METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #13 PHISHING A CLIENTES

Guías para gestionar incidentes de phishing a clientes.

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 pertenecientes a tu empresa. Esto ayudará a analizar la situación y evitará que inicies un procedimiento de takedown (eliminación) en un sitio web legítimo olvidado.
- Prepara una página web alojada en tu infraestructura, lista para ser publicada en cualquier momento, para advertir a tus clientes sobre un ataque de phishing en curso. Prepara y prueba un procedimiento de despliegue claro también.
- Prepara formularios de correo electrónico para takedown. Los usarás para cada caso de phishing, si es posible, en varios idiomas. Esto acelerará las cosas al intentar contactar a la empresa de alojamiento, etc., durante el proceso de takedown.
- Implementa DKIM, DMARC y SPF en toda la cadena de correo.
- Monitorea los dominios con cybersquatting y el contenido publicado en ellos. Reúne información de contacto y de abuso para estar preparado en caso de que necesites usarlos.

Contactos Internos.

- Mantén una lista de todas las personas involucradas en el registro de nombres de dominio en la empresa.
- Mantén una lista de todas las personas acreditadas para tomar decisiones sobre ciberdelincuencia y posibles acciones relacionadas con el phishing. Si es posible, ten un contrato que mencione que puedes tomar decisiones.

Contactos Externos.

- Ten varias formas de ser contactado de manera oportuna (24/7 si es posible):
  - Dirección de correo electrónico, fácil de recordar para todos (ej: security@yourcompany).
  - 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.
- Establece y mantén una lista de contactos de takedown en:
  - Empresas de alojamiento (Hosting companies).
  - Empresas de registro (Registry companies).
  - Proveedores de correo electrónico (E-Mail providers).
- Establece y mantén contactos en CERTs a nivel mundial, probablemente siempre podrán ayudar si es necesario

Concientización del Cliente.

No esperes a los incidentes de phishing para comunicarte con tus clientes. Concientiza sobre el fraude de phishing, explica qué es el phishing y asegúrate de que tus clientes sepan que nunca les pedirás credenciales/información bancaria por correo electrónico o por teléfono.

Concientización de la Línea de Negocio.

Las personas en las líneas de negocio deben ser conscientes de los problemas de phishing y considerar la seguridad como una prioridad. Por lo tanto, deben aplicar buenas prácticas como evitar enviar enlaces (URL) a los clientes y utilizar una firma que indique que la empresa nunca les pedirá credenciales/información bancaria en línea.

2.2 IDENTIFICACIÓN

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

Detección de Phishing.

- Monitorea de cerca todos tus puntos de contacto (correo electrónico, formularios web, etc.).
- Implementa trampas de spam y trata de recopilar spam de socios/terceros.
- Implementa la monitorización activa de repositorios de phishing, como Phish Tank y Google Safe Browsing, por ejemplo.
- Monitorea cualquier lista de correo especializada a la que puedas tener acceso, o cualquier fuente RSS/Twitter, que pueda estar reportando casos de phishing.
- Utiliza sistemas de monitorización automatizados en todas estas fuentes, de modo que cada detección active una alarma para una reacción instantánea.
- Monitorea tus registros web. Verifica que no haya un referente sospechoso que dirija a las personas a tu sitio web. Este suele ser el caso cuando los sitios web de phishing llevan al usuario al sitio web legítimo después de haber sido engañado.

Involucrar a las partes apropiadas.

Tan pronto como se detecte un sitio web de phishing, contacta a las personas de tu empresa que estén acreditadas para tomar una decisión, si no eres tú.
La decisión de actuar sobre el sitio web/dirección de correo electrónico fraudulento debe tomarse lo antes posible, en cuestión de minutos.

Recolección de evidencia.

Haz una copia con marca de tiempo de las páginas web de phishing. Utiliza una herramienta eficiente para hacerlo, como HTTrack por ejemplo. No olvides tomar todas las páginas del esquema de phishing, no solo la primera si hay varias. Si es necesario, toma capturas de pantalla de las páginas.
Revisa el código fuente del sitio web de phishing:

- Revisa dónde se exportan los datos: ya sea a otro contenido web al que no puedes acceder (generalmente un script PHP), enviado por correo electrónico al estafador o utilizando una API de aplicación (como Telegram, por ejemplo).
- Reúne información sobre el actor de phishing que pueda estar disponible en la URI, el código fuente y el sistema de depósito de credenciales (direcciones de correo electrónico, bots de Telegram, etc.).
- ¿Los gráficos provienen de uno de tus sitios web legítimos o están almacenados localmente?

Si es posible, en caso de que los gráficos se tomen de uno de tus propios sitios web, podrías cambiar los gráficos para mostrar un logotipo de "SITIO WEB DE PHISHING" en la página del estafador.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

Difundir la URL del ataque en caso de un sitio web de phishing:

Utiliza todas las formas que tengas para difundir la URL fraudulenta en todos los navegadores web: usa las opciones de Internet Explorer, Chrome, Safari, Firefox, la barra de herramientas Netcraft, Phishing-Initiative, etc.
Esto evitará que los usuarios accedan al sitio web mientras trabajas en la fase de remediación.

Difunde el contenido del correo electrónico fraudulento en sitios web/socios de denuncia de spam.

Comunícate con tus clientes:

Despliega la página de alerta/advertencia con información sobre el ataque de phishing actual.

En caso de que te veas impactado varias veces a la semana, no siempre despliegues un mensaje de alerta/advertencia, sino más bien una página de phishing muy informativa para crear 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.

- Contacta a la empresa de alojamiento de correo electrónico para cerrar las cuentas fraudulentas que reciben las credenciales robadas o la información de la tarjeta de crédito (ya sea en un caso de phishing "solo por correo electrónico" o en uno habitual, si lograste obtener la dirección de correo electrónico de destino).

- En caso de que haya una redirección (el enlace contenido en el correo electrónico a menudo va a una URL de redireccionamiento), también retira la redirección contactando a la empresa responsable del servicio.

- En caso de que no obtengas respuesta, o no se tome ninguna medida, no dudes en volver a llamar y enviar correos electrónicos de forma regular.

- Si el takedown es demasiado lento, contacta a un CERT local en el país involucrado, que podría ayudar a eliminar el fraude.

2.5 RECUPERACIÓN

OBJETIVO: RESTAURAR EL SISTEMA A SUS OPERACIONES NORMALES.

Evaluar el fin del caso de phishing.

- Asegúrate de que las páginas fraudulentas y/o la dirección de correo electrónico estén caídas.
- Sigue monitoreando la URL fraudulenta. A veces, un sitio web de phishing puede reaparecer horas más tarde. En caso de que se utilice una redirección y no se elimine, monitoréala muy de cerca.
- Al final de una campaña de phishing, elimina la página de advertencia asociada de tu sitio web.

2.6 LECCIONES APRENDIDAS

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

Informe a su jerarquía, subsidiarias y socios para compartir las mejores prácticas aplicadas en este incidente y hacer cumplir reglas similares en otras ubicaciones.

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.