METODOLOGÍA DE RESPUESTA A INCIDENTES

IRM #16 PHISHING

Directrices para manejar y responder ataques de phishing dirigidos a colaboradores.

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 referencia dedicada a los encargados de manejar e investigar 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

2.1 **Preparación**: prepárese para manejar el incidente

2.2 **Identificación**: detectar el incidente

2.3 **Contención**: limitar el impacto del incidente

2.4 **Remediación**: eliminar la amenaza

2.5 **Recuperación**: recuperarse a una etapa normal

2.6 **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.

Acciones de Preparación.

- Prepara una comunicación lista para ser publicada en cualquier momento, para advertir a tus colaboradores sobre un ataque de phishing en curso. Prepara y prueba un procedimiento de despliegue claro.
- Despliega DKIM, DMARC y SPF en toda la cadena de correo.
- Implementa mecanismos de autenticación multifactor.
- Monitoriza dominios cybersquatted (ocupados ilícitamente) y el contenido publicado en ellos. Recopila información de contacto y de abuso para estar preparado en caso de que necesites utilizarlos.

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 acciones eventuales 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@tuempresa).
    - Formularios web en el sitio web de tu empresa (la ubicación del formulario es importante, no más de 2 clics de distancia de la página principal).
    - Cuenta de Twitter visible.
- Establece y mantén una lista de contactos para la retirada (takedown) en:
    - Empresas de alojamiento (hosting).
    - Empresas de registro (registry).
    - Proveedores de correo electrónico.
- Establece y mantén contactos en CERTS a nivel mundial, probablemente siempre podrán ayudar si es necesario

Concienciación 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.

Concienciación 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 el envío de enlaces (URL) a los clientes y utilizar una firma que indique que la empresa nunca les pedirá credenciales/información bancaria en línea.
- Ejecuta campañas periódicas de phishing de concienciación.
- Despliega una solución técnica que permita a los colaboradores reportar fácilmente correos electrónicos a los equipos de seguridad.
- Establece procedimientos específicos para el análisis de archivos adjuntos y URLs.

2.2 IDENTIFICACIÓN

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

Detección de Phishing.

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

Determinación del Alcance del Ataque de Phishing.

- Determina el número de usuarios objetivo.
- Busca cuentas comprometidas explotadas e identifica actividades maliciosas relacionadas.

Analiza el Phishing.

Recuerda seguir los procedimientos de análisis establecidos.

- Determina:
  - Si es una campaña de recolección de credenciales (credential harvesting) o una campaña de propagación de malware.
  - Si es una campaña dirigida o no.
- Inspecciona el asunto y el cuerpo del mensaje.
- Utiliza un entorno de sandbox para analizar archivos adjuntos maliciosos y extraer IOCs (Indicadores de Compromiso)
- Analiza enlaces, dominios y nombres de host con servicios de inteligencia de amenazas.
- Verifica el código fuente del sitio web de phishing.
- Investiga los encabezados del correo electrónico en busca de artefactos interesantes: servidor de origen e información del remitente, por ejemplo.

Recolección de Evidencia.

Haz una copia con marca de tiempo de las páginas web de phishing. Utiliza una herramienta eficiente para ello, como HTTrack, por ejemplo.
No olvides tomar cada página del esquema de phishing, no solo la primera si hay varias. Si es necesario, toma capturas de pantalla de las páginas.
Si la campaña de phishing está distribuyendo malware, debes consultar el IRM 7 Detección de Malware de Windows.

2.3 CONTENCIÓN

OBJETIVO: MITIGAR LOS EFECTOS DEL ATAQUE EN EL ENTORNO.

- Bloquea los IOCs de red descubiertos a través del análisis de archivos adjuntos / URLs en DNS, firewalls o proxies.
- Bloquea la campaña de phishing basándote en remitentes, asuntos u otros artefactos de correo electrónico a través de la puerta de enlace de correo (email gateway).
- Intenta eliminar los correos electrónicos de phishing de la bandeja de entrada.
- Aplica DNS Sinkhole en la URL sospechosa (opcional, dependiendo de la arquitectura de DNS).
- Comunícate con tus colaboradores.
- Despliega la página de alerta/advertencia con información sobre el ataque de phishing actual.

2.4 REMEDIACIÓN

OBJETIVO: TOMAR ACCIONES PARA DETENER LA CAMPAÑA DE PHISHING.

- Cambia y/o bloquea temporalmente las credenciales de inicio de sesión de las cuentas comprometidas.

Si la campaña de phishing fue dirigida, considera contactar a las autoridades y a los reguladores.
Puedes considerar contactar a tu CERT local.

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 fuera de servicio (down).
- Sigue monitorizando 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, monitorízala 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

Se debe redactar un informe de crisis y ponerlo a disposición de todos los actores de la célula de gestión de crisis.

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 añade 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 lega

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 Incidentes Informáticos
NIST	Instituto Nacional de Estándares y Tecnología
EDR	Detección y Respuesta de Puntos de Acceso
IDS	Sistema de Detección de Intrusiones
DKIM (DomainKeys Identified Mail)	Un método de autenticación de correo electrónico que permite al receptor verificar que un correo electrónico supuestamente proveniente de un dