METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #14 ESTAFA FRAUDULENTAS (SCAMS)

Una guía práctica diseñada para gestionar incidentes de estafas fraudulentas (scams).

Autor IRM: CERT SG
Contribución: CERT a Dvens / Paloma Vargas
Versión del IRM: 2.0
E-Mail: cert.sg@socgen.com
Web: https://cert.societegenerale.com
Twitter: @CertSG

Traducción al Español

Paloma Amilene Vargas Alvarado
E-Mail: amilenhalvarado@gmail.com
Twitter / X: @AmileneVargas

CONTENIDO

1. ABSTRACTO

Esta metodología de respuesta a incidentes, es una hoja de consulta dedicada a los encargados que investigan un problema preciso de seguridad.

¿QUIÉN DEBE UTILIZAR HOJAS IRM?

- Administradores.
- Centro de Operaciones de Seguridad.
- CISO y adjuntos.
- CERT (Equipo de respuesta ante emergencias informáticas).

Recuerde: Si se enfrenta a un incidente, siga el IRM y tome notas. **Mantenga la calma** y, si es necesario, contacte inmediatamente con el equipo de Respuesta a Incidentes o el CERT de su línea de negocio.

2. PASOS PARA LA GESTIÓN DE INCIDENTES

SE DEFINEN 6 PASOS PARA GESTIONAR INCIDENTES DE SEGURIDAD

1. **Preparación**: prepárese para manejar el incidente
2. **Identificación**: detectar el incidente
3. **Contención**: limitar el impacto del incidente
4. **Remediación**: eliminar la amenaza
5. **Recuperación**: recuperarse a una etapa normal
6. **Lecciones aprendidas**: elaborar y mejorar el proceso

IRM proporciona información detallada para cada paso del proceso de respuesta a incidentes. Los pasos provienen de la Guía de Gestión de Incidentes de Seguridad Informática del NIST.

2.1 PREPARACIÓN

OBJETIVO: ESTABLECER CONTACTOS, DEFINIR PROCEDIMIENTOS, REUNIR INFORMACIÓN PARA AHORRAR TIEMPO DURANTE UN INCIDENTE.

- Crea una lista de todos los dominios legítimos que pertenecen a tu empresa. Esto ayudará a analizar la situación y prevenir que comiences un procedimiento de eliminación en un sitio web legítimo “olvidado”.
- Prepara una página web alojada en tu infraestructura, lista para publicarse en cualquier momento, para advertir a tus clientes sobre un gran ataque de estafa en curso. Prepara y prueba también un procedimiento de implementación claro.
- Prepara formularios de correo electrónico para la eliminación de contenido. Los usarás en cada caso de estafa fraudulenta, si es posible, en varios idiomas. Esto acelerará el proceso al intentar contactar a compañías operadoras de Internet durante el procedimiento de eliminación.
- Ten varias formas de ser contactado de manera oportuna (24/7 si es posible):
    - Dirección de correo electrónico, fácil de recordar por todos (ej: security@tueempresa).
    - Formularios web en el sitio web de tu empresa (la ubicación del formulario es importante, no más de 2 clics desde la página principal)
    - Cuenta de Twitter visible.
- Implementa DKIM, DMARC y SPF en toda la cadena de correos.

Contactos.

- Mantén una lista de todas las personas autorizadas para tomar decisiones sobre ciberdelitos y posibles acciones respecto al tema. Si es posible, establece un contrato con procesos claros.
- Establece y mantén una lista de contactos para la eliminación de contenido en:
    - Compañías de hosting.
    - Registradores.
    - Compañías registradoras
    - Proveedores de correo electrónico.
- Establece y mantiene contactos en CERTs a nivel mundial, ellos probablemente siempre podrán ayudar si se les involucra.

Aumente la conciencia del cliente.

No espere a que ocurran incidentes de estafa para comunicarse con sus clientes. Aumente la conciencia sobre varios tipos de fraudes (estafa de lotería, estafa 419, etc.), explique en qué consisten y asegúrese de que sus clientes sepan que usted nunca los contactará por correo electrónico para asuntos de este tipo.

2.2 IDENTIFICACIÓN

OBJETIVO: DETECTAR EL INCIDENTE, DETERMINAR SU ALCANCE E INVOLUCRAR A LAS PARTES APROPIADAS.

Advertencia: Utilice un equipo corporativo dedicado para identificar o intercambiar información con el estafador, no use su equipo personal.

Detección de estafas fraudulentas.

- Monitoree de cerca todos sus puntos de contacto (correo electrónico, formularios web, etc.).
- Monitoree dominios cybersquatted y el contenido publicado en ellos. Recoja información de contacto y de abuso para estar preparado en caso de que necesite usarlos.
- Monitoree cuentas de redes sociales que usurpen a la alta dirección o su marca registrada.
- Implemente trampas de spam y trate de recopilar spam de socios/terceros. ▪ Implemente monitoreo activo de repositorios de estafas, como 419scam, por ejemplo.
- Monitoree cualquier lista de correo especializada a la que tenga acceso, o cualquier fuente RSS/Twitter, que pueda reportar cartas de estafa.

Utilice sistemas de monitoreo automatizados en todas estas fuentes, de modo que cada detección genere una alarma para reaccionar de inmediato.

Involucre a las partes correspondientes.

- Tan pronto como se detecte una campaña de estafa, contacte a las personas de su empresa que estén acreditadas para tomar una decisión, si no es usted.
- La decisión de actuar sobre la dirección de correo electrónico fraudulenta debe tomarse lo antes posible, en cuestión de minutos.

