Retos de la "conciencia situacional" en la Ciberdefensa

Aunque está claro que para lograr el control adecuado sobre nuestras infraestructuras TIC es necesario que funcionen nuestros sistemas de conciencia situacional, en muchas ocasiones nos olvidamos de los retos que supone la introducción de nuevas formas de trabajar y nos centramos demasiado en las tecnologías que vamos a adquirir, olvidando prestar una atención adecuada a los procesos que deben ser creados, modificados y adaptados en la empresa y en los cambios organizativos necesarios, que incluyen, en muchas ocasiones, una mejor utilización de los recursos humanos, para integrar esos nuevos sistemas con los existentes en la organización. Se presentan aquí algunos de esos retos junto con recomendaciones de cómo se pueden minimizar los riesgos asociados.

José Ramón Coz Fernández / Vicente José Pastor Pérez

En la edición previa de SIC (febrero de 2013), ya tratamos el concepto de conciencia situacional (*Situational Awareness*) de un modo amplio y su aplicación al ciberespacio, y como ésta tiene un impacto en la mejora general de nuestras capacidades de Ciberdefensa. A modo de resumen mencionaremos que se trata de una dimensión más de la Ciberdefensa, complementaria con otras como las ciberoperaciones, la ciberformación, la gestión de ciberincidentes, la ciberinnovación o la ciberinteligencia. Esta dimensión nos permite conocer el estado en el que se encuentra nuestra organización en términos de seguridad de la información y proyectar su estado futuro.

La conciencia situacional es clave para todas las capas de decisión en el campo de la Ciberdefensa, desde los analistas de seguridad hasta los que han de tomar decisiones de carácter global, incluso en ámbitos fuera del propio ciberespacio. En el caso de la Ciberdefensa, los decisores finales pueden estar relacionados con misiones y objetivos que reciben soporte de los sistemas a los que se refiere el conocimiento de la situación de las amenazas, vulnerabilidades, debilidades y ataques que afecten al nivel de ciberseguridad y al éxito de las misiones. En el caso de organizaciones o empresas, la conciencia situacional se puede constituir también en un elemento clave para todas las capas de decisión, incluso las relacionadas con las estrategias organizativas y los objetivos de negocio.

En adelante se exponen los principales avances de los sistemas de conciencia situacional para Ciberdefensa y se esbozan los retos esenciales a los que se enfrentan las organizaciones en este campo.

Avances de la Conciencia Situacional en la Ciberdefensa

En el caso de algunas organizaciones en el campo de la Ciberdefensa se hace uso del concepto "*sensemaking*", que es el proceso por el cual un analista de seguridad puede, desde la conciencia situacional, dar sentido a la información que percibe sobre los ciberincidentes, y desde ese nivel hacer fluir la información hasta las capas de toma de decisión, en el caso necesario y con el nivel de detalle adecuado. Para conseguir este propósito, las entidades más avanzadas hacen uso de modelos que permiten relacionar todas las capas de información de la conciencia situacional. Las decisiones y acciones que se llevan a cabo en el ámbito de la Ciberdefensa, que son medidas *a posteriori*, varían en función del estado, que es analizado a través de diferentes niveles (percepción, compresión y proyección), tal y como se puede observar en la **Figura 1**. En función de las habilidades, la formación y la experiencia

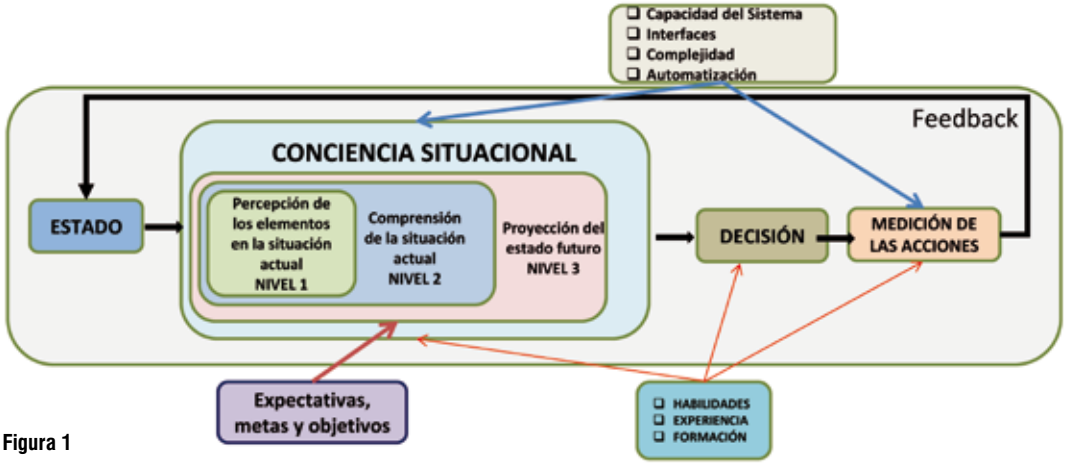

Figura 1

Es necesario tener personal cualificado y motivado que exprima los beneficios de los nuevos desarrollos tecnológicos. Los procesos son ese "pegamento" que consigue que se trabaje de forma coordinada. Cuando vamos añadiendo sistemas es necesario crear nuevos procesos y adaptar los existentes a la nueva situación.

de los roles que participan en el flujo de decisión, estos alimentan un bucle que es soportado por un sistema con diversidad de interfaces y con un cierto grado de automatización y complejidad. La principal entrada del modelo son las expectativas, metas y objetivos de las misiones encomendadas.

Puede citarse el caso de la **Secretaría de Defensa de Estados Unidos**, que utiliza una visión holística de la conciencia situacional, como una capacidad de monitorización continua, que unifica las capacidades existentes dispares de la gestión operativa y del control para construir una solución robusta, automatizada e integrada que puede dar soporte a los procesos de decisión de todos los aspectos de las futuras operaciones TIC, tal como se puede apreciar en la figura. Esta visión incluye los habituales procesos de gestión de servicios TI y los servicios de gestión de seguridad de la información, junto con las capacidades de protección; todo ello, orientado a un proceso de gestión del conocimiento de los activos de información.

Figura 2

Los retos de la Conciencia Situacional en la Ciberdefensa

Por desgracia, aún queda un gran camino que recorrer en el área de la conciencia situacional. Por ejemplo, la mayor parte de las herramientas que proporcionan la información de base no son interoperables entre sí. Además, muchos fabricantes de este tipo de sistemas no proporcionan una vía fácil para integrar los productos y ven como una desventaja abrir los datos de sus sistemas a la explotación por terceros.

Queda un gran camino que recorrer en el área de la conciencia situacional. Por ejemplo, la mayor parte de las herramientas que proporcionan la información de base no son interoperables entre sí. Además, muchos fabricantes no proporcionan una vía fácil para integrar los productos y ven como una desventaja abrir los datos de sus sistemas a la explotación por terceros.

Aunque hay muchos esfuerzos por estandarizar, los fabricantes no implementan estos estándares tanto como sería deseable. Uno de los mayores esfuerzos para estandarizar los datos y protocolos relacionados con la Ciberdefensa lo soporta la **Corporación Mitre**, una organización sin ánimo de lucro que da soporte a diversos departamentos de la Administración Central de EE.UU., pero, principalmente, al Departamento de Defensa (DoD). Mitre divulga en un portal web público todos los esfuerzos realizados por diversos organismos y por la comunidad, en su sentido más amplio, para producir estos estándares con un gran hincapié en las métricas de seguridad. Así, el portal "*Making Security Measurable*" aglutina esfuerzos en los que se estandarizan las representaciones del conocimiento, enumeraciones, formatos y lenguajes de intercambio de información. Mitre ha dividido este esfuerzo en cuatro grandes bloques: Registros, Formatos/Lenguajes, Utilización Estandarizada y Procesos Estandarizados.

También hay que destacar al **Instituto Nacional de Estándares y Tecnología** (**NIST**), en la actualidad una Agencia del Departamento de Comercio de EE.UU, y cuya misión principal, a pesar de no ser un organismo regulatorio, son los avances en las ciencias de medición, la estandarización y la tecnología. Cualquier profesional del ramo conoce sus Publicaciones Especiales y, principalmente, la serie 800, que el Instituto lleva publicando desde el año 1990. Recientemente se ha anunciado el desarrollo de un nuevo marco de trabajo para la ciberseguridad a raíz del llamamiento realizado por el Presidente Obama.

La mayoría de las soluciones para la Ciberdefensa que se pueden encontrar en la actualidad están orientadas a la visualización de datos de muy bajo nivel para aumentar la conciencia situacional, como pueden ser los flujos de tráfico de red, los sistemas de prevención de intrusos, los dispositivos de protección perimetral, los sistemas de gestión de ciberidentidades, los sistemas forenses, los detectores de vulnerabilidades o los analizadores de *logs*. Esto hace que los analistas de seguridad tengan que realizar sus análisis de alto nivel manualmente para hacer fluir esa información a lo largo de la cadena, lo cual lleva un considerable esfuerzo, tiempo y, además, es una actividad propensa a errores. Sin embargo, no son muchas las soluciones que realizan una mayor integración de datos e incluyen las vulnerabilidades y debilidades de los sistemas y

sus niveles de riesgo para ayudar, o incluso automatizar, la gestión de esos riesgos de forma dinámica.

Todavía en menor medida nos encontramos con sistemas específicamente diseñados para tener en cuenta la relación entre todos esos datos, que provienen de redes complejas y de gran tamaño, y las misiones de defensa planificadas de alto nivel, y las amenazas a los objetivos de las mismas. Por ello se hace necesario contar con sistemas avanzados de visualización que permitan reducir el tiempo de análisis sin producir una falta de datos, al haberlos resumido en exceso, y acorten el tiempo necesario para la toma de decisiones. La abstracción en cada nivel, explicada en el artículo de la edición previa de SIC, hace que sólo los datos necesarios sean mostrados en cada momento, pero sin eliminar la posibilidad de analizar en profundidad (*"drill-down"*) esos datos mostrando un mayor nivel de detalle, hasta llegar al origen de los mismos.

