Preparación 1

Objetivo: Establecer contactos, definir procedimientos y recopilar información para ahorrar tiempo durante un ataque.

- Tenga al día los esquemas que describen los componentes aplicativos relacionados con el servidor web.
- Construya y tenga listo un sitio web de respaldo, en que se pueda publicar contenido.
- Defina un procedimiento para redirigir a todos los visitantes a este sitio web de respaldo.
- Implemente herramientas de monitoreo para detectar rápidamente cualquier comportamiento anormal en sus sitios web críticos.
- Exporte los archivos de registro (logs) del servidor web a un servidor externo. Haga sincronizar sus relojes. en cada servidor.
- Referencie los contenidos externos (estático o dinámico) y cree una lista para cada uno de ellos. No olvide el contenido de terceros.
- Referencie los puntos de contacto de su proveedor de alojamiento.
- Asegúrese de que su proveedor de hosting cumpla las políticas para registrar todos los eventos.
- Asegúrese de que dispone un mapa actualizado de la red.

Identificación 2

Objetivo: Detectar los hechos, determinar su alcance, e involucrar a las partes apropiadas.

Los canales usuales de detección son:
Control Página Web: El contenido de la página web ha sido alterado. El nuevo contenido es o muy discreto (una inyección de "iframe") o evidente ("You have been 0wn3d by xyz")
Usuario: Llamadas de usuarios o notificaciones por parte de los empleados acerca de problemas que notan durante la navegación por el sitio web.
Controles de seguridad con herramientas como Google SafeBrowsing

Verifique el defacement y detecte su origen:

- Compruebe los archivos de contenido estático (en particular, compruebe las fechas de modificación, la firma hash, etc.).
- Compruebe los proveedores de contenido mashup.
- Compruebe los enlaces presentes en la página web (src, meta, css, script, ...).
- Revise los archivos de registro (logs).
- Busque contenido malicioso en las bases de datos.

→ El código fuente de la página sospechosa debe ser analizado cuidadosamente para identificar el problema con claridad. Específicamente, asegúrese que el problema está en un servidor web que pertenece a la empresa y no de un contenido web localizado fuera de su infraestructura, como banners comerciales de un tercero.

Contención 3

Objetivo: Mitigar los efectos del ataque sobre el entorno objetivo.

- Respalde todos los datos almacenados en el servidor web con fines forenses y recopilación de evidencia. En este caso, la mejor práctica es hacer una completa copia “bit a bit” del disco duro que contiene el servidor web. Esto será útil para recuperar archivos borrados.
- Revise su mapa de arquitectura de red. Compruebe que la vulnerabilidad explotada por el atacante no se encuentre además en otra parte:
  - Revise el sistema en el que el que está corriendo el servidor Web,
  - Revise otros servicios que estén ejecutándose en esa servidor,
  - Compruebe las conexiones con otros sistemas, lo que podría estar en peligro.

Si el origen del ataque es otro sistema de la red, desconéctelo si es físicamente posible e investíguelo.

- Trate de hallar evidencia de cada acción del atacante:
- Averigüe cómo entró el atacante al sistema en primer lugar y corrija:
  - Vulnerabilidad de componente que permite el acceso a escritura: corregir la vulnerabilidad aplicando solución del autor.
  - Carpeta pública abierta: arreglar el fallo.
  - Vulnerabilidad SQL que permite inyección: corregir el código.
  - Componentes mashup: cierre el ingreso mashup.
  - Modificación administrativa por acceso físico: modificar los derechos de acceso.
- Si es necesario (tema complejo y web server muy importante), implemente un servidor web temporal, con aplicaciones actualizadas. Deberá ofrecer el mismo contenido que el servidor web comprometido o por lo menos mostrar otro contenido legítimo, como "Temporalmente no disponible". Lo mejor es mostrar contenido temporal estático, que sólo contenga código HTML. Esto evita otra infección en caso de que el atacante ha utilizado la vulnerabilidad en el coódigo legítimo PHP, ASP, CGI, PL, etc.

Remedio 4

<u>Objetivo</u>: Adoptar medidas para eliminar la amenaza y evitar futuros defacements.

Eliminar todo el contenido alterado y sustituirlo por el contenido legítimo, restaurado de copias de seguridad previas. Asegúrese de que este contenido esté libre de vulnerabilidades.

Recuperación 5

<u>Objetivo</u>: Restaurar el sistema a las operaciones normales.

Si el servidor web proporciona autenticación de usuarios, y tienen evidencia o razones para creer que las contraseñas han sido comprometidos, cambie todas las contraseñas de los usuarios. Esto puede requerir una gran comunicación con los usuarios.
Si se ha usado un servidor respaldo, restaure el servidor web principal.

Repercusiones 6

<u>Objetivo</u>: Documentar los detalles del incidente, discutir lecciones aprendidas y ajustar los planes y defensas.

Comunicación
Si el defacement ha sido visible por parte de los usuarios, planee cómo explicar el incidente públicamente.

Informe
Debe escribirse un informe de crisis y ser puesto a disposición de todas las partes involucradas.

Deben describirse los siguientes temas:

- Detección Inicial;
- Las acciones y los plazos;
- ¿Qué salió bien;
- ¿Qué salió mal;
- Costo del incidente.

En caso de descubrimiento de vulnerabilidades, reporte cualquier vulnerabilidad no documentada que tenga un producto que se ejecuta en el servidor web (como un foro PHP) a su autor, para que el código pueda ser actualizado con el fin de lanzar un “fix”.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM #6

Defacement a sitios web

Respuesta en vivo en servidores comprometidos

Autor IRM: CERT SG / Cédric Pernet
Versión IRM: 1.2
email: cert.sg@socgen.com
web: http://cert.societegenerale.com
Traducción: Francisco Neira
email: neira.francisco@gmail.com
Twitter: @neirafrancisco

Extracto

Esta “Metodología de Respuesta a Incidentes” (IRM, por sus siglas en inglés) es una hoja resumen dedicada a los manejadores de incidentes que investigan un asunto de seguridad específico. Quién debe de usar estas hojas IRM?

- Administradores
- Centro de Operaciones de Seguridad (SOC)
- CISOs y sus delegados
- CSIRT (equipos de respuesta a incidentes informáticos)

Recuerde: Si usted afronta un incidente, siga el IRM, tome notas y no pierda el control. Contacte su CSIRT inmediamente si es necesario.

Pasos del manejo de incidentes

Se definen 6 pasos para manejar los incidentes de seguridad:

- Preparación: Alistarse para manejar el incidente
- Identificación: Detectar el incidente
- Contención: Limitar el impacto del incidente
- Remedio: Remover la amenaza
- Recuperación: Recobrar a una etapa normal
- Repercusiones: Delinear y mejorar el proceso