Taller "Creación de un CSIRT"

Curso CEM 2024

1. En los grupos de trabajo ya definidos en clase realizar un documente de acuerdo a su "realidad" cada una de las siguientes acciones a fin de generar una propuesta ejecutiva de creación de un CSIRT.
2. Investigue y elija, cree o adapte un formato pertinente al tipo de documento solicitado.

Lista de acciones para el desarrollo de un CSIRT.

Este documento proporciona una visión general de alto nivel de las acciones a tomar y los temas a abordar en la planificación y la implementación de un incidente de seguridad informática del Equipo de Respuesta (CSIRT). También identifica algunos problemas comunes de los equipos puede encontrar en su aplicación. La lista se basa en el material presentado en profundidad a través de cursos de formación del CERT y publicaciones, e incorpora las lecciones aprendidas por el personal durante sus experiencias de planificación y ejecución de tales equipos. Utilice esta lista como punto de partida para planificar un CSIRT. Información más detallada se puede encontrar en la lista de recursos al final de este artículo.

1) Identificar las partes interesadas y participantes.

a. Determinar quién debe participar en cada nivel de la planificación del CSIRT, la implementación y operación.

b. Determinar quién se sirve o apoyados por el CSIRT.

c. Identificar a las personas con quien se pueda coordinar o compartir la información, tanto dentro como fuera de la organización. (Es posible que desee hablar con ellos como a recopilar información. Considere la posibilidad de pedirles que participen en el proyecto de desarrollo o ayudar a la revisión del diseño del CSIRT y los planes de ejecución.)

d. Identificar las personas que realizan la seguridad o las funciones de respuesta a incidentes y hablar con ellos.

e. Identificar qué organizaciones internas y externas podrían interactuar con o participar en el CSIRT.

Problemas comunes: una amplia gama de partes interesadas y los participantes no están identificados e incluidos en la fase de planificación y desarrollo, la falta de identificar y entender la seguridad informática en las actividades de respuesta a incidentes se llevan a cabo y cómo puede cambiar esto con cualquier nuevo plan para un CSIRT.

2) Obtener el apoyo de la gestión y el patrocinio.

a. Encontrar un director ejecutivo para patrocinar y defender el establecimiento del CSIRT.

Esta persona puede ser un buen enlace con los demás ejecutivos y gerentes de negocios en la circunscripción o la organización de padres.

b. Presentamos un caso de negocio para la gestión señalando los beneficios del CSIRT traerá a la organización o colectivo.

c. Obtener apoyo a la gestión por el tiempo y los recursos del equipo pasará la investigación y recopilación de información durante el proceso de planificación.

d. Explicar el porque del establecimiento de un CSIRT dentro de una organización, explicar las ideas, conceptos y beneficios a otros gerentes .

Si el establecimiento de un equipo nacional, se explican los conceptos y beneficios para las organizaciones y los potenciales socios estratégicos que serán apoyados por el CSIRT.

e. Solicitar a la administración para anunciar la formación del proyecto CSIRT y pedir las personas a proporcionar información cuando sea necesario durante la fase de planificación como de ejecución.

Los problemas más comunes: las partes interesadas, los participantes, los gerentes de empresas y socios estratégicos no son conscientes de que un CSIRT se está planificando.

3) Desarrollar un plan de proyecto CSIRT.

a. Forma un equipo de proyecto para ayudar a planear y establecer el CSIRT.

b. Nombrar a un jefe de proyecto. Esta persona puede informar a la dirección sobre los progresos realizados en la planificación.

c. Aplicar los conceptos de gestión de proyectos a la tarea de la creación de un CSIRT.

Los problemas más comunes: el equipo del proyecto no involucra un conjunto diverso de partes interesadas, de un plazo razonable no se ha establecido para la finalización del proyecto - a menudo los plazos son demasiado cortos o poco realista para un CSIRT esté plenamente operativo, un jefe de proyecto no está establecido y el proyecto languidece sin la dirección o realización.

4) Reunir información.

a. Mantener conversaciones con una variedad de partes interesadas para

- Determinar las necesidades y requerimientos de los electores y cualquier otra organización de padres o de acogida.
- Recoger información sobre los tipos de incidentes ya está ocurriendo para comprender mejor la experiencia y los servicios del CSIRT tendrá que proporcionar.
- Entender cualquier gestión de incidencias o la respuesta que ya está ocurriendo.
- Comprender las cuestiones jurídicas, políticas, empresariales o culturales que definen el entorno en el que el CSIRT funcionará.
- Entender propiedad de los datos y la propiedad intelectual (PI) y la autoridad, en relación con cualquier tipo de publicaciones, productos o información obtenida o desarrollada por el CSIRT.

b. Definir políticas y el cumplimiento de normativo, incluyendo los sectores público, privado, académico, gubernamental, militar o de las normas, reglamentos o políticas que se deben seguir o abordada como un CSIRT establecido.

c. Entender la historia anterior.