Como citamos en la sección anterior, es menester contar con una monitorización continua de los sistemas para alcanzar el nivel requerido de conciencia situacional. Para ello necesitamos esos estándares de medición, independientes del vendedor (*"vendor-agnostic"*) y sensores estratégicamente distribuidos en nuestra infraestructura federada, que integre la información de los mismos. La monitorización continua es un término que procede del lenguaje financiero donde se utiliza para detectar problemas de cumplimiento y riesgos en procesos de auditoría continua y, como ya hemos mencionado, es una de las estrategias seguidas por la Secretaría de Defensa de EE.UU. Esta infraestructura forma la base para cuadros de mando unificados que permiten que los datos de seguridad sean visibles, medibles y accionables consiguiendo que los líderes con poder de decisión puedan entender, priorizar, gestionar y defender sus redes de los riesgos que las acechan casi en tiempo real.

Otro factor de mejora es el mayor entendimiento "entre las partes". Abogamos por la unión de los Centros de Operaciones de Red con los Centros de Operaciones de Seguridad, pero en muchas ocasiones se nos olvida la coordinación de dichas operaciones. Otro de los retos es el relacionado con el coste de estos sistemas. Para tener una información completa y en tiempo real del estado de nuestras redes y sistemas es necesario disponer de sensores en múltiples localizaciones que recojan lo que sucede en ellas y centralicen esos datos para su análisis posterior. Ese análisis puede realizarse en tiempo real, contribuyendo así a las fases de detección de intrusiones u otros problemas de seguridad en nuestras redes, o *post-mortem*, una vez que las intrusiones ya han sucedido y para determinar el alcance de las mismas, las medidas de seguridad que fallaron o para relacionar casos actuales con otros sucedidos anteriormente que pudieran haber sido detectados, o no, en su momento. Esto supone un acceso rápido a grandes volúmenes de datos, lo cual es un reto al que las nuevas propuestas de *big data* están intentando dar una solución.

Es menester contar con una monitorización continua de los sistemas para alcanzar el nivel requerido de conciencia situacional. Para ello necesitamos esos estándares de medición, independientes del vendedor; así como sensores estratégicamente distribuidos en nuestra infraestructura federada, que integre la información de los mismos.

También mencionaremos que el coste de estos sistemas no es, en absoluto, un factor a dejar de tener en cuenta, y eso sin haber aún sumado a la ecuación que el desarrollo de soluciones "llave en mano" está aún empezando y no es fácil encontrar en el mercado productos que recojan todas o gran parte de las funcionalidades requeridas. Ello hace que, en la mayor parte de las ocasiones, sea necesario desarrollar sistemas "a medida" para dar respuesta a estas necesidades, junto con otros trabajos de ingeniería orientados, principalmente, a integrar al máximo los sistemas existentes entre sí.

Conclusiones

Como hemos analizado queda un largo camino que recorrer en este campo. En las organizaciones tenemos que hacer ese esfuerzo adicional que se requiere para tener una imagen completa de la situación y, para ello, todas las piezas de nuestra maquinaria deben funcionar al unísono y en perfecta armonía y coordinación. Hay que conseguir que esas piezas "hablen el mismo idioma". Una forma de conseguirlo es hacer que el grado de interoperabilidad sea uno de los factores que incline la balanza a la hora de adquirir uno u otro producto.

Además, es necesario tener personal cualificado y motivado que exprima los beneficios de los nuevos desarrollos tecnológicos. Los procesos son ese "pegamento" que consigue que se trabaje de forma coordinada. Cuando vamos añadiendo sistemas es necesario crear nuevos procesos y adaptar los existentes a la nueva situación. Tengamos también presente la integración con el resto de la gestión de servicios de tecnologías de la información y con el negocio que esta soporta y que queremos proteger. Ir cada uno por su lado no funciona.

Finalmente, en tiempos de crisis, en los que los presupuestos no son tan holgados como sería deseable, conviene saber que esto que queremos hacer no es precisamente barato. Por ello, hay que presentar los casos de negocio de la forma adecuada en torno a la gestión de riesgos que pueden impactar a la organización. Si se ven claramente los beneficios será más fácil obtener la aprobación. No esperemos obtener financiación para una aproximación big-bang. Es mejor repartir el esfuerzo en varias fases e ir consolidando los logros obtenidos en cada una de las anteriores. ■

José Ramón Coz Fernández
Auditor del proyecto de Ciberseguridad (NCIRC FOC). Bi-SC AIS Programme Management Integration Capability (PMIC).
NATO Communications and Information Agency (NCIA)
ISDEFE
JoseRamon.Coz@ncia.nato.int

Vicente José Pastor Pérez
Jefe de Datos y Aplicaciones Especializadas. Capacidad de Respuesta a Incidentes de Seguridad Informática de la OTAN (NCIRC)
OTAN
Vicente.pastor@ncirc.nato.int