Special Report: HP Enterprise let Russia scrutinize cyberdefense system used by Pentagon

Enviado por Iván Fuentes López en Mar, 11/06/2018 - 21:05
Cita:

Schectman, Joel. Dustin Volz, Jack Stubbs [2017], “Special Report: HP Enterprise let Russia scrutinize cyberdefense system used by Pentagon”, Reuters, 2 de octubre, https://www.reuters.com/article/us-usa-cyber-russia-hpe-specialreport/sp... [1]

Fuente:
Otra
Fecha de publicación:
Lunes, Octubre 2, 2017
Revista descriptores:
Competencia mundial. Disputa hegemónica [2]
Empresas transnacionales y gobernanza mundial [3]
Estudios de caso: actividades - empresas [4]
Relaciones entre empresas estados y sociedad [5]
Tema:
Hewlett Packard Enterprise permitió a una agencia de defensa rusa revisar el funcionamiento interno del software de defensa cibernética utilizado por el Pentágono.
Idea principal:

HPE (Hewlett Packard Enterprise) aceptó ser sometida a una revisión por parte de una agencia de seguridad rusa, quien revisó el código fuente de uno de sus productos de cyber-seguridad, llamado ArcSight, utilizado por el Pentágono. El programa detecta posibles ataques a sus sistemas informáticos y es utilizado por gran parte del ejército estadounidense y por empresas privadas.

La razón de la revisión gira en torno a la actual política del gobierno ruso de revisar el código fuente de cualquier empresa de ciberseguridad estadounidense para asegurarse de que los servicios de inteligencia de Estados Unidos no hayan colocado herramientas de espionaje en el software. HPE realizó esfuerzos por obtener la certificación necesaria para vender el producto al sector público de Rusia permitiendo la revisión.

De acuerdo a funcionarios del Pentágono, ex empleados de ArcSight y expertos independientes en seguridad, la revisión implica un hecho grave en tanto vulnera al gobierno estadounidense de posibles ataques del gobierno ruso, pues deja al descubierto las debilidades del software. Sin embargo desde el Pentágono aseguran que no existe ningún hackeo o espionaje cibernético que provenga de la revisión de ArcSight.

La revisión tuvo lugar durante el año 2016, en medio de las acusaciones del gobierno estadounidense a Rusia de ataques cibernéticos a empresas y agencias gubernamentales. El

caso de HPE pone en el centro de la polémica a las empresas de tecnología estadounidenses que realizan negocios con Rusia y China, que deben considerar el papel que juegan en la cyber-seguridad estadounidense.

La revisión fue realizada por la empresa Echelon, en nombre del Servicio Federal de Control Técnico y de Exportaciones de Rusia (FSTEC, por sus siglas en inglés), un organismo de defensa encargado de combatir el ciberespionaje. Alexey Markov, propietario mayoritario de la empresa, afirmó que el papel que realizan consiste en dar a aviso al gobierno ruso de cualquier vulnerabilidad que detecten, no sin antes haber sido autorizados por la empresa de dar datos sensibles, además de existir un acuerdo de confidencialidad con las empresas revisadas. Lo mismo asegura la FSTEC, que da aviso de cualquier vulneración a una base de datos de amenazas del gobierno ruso. En el caso de HPE, de acuerdo a un portavoz de la empresa, no se detectó debilidad alguna a su producto. También ha dicho que las revisiones del código fuente son realizadas en un centro de investigación de HPE fuera de territorio ruso, donde no se permite la salida de ningún código.

De acuerdo a un informe de Echelon en 2014, en el 50% de los software extranjeros y rusos descubrió vulnerabilidades. No obstante Alan Paller, fundador del SANS Institute afirma que las revisiones no lograrían que alguien hackeara los sistemas militares, pues primero tendrían que pasar otros filtros de seguridad. Paller ha dicho también que no tiene nada de alarmante la revisión a HPE, pues es indispensable para cualquier negocio con Rusia. ArcSight es utilizado actualmente por varias empresas estatales y compañías rusas, como el banco VTB y el grupo de medio de comunicación Rossiya Seyodnya, aunque se desconoce el tamaño de sus negocios en aquel país.

Cualquier error en su producto hace vulnerable a cualquier cliente, sea del país que sea, un error en el código de software lo vuelve vulnerable al hackeo, Allen Pomeroy, un antiguo empleado de ArcSight que ayudó a los clientes a construir sus sistemas de defensa cibernética ha declarado que un error haría imposible defenderse de cualquier amenaza.

