La OTAN se infiltrará en Anonymous y la perseguirá

MATTHEW LASAR :: 18/06/2011

WikiLeaks y Anonymous figuran en los primeros puestos de la lista de amenazas para los desvelos de la organización terrorista OTAN por mantener secreta su información

La Organización del Tratado del Atlántico Norte aúna la fuerza militar de 28 países miembros, entre los que se encuentran Alemania, Reino Unido y Francia. Estos tres países y Estados Unidos poseen unos ejércitos inmensos, armas nucleares y están comprometidos con el Artículo Cinco de la carta de la OTAN:

Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas

Pero al leer el nuevo borrador de informe general sobre ciberseguridad se obtiene la impresión de que lo que más preocupa a la alianza en estos tiempos no es un «ataque armado», sino un ciberataque contra su red de servidores, o contra las infraestructuras de red de cualquiera de sus países miembros.

«En la era de la información en que vivimos, la Alianza del Atlántico Norte se enfrenta al dilema de cómo mantener la cohesión en un entorno en el que compartir información con los aliados acrecienta los riesgos de seguridad de la misma», señala la investigación sobre Seguridad Nacional y de la Información, «pero donde ocultarla merma la relevancia y las potencialidades de la Alianza».

Y WikiLeaks y Anonymous figuran en los primeros puestos de la lista de amenazas visibles para los desvelos de la OTAN por controlar el perímetro de su información.

«El tiempo que cuesta atravesar el Atlántico se ha reducido a 30 milisegundos, y ya no son los treinta minutos de los misiles balísticos intercontinentales, ni las semanas que cuesta cruzarlo en barco», advierte el informe. «Mientras tanto, aparece en escena toda una nueva familia de actores, como los grupos de «hacktivistas» virtuales. Ellos podrían desencadenar una nueva categoría de conflicto internacional entre sus grupos y los Estados-nación, o incluso entre entidades netamente virtuales.»

La ironía del 11-S

El estudio, firmado por Michael Jopling como relator para la OTAN, empieza con una ironía. Tras los ataques del 11 de septiembre de 2011 contra Nueva York y Washington D.C., el gobierno estadounidense concluyó que uno de los motivos por los que el complot había triunfado era que las agencias de inteligencia estadounidenses, sobre todo el Departamento de Defensa, la CIA, el Departamento de Estado y el FBI, no compartían la información disponible sobre quienes lo perpetraron.

Y así fue como Estados Unidos inauguró sus prácticas de compartir información. Jopling parece sugerir que la nueva práctica ha empeorado la situación. «Daba lugar a que un número de personas exponencialmente mayor obtuviera acceso a información secreta.» Hoy día, más de 850.000 funcionarios gozan de algún tipo de reconocimiento de seguridad para acceder a algún «máximo secreto», afirma. Muchos tienen acceso al protocolo secreto de redes de enrutado de Internet (SPIRNet, Secret Internet Protocol Router Network) del Departamento de Defensa, el sistema a través del cual se envían los telegramas de las embajadas.

El estudio cita a críticos del SIPRNet que afirman que carece de la posibilidad de detectar accesos no autorizados. «Por tanto, los responsables del diseño de la red confiaron en que quienes tenían acceso a datos sensibles lo protegerían de posibles infracciones. Esos usuarios jamás fueron examinados por ningún organismo federal responsable del sistema de información compartido.

Jopling no culpa del fenómeno de WikiLeaks explícitamente a esta política de apertura, pero su narración desemboca directamente en el soldado Bradley Manning, acusado de suministrar a la organización documentos que dieron lugar a la célebre publicación por parte de este colectivo de un aluvión incesante de telegramas del Departamento de Estado.

Como no podía ser de otra manera, piensa que es malo:

El relator cree que, aun cuando se esté a favor de la transparencia, las operaciones militares y de inteligencia sencillamente no se pueden planificar y consultar con la opinión pública. No hay transparencia sin control. El gobierno y, sobre todo, sus agencias de seguridad deben tener derecho a restringir el acceso a la información con el fin de gobernar y proteger. La idea se basa en la premisa de que los Estados y las empresas tienen derecho a la intimidad en igual medida que los individuos, y en que el secreto es necesario para una gestión eficiente de las instituciones y organismos del Estado.

«Hacktividad»

Un buen pedazo de la evaluación está dedicado a las actividades de Anonymous, sobre todo por los ataques de denegación de servicio contra PayPal, MasterCard, Visa y Amazon.com por bloquear la prestación de servicios económicos y de servidores a WikiLeaks. Luego viene el ataque contra Anonymous en HBGary Federal, que había planeado varios mecanismos para derribar a WikiLeaks y dejar al descubierto a Anonymous. No salió así, claro está. Más bien, Anonymous penetró en la empresa de seguridad, borró datos, hizo públicos correos electrónicos y dejó maltrecho su portal web.

En todo caso, el autor parece sentirse seguro de que los días del afamado grupo están contados. «Todavía está por ver de cuánto tiempo dispone Anonymous para seguir por ese camino», escribe Jopling. «Cuanto más se prolonguen los ataques, más probable es que se desarrollen e implanten contramedidas, o que se infiltren agentes en los grupos y que se persiga a los culpables.»

Pero la pregunta más general que recorre el documento es qué debería hacer la OTAN si uno de sus más de dos docenas de países miembros es objeto de un ciberataque. Estados

Unidos también ha estado sopesando esta disyuntiva recientemente.

«Determinados actos hostiles perpetrados a través del ciberespacio podrían obligarnos a emprender acciones inscritas en los compromisos suscritos con nuestros socios militares del tratado», afirma un informe estratégico de la Casa Blanca publicado a mediados de mayo. «Cuando tenga certeza de que se han producido, Estados Unidos responderá a los actos hostiles en el ciberespacio como haríamos con cualquier otra amenaza para nuestro país.»

Este borrador de la OTAN parece querer adoptar una orientación similar; sobre todo si se emprende contra un país miembro algo de la envergadura del ataque con software malintencionado de Stuxnet [realizado por el régimen de Israel, con ayuda de EE.UU. y Alemania, contra una central nuclear civil iraní]. los investigadores creen que el blanco original de ese software , concebido para penetrar en el los sistemas informáticos de los equipos industriales, era el programa nuclear de Irán.

«Hay quien sostiene que no se debería aplicar el Artículo 5 en el caso de ciberataques porque su efecto hasta el momento se ha visto circunscrito a producir incomodidad en lugar de a causar la pérdida de vidas humanas, y también porque es difícil identificar al atacante», señala Jopling. «Sin embargo, el relator cree que no se debería descartar la aplicación del Artículo 5, dado que los nuevos desarrollos de armas cibernéticas como Stuxnet podrían en última instancia causar daños comparables a los de un ataque militar convencional.»

Ars technica. Traducido para Rebelión por Ricardo García Pérez

---

https://www.lahaine.org/mundo.php/la-otan-se-infiltrara-en-anonymous-y-la