Preparación 1

Objetivo: Establecer contactos, definir procedimientos y recopilar información para ahorrar tiempo en la gestión de incidentes.

Contactos

■ Identifique los contactos técnicos internos (equipo de seguridad, equipo de respuesta a incidentes, etc.)
■ Asegúrese de tener puntos de contacto en los equipos de relaciones públicas, en el de recursos humanos y el departamento legal.
■ Identifique los contactos externos que pudieran ser necesarios, sobre todo para fines de investigación (como agentes del orden, por ejemplo).

La política de seguridad

■ Asegúrese de que se explique el valor de la información corporativa en las reglas del procedimiento, los diagramas de TI, y en las sesiones de sensibilización y capacitación.
■ Asegúrese de que todos los activos valiosos son identificados adecuadamente
■ Asegúrese de que el proceso de escalamiento de incidentes de seguridad está definido y los actores están claramente definidos e identificados.

Identificación 2

Objetivo: Detectar el incidente, determinar su alcance, e involucrar a las partes apropiadas.

La pérdida de datos puede ocurrir en cualquier lugar. Recuerde que la causa de la fuga puede ser un empleado individual que voluntaria o involuntariamente, obvie asuntos de seguridad, o comprometa una computadora.

Paso 1: DETECTAR EL INCIDENTE

■ proceso de notificación del incidente:
La información interna puede ser una buena fuente de detección: confianza en empleados, el equipo de seguridad identificando un problema, etc
■ Herramienta pública de monitoreo:
Una revisión en los motores de búsqueda de Internet y bases de datos públicos puede ser muy útil para detectar la fuga de información.
■ Herramienta DLP (“Data Loss Prevention”, “Prevención de Pérdida de Datos”):
Una herramienta DLP en la empresa, puede proporcionar información valiosa para los administradores de incidentes de trabajo sobre la fuga de información.

Paso 2: CONFIRMAR EL INCIDENTE

No haga nada sin antes tener una solicitud escrita del CISO / persona a cargo interesado(a) . Basándose en consejo de su equipo legal, también podría ser útil una autorización escrita por parte del usuario en cuestión.
■ **E-Mail:**
La fuente de la divulgación podría haber enviado datos utilizando su dirección de correo electrónico corporativo.
Busque los correos electrónicos enviados o recibidos desde una cuenta sospechosa o con un objeto especial.
En el cliente de correo electrónico en el escritorio del sospechoso (si está disponible), utilice una herramienta que permita realizar búsquedas mediante el filtrado de los emails marcados como "PRIVADO". Si usted realmente lo necesita, pida al usuario un consentimiento escrito o pídale que esté presente.
Dado el caso, busque entre los archivos de log relacionados.
Utilice herramientas forenses para comprobar el borrado del historial de navegación. También revise el contenido “offline” dejado luego de la navegación (caches).

■ **Navegación:**
Los datos pueden haber sido enviado por correo web / foros / sitios web dedicados.
En el servidor proxy, compruebe los logs relativos a conexiones de cuentas sospechosas hacia URL utilizado para divulgar los datos.
En el escritorio (si está disponible), revise el historial de los navegadores instalados. Recuerde que algunas personas pueden tener diferentes navegadores en el mismo equipo de escritorio, asegúrese de revisar el historial de cada navegador. Algunos archivos de registro pueden proporcionar información útil pues el momento de la fuga de datos es una marca en el tiempo,.

