ieee.es
Instituto Español de Estudios Estratégicos

Documento
Informativo

16/2012 28 marzo de 2012

Mª José Caro Bejarano

CIBERDEFENSA. EQUIPOS DE RESPUESTA INMEDIATA DE LA OTAN

Visitar la WEB

Recibir BOLETÍN ELECTRÓNICO

CIBERDEFENSA. EQUIPOS DE RESPUESTA INMEDIATA DE LA OTAN

Resumen:

Continuando con el calendario marcado por el Nuevo Concepto Estratégico de la OTAN, en Lisboa en 2010, la Alianza, tras revisar y aprobar el nuevo concepto de ciberdefensa en marzo y la política de ciberdefensa en junio de 2011, continúa con su plan de acción. En este documento se analiza los avances realizados en la definición y puesta en marcha de los llamados RTT o Equipos de Respuesta Inmediata.

Abstract:

Following the schedule set by the new Strategic Concept of NATO in Lisbon in 2010, the Alliance, after reviewing and approving the new concept of cyber defense in March and the cyber defense policy in June 2011, continues its plan of action. This paper reviews the progress made in the definition and implementation of so-called RTT or Rapid Reaction Response Teams.

Palabras clave:

OTAN, ciberdefensa, ciberataques, Equipos de Respuesta Inmediata.

Keywords:

NATO, cyber defence, cyber attacks, Rapid Reaction Team.

LA OTAN ESTÁ FINALIZANDO EL NUEVO PLAN DE CIBERDEFENSA

Siguiendo lo marcado por el Nuevo Concepto Estratégico de la OTAN de noviembre de 2010, los ministros de Defensa de la OTAN aprobaron el *Nuevo Concepto de Ciberdefensa* de la Alianza[1] en marzo de 2011 y en junio del mismo año aprobaron una *revisión de la Política de Ciberdefensa y un Plan de Acción de Ciberdefensa*[2]. Como objetivos, la OTAN implementará un enfoque coordinado de ciberdefensa para abarcar aspectos de planificación y desarrollo de capacidades junto con mecanismos de respuesta en caso de ciberataque. Para ello la Alianza incorporará e integrará las medidas de ciberdefensa en las misiones. El Plan de Acción detallado habrá de estar listo para finales de abril y permitirá el despliegue de nuevos niveles de ciberdefensa para principios de 2013, según fuentes de la Alianza. Este plan es la primera fase de un nuevo contrato quinquenal para proteger de un ataque a las instalaciones civiles y militares de la OTAN.

CAPACIDADES DE CIBERDEFENSA

Según la Alianza, la ciberguerra es una guerra sin ruido, tanques o aviones. Actualmente es un delito rentable, relativamente libre de riesgos y anónimo. Resulta difícil identificar el origen o autores del ataque, y este es el principal problema. Para ser más efectivos todas las partes involucradas deben trabajar juntas: la OTAN, el sector privado, las organizaciones internacionales y la academia. Hacia finales de 2012, la capacidad de los equipos de respuesta inmediata (RRT) de expertos en ciberdefensa de la OTAN estará operativa.

El NCIRC[3] (capacidad de respuesta ante incidentes informáticos de la OTAN) es el centro neurálgico de la lucha de la Alianza contra el ciberdelito. El NCIRC es responsable de la ciberdefensa en todas las instalaciones OTAN, sean cuarteles generales estáticos o desplegados para operaciones o ejercicios.

Para dotarse de medios técnicos la OTAN ha firmado contratos de ciberdefensa. La Agencia de Consulta, Mando y Control-NC3A[4] ha adjudicado contratos para actualizar las capacidades de ciberdefensa con empresas privadas que permitirán que el NCIRC alcance la capacidad operativa completa para finales de 2012.

---

[1] Documento Informativo del IEEE 09/2011, Nuevo Concepto de Ciberdefensa de la OTAN, (marzo de 2011).
[2] Documento Informativo del IEEE 37-2011, La Política de Ciberdefensa de la OTAN, (octubre de 2011).
[3] NATO Computer Incidents Response Capability Technical Centre – NCIRC. Este centro consta de un centro de apoyo y coordinación de ciberdefensa y de un centro técnico que serían como el NATO CERT.
[4] Las Autoridades Militares - NMA y la NATO's Consultation, Control and Command Agency - NC3A tienen la responsabilidad de identificar los requisitos operacionales y la adquisición e implementación de las capacidades de ciberdefensa.

"El proyecto es el resultado directo del compromiso de las naciones OTAN de detectar, defender y recuperar en caso de un ciberataque contra sistemas críticos de la Alianza. Esta adjudicación es un paso importante hacia la entrega de estas capacidades para el fin de 2012", según palabras de Gabor Iklody, Subsecretario General, jefe del órgano rector de ciberdefensa del cuartel general de la OTAN.

La adjudicación del contrato, de aproximadamente 58 millones de euros, representa la mayor inversión hasta ahora en materia de ciberdefensa. La empresa elegida ha sido Northrop Grumman and Finmeccanica. El contrato incluye el despliegue de las capacidades de ciberdefensa durante el próximo año, junto con el mantenimiento y actualizaciones por el resto de su vida útil.

En el caso de un ataque contra un sistema de información OTAN, los expertos afectados se reúnen inmediatamente y preparar un plan de acción. El objetivo es restablecer los sistemas de modo que todo vuelva a su funcionamiento normal tan pronto como sea posible.

