
Expertos de Internet buscan renovar seguridad por espionaje de NSA

08/09/2013



Pero reconocieron que la tarea no es fácil, en parte porque la seguridad en Internet ha recaído en gran medida en brillantes científicos del Gobierno que ahora parecen sospechosos para muchos.

Los tecnólogos dicen que se sienten traicionados por el hecho de que la NSA, que ha contribuido a desarrollar algunos importantes estándares de seguridad, esté intentando asegurarse de que sean lo suficientemente débiles como para que la agencia los pueda traspasar.

Algunos dicen estar estupefactos porque el Gobierno valore tanto su capacidad de vigilancia como para querer reducir la seguridad de todos.

"Tenemos la suposición de que podrían usar su capacidad para hacer unos bajos estándares, pero eso dejaría sin seguridad a todo el mundo en Estados Unidos", dijo, Matthew Green, profesor de criptografía de la Universidad Johns Hopkins. "Pensábamos que nunca estarían tan locos como para disparar contra el suelo que nos mantiene en pie, y ahora no estamos tan seguros", dijo.

El jefe del grupo de voluntarios a cargo de las normas tecnológicas fundamentales de Internet dijo a Reuters que el panel intensificará su trabajo para que la encriptación se añada al tráfico normal de la Web y para fortalecer el denominado estrato seguro que protege a bancos, el correo electrónico y a otras páginas que comienzan con

"Https".

"Este es uno de los peligros a los que nos enfrentamos en la era en red", dijo Jari Arkko, un científico de Ericsson que preside el Equipo de Trabajo de Ingeniería en Internet. "Tenemos que responder a las nuevas amenazas", dijo.

Otros expertos coincidieron al responder sobre las informaciones de prensa basadas en los documentos del exanalista de la NSA Edward Snowden que mostraban que la NSA había manipulado esos estándares.

Los documentos que obtuvo The Guardian, The New York Times y otros medios muestran que la agencia trabajó para introducir vulnerabilidades en las herramientas de encriptación comercial, encubriendo la influencia de que otros diseños permitan una entrada en el futuro, y debilitando los estándares de todo el sector para beneficio de la agencia.

Junto con otras técnicas, esos esfuerzos llevaron a la NSA a decir internamente que tenía la capacidad de acceder a muchas formas de tráfico de Internet que se habían considerado seguras, entre ellas al menos algunas redes privadas virtuales, que crean redes seguras en Internet, y el nivel general de seguridad para sitios web empleados por la banca o el comercio online.

La oficina del director de Inteligencia Nacional dijo el viernes que la NSA "no estaría haciendo su trabajo" si no trataba de contrarrestar el uso del encriptado por parte de adversarios como "terroristas, ciberdelincuentes, traficantes de personas y otros".

Green y otros dijeron que una gran cantidad de protocolos de seguridad se necesitaban escribir "desde cero" sin la ayuda del Gobierno.

Vint Cerf, autor de algunos de los principales protocolos de Internet, dijo que no sabía si la NSA había causado mucho daño, subrayando que la incertidumbre de las nuevas informaciones en torno al uso de la NSA sobre sus capacidades.

"Existía una tensión entre la misión de vigilar y la de proteger las comunicaciones, y esa tensión se resolvió hace algún tiempo a favor de la protección al menos para las comunicaciones estadounidenses", dijo Cerf.

El empleador de Cerf, Google, confirmó que está encriptando los datos entre sus centros, un proceso que se aceleró tras salir a la luz los documentos de Snowden en junio.

El autor Bruce Schneier, una de las figuras más admiradas en la criptografía moderna, escribió en una columna en el Guardian que la NSA "ha minado un contrato social fundamental", y que los ingenieros del mundo tenían "una obligación moral" para recuperar Internet.

