Barack Obama estableció en enero que los problemas de Internet no debían ser explotados por la Agencia de Seguridad Nacional (NSA). Pero señaló una excepción tan amplia como polémica: los espías estadounidenses podrán indagar en los fallos informáticos para prevenir un delito o proteger «la seguridad nacional».

El presidente tomó la decisión a mediados de enero al revisar las normas por las que se rigen los miembros de la NSA. Pero la Casa Blanca no la ha desvelado hasta esta semana, cuando desmintió que los miembros de la agencia hubieran creado o explotado‘ Heartbleed’: el agujero informático que ha obligado a cambiar sus contraseñas a millones de usuarios de Internet.

La agencia Bloomberg citaba el viernes a dos fuentes anónimas que acusaban a los miembros de la NSA de ser conscientes del fallo «durante al menos dos años» y de haberlo usado para robar contraseñas y otros documentos reservados de varios usuarios de Internet. Un extremo que negaron unas horas después los responsables de la agencia y de la Casa Blanca, que dijeron que ‘Heartbleed’ no estaba entre las herramientas digitales de la NSA.

El entorno de Obama explicó esta semana que la agencia «se inclina ahora por desvelar responsablemente cualquier vulnerabilidad» a los responsables de los programas afectados. Pero recordó que la Casa Blanca permite a los espías estadounidenses usar fallos como ‘Heartbleed’ para prevenir un delito o proteger la seguridad nacional.

Los documentos del analista Edward Snowden indican que la NSA llevaba al menos dos años intentando encontrar una fórmula para hacer precisamente lo que ‘Heartbleed’ hizo por error. Varios diarios han desvelado la existencia del programa llamado BullRun, que los miembros de la agencia crearon para desvelar el contenido de mensajes cifrados y que podría haber logrado su objetivo en alguna ocasión.

Obama encargó a cinco expertos un informe sobre la reforma de la NSA. Se trataba de devolver la confianza a la opinión pública, espantada por las revelaciones del analista Edward Snowden sobre los excesos de la NSA.

Los titulares subrayaron entonces que los expertos habían recomendado que el Estado dejara de almacenar los datos de lasllamadas de los ciudadanos y que dejaran de espiar a líderes foráneos como Angela Merkel o Dilma Rousseff. Pero el informe advertía también que la NSA debía dejar de dedicar parte de sus recursos a explotar fallos que permitieran el acceso a mensajes cifrados y dejar de construir 'puertas traseras' para acceder a los servidores de grandes empresas digitales como Google, Yahoo o Microsoft.

Los responsables de esas empresas han expresado varias veces suenfado con la Casa Blanca, a la que acusan de poner en peligro su volumen de negocio en lugares como Francia, Alemania o Brasil. Conscientes de esas protestas, los expertos dijeron que la NSA debía limitar el uso de lo que se conoce como 'zero days': defectos de programas como Windows que permiten penetrar en los ordenadores de una empresa o un organismo gubernamental.

La NSA utilizó cuatro 'zero days' durante el ataque a uno de los complejos atómicos del régimen iraní. Los expertos creen que la operación logró dañar unas mil centrifugadoras de uranio y que su éxito ayudó a convencer al régimen de que merecía la pena sentarse a negociar sobre su programa nuclear.

¿Debería un presidente renunciar a armas informáticas cada vez más poderosas que podrían evitar víctimas? «Los chinos no renunciarán a usar fallos informáticos sólo porque nosotros renunciemos a ellas», advertían este domingo fuentes de las agencias de espionaje. «No puedo imaginar a ningún presidente renunciando a una tecnología que pudiera permitirle llevar a cabo una acción encubierta que pudiera evitar una guerra», afirmaba un portavoz de la Casa Blanca en las páginas del 'New York Times'.

Fuente: elmundo