CREACIÓN DE UN EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD INFORMÁTICA: UN PROCESO PARA EMPEZARLO

Mantener seguros los activos de información de la organización en un entorno informático interconectado hoy en día es un verdadero reto que se hace más difícil con cada nuevo servicio y con cada nueva herramienta de intrusión. La mayoría de las organizaciones se percatan que no existe una única solución o una panacea para asegurar sistemas y datos; en su lugar se necesita una estrategia de seguridad multi-capa. Una de las capas que actualmente muchas organizaciones están incluyendo en su estrategia es la creación de un Equipo de Respuesta a Incidentes de Seguridad Informática, generalmente llamado un CSIRT.

Entre los eventos motivadores que conducen al establecimiento de CSIRTs se incluye:

- Un aumento general en el número de incidentes de seguridad informática reportados
- Un aumento general en el número y tipo de organizaciones afectadas por incidentes de seguridad informática
- Una sensibilización más enfocada, por parte de las organizaciones, en la necesidad de contar con políticas y prácticas de seguridad como parte de su estrategia general de gestión de riesgo
- Nuevas leyes y reglamentos que impacten en la forma en que las organizaciones deben proteger sus activos de información
- Percatarse que los administradores de sistemas y de red no pueden por sí solos proteger los sistemas organizacionales y sus activos.

¿Cuáles son las preguntas?

A medida que las organizaciones comienzan a construir su capacidad de respuesta a incidentes, buscan

determinar la mejor estrategia para armar este tipo de estructura. Éstas no sólo quieren saber lo que ha funcionado bien para las demás, sino también contar con cierta orientación en el proceso y los requisitos que se deben de cumplir para establecer una capacidad eficaz de respuesta a incidentes.

Los CSIRTs y sus organizaciones padre tienen numerosas preguntas que quieren se les responda para ayudarles a diseñar su capacidad de respuesta. También están interesados en saber lo que están haciendo otros equipos similares en ese sector de la industria. Las preguntas típicas que se hacen son algunas de las siguientes:

¿Cuáles son los requisitos básicos para el establecimiento de un CSIRT?
¿Qué tipo de CSIRT se necesitará?
¿Qué tipo de servicios se debe ofrecer?
¿Qué tan grande debería ser el CSIRT?
¿Dónde debe estar ubicado el CSIRT dentro de la organización?
¿Cuánto va a costar para implementar y apoyar al equipo?
¿Cuáles son los pasos iniciales a dar para crear un CSIRT?

No hay un conjunto estándar de respuestas a estas preguntas. Los CSIRT son tan únicos como las organizaciones a las que sirven, y como tal, no es probable que dos equipos operen exactamente igual. Es importante para la organización decidir por qué instala un CSIRT y qué es lo que quiere que logre ese CSIRT. Una vez que esto esté determinado, entonces se podrá formular el conjunto único de respuestas a estas preguntas.

Este documento es el primero de una serie de artículos que tratarán temas y decisiones que deben abordarse en la planificación e implementación de un CSIRT. Este primer artículo se centrará en una visión general de los pasos básicos de alto nivel que se deben dar las organizaciones, que diseñarán y construirán un CSIRT. El artículo está escrito como una guía general para cualquier organización que esté pensando en llevar a cabo este propósito o para las personas que son miembros de un equipo de proyecto que está trabajando para establecer un CSIRT.

¿Cuáles son algunas de las mejores prácticas para crear un CSIRT?

Aunque los CSIRT diferirán en la forma en que operan en función de los recursos humanos disponibles, la experiencia, los recursos del presupuesto, y las circunstancias particulares de cada organización, hay algunas prácticas básicas que se aplican a todos los CSIRT. Discutiremos algunas de estas prácticas que se relacionan con la creación de un CSIRT. (Para más información sobre qué es un CSIRT, consulte FAQ CSIRT). Aunque estas acciones se presentan como pasos, el proceso no es secuencial; muchos pasos pueden realizarse en paralelo.

