La ONDA digital
Revista de análisis y reflexión
Montevideo Uruguay - 2012

El ejército brasileño prepara un sistema de prevención contra ataques cibernéticos

Por Camilla Costa*

El ejército brasileño anunció la compra de nuevo software para seguridad y prevención contra ataques cibernéticos.

Las medidas forman parte de una planificación más amplia del gobierno brasileño para crear un sistema de defensa y contra-ataque de posibles amenazas a páginas y redes institucionales y de protección a datos sensibles.

Noticias relacionadas: Israel sufre un nuevo ataque de hackers en una escalada de guerra cibernética. Hacker exige rescate para 'liberar' el e-mail de un periodista y dice: 'es mejor que robar'. Un libro describe la propagación de la delincuencia cibernética y revela el perfil de los hackers. Tópicos relacionados: Brasil, Ciencia y Tecnología, Internacional "Hoy tenemos un mínimo de preparación para los escenarios de ataque. Tenemos una grande red, la EBnet, que reúne a los cuarteles en todo el país, y está bien blindada, pero existen puntos de vulnerabilidad", dijo a la BBC Brasil el general Antonino Santos Guerra, director del Centro de Comunicaciones y Guerra Electrónica del Ejército (Ccomgex).

En enero, las Fuerzas Armadas concluyeron dos licitaciones para la compra de un antivirus y de un programa que simula ataques cibernéticos, por un valor total de cerca de R$ 6 millones. Los dos programas serán desarrollados por empresas brasileñas.

El viernes pasado, el grupo de hackers Anonymous Brasil atacó el sitio del Banco Central y las páginas de los bancos BMG, Citibank y Panamericano, que quedaron temporalmente inestables.

El grupo también asumió la autoría de ataques a los sitios de los bancos Itaú, Bradesco, Banco do Brasil y HSBC, que se sucedieron durante la semana.

También el viernes pasado, el FBI anunció que está investigando cómo activistas ligados al grupo Anonymous consiguieron interceptar una conferencia telefónica entre agentes americanos y la británica Scotland Yard, en la que se discutían acciones legales contra los hackers.

Asimismo, se lograron registrar otros ataques en sitios institucionales americanos y griegos.

Defensa cibernética:"Los ataques que registramos hasta ahora son parecidos a los que se dan en cualquier empresa. Intentos de robos de contraseñas, negaciones de servicio, etc. Pero el modo como se obtiene una contraseña de banco es el mismo que se puede usar para obtener datos confidenciales del ejército. Y ya tuvimos sitios web del gobierno derribados", afirma Guerra.

Según el general, el simulador de guerra cibernética entrenará a los oficiales en por lo menos 25 escenarios de diversos tipos de ataque contra redes similares a las del ejército.

La Ccomgex, que coordina la compra del antivirus y del simulador de ataques cibernéticos, forma parte del Centro de Defensa Cibernética del Ejército (CDCiber), creado en 2010 para concentrar la administración de todas las acciones de protección virtual de la organización.

El programa adquirido por R$ 5,1 millones será desarrollado por la empresa carioca Decatron y actualizado de acuerdo con las necesidades de la organización, lo que deberá facilitar el mantenimiento del sistema de seguridad, de acuerdo con el general.

El antivirus, por un valor de R$ 800 mil, también está en fase de desarrollo y deberá ser entregado por la empresa BluePex, de Campinas (SP), dentro de 12 meses. "El desarrollo de software en Brasil es muy competitivo, está avanzando. Para garantizar la participación de empresas nacionales, tenemos que hacer las cosas en una escalada."

General Antonino Guerra, del Ccomgex
El director del Ccomgex dice que la preferencia por empresas nacionales para el programa de protección del ejército debe estimular la competencia y el avance de las empresas de tecnología y sistemas de seguridad en Brasil.

Por esto, las empresas que ganaron las licitaciones tendrán plazos mayores para realizar cambios personalizados en los programas, de acuerdo con las necesidades de las Fuerzas Armadas.

