a datos irrelevantes y secundarios, así como su recogida;

(vi) Garantizar que únicamente la autoridad especificada accederá a dichos datos y los recogerá, y que dichos datos serán utilizados y compartidos solo a los fines para los que la autorización ha sido otorgada, y durante el tiempo especificado en ella;

(vii) Determinar los daños y perjuicios potenciales a la seguridad y la integridad del sistema objetivo y los sistemas en general, al igual que las de los datos del sistema objetivo y los sistemas en general, y cómo se mitigarán o corregirán dichos riesgos o perjuicios potenciales, para permitir una evaluación de la proporcionalidad de la medida de hackeo propuesta según las implicancias de seguridad.

4. Autorización judicial

Antes de implementar alguna medida de hackeo, las autoridades gubernamentales deben completar una solicitud, estableciendo la necesidad y la proporcionalidad de las medidas propuestas ante una autoridad judicial imparcial e independiente, que determinará si aprueba dichas medidas, y que controlará su implementación.

La autoridad judicial debe tener la facultad de consultar a personas con pericia técnica en las tecnologías relevantes y solicitar su colaboración para comprender cómo afectarán las medidas propuestas el sistema objetivo y los sistemas en general, y los datos en todos estos sistemas.

La autoridad judicial también debe tener la facultad de consultar a personas con pericia en materia de privacidad y derechos humanos, para obtener asesoramiento y comprender cómo interferirán las medidas propuestas con los derechos de la persona sobre la que se aplicarán, y de otras personas que podrían verse afectadas.

5. 5. Integridad de la información

Las autoridades gubernamentales no deben agregar, alterar o eliminar datos en el sistema objetivo, excepto hasta donde sea técnicamente necesario para implementar la medida de hackeo propuesta.

Deben llevar un registro de auditoría verificable e independiente que incluya sus actividades de hackeo y cualquier tipo de adición, alteración o eliminación realizada. Si las autoridades gubernamentales recurren a datos obtenidos mediante una medida de hackeo autorizada, deben dar a conocer el método, la extensión y la duración de dicha medida, al igual que el registro de auditoría, de modo que la persona objetivo pueda comprender la naturaleza de los datos obtenidos e investigar las adiciones, alteraciones o eliminaciones de información realizadas, o las interrupciones en la cadena de custodia, según sea apropiado.

6. Notificación

Las autoridades gubernamentales deben notificar sobre la intercepción realizada a la(s) persona(s) cuyo(s) sistema ha sido objeto de interferencias, en conformidad con una medida de hackeo autorizada, independientemente de la residencia de dicha(s) persona(s). También deben notificar a los fabricantes de software y hardware y a los proveedores de servicios afectados, brindándoles detalles sobre el método, la extensión y la duración de las medidas de hackeo, incluidas las configuraciones específicas del sistema objetivo.

Las demoras en las notificaciones solo están justificadas si dichas notificaciones pusieran en grave peligro la finalidad por la que se autorizó la medida de hackeo, o si existieran peligros inminentes para la vida humana, y se obtuviera un permiso para demorar la notificación por parte de una autoridad judicial imparcial e independiente.

7. Destrucción y devolución de datos

Las autoridades gubernamentales deben destruir inmediatamente cualquier tipo de datos irrelevantes o no significativos que se obtengan mediante la implementación de una medida de hackeo autorizada. Dicha destrucción debe incluirse en el registro de auditoría verificable e independiente de las actividades de hackeo.

Después de que las autoridades gubernamentales han utilizado los datos obtenidos mediante una medida de hackeo autorizada para la finalidad por la que se obtuvo permiso, deben devolver los datos a la persona objeto de estas medidas y destruir cualquier otra copia de ellos que exista.

8. Control y transparencia

Las autoridades gubernamentales deben ser transparentes en cuanto al alcance y el uso de sus facultades y actividades de hackeo, y deben someter dichas facultades y actividades a un mecanismo de control independiente.

Deben publicar periódicamente, como mínimo, información sobre el número de solicitudes para autorizar hackeos que hayan sido aprobadas y rechazadas, la identidad de las autoridades gubernamentales que realizaron la solicitud, los delitos especificados en las solicitudes y el método, la extensión y la duración de las medidas de hackeo autorizadas, incluidas las configuraciones específicas de los sistemas objetivo.

9. Extraterritorialidad

Al poner en práctica una medida de hackeo extraterritorial, las autoridades gubernamentales deben cumplir en todo momento con las obligaciones legales internacionales, incluidos los principios de soberanía y no intervención, que expresan restricciones al ejercicio de la jurisdicción extraterritorial.

Las autoridades gubernamentales no deben utilizar el hackeo para evadir otros mecanismos legales (como tratados de asistencia legal mutua u otros mecanismos consensuados) con el fin de obtener datos localizados fuera de su territorio. Estos mecanismos deben documentarse claramente, ponerse a disposición del público y estar sujetos a garantías de equidad procedimental y sustantiva.

10. Recurso efectivo a la autoridad

Las personas que han sido víctimas de actividades de hackeo ilícitas por parte del Gobierno, independientemente de dónde residan, deben tener acceso a recursos efectivos ante el mismo, que permitan remediar la situación.

PRIVACY INTERNATIONAL

Privacy International
62 Britton Street, London EC1M 5UY
United Kingdom

Phone +44 (0)20 3422 4321
www.privacyinternational.org
Twitter @privacyint

UK Registered Charity No. 1147471