Los pasos son los siguientes:

Paso 1: Obtener aceptación y apoyo de la Alta Dirección
Paso 2: Determinar el plan estratégico del CSIRT
Paso 3: Recopilar información relevante
Paso 4: Diseñar la visión del CSIRT

Paso 5: Comunicar la visión y el plan operativo del CSIRT
Paso 6: Comenzar la implementación CSIRT
Paso 7: Anunciar que el CSIRT está operando
Paso 8: Evaluar la efectividad del CSIRT

Paso 1: Obtener apoyo y compromiso de la Alta Dirección

Nuestra experiencia muestra que sin la aprobación y apoyo de la Alta Dirección, crear una capacidad de respuesta a incidentes efectiva puede ser extremadamente difícil y problemático. Este apoyo se debe demostrar de muchas maneras, incluyendo la provisión de recursos, la financiación y el tiempo a la persona o grupo de personas que actuarán como el equipo del proyecto para implementar el CSIRT. Esto incluye a ejecutivos y gerentes de área o departamento y el tiempo que su personal dedica a participar en este proceso de planificación; su aporte es esencial durante el esfuerzo de diseño.

Es importante obtener las expectativas y percepciones de la Gerencia sobre las funciones y responsabilidades del CSIRT. Sin esta información, podría armarse un equipo, cuyos servicios y autoridad no sean comprendidos o usados apropiadamente por el resto de la organización.

Junto con obtener el apoyo para el proceso de planificación y ejecución de parte de la Gerencia, es igualmente importante obtener su compromiso de mantener las operaciones y la autoridad del CSIRT para el largo plazo. Una vez establecido el equipo, cómo se le mantiene y expande con los recursos de presupuesto, personal y equipo? ¿La función y la autoridad del CSIRT seguirán respaldados por la Gerencia ante los diversos grupos y la organización padre? Sin este apoyo contínuo, el éxito del CSIRT a largo plazo estará en peligro.

Paso 2: Determinar el Plan Estratégico de Desarrollo de CSIRT

Piense cómo administrar el desarrollo del CSIRT. ¿Qué temas administrativos deben tratarse, y qué temas de gestión de proyectos deben abordarse?

- ¿Existen plazos específicos que cumplir? ¿Son realistas, y si no, pueden ser cambiados?
- ¿Hay un equipo de proyectos? ¿De dónde provienen los miembros del equipo? Usted querrá asegurarse que todos los interesados estén representados. Algunos pueden no estar en el equipo durante todo el proyecto, pero pueden incorporarse para proporcionar su experiencia en el tema y prestar sus aportes según sea necesario. Usted también querrá incorporar en su plan, teoría del comportamiento organizacional y teoría de la comunicación. Si alguien tiene experiencia en estas áreas, considere la posibilidad de que participe en el equipo.
- ¿Cómo usted le hace saber a la organización sobre desarrollo del CSIRT? Una buena manera de empezar es con una nota enviada por el CIO, CEO, u otro ejecutivo de alto nivel anunciando el proyecto y pidiendo a cada grupo de interés y áreas clave que proporcionen apoyo en cualquier forma posible. Hacer que la organización sepa del proyecto de un CSIRT en las primeras etapas de desarrollo puede ayudar al personal a sentir que son parte del proceso de diseño.
- Si usted tiene un equipo de proyecto, ¿cómo registrará y comunicará la información que está recogiendo, más aún si el equipo está geográficamente disperso?

Paso 3: Recopilar información relevante

Recolecte información para determinar las necesidades de la organización en cuanto a respuesta a incidentes y servicios. Revise los tipos de actividades de incidentes que están siendo reportadas en su comunidad objetivo. Esto ayuda a determinar no sólo el tipo de servicios que esnecesario ofrecer, sino también los tipos de habilidades y conocimientos del personal del CSIRT. Por ejemplo, si su organización ha sido víctima de virus informáticos o actividad de gusanos, necesitará personal con experiencia en virus para manejar la respuesta. También necesitará procedimientos de detección de virus, eliminación y de recuperación, junto con las herramientas anti-virus apropiadas. Es posible que usted quiera contar con personal con buena formación y habilidades de documentación para ayudar a desarrollar programas de sensibilización de usuarios como un paso proactivo para hacer frente a la actividad viral.

