MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUÍA DE ACCIÓN ANTE INCIDENTES DE PHISHING

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

Phishing

Estafa cibernética en la cual el atacante intenta conseguir información confidencial de usuarios por medio de la suplantación de identidad de una entidad de confianza.

Detalles: el término "phishing" proviene de la combinación de las palabras "password" (contraseña) y "fishing" (pesca), haciendo alusión al acto de "pescar" información confidencial de las víctimas.

Además del *phishing* tradicional existe el *phishing* dirigido (*spear phishing*), el cual se encuentra orientado a una organización u organizaciones determinadas, más concretamente a uno o varios miembros que trabajan dentro de la organización, donde pueden llegar a suplantar a alguno de ellos o proveedor que trabaje con la misma. Se trata de un ataque mucho más elaborado y personalizado ya que se realiza una investigación previa para recopilar toda la información posible de las víctimas, por lo que el porcentaje de éxito es mayor.

Los principales motivos detrás de un phishing dirigido pueden ser robo de información, motivaciones políticas, reivindicaciones, venganza, extorsión, daños en la imagen de la organización, fines activistas, entre otros.
Los atacantes de phishing suelen utilizar métodos como correos electrónicos fraudulentos, mensajes de texto, llamadas telefónicas o sitios web falsificados para engañar a las personas. Estos mensajes o sitios web falsos suelen tener una apariencia muy similar a los de las organizaciones legítimas, como bancos,

empresas, redes sociales u otras instituciones reconocidas. Los atacantes intentan convencer a los usuarios de que proporcionen sus datos personales o financieros al hacerles creer que están interactuando con una entidad de confianza (ingeniería social).

Impacto

El phishing es una forma de fraude muy común y puede tener consecuencias graves, como el robo de identidad, pérdida financiera o acceso no autorizado a cuentas en línea.

1. Fase de Identificación

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciber incidente que pueda sufrir un organismo o entidad, y notificarlo a la brevedad para tomar acciones ante el incidente.

- ✓ Identificar qué persona o personas han sufrido el phishing dirigido.
- ✓ Desconfiar de peticiones inusuales que se salgan del procedimiento habitual independientemente de quien las solicite.
- ✓ Comprobar las direcciones de correo electrónico, teléfono o similares, para verificar la procedencia de estos.

- ✓ Notificar al equipo de sistemas y el equipo de relaciones públicas sobre cualquier correo electrónico, formulario web o llamada telefónica sospechosa, para coordinar la respuesta y garantizar una acción rápida.
- ✓ Recopilar información sobre el incidente, como la dirección de correo electrónico o el sitio web utilizado para el phishing, el contenido del mensaje y cualquier otra información relevante.
- ✓ Notificar al equipo de respuesta a incidentes de seguridad (CSIRT) de la organización o al equipo de seguridad de la empresa.
- ✓ Notificar a los usuarios afectados y proporcionar instrucciones claras sobre cómo manejar los mensajes de phishing, cómo cambiar las contraseñas y cómo informar sobre posibles incidentes adicionales.

2. Fase de Contención

La máxima prioridad en esta fase es contener el impacto negativo que pueda sufrir la organización a causa del phishing.

Evaluación de la situación:

- ✓ Obtener toda la información posible sobre el ataque: o Realizar una copia del correo electrónico sospechoso, manteniendo las cabeceras.
- ✓ Tomar evidencias gráficas, como capturas de pantalla de las páginas sospechosas.

- ✓ Analizar el contenido del mensaje de phishing y evaluar si existe algún riesgo adicional, como enlaces maliciosos o archivos adjuntos infectados.
- ✓ Realizar un análisis forense de los mensajes de phishing y los sitios web falsos para identificar la fuente y los métodos utilizados por los atacantes.
- ✓ Examinar los registros de correo electrónico, registros del servidor web y cualquier otro registro o archivo relevante para obtener más información sobre la campaña de phishing.
- ✓ Determinar el alcance del incidente de phishing.
- ✓ Documentar y recopilar todas las pruebas disponibles, como copias de los correos electrónicos de phishing, capturas de pantalla del sitio web falso y cualquier otro dato relacionado.
- ✓ Realizar copias de respaldo de la evidencia recopilada para su posterior análisis y referencia.

Contención

- ✓ No descargar ni ejecutar ningún archivo adjunto sospechoso.
- ✓ Tratar de contactar con el “emisor” mediante un medio alternativo conocido, empleando datos de contacto confiables (correo electrónico, teléfono de contacto, etc.).

3. Fase de Mitigación

- ✓ Una vez recopilada y analizada la información obtenida en la fase de contención, deben tomarse medidas reactivas para gestionar el incidente.
- ✓ Alertar a la organización sobre la existencia de una posible campaña de phishing dirigido, para que todos los miembros estén al corriente, junto con unas pautas a seguir ante este ataque.
- ✓ Identificar y bloquear los sitios web, direcciones IPs y/o direcciones de correo electrónico utilizados para el phishing, para evitar la propagación.
- ✓ Interactuar con los proveedores de servicios de correo electrónico y sitios web para informar sobre el incidente y solicitar el bloqueo de los dominios o direcciones involucrados.
- ✓ En función del medio por el que hemos sufrido el phishing dirigido:
  - Formulario web al que hemos accedido a través de una URL:
  - Filtrar las URL maliciosas
- ✓ Llamada telefónica:
  - Bloquear las llamadas provenientes de ese número. En caso de que no sea posible, no atender las llamadas.

    Correo electrónico:
  - Filtrar la dirección de correo electrónico o la IP de origen del servidor de correo de donde provienen los emails sospechosos.
- ✓ En caso de que algún usuario de la organización haya ejecutado o abierto un archivo adjunto:

- Aislar el dispositivo.
- Notificar al equipo de sistemas de la organización para que realicen labores de investigación y desinfección.

✓ En caso de sospecha sobre credenciales comprometidas, restablecerlas y asegurar que los usuarios utilicen contraseñas fuertes y únicas

4. Fase de Recuperación

La finalidad de la fase de recuperación consiste en devolver el nivel de operación a su estado normal y que las áreas de negocio afectadas puedan retomar su actividad. Es importante buscar cualquier signo de actividad sospechosa en los servicios afectados y monitorizarlos temporalmente.

✓ Si se dispone de un equipo legal, coordinarse con éste para tener en cuenta las posibles consecuencias legales y de reputación.

✓ Determinar las posibles consecuencias económicas.

✓ Realizar una revisión exhaustiva de las medidas de seguridad existentes, como autenticación de dos factores, filtros de correo electrónico y sistemas de detección de intrusiones.

5. Fase Post- Incidente

Una vez que el ciber incidente está controlado y la actividad ha vuelto a la normalidad, es necesario reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciber incidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de lo sucedido y que se puedan tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

6. Lecciones aprendidas

- ✓ Realizar una revisión post-incidente para identificar las lecciones aprendidas y las áreas de mejora en las políticas.
- ✓ Proporcionar capacitación en seguridad a los empleados para aumentar la conciencia sobre los riesgos asociados con el phishing, además de brindar pautas para identificar y evitar dichos mensajes.

7. Diagrama de flujo