El presupuesto previsto para el CDCiber en 2012 es de R$ 83 millones, que deben ser destinados a por lo menos otras cuatro

adquisiciones que incluyen equipamientos, software y el entrenamiento de por lo menos 500 oficiales.

"Tenemos cursos externos para militares de las tres Fuerzas y también en el mercado universitario, para post grados. En el futuro, queremos contratar personas que conozcan el área para trabajar aquí, o que puedan dar consultoría", dijo Guerra. Robos electrónicos: El especialista en seguridad cibernética Mikko Hypponen, de la empresa finlandesa F-Secure, dijo que Brasil se distingue de otros países por la frecuencia de ataques cibernéticos relacionados al robo de dinero.

Sin embargo, el país ya comienza a registrar ataques a sitios de instituciones gubernamentales y empresas privadas de grupos de activistas, como el Anonymous y el LulzSec, que tienen "divisiones" nacionales.

"En la mayoría de los países, los ataques son realizados por personas de afuera. Brasil es diferente porque buena parte de los ataques tiene como destino los bancos y la mayoría de ellos es llevada a cabo por personas del propio país", dijo Hypponnen a la BBC Brasil.

Según el especialista, Brasil está considerado el número uno en crear "caballos de Troya", una especie de programas maliciosos, para atacar bancos.

"Estos programas no intentan quebrar los sistemas de seguridad de los bancos, que son, en general, muy buenos en Brasil. Pero infectan las computadoras personales de los clientes, para poder entrar en sus cuentas cuando estos acceden a los bancos online", explica.

Para el general Antonino Guerra, Brasil todavía no debe preocuparse por los ataques realizados por otros países ni con el espionaje de sus ciudadanos. "Somos un país pacífico, no es este el tipo de problema que tenemos aquí", dice.

Sin embargo, Hypponnen cree que el gobierno brasileño deberá preocuparse también con la seguridad de las empresas privadas, en caso de que quiera prevenir posibles crisis.

"Buena parte de la infraestructura crítica de Brasil no está generada por el gobierno sino por compañías privadas, como la telefonía y las usinas nucleares. Para garantizar que el país consiga operar durante una crisis, es preciso garantizar que esta infraestructura continuará funcionando. El gobierno tiene que tener un papel más activo en ayudar a las empresas a proteger sus redes", afirma.

En un comunicado enviado a la BBC Brasil, el Gabinete de Seguridad Institucional de la Presidencia (GSI) dijo que "los ataques más preocupantes son aquellos que apuntan al acceso indebido a informaciones secretas de la Administración Pública Federal" y afirmó que la preparación del órgano contra posibles ataques ha sido la "adecuada".

De acuerdo con el Centro de Estudios, Respuesta y Tratamiento de Incidentes de Seguridad (CERT), que reúne notificaciones de ataques electrónicos en todo el país, Brasil registró casi 400 mil ataques a computadoras en 2011.

Cerca de la mitad de los fraudes registrados, según el CERT, fueron páginas falsas, generalmente de bancos, creadas para robar dinero de los usuarios. La otra mitad de las notificaciones corresponde casi en su totalidad a los caballos de Troya, que permiten el acceso a cuentas bancarias cuando son accesibles a través de internet.

El centro, que recibe datos de empresas, universidades, proveedores de Internet y Grupos de Seguridad y Respuesta a Incidentes (CSIRT), dice que los lunes son los días con más incidentes reportados y que más del 80% de los ataques tienen origen en Brasil.

De acuerdo a datos de la Federación Brasileña de los Bancos (Febraban), los fraudes bancarios realizados por internet y computadoras de clientes, le costaron R$ 685 millones a los bancos sólo en el primer semestre de 2011, 36% más que en el mismo período en 2010.

Traducido para ***LA ONDA digital*** *por* ***Cristina Iriarte***

La ONDA digital
Revista de análisis y reflexión
Montevideo Uruguay - 2012