Identifique qué información necesita para planificar e implementar el CSIRT. Determine quién tiene esa información y la mejor manera de obtenerla, ya sea a través de conversaciones generales, entrevistas o involucrando a esas personas en el proyecto.

Reúnase con los principales interesados para discutir no sólo sus necesidades de respuesta a incidentes, sino para lograr además un consenso inicial sobre expectativas, dirección estratégica, definiciones y responsabilidades del CSIRT. Su definición de qué es un CSIRT puede ser muy diferente de la definición de su gerente o de la definición de otras áreas de su organización. Utilice estas discusiones con los interesados para delinear e identificar la forma en que cada grupo necesita para interactuar con el CSIRT. Los interesados pueden ser, pero no se limitan a:

- **Gerentes de negocio**. Tienen que entender qué es el CSIRT y cómo puede ayudarlos a mantener sus procesos de negocio. Se deben de establecer acuerdos sobre la autoridad del CSIRT sobre sistemas de negocio y quién tomará las decisiones si los sistemas de negocio críticos deben de apagarse o desconectarse de la red.
- **Representantes de TI**. ¿Cómo interactúan el personal de TI y el CSIRT? ¿Qué acciones son tomadas por el personal de TI y qué acciones son tomadas por los miembros del CSIRT durante las operaciones de respuesta? ¿El CSIRT tiene fácil acceso a la red y a los logs de los sistemas para su análisis? ¿Podrá el CSIRT hacer recomendaciones para mejorar la seguridad de la infraestructura de la organización?
- **Representantes del departamento legal**. ¿Cuándo y cómo se involucra al departamento jurídico en los esfuerzos de respuesta a incidentes? Puede ser también necesario el equipo legal para revisar acuerdos de no divulgación, desarrollar la redacción adecuada para comunicarse con otros sitios y organizaciones, y para determinar la responsabilidad del sitio en incidentes de seguridad informática.
- **Representantes de Recursos Humanos**. Pueden ayudar a desarrollar descripciones perfiles para contratar al personal del CSIRT y desarrollar políticas y procedimientos para remover al personal interno involucrado en actividad informática no autorizada o ilegal.
- **Representantes de Relaciones Públicas**. Deben estar preparados para manejar cualquier consulta de los medios de comunicación y ayudar a desarrollar políticas y prácticas de revelación de información.
- **Grupos de seguridad ya existentes, incluídos los de seguridad física**. El CSIRT necesitará

intercambiar información con estos grupos sobre incidentes informáticos y podrán compartir la responsabilidad con ellos para resolver asuntos relacionados con robo de datos o de computadoras.

- **Especialistas en Auditoría y Gestión de Riesgos**. Ellos pueden ayudar a desarrollar métricas de amenazas y evaluación de vulnerabilidades, así como a fomentar mejores prácticas de seguridad informática en la comunidad objetivo o la organización.
- **Representantes generales de la comunidad objetivo**, que pueden mejorar la percepción de sus necesidades y requerimientos.

Los interesados también deberán incluir a cualquier persona que participe en el manejo de incidentes o en el proceso de notificación. Piense quiénes tendrán que ser notificados en los diferentes tipos de incidentes. ¿Hay personas en otras partes de la organización o comunidad que puedan proporcionar información con el CSIRT, o con quien el CSIRT tenga que compartir u obtener información? Esto puede incluir otras partes de los departamentos de TI o de Seguridad, incluídos los grupos que realicen evaluaciones de vulnerabilidad, detección de intrusos, o monitoreo de red. Saber lo que CSIRT necesitará ayudará a identificar a las personas adecuadas para participar en el desarrollo de los procedimientos.