■ **Dispositivos de almacenamiento externos:**
Se pueden utilizar diversos dispositivos para almacenar datos: memorias USB, CD-ROM, DVD, discos duros externos, teléfonos inteligentes, tarjetas de memoria, etc.
Hay poca información disponible con relación a la transferencia de datos usando estos dispositivos. Se puede referenciar por el sistema operativo la serie del dispositivo USB utilizado para transferir datos. Un análisis forense puede confirmar el uso de hardware, pero no los datos transferidos.
■ **Los archivos locales:**
Si no ha encontrado nada todavía, aún hay posibilidades de encontrar pistas en el sistema de archivos local del sospechoso. Al igual que para la exploración de correo electrónico, utilice una herramienta de análisis que prohíba el acceso a la zona privada del usuario. Si realmente necesita acceder, actúe de acuerdo a la legislación laboral local.
■ **Transferencia de la red:**
Pueden utilizarse múltiples maneras para transferir datos de la institución: FTP, mensajería instantánea, etc Trate de indagar en los archivos de log que muestran dicha actividad.
Los datos también podrían haber sido enviados mediante un túnel VPN o en un servidor SSH. En este caso, se puede probar la conexión por observación de los archivos de log, pero no se podrá ver el contenido de la transmisión.
■ **Impresora:**
Los datos pueden ser enviados a impresoras conectadas a la red. En este caso, compruebe si hay huellas en la cola de impresión o directamente en la impresora, ya que algunos fabricantes almacenan los documentos impresos en un disco duro local.
■ **Malware:**
Si no ha encontrado nada, piense en un posible malware y actúe según el IRM "Detección de Malware".
Nota: Incluso cuando se haya encontrado suficiente evidencia, siempre busque más. No porque haya demostrado que los datos llegaron de manera fraudulenta de A a B con un método significa que no se envió a C con otro método. Además, no olvide que otra persona podría haber accedido al ordenador. ¿El empleado sospechoso estaba realmente frente a su computadora cuando se produjo la fuga?

Contención 3

Objetivo: Mitigar los efectos del ataque sobre el medio ambiente dirigida.

Notifique a la Alta Dirección, al equipo legal y al de Relaciones Públicas para asegurarse de que están

preparados para hacer frente a una divulgación masiva o selectiva.

Dependiendo del vector de fuga, impida el acceso a la URI de la divulgación, el servidor de la divulgación, la fuente o los destinatarios de la divulgación. Esta acción deberá realizarse en todos los puntos de la infraestructura.

Si la fuga se ha confirmado, suspenda las credenciales lógicas y físicas de la información privilegiada. Involucre a RRHH y al equipo legal antes de cualquier acción.

Aisle el sistema de computación (escritorio, impresora) utilizado para revelar los datos con el fin de realizar un análisis forense más tarde. Esta manipulación se debe hacer de la manera “dura”: quitando el cable de alimentación eléctrica (y la batería en caso de una computadora portátil).

Remedio 4

Objetivo: Adoptar medidas para eliminar la amenaza y evitar futuros incidentes.

Si los datos han sido enviado a servidores públicos, solicite al propietario (o webmaster) que elimine los datos divulgados. Asegúrese de preparar su petición según el destinatario (un webmaster hacktivista no se comportará como un webmaster de la Prensa)
Si no es posible eliminar los datos divulgados, proporciónele un análisis completo del equipo de relaciones públicas y a la Alta Dirección. Monitoree la dispersión de los documentos filtrados en los diferentes sitios web y redes sociañes(FB, Twitter, etc) así como los comentarios y reacciones de los usuarios de Internet.

Proporcione los elementos necesarios al equipo de RRHH para preparar una eventual demanda contra el “insider”.

Recuperación 5

Objetivo: Restaurar el sistema a las operaciones normales.

Si un sistema ha sido comprometido, restaure por completo.

Finalmente, advierta a sus empleados o algunos equipos locales sobre el tema para crear conciencia y aumente las normas de seguridad.

Cuando la situación vuelva a la normalidad, considere eliminar la comunicación oficial.

Repercusiones 6

Objetivo: Documento detalles del incidente, discutir las lecciones aprendidas, y ajustar los planes y las defensas.

Informar a la jerarquía, filiales y socios para compartir las mejores prácticas aplicadas en este incidente para hacer cumplir normas similares en otros lugares.

Informe
Debe escribirse un informe de incidente que se pondrá a disposición de todos los actores del incidente.

Los describirse los siguientes temas:
- Detección Inicial
- Las acciones y los plazos
- ¿Qué salió bien
- ¿Qué salió mal
- Impacto de Incidentes

Capitalice
Deben definirse acciones para mejorar los procesos de manejo de las fugas de información y así sacar provecho de esta experiencia.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM # 11

Fuga de Información

Manejo de divulgación intencional de información interna

Autor IRM: CERT-SG / Cédric Pernet, David Bizeul
Versión IRM: 1.1
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