Recolecte evidencia.

Obtenga muestras de los correos electrónicos fraudulentos enviados por los estafadores. Tenga cuidado de recolectar los encabezados de los correos además del contenido del mismo. Recoja varios correos electrónicos, si es posible, para verificar la verdadera dirección IP del remitente. Esto ayudará en la investigación, analizando si la campaña se envía desde una sola máquina o desde un botnet.

Si se siente inseguro al recolectar los encabezados de los correos electrónicos, consulte http://spamcop.net/fom-serve/cache/19.html

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

- Difundir el contenido del correo electrónico fraudulento en sitios web/herramientas/partners de reporte de spam/fraude.
- Comunicarte con tus clientes.
- Agregar las URL en tu DNS Blackhole, proxies y lista de bloqueo del firewall.

Desplegar la página de alerta/advertencia con información sobre el ataque de estafa actual si la marca está afectada.

En caso de que seas afectado varias veces por semana, no siempre despliegues un mensaje de alerta/advertencia, sino más bien una página muy informativa sobre la estafa, para aumentar la conciencia.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA DETENERLA CAMPAÑA DE PHISHING.

- En caso de que las páginas de phishing fraudulentas estén alojadas en un sitio web comprometido, **intenta contactar al propietario del sitio web**. Explícale claramente el fraude al propietario, para que tome las medidas apropiadas: eliminar el contenido fraudulento y, sobre todo, mejorar la seguridad del mismo, para que el estafador no pueda regresar utilizando la misma vulnerabilidad.
- En cualquier caso, contacta también a la empresa de alojamiento del sitio web. Envía correos electrónicos a las direcciones de **contacto de la empresa de alojamiento** (generalmente hay un abuse@hostingcompany) y luego intenta hablar con alguien por teléfono, para acelerar las cosas.
- **Contacte a la empresa de alojamiento de correo electrónico** para cerrar la cuenta fraudulenta del estafador. No olvide enviarles una copia del correo electrónico fraudulento.
- **Contacte al equipo de abuso de redes sociales** para eliminar cuentas fraudulentas.
- **Bloquee el intercambio de correos electrónicos** con esta empresa o persona.

En caso de que no recibas respuesta o no se tomen medidas, **vuelve a llamar y envía correos electrónicos de forma regular.**

Si la eliminación es demasiado lenta, **contacta con un CERT local en el país involucrado**, que podría ayudar a eliminar el fraude, y explícales las dificultades que enfrentas.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Evaluar el final del caso.

- Asegurarse de que la dirección de correo electrónico fraudulenta haya sido cerrada.
- Si hay algún sitio web fraudulento asociado al fraude, seguir monitoreándolo.
- Al final de una campaña de estafa fraudulenta, eliminar la página de advertencia asociada de su sitio web.

2.6 LECCIONES APRENDIDAS

OBJETIVO: DOCUMENTAR LOS DETALLES DEL INCIDENTE, DISCUTIR LAS LECCIONES APRENDIDAS Y AJUSTAR LOS PLANES Y LAS DEFENSAS.

Informe

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores del incidente.

Se deberán describir los siguientes temas:

- Causa inicial de la infección
- Acciones y cronogramas de cada evento importante
- ¿Qué salió bien?
- ¿Qué salió mal?
- Costo del incidente
- Indicadores de compromiso

Capitalizar

- Considera qué pasos de preparación, podrías haber tomado para responder al incidente más rápido o de manera más eficiente.
- Actualiza tus listas de contactos y agrega notas sobre cuál es la forma más efectiva de contactar a cada parte involucrada.
- Considera qué relaciones dentro y fuera de tu organización podrían ayudarte con futuros incidentes.
- Colabora con los equipos legales si se requiere una acción legal.

3. DEFINICIONES

CONCEPTO	DESCRIPCIÓN
IRM	Metodología de Respuesta a Incidentes
CISO	Chief Information Security Officer (ejecutivo responsable de la seguridad de la información)
CERT	Equipo de Respuesta a Emergencias Informáticas.
CSIRT	Equipo de respuesta a Incidentes de Seguridad, implícito como sinónimo/similar a CERT en la accesión de red phone.
NIST	Instituto Nacional de Estándares y Tecnología
TLP	Indica que la información puede ser distribuida sin restricciones
DLP	Una herramienta que, si está presente en la empresa, puede proporcionar información valiosa a los gestores de incidentes que trabajan en la fuga de información.
Phishing al Cliente	El tema específico del incidente de seguridad tratado por esta metodología IRM #13.
Takedown	El procedimiento para eliminar o dar de baja sitios web o contenidos fraudulentos.
Cybersquatting	La monitorización de dominios registrados de forma abusiva (similares a los legítimos) y el contenido publicado en ellos.
DKIM, DMARC, SPF	Mecanismos de autenticación de correo electrónico que deben implementarse en toda la cadena de correo para prevenir el phishing.
Spam traps	Mecanismos utilizados para desplegar y recopilar spam, a menudo para identificar nuevas campañas de phishing.
Phishing Repositories	Bases de datos activas de monitoreo de phishing, como Phish Tank y Google Safe Browsing, que deben ser consultadas para detectar casos.
Credential Dropping System	El sistema utilizado por el atacante para recibir las credenciales robadas, que puede ser una dirección de correo electrónico, un bot de Telegram, etc.

Handlers	Personas dedicadas a investigar un problema de seguridad preciso, quienes deben usar las hojas IRM.
Abuse Contact	Las direcciones de contacto estándar (ej. abuse@hostingcompany) utilizadas para solicitar un takedown a la empresa de alojamiento.