Indentifique quién más está realizando alguno de los servicios que el CSIRT busque proporcionar. Determine si los servicios deben permanecer en el grupo actual o pasar al CSIRT en un período acordado de tiempo. Enfrentar este tipo de temas en las etapas de planificación puede ayudar a identificar cuáles responsabilidades tendrán que definirse y qué información necesitará recogerse. Pueden también haber algunos recursos disponibles para revisión que le ayuden en la recopilación de información. Estos pueden incluir:

- Organigramas de la organización y de funciones específicas de negocio
- Topologías de los sistemas y redes de la organización o de la comunidad objetivo
- Inventarios de activos y sistemas críticos
- Planes existentes de recuperación de desastres o de continuidad de operaciones
- Directrices existentes para notificar a la organización ante un fallo de seguridad física
- Todo plan de respuesta a incidentes existente
- Toda regulación parental o institucional
- Todas las políticas y procedimientos de seguridad existentes

La revisión de estos documentos tiene un doble propósito: en primer lugar, identificar a los interesados, los recursos y los dueños de redes existentes; y en segundo lugar, proveer una visión general de las políticas existentes a los que el CSIRT debe adherirse. Como beneficio adicional, estos documentos pueden contener texto que se pueda adaptar cuando se desarrollen las políticas, procedimientos o documentación del CSIRT. También pueden incluir listas de notificación generales de los representantes de la organización que deban contactarse en caso de emergencia. Estas listas pueden ser adaptadas para el trabajo y los procesos de CSIRT.

Adicionalmente, investigue que hacen las organizaciones similares para prestar servicios de manejo de incidentes o para organizar un CSIRT. Si tiene contactos en estas organizaciones, vea si puede hablar

con ellos sobre cómo formó su equipo. Visite los sitios web de otros CSIRTs, y revise sus misiones, estatutos, financiamiento, y la lista de servicios. Esto le puede dar ideas para organizar su equipo. Revise los libros u otras publicaciones sobre manejo de incidentes o CSIRT. Podrá encontrar una lista inicial de los recursos en la página web de Desarrollos de CSIRTs del CERT.

Asista a cursos o conferencias que incluyan sesiones para el desarrollo de estrategias de respuesta a incidentes o la creación de CSIRTs. Estos lugares le pueden ofrecer oportunidades de intercambiar ideas e interactuar con otros en el campo de respuesta a incidentes. Un buen punto de partida puede ser la de asistir a la conferencia FIRST anual.

Paso 4: Diseñar la visión del CSIRT

A medida que la información recogida pone en primer plano necesidad de la respuesta a incidentes de la comunidad objetivo y a medida de que usted va comprendiendo las expectativas de la Dirección, usted podrá comenzar a identificar los componentes clave del CSIRT. Esto le permitirá definir la visión del CSIRT, sus objetivos y funciones. Para tener éxito usted necesita del apoyo y la aceptación de estos objetivos y funciones del CSIRT por parte tanto de la Dirección como de la comunidad objetivo.

Es importante llegar a un acuerdo claro en la definición y expectativas del CSIRT que se está formando. Lo que el staff del CSIRT piense que el equipo hace, y lo que los gerentes y la comunidad piense que el CSIRT hace puede ser completamente distinto. Un número de personas puede tener la percepción de que un CSIRT es una "ciber policía" para la organización o comunidad. Si bien esto podría ser cierto para un pequeño número de equipos, no es generalmente el objetivo principal de un CSIRT. El objetivo principal es prevenir y responder a incidentes. La visión del CSIRT debe incluir una explicación clara de donde encajan estas funciones del CSIRT en la estructura organizativa actual y de cómo el CSIRT interactúa con su comunidad objetivo. La visión explica qué beneficios proporciona el CSIRT, qué procesos se promulga, con quién coordina, y cómo ejecuta sus actividades de respuesta.

En la creación de su visión, usted debe:

- Identificar su comunidad objetivo. ¿A quién apoya y da servicios el CSIRT?
- Definir la misión, metas y objetivos de su CSIRT. ¿Qué hace el CSIRT para su comunidad objetivo identificada?
- Seleccionar qué servicios proporcionará el CSIRT a su comunidad objetivo (u otros). ¿Cómo apoya el CSIRT la misión de ésta?
- Determinar el modelo organizacional. ¿Cómo está estructurado y organizado el CSIRT?
- Identificar los recursos necesarios. Qué personal, equipo e infraestructura se necesita para operar el CSIRT?
- Determinar el financiamiento del CSIRT. ¿Cómo se financiarán la puesta en marcha del CSIRT, su mantenimiento a largo plazo y su crecimiento?

Paso 5: Comunicar la visión del CSIRT

Comunicar la visión del CSIRT y su plan operativo a la Dirección, a su comunidad objetivo, y otros que necesiten saber y comprender su funcionamiento. Según convenga, realice ajustes al plan

basándose en sus comentarios.

Comunicar de antemano su visión puede ayudarlo a identificar problemas en los procesos u organización antes de su implementación. Es una manera de que las personas sepan lo que viene y les permite hacer aportaciones al desarrollo del CSIRT. Esta es una manera de empezar a promocionar el CSIRT a la comunidad y a obtener la aceptación necesaria por parte de todos los niveles de la organización.

Usted podrá recibir información faltante o que no hubiera estado disponible durante la etapa de recopilación de información. Utilice esta información y aportes para hacer ajustes finales a la estructura organizativa y los procesos del CSIRT.

Paso 6: Comenzar la implementación del CSIRT

Una vez que se obtiene aprobación de la visión por parte de la Dirección y la comunidad objetivo, comience la implementación:

- Contrate y capacite al personal inicial del CSIRT.
- Compre los equipos y construya la infraestructura de red necesaria para apoyar al equipo.
- Desarrolle el conjunto inicial de políticas y procedimientos que apoyan los servicios del CSIRT.
- Defina las especificaciones y construir su sistema de seguimiento de incidentes.
- Elabore las directrices para notificar incidentes y sus formatos para la comunidad objetivo.

Un recurso principal que usted necesitará para su comunidad son las directrices (pautas) para la notificación de incidentes. Estas directrices definen cómo debe interactuar su comunidad con el CSIRT, qué constituye un incidente, qué tipos de incidentes reportar, quién debe reportar un incidente, por qué un incidente debe ser reportado, el proceso para reportar un incidente, y el proceso para responder al incidente. Estas directrices deben ser claras y comprensibles para la comunidad objetivo atendida.

El proceso para reportar un incidente incluirá una descripción detallada de los mecanismos para enviar los reportes: teléfono, correo electrónico, formulario web o algún otro mecanismo. También deberá incluir detalles sobre qué tipo de información debe incluirse en el reporte.

El proceso para responder a un incidente detalla cómo el CSIRT priorizará y manejará los reportes recibidos. Esto incluye la forma en que se notificará su resolución a la persona que reportó, los plazos de respuesta que se deben cumplir así como cualquier otra notificación que se produzca.

Paso 7: Anunciar que el CSIRT está operando

Cuando el CSIRT esté en funcionamiento, anúncielo ampliamente a la comunidad objetivo u organización madre. Es mejor si este anuncio viene desde la gerencia que lo patrocina. En el anuncio incluya información de contacto y el horario de atención del CSIRT. Esta es una excelente oportunidad para difundir las directrices de reporte de incidentes al CSIRT. Usted también podría querer desarrollar información para publicitar el CSIRT, como un volante sencillo o un folleto esbozando la misión y los servicios del CSIRT, que podrían ser distribuídos junto con el anuncio. Algunos equipos han celebrado

una jornada a puertas abiertas (“*open house”*) o una celebración especial para anunciar el inicio de operaciones del CSIRT.

Paso 8: Evaluar la efectividad del CSIRT

Una vez que el CSIRT haya estado en operación por un tiempo, la Dirección querrá determinar la efectividad del equipo y usar los resultados de la evaluación para mejorar los procesos del CSIRT y asegurarse que el equipo está cumpliendo con las necesidades de la comunidad objetivo. El CSIRT, junto con la Dirección y la comunidad objetivo necesitarán desarrollar un mecanismo para llevar a cabo esta evaluación.

La información sobre la efectividad puede ser recolectada a través de una variedad de mecanismos de retroalimentación, incluyendo:

- evaluación comparativa con otros CSIRT
- discusiones generales con representantes de la comunidad objetivo
- encuestas de evaluación distribuídas periódicamente a miembros de la comunidad objetivo
- creación de un conjunto de criterios o parámetros de calidad que sean utilizados luego por una auditoría o terceros, para evaluar el equipo

Puede ser útil revisar la información recolectada previamente sobre el estado de la comunidad o de la organización antes de la implementación del equipo. Esta información se puede utilizar como una línea de base para determinar el efecto del CSIRT en la comunidad.

La información recolectada para la comparación puede incluir:

- número de incidentes reportados
- tiempo de respuesta o el tiempo de vida de un incidente
- número de incidentes exitosamente resueltos
- información reportada a la comunidad sobre temas de seguridad informática o de la actividad en curso
- esmero en la atención a los problemas de seguridad dentro de la organización
- técnicas preventivas y prácticas de seguridad en vigencia

Para más información sobre la evaluación de la calidad de los servicios del CSIRT, vea la sección 2.2.4 del *Handbook for Computer Security Incident Response Teams*. (Guía para Equipos de Respuesta a Incidentes de Seguridad Informática)

Recuerde que la paciencia puede ser clave

El tiempo que tome diseñar, planificar e implementar un equipo variará con cada situación organizativa. Hemos visto CSIRT entrar en funcionamiento en un amplio rango de tiempos, desde dos meses hasta dos años. Es importante tener en cuenta que puede tomar alrededor de 12 a 18 meses para

consolidar los procesos y procedimientos, especialmente en una empresa distribuída de gran tamaño. Una vez que un equipo esté operativo, puede tomar otros 12 a 18 meses para obtener un buen nivel de confianza y comodidad con su comunidad objetivo. Muchos equipos muestran un gran crecimiento en el número de incidentes reportados durante su primer año de operación. Cuanto más tiempo esté operando, mayor será la comprensión de su comunidad del trabajo que el equipo realiza y más probable que le reporten incidentes.

Recursos y más información sobre la creación de un CSIRT

Los componentes mencionados anteriormente se explican con más detalle en los siguientes:

- *Creating a CSIRT Workshop* (Taller "Creación de un CSIRT", un día de duración, CERT / CC)
- *Handbook for Computer Security Incident Response Teams* (Manual para Equipos de Respuesta a Incidentes de Seguridad Informática, pdf, en inglés)

Estos recursos pueden proporcionar información adicional:

- *Forming an Incident Response Team* (Formando un Equipo de Respuesta a Incidentes, en inglés)
  Un documento que examina el rol que un equipo de respuesta puede jugar en la comunidad y los problemas que debe abordar tanto durante la formación como después del comienzo de las operaciones. Este documento ha sido escrito por un ex miembro del Equipo de Respuesta a Emergencias Informáticas de Australia.

- *Expectations for Computer Security Incident Response* (Expectativas para la Respuesta a Incidentes de Seguridad Informática, en inglés, RFC 2350)
  Se trata de un documento de mejores prácticas, que recomienda requisitos los comportamientos generales que un CSIRT debe seguir cuando establece u opera un equipo. Se enfoca en los métodos para permitir que la comunidad objetivo del CSIRT sepa sobre los servicios y procesos del equipo.

- *Avoiding the Trial-by-Fire Approach to Security Incidents* (Evitando el Enfoque de "prueba por fuego" a Incidentes de Seguridad, en inglés)
  En este artículo se discute la importancia de contar con un proceso organizado y definido para detectar y responder a incidentes de seguridad informática.

responsibility of Francisco Neira. Neither Carnegie Mellon University nor its Software Engineering Institute has participated in the creation of this translation.

ANY MATERIAL OF CARNEGIE MELLON UNIVERSITY AND/OR ITS SOFTWARE ENGINEERING INSTITUTE CONTAINED HEREIN IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTERINCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

CERT® is a registered trademark of Carnegie Mellon University.