HPE asegura que los cuestionamientos de Reuters sobre la revisión son de materia especulativa, aseguró que sus clientes siempre están informados de cualquier acontecimiento que los inquiete, pero desde el pentágono se dice otra cosa, una portavoz de la Agencia de Sistemas de Información de Defensa del Pentágono, dijo que HPE no reveló la revisión a la agencia estadounidense, pues los contratos no requieren que esa información sea divulgada. En el caso del Pentágono, las revisiones a los software no son un requisito indispensable para hacer negocios.

Echelon funciona como un laboratorio oficial y probador de software de FSTEC y de la agencia de espionaje FSB (Servicio Federal de Seguridad, por su acrónimo ruso) la cual ha sido acusada de orquestar los ataques cibernéticos en las elecciones de 2016, sin embargo, el presidente de Echelon afirma que las revisiones son útiles para todo el mundo, pues al detectar algún error, el producto mejorará. Cisco Systems Inc, el fabricante de equipos para redes y SAP, fabricante de software han aceptado las revisiones, no así Symantec, una empresa estadounidense de ciberseguridad, por cuestiones de seguridad.

ArcSight es considerado un baluarte clave de la ciberdefensa en gran parte de las fuerzas armadas de Estados Unidos, es utilizado para proteger la red secreta de enrutadores de

protocolo de Internet del Pentágono (SIPRNet, por sus siglas en inglés). Una portavoz del Pentágono afirma que el software es revisado y evaluado constantemente para evitar alguna vulneración.

ArcSight es pionero en cyber-seguridad, creada como compañía independiente en el 2000, desarrollo softwares para que grandes organizaciones recibieran alertas en tiempo real sobre posibles ataques. Para 2010, ArcSight se había convertido en "la principal" herramienta de defensa de redes cibernéticas del Pentágono, es prácticamente irremplazable para muchas partes del ejército estadounidensepues su integración es tal, que cambiar de producto implicaría cambiar toda la estructura de cyber-seguridad.

HPE pasó a manos de Micro Focus International Plc, una corporación británica de tecnología, en septiembre de 2016, se espera que genere un poco menos de la mitad de ingresos anuales de la empresa, de acuerdo a Jason Schmitt, el actual jefe de la división ArcSight, quien se negó a declarar sobre la revisión del código fuente, ya que ocurrió antes de la adquisición, pero aseguró que las revisiones no eran llevadas a cabo en ese momento (2017).

Datos cruciales:

1- En un artículo de investigación de 2014, los directores de Echelon dijeron que la compañía descubrió vulnerabilidades en el 50 por ciento del software extranjero y ruso que revisó.

2- Echelon funciona como un laboratorio oficial y probador de software de FSTEC y de la agencia de espionaje FSB de Rusia. La inteligencia de Estados Unidos ha acusado al FSB de ayudar a montar ciberataques contra Estados Unidos e interferir en las elecciones presidenciales de 2016.

3- HPE acordó en 2016 vender ArcSight y otros productos de seguridad a la empresa tecnológica británica Micro Focus International Plc en una transacción que se completó en septiembre, empresa que espera generar del producto, un poco menos de la mitad de los 800 millones de dólares en ingresos anuales.

Nexo con el tema que estudiamos:

El software ArcSight, es un producto absolutamente indispensable para el Pentágono, lo que lo vueleve un actor que define las políticas de seguridad nacional estadounidense, al mismo tiempo es cliente del gobierno ruso, esto implica ser parte de la disputa hegemónica actual.

La privatización de muchos de los servicios indispensables hoy en día en la seguridad pone en dilema los "intereses" de los involucrados, sobre todo de los usuarios "públicos" o "gubernamentales"; porque de alguna forma se intercambia información de "seguridad nacional" que pasan a manos de empresas privadas. La tensión se agudiza cuando las empresas privadas, en sus fines de seguir generando ganancias en otros mercados, desbordan las fronteras nacionales y son contratadas por clientes de nacionalidades distintas. El artículo deja ver: i) la expansión sin fronteras de las ahora grandes corporaciones de servicios informáticos militares y de seguridad; ii) la ambigüedad o poca claridad respecto la "seguridad nacional"; y quizá lo más importante, iii) una tendencia creciente de acumulación y concentración de datos procedentes de distintas nacionalidades (de diferenes "seguridad(es) nacional(es)" en pocas corporaciones

privadas.

Links
[1] https://www.reuters.com/article/us-usa-cyber-russia-hpe-specialreport/special-report-hp-enterprise-let-russia-scrutinize-cyberdefense-system-used-by-pentagon-idUSKCN1C716M
[2] http://let.iiec.unam.mx/taxonomy/term/12
[3] http://let.iiec.unam.mx/taxonomy/term/14
[4] http://let.iiec.unam.mx/taxonomy/term/16
[5] http://let.iiec.unam.mx/taxonomy/term/20