- Averigüe si alguien ha intentado crear un CSIRT en la organización antes. Si es así, averigüe lo sucedido y comprobar si hay información que puede utilizar.
- Identificar las expectativas de la organización del CSIRT, sobre la base de esta actividad anterior, que el equipo tendrá que corregir.
- Determinar si el nombre de dominio deseado está disponible (es decir, si el CSIRT tendrá su propio nombre de dominio). Si el nombre está disponible, obtener lo más pronto posible.

Los problemas más comunes: el CSIRT no implica o reunir opiniones y sugerencias de todos los interesados, hay desacuerdos sobre quién posee los datos y la propiedad intelectual que puede causar retrasos en el suministro de información del CSIRT a la circunscripción.

5) Identificar la circunscripción CSIRT.

a. Determinar el grupo inicial de personas u organizaciones a las que el CSIRT proporcionar servicio y soporte.

b. Identificar qué tipos de servicios de los CSIRT ofrecerá a los diferentes segmentos del electorado. Por ejemplo, los servicios prestados al público en general puede ser diferente a los servicios prestados a las organizaciones gubernamentales o las infraestructuras críticas. La comprensión del electorado también le ayudará a definir qué grupos al objetivo para los servicios de CSIRT marketing.

c. Identificar y establecer socios estratégicos, en su caso. Socios estratégicos pueden

- Ayudar a orientar las prioridades y la dirección del CSIRT, y ayudar a definir y madurar las capacidades del CSIRT y servicios.
- Participar en el intercambio de información e investigación.
- Participar en las interacciones personalizadas con el CSIRT.
- Ayudar a aumentar la visibilidad y la influencia del equipo.
- Ayudar a promover la adopción y el uso de mejores prácticas de seguridad en toda la empresa o colectivo.

d. Identificar cómo los miembros de la circunscripción obtener los servicios del CSIRT.

e. Identificar los componentes que el CSIRT inicialmente no pueden apoyar, pero puede apoyar en el largo plazo, después de que el CSIRT está en funcionamiento y está lista para ampliar sus servicios.

Los problemas más comunes: no todos los componentes se tratan o se define, por lo que no tienen oficiales de contacto con el CSIRT, el CSIRT no adecuadamente crear una comprensión de los beneficios de sus servicios puede ofrecer para el distrito electoral definido, no está claro cómo el electorado debe ponerse en contacto la asistencia y obtener CSIRT, el CSIRT trata de apoyar a diversos grupos también muchas veces durante su inicio.

6) Definir la misión del CSIRT.

a. Determinar la misión del CSIRT. Este proceso es a largo plazo y de carácter general. La misión no debería cambiar mucho con el tiempo, por lo que deben ser escritos de manera suficientemente amplia para dar cabida a cualquier cambio en los servicios o funciones sin dejar de definir brevemente el propósito y la función del CSIRT. La declaración de misión debe proporcionar valor tanto a la circunscripción y de los padres o de acogida la organización.

b. Determinar las metas y objetivos principales del CSIRT. Estos serán más prácticos y pueden ser modificados como el CSIRT amplía su ámbito de aplicación o servicios.

c. Obtener un acuerdo sobre la misión de todas las partes interesadas (por ejemplo, la gestión electoral, colaboradores y personal); asegurar que todos entiende la misión.

Los problemas más comunes: el personal no entiende la misión y la "ampliación de la misión" 4 se produce (el CSIRT pierde el foco en su objetivo definido y se vuelve menos eficaz), terceros (tales como los políticos) pueden tener una perspectiva sobre la misión que no coinciden con la misión del CSIRT y tratar de sacar al equipo en las actividades no está preparado para manejar.

7) Asegurar el financiamiento para las operaciones de CSIRT.

a. Obtener financiación para las operaciones de puesta en marcha, a corto y largo plazo. Esto incluirá

- Plantilla inicial, a corto y largo plazo el desarrollo profesional y capacitación.
- Equipos, herramientas e infraestructura de red para la detección, análisis, seguimiento y respuesta a incidentes de seguridad informática.
- Instalaciones para la protección y seguridad de los datos del CSIRT, sistemas y personal.

b. Decidir qué modelo de financiación que va a utilizar para apoyar el CSIRT, lo que podría incluir pago por servicio, cuotas de sus miembros, el apoyo del gobierno, o una línea de presupuesto de la organización de padres.

Los problemas más comunes: CSIRT puede perder eficacia por no financiar esfuerzos para ayudar al personal a mantenerse al día con las nuevas tecnologías o por no permitir que el personal para asistir a conferencias y capacitación para mejorar sus habilidades, conocimientos y habilidades, lo que puede hacer el equipo menos capaz de manejar las nuevas amenazas , los ataques, y los riesgos que afectan a sus electores.

8) Decidir sobre la amplitud y el nivel de los servicios del CSIRT ofrecerá.

a. Comience con algo pequeño y crecer. Sea realista acerca del tipo y cantidad de servicios nuevos CSIRT puede aportar una experiencia dada y los recursos existentes.

b. Determinar los servicios del CSIRT proveerá e identificar a qué parte del electorado que se ofrecerán.

c. Definir el proceso de prestación de servicios (por ejemplo, horas de operación, póngase en contacto con los métodos, los métodos de difusión de la información y los procesos relacionados). d. Decida cómo el CSIRT mercado su servicio.

Problemas comunes: la gente quiere que el CSIRT para llevar a cabo los servicios antes de estar listo, tratando de ofrecer demasiados servicios a la vez, tratando de jugar demasiadas funciones, la creación de servicios que no son necesarios o que otra organización que ofrece es, no comercialización de los servicios necesarios.

9) Determinar la estructura de información del CSIRT, la autoridad, y el modelo organizativo.

a. Determinar dónde está el CSIRT se ajusta a la estructura de la organización. Por ejemplo, un CSIRT a nivel nacional puede funcionar dentro del gobierno, como una entidad nacional independiente, o como parte de otra organización. Si se coloca dentro de otra organización,

¿cómo es percibido por el electorado y cómo estas percepciones afectan a su funcionamiento?

b. Crear un organigrama y mantenerlo al día.

c. Determinar si el CSIRT debe informar "a" la jerarquía de cualquier otra organización o entidad matriz.

d. Prepárese para educar a la gente sobre el trabajo del CSIRT será capaz de hacer. Los miembros del equipo puede necesitar para rechazar diplomáticamente algunas de las solicitudes de trabajo y debe preparar las respuestas adecuadas.

Los problemas más comunes: no CSIRT tareas son impuestas por las partes interesadas externas que tengan personal fuera de sus funciones CSIRT principal e inhiben el desempeño eficaz de los servicios normales.

10) Identificar los recursos necesarios, tales como personal, equipo e infraestructura.

a. Determinar la forma en la infraestructura del CSIRT será protegida, segura, y controlado, en especial las instalaciones físicas y los repositorios de datos.

b. Definir los procesos de recolección, registro, seguimiento y archivo de la información.

c. Crear descripciones de las funciones que se enumeran los conocimientos requeridos, destrezas y habilidades (KSA) para cada posición del CSIRT.

d. Crear un plan de orientación y capacitación para el personal, y asegurarse de que están entrenados en una experiencia única o servicios.

e. Determinar los requisitos para la verificación de antecedentes apropiados, certificados o autorizaciones de seguridad.

Los problemas más comunes: el personal no es capacitación cruzada, dando lugar a "puntos únicos de fallo" si alguien realiza una función que requiere una habilidad única hojas, y el personal no se les da oportunidad y un camino para el desarrollo profesional o de carrera, lo que resulta en el agotamiento y los altos niveles de trabajo de volumen de negocio.

11) Definir las interacciones e interfaces.

a. Identificar las interacciones y las interfaces con las piezas clave de la circunscripción, las partes interesadas, y con los socios internos o externos, colaboradores o contratistas.

b. Determinar qué otras entidades, el CSIRT coordinará con.

c. Identificar cómo fluye la información entre estas entidades.

d. Definir y establecer las interfaces y los métodos de colaboración y comunicación con otros, según proceda, incluida la aplicación de la ley, los vendedores, críticos componentes de la infraestructura, los proveedores de servicios de Internet (ISP), otros grupos de seguridad, y otros CSIRT.

e. Asegúrese de que no son buenos métodos para la comunicación interna entre los CSIRT del personal.

f. Por todas estas interfaces, entender

- Quién posee los datos que se comparte.
- Que tiene la autoridad y la responsabilidad de los datos.
- Cómo los datos se comparten y con quién se comparte.
- Cómo los datos son protegidos, controlados y almacenados de forma segura.

g. Definir los métodos para difundir la información a los electores y las partes interesadas.

h. Desarrollar y explicar los tipos de documentos estándar para la difusión de información para el electorado.