El NCIRC se ocupa de desarrollar guías de seguridad y aconsejar sobre la protección de los ordenadores y las redes de información de la OTAN y reducir sus vulnerabilidades. Se analizan los dispositivos digitales y el tráfico de red relacionado con el incidente. Es decir, determinar tan pronto como sea posible si el incidente ocurrió realmente y su impacto, encontrar formas de limitar el daño y, si es apropiado, identificar la fuente del compromiso.

ATAQUES MÁS SOFISTICADOS Y MÁS FRECUENTES

Cada vez suceden más ciberataques en el mundo y se vuelven más sofisticados. Las sociedades interconectadas dependen de las nuevas tecnologías y esto las hace más vulnerables a los ataques. Se han extendido el espionaje, la destrucción, los delitos, y el robo de secretos militares e industriales. Los ataques orientados a una organización o un país están motivados, desarrollados y ejecutados por expertos organizados. No tienen punto de comparación con los hackers originales que consideraban los ataques como un pasatiempo.

La experiencia del virus Stuxnet que, según se informó, impactó significativamente en el programa nuclear iraní en 2010, marcó la transición del mundo cibernético al mundo físico. El suministro de agua, electricidad, hospitalario, así como la seguridad aérea, la defensa y los servicios bancarios, descansan sobre redes de información. Tantas instalaciones sensibles cuyo ataque puede causar un daño a una organización o a un país entero. El número de ciberataques crece cada día, sean contra sistemas OTAN o contra sistemas vitales de las naciones miembro. La OTAN debe ser capaz de ofrecer asistencia de ciberdefensa a sus

miembros para ayudarlas a protegerse contra estos ataques, a detectarlos, y una vez que han sucedido, a reaccionar con rapidez para limitar el daño.

EQUIPO DE RESPUESTA INMEDIATA DE LA OTAN CONTRA LOS CIBERATAQUES

En 2011 la OTAN comenzó a formular el concepto de RRT para este propósito: "los expertos en ciberdefensa son responsables de asistir a los estados miembros que solicitan ayuda en el caso de un ataque de relevancia nacional". La creación de este equipo es resultado de la política de ciberdefensa de la OTAN, revisada por los ministros de defensa en mayo de 2011. En el futuro se dedicarán esfuerzos adicionales a la prevención de riesgos y mejorar la resiliencia.

Los tipos de ciberataques sufridos por Estonia y Georgia serán los ciberataques más frecuentes en el futuro. Una mezcla de protesta, o guerra tradicional junto con un elemento cibernético. Estos equipos, por tanto, deben estar preparados para actuar cuando se solicite la asistencia. Hasta ahora se han llevado a cabo una serie de pasos y el NCIRC alcanzará la capacidad operacional completa a comienzos de 2013. Todos los requisitos técnicos se han identificado y se ha lanzado una petición de ofertas. Se han desarrollado los acuerdos de cooperación, incluyendo expertos de mutua confianza procedentes de las naciones, de la industria, academia y de la OTAN. Estos acuerdos, finalmente, abrirán el acceso a conocimiento especializado en todas las áreas de ciberseguridad. Se están preparando perfiles de expertos necesarios para misiones de asistencia según las áreas de competencia.

Todos los procedimientos RRT y las acciones posibles están definidos en un manual que deberá terminarse para verano de 2012. Este manual establece las guías de la respuesta OTAN a sus aliados y socios que soliciten asistencia en la protección de sus sistemas de información y comunicación. Se ha establecido un grupo de trabajo ad hoc para trabajar sobre este manual que aglutina a expertos de países aliados incluyendo expertos de planificación en emergencias civiles. Con los RRT, la OTAN podrá ofrecer, bajo petición, asistencia profesional y bien organizada a sus miembros y socios, pero principalmente a aquellos países que aún no tienen los recursos para establecer capacidades de ciberdefensa de este tipo. Es una versión del principio militar de mutua asistencia y defensa colectiva.

Perfiles, formación y equipamiento del equipo operativo de respuesta inmediata

La capacidad RRT consistirá en un núcleo permanente de seis expertos especializados que pueden coordinar y ejecutar misiones RRT. Habrá también expertos nacionales o de OTAN en áreas específicas. El número y el perfile vendrán determinados por la misión a cumplir.

Los RRT tendrán todo el equipo que necesiten: equipo IT y de telecomunicación, como teléfonos satélite, y equipo de recogida de prueba, criptografía, análisis forense, gestión de vulnerabilidades, seguridad en red, etc.

Todos estos expertos se formarán según los procedimientos OTAN y en el manejo del equipo. También participarán en el Ciberejercicio que se celebra en noviembre cada año.

Activación del equipo de respuesta inmediata

Cualquier nación miembro de la OTAN que sufra un ciberataque significativo podrá solicitar ayuda de la OTAN. La petición será considerada por el CDMB comité de gestión de ciberdefensas. Las solicitudes de ayuda que provengan de países no miembros tendrán que ser aprobadas por el Consejo de la Alianza.

Durante el Ciberejercicio 2010, se practicó el mecanismo de consulta y toma de decisiones por el RRT al nivel del CDMB. Se aprendieron lecciones de mejora de los procedimientos. En noviembre de 2012, se abordará la segunda fase: prueba de la fase de intervención del RRT y específicamente, la utilidad del manual que se está preparando.

Una vez activado, los RRTs responderán dentro de las 24 horas del incidente.

Se invitará a la industria por primera vez como observadores a este Ciberejercicio 2012 y "probablemente sean participantes en ediciones futuras" según fuentes de la OTAN, para ello el NIAG (el grupo asesor de industria de la OTAN)[5] habrá estructurado en julio la cooperación entre la Alianza y la Industria en estos temas de ciberdefensa.

Mª José Caro Bejarano
Analista del IEEE

[5] NIAG – NATO Industry Advisory Group.