Preparación 1

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

Contactos

■ Asegúrese de tener también puntos de contacto en su equipo de relaciones públicas, en el de recursos humanos y en el departamento legal

■ Tenga una instalación de logs centralizados

■ Asegúrese de tener un proceso global de aprobación y autorización. Este proceso debe tener especial cuidado en la eliminación de privilegios en trabajos anteriores

■ Proporcione autenticación fuerte acorde al riesgo de la aplicación de negocios

Identificación 2

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

Los abusos de los "inisders" son difíciles de detectar y no hay consejos para un 100% de éxito.

Identificación técnica

■ Alertas de una SIEM o herramientas de correlación

Se ha detectado comportamiento malicioso en correlación con varios eventos anormales

■ Alertas de un IDS / IPS detectando una intrusión

En caso que el insider hubiera tratado de hackear el sistema, el sistema de detección de intrusiones ("Intrusion Prevention System") podría haber activado una alerta.

La identificación humana

■ Gerencia:

El gerente del insider puede ser el primero en observar comportamiento sospechoso.

■ Control, riesgo, cumplimiento:

Estos equipos tienen sus propios sistemas para detectar anomalías operacionales en el funcionamiento y también podrían activar alertas si se detectan algo anormal.

■ Colegas:

Los colegas del insider son tal vez el canal de comunicación más valioso porque saben perfectamente las tareas, el proceso y los impactos en sus tareas de trabajo. Pueden adivinar fácilmente lo que está sucediendo.

■ Las partes externas:

Los socios externos o la estructura también pueden tener sus propias capacidades de detección. Si las operaciones se han falsificado internamente, estas entidades externas pueden realmente aportar con luces en el tema.

Contención 3

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

No haga nada, sin una solicitud por escrito del CISO o persona a cargo interesada. Basado en su equipo de asesoramiento legal, también podría ser útil contar con una autorización por escrito por parte del afectado.

■ **Involucre a las personas:**

Deben ser informadas diferentes personas acerca del abuso para que puedan ayudar en el tema. Esto incluye a las gerencias de recursos humanos, legal, de relaciones públicas y de negocios del supuesto "insider".

■ **Reunión:**

Un gerente de RRHH debe reunirse con el supuesto insider para explicarle lo que se ha encontrado y lo que sucederá. Puede ser necesario el apoyo de personas jurídicas, técnicas y de gerencia.

■ **Disminución de privilegios:**

Si se permite que el supuesto insider permanezca en el trabajo hasta el final de la investigación, proporciónele una computadora con autorizaciones mínimas.

■ **Congelamiento de autorización**:

Suspenda el acceso y las autorizaciones del supuesto insider. Esto debe incluir el acceso a la aplicación. Esto también puede incluir la cuenta del sistema, llaves y el "badge" o tarjeta de identificación.

■ **Acceso remoto:**

Suspenda la capacidad de acceso remoto, es decir: smartphones, cuentas VPN, tokens, etc.

■ **Incautación:**

Incaute todo dispositivo de computación de uso laboral del presunto insider.

Remedio 4

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

La parte de remediación es bastante limitada en caso de abuso de información privilegiada. Se pueden considerar las siguientes acciones, según el caso:

■ Tome medidas disciplinarias contra el empleado malintencionado (o rescinda el contrato) y retire todas sus credenciales.

■ Elimine todas las operaciones ficticias o fraudulentas hechas por el "insider"

■ Revise todos los programas o scripts hechos por el insider y retire todo código innecesario

Recuperación 5

Objetivo: Restaurar el sistema a las operaciones normales.

Si el incidente aún no se ha hecho público, asegúrese de advertir a todos los actores afectados (clientes, socios interesados, etc.) y a las autoridades requeridas. En el caso de grandes impactos, esta comunicación debe ser hecha por la Alta Dirección.

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

Repercusiones 6

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

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 # 12

Abuso de "insider"

Tratar con información interna divulgada intencionalmente

Autor IRM: CERT SG / David Bizeul
Versión IRM: 1.0
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