Los problemas más comunes: los datos no se comparte de una manera controlada y segura, lo que resulta en confidencias se rompe, y el personal CSIRT no está informado sobre las actividades del CSIRT, reduciendo la eficacia en las funciones normales de trabajo; interfaces definidas no se han establecido, causando una ruptura del proceso cuando la escalada o los datos el intercambio y la coordinación es necesaria.

12) Definir las funciones, responsabilidades y la autoridad correspondiente.

a. Desarrollar las funciones y responsabilidades de todas las funciones del CSIRT.

b. Definir y desarrollar las interfaces entre las funciones del CSIRT y otras funciones externas y colaboraciones.

c. Identificar las áreas en donde la autoridad puede ser ambigua o que se superponen, y definir funciones y roles entre los grupos.

Problemas comunes: la gente no sabe que su función termina y alguien más comienza, más de un grupo se le da la misma responsabilidad, nadie se da una responsabilidad específica y la tarea no es nunca completa.

13) Documento del flujo de trabajo.

a. Crear un diagrama (gráfico carril, diagrama de flujo, etc) para documentar los procesos del CSIRT y las interacciones correspondientes, incluida la que realiza la obra y en qué parte del proceso de las interfaces y los traspasos se producen.

b. Construcción de medidas de garantía de calidad y componentes en los procesos y flujos de trabajo CSIRT correspondiente.

Los problemas más comunes: el personal es incierto cómo seguir determinados procesos o llevar a cabo la coordinación y actividades de colaboración.

14) Desarrollar políticas y procedimientos correspondientes.

a. Establecer las definiciones de la terminología (por ejemplo, "evento de seguridad informática y el incidente"), junto con otros términos exclusivos de la organización.

b. Determinar las categorías correspondientes incidente, las prioridades y criterios de progresividad.

c. Identificar las políticas y procedimientos iniciales que se deben formalizar ante operación, y los que se pueden crear después de que el CSIRT está en funcionamiento.

d. Elaborar directrices de notificación de incidentes para el distrito electoral y las formas de publicidad.

e. Definir y documentar los criterios para la prestación de servicios CSIRT a garantizar la coherencia, procesos fiables, repetibles y son seguidos por el personal.

Los problemas más comunes: definiciones comunes no son compartidas entre el CSIRT y el electorado, lo que resulta en confusión y el malentendido, la imposibilidad de resumir los datos sobre las tendencias del incidente, porque no existe una definición clara de los términos, la falta de políticas formalizadas pueden retrasar el tiempo de respuesta ya que los procesos se debe definir cada uno vez que ocurra un incidente.

15) Crear un plan de aplicación y solicitar comentarios.

a. Obtener su opinión sobre el plan de implementación de los actores y componentes (u otros expertos CSIRT), pregunte por sus comentarios, y asegurar que el plan coincida con la misión.

b. Actualizar y mejorar el plan basado en la retroalimentación.

c. Obtener de gestión y apoyo constituyente para la puesta en práctica.

Los problemas más comunes: el distrito electoral no ha sido informado acerca de la implementación del CSIRT y no proporciona apoyo, lo que puede dar lugar a incidentes que no se informó al consejo CSIRT o CSIRT y recomendaciones no se siguieron, el plan de ejecución no se envía para su revisión, lo que resulta en una plan que no es compatible o implementado.

16) Anunciar que el CSIRT cuando entre en funcionamiento.

a. Solicitar a la administración para hacer un anuncio formal.

b. Proporcionar material de marketing y las directrices de notificación de incidentes que explica cómo el electorado debe interactuar con el CSIRT.

c. Incorporar la formación sobre los servicios del CSIRT y las interacciones en los programas de orientación personal.

d. Encontrar maneras de difundir información sobre los servicios del CSIRT, como las intranets de la organización, sitios web, folletos, seminarios, y cursos de formación.

Los problemas más comunes: el CSIRT no está anunciado oficialmente, y nadie entiende cómo o cuándo la interfaz con el equipo.

17) Definir los métodos para evaluar el desempeño del CSIRT.

a. Definir líneas de base para la notificación de incidentes y manejo dentro de la organización antes de que el CSIRT se lleva a cabo. Use las líneas de base para comparar el rendimiento una vez que el CSIRT está en funcionamiento.

b. Definir los criterios de medición y los parámetros de control de calidad para que el CSIRT se puede medir de una manera coherente.

c. Definir los métodos para la obtención de información electoral.

d. Implementar procedimientos de informes y auditoría para asegurar que el CSIRT está llevando a cabo de manera eficiente y cumple con establecido acuerdos de nivel de servicio o indicadores de desempeño.

