MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUÍA DE ACCIÓN ANTE INCIDENTE DE DEFACEMENT

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

***Defacement**: alteración no autorizada de un sitio web o una aplicación por parte de un atacante.*

Detalles: en un incidente de defacement, un intruso accede ilegalmente a un sistema y modifica su apariencia o contenido, generalmente con el objetivo de transmitir un mensaje. El defacement suele ser visible para los visitantes del sitio web, ya que los atacantes reemplazan la página principal o las páginas internas con su propio contenido.

Los ataques de defacement pueden variar en su alcance y motivación. Algunos atacantes simplemente cambian la apariencia de un sitio web con mensajes políticos, vandalismo digital o contenido ofensivo. Otros pueden utilizar el defacement como una forma de hacer propaganda, difundir un mensaje o reclamar la responsabilidad de un ataque. Además, los atacantes también pueden aprovechar el defacement como una distracción para ocultar otras actividades maliciosas, como la extracción de datos o la instalación de malware.

Impacto: el defacement no solo afecta la imagen y la reputación de una organización, sino que también puede generar pérdida de confianza en los usuarios y causar interrupciones en los servicios en línea.

1. Fase de Identificación

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

Verificar el defacement y detectar su origen

1. Comprobar los archivos de contenido estático como, por ejemplo, las fechas de modificación.
2. Comprobar el contenido mashup (contenido reutilizado de otra página web, API, RRS, REST y Web Service).
3. Comprobar los enlaces presentes en la página web (src, meta, css, script, etc.).
4. Revisar los archivos de registro (logs).
5. Buscar contenido malicioso en las bases de datos.
6. Analizar el código fuente de la página sospechosa para identificar el problema con claridad. Se debe tener claro que el problema está en un servidor web que pertenece a la empresa y no en un contenido web localizado fuera de su infraestructura, como banners comerciales de un tercero.
7. Recopilar información relevante sobre el incidente, incluyendo la URL afectada, la fecha y hora de detección.

8. Notificar al equipo de respuesta a incidentes de seguridad (CSIRT) de la organización o al equipo de seguridad de la empresa.
9. Comunicar internamente a los equipos pertinentes, como el equipo de relaciones públicas y el equipo legal, para coordinar la respuesta y garantizar una acción rápida.

2. Fase de Contención

La máxima prioridad en esta fase es contener el impacto negativo que pueda sufrir la organización a causa del defacement.

Evaluación de la situación

1. Documentar y recopilar todas las pruebas disponibles, como capturas de pantalla del defacement, registros de acceso, registros del sistema, etc.

2. Realizar una copia de seguridad de todos los datos, con fines forenses y para la recopilación de evidencias, teniendo en cuenta:

    - Logs de los sistemas
    - Versiones desactualizadas de software/hardware
    - Vulnerabilidades no parcheadas
    - Credenciales de usuario por defecto o contraseñas poco robustas

Comprobar la repercusión en los medios de comunicación

1. Determinar el alcance de la publicación.
2. Concretar la cantidad de información que se ha hecho pública.
3. Estipular el impacto y cómo afecta a la organización.
4. Recabar toda la información posible.

Contención

1. Despublicar el portal, publicando una página de mantenimiento en su lugar y, si es posible, con contenido únicamente HTML para evitar cualquier vector de ataque.

2. Si es posible, restaurar una versión limpia y confiable del sitio web o la aplicación.

3. Realizar un análisis forense del sistema afectado para identificar el origen del ataque y los puntos de entrada utilizados por el atacante.

4. Examinar los registros de acceso, los registros del servidor y cualquier otro registro o archivo relevante para obtener más información sobre la brecha de seguridad.

3. Fase de Mitigación

Una vez recopilada y analizada la información obtenida en la fase de contención, deben tomarse medidas reactivas para gestionar el incidente.

Tomar acciones para terminar con el defacement

1. Bloquear/restringir el acceso al backend del servicio web, CMS o servidor.
1. Eliminar los posibles ficheros u otros contenidos maliciosos detectados.
2. Aplicar las actualizaciones pertinentes del servidor, CMS y plugin del CMS. Es recomendable hacerlo en un entorno destinado para pruebas antes de realizar esta operación en el entorno final.
3. Cambiar las credenciales de los usuarios que se hayan visto comprometidas, en caso de no tener una seguridad del alcance, revocar todas las contraseñas por unas nuevas y robustas.
4. Establecer una política para el cambio periódico de credenciales.
5. Realizar copias de seguridad del portal, tras aplicar las acciones anteriores.
6. Realizar comunicados internos para informar del estado del defacement.

4. Fase de Recuperación

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

1. Restaurar el sitio web o la aplicación a un estado seguro y confiable.
2. Realizar una revisión exhaustiva de la seguridad del sistema y aplicar las medidas necesarias para fortalecerlo y prevenir futuros incidentes similares.

3. Actualizar y parchear el software y los sistemas subyacentes para corregir posibles vulnerabilidades.
4. Realizar un comunicado externo sobre los hechos, con el fin de controlar la repercusión mediática del incidente.
5. Comprobar el portal en la medida de lo posible para verificar que todo funciona de forma adecuada.
6. En caso de disponer de un equipo legal, coordinarse con éste para tener en cuenta las posibles consecuencias legales y de reputación.
7. Determinar las posibles consecuencias económicas.

5. Fase Post- Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

6. Lecciones aprendidas

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma.

1. Realizar una revisión post-incidente para identificar las lecciones aprendidas y las áreas de mejora.
2. Actualizar las políticas y procedimientos de seguridad de la organización en base a los hallazgos del incidente.
3. Proporcionar capacitación y concientización en seguridad a los empleados para prevenir futuros incidentes.

7. Diagrama de flujo