Los problemas más comunes: no se instituyen métodos para evaluar si el CSIRT es el cumplimiento de su misión, los métodos para la mejora de los procesos no se implementan, las métricas de rendimiento no miden adecuadamente el desempeño del CSIRT.

18) Tener un plan de copia de seguridad para cada elemento del CSIRT.

a. Identificar las funciones clave del CSIRT y crítica, servicios y equipos.

b. Diseñar un plan de recuperación ante desastres y continuidad del negocio para los servicios de CSIRT y procesos críticos, estos planes deben atar en planes similares para la organización matriz.

c. Plan de lo que sucederá si alguien no puede cumplir su función o no puede proporcionar el espacio o el equipo necesario por el CSIRT.

d. Instituto se burlan de ejercicios para probar si las funciones de CSIRT y las instalaciones pueden ser operativos en situaciones de emergencia.

Los problemas más comunes: el CSIRT no llegar a la capacidad de devolución de 5 listas de personal adicional si es necesario durante las horas punta o situaciones de emergencia, sistemas de clave CSIRT y las redes que proporcionan funciones y servicios no son una copia de seguridad, lo que resulta en el CSIRT no ser capaz de funcionar durante una situación de emergencia.

19) Sea flexible.

a. No trate de hacer demasiadas cosas a la vez. Sin embargo, estar preparada para adaptarse y aprovechar las buenas oportunidades que puedan surgir, y si esas oportunidades se los recursos de la CSIRT severamente impuestos y causar problemas de prestación de servicios existentes CSIRT.

b. Entiendo que los servicios pueden evolucionar con el tiempo y estar dispuesto a aprender nuevas habilidades y adquirir nuevos conocimientos.

c. Seguir aprendiendo sobre el cambio de tecnologías para asegurar que las estrategias de respuesta son eficaz para hacer frente a nuevas amenazas y riesgos.

d. Busque maneras de colaborar con otros en el CSIRT y de seguridad.

CSIRT Recursos

Manual para la seguridad informática de Respuesta a Incidentes equipos http://www.cert.org/archive/pdf/csirt-handbook.pdf

CSIRT Servicios http://www.cert.org/csirts/services.html

Modelos de organización para los CSIRT http://www.cert.org/archive/pdf/03hb001.pdf

Estado de la práctica para los CSIRT http://www.cert.org/archive/pdf/03tr001.pdf

Pasos para la creación de CSIRT Nacional http://www.cert.org/archive/pdf/NationalCSIRTs.pdf

Definición de Procesos de Gestión de Incidentes http://www.cert.org/archive/pdf/04tr015.pdf

Su dotación de personal CSIRT http://www.cert.org/csirts/csirt-staffing.html

Notas:

1. A una "parte interesada" es cualquier individuo o grupo con un interés en el éxito del CSIRT y su misión. Los interesados pueden ser los que se informe a los CSIRT, recibir ayuda del CSIRT, proporcionar fondos y el patrocinio del CSIRT, o interfaz con el CSIRT a través del intercambio de información o la coordinación de los incidentes y las actividades de manejo de la vulnerabilidad.
2. El "distrito electoral" son las personas u organizaciones de servicio o con el apoyo de la CSIRT.
3. "cumplimiento" se refiere a asegurar que las políticas o procedimientos de CSIRT está de acuerdo con las leyes o políticas que están en su lugar organizativamente, a nivel local, nacional o internacional. Por ejemplo, en los EE.UU. hay muchas leyes estatales que exigen a las empresas a notificar a los clientes si sus datos personales es puesto en libertad sin su consentimiento o autorización. Si un CSIRT en un estado con leyes como se encarga de la manipulación de violaciones de seguridad informática, él (o su organización matriz) debe cumplir con la ley con respecto a cualquier notificación requerida.
4. "ampliación de la misión" se refiere a una situación en la que un CSIRT comienza a realizar actividades fuera del ámbito de su misión o propósito definido y función.
5. Alcance de devolución de la capacidad es la habilidad de llamar a personal adicional fuera de su personal de CSIRT normal durante las horas punta. Por ejemplo, si usted está usando un contratista a completar el personal de CSIRT y se produce un incidente grave, una capacidad de alcance de devolución permitirá que el contratista que llamar a más personas para ayudar a manejar el incidente. En este caso el contratista "se remontan" en su conjunto total de los empleados para complementar temporalmente el personal del CSIRT hasta que el incidente se resolvió y las operaciones volvieron a normales. Si el CSIRT no tiene contratistas que proveen de personal, y luego llegar-back puede ser manejado por sacar a la gente de otras partes de la organización para ayudar hasta que el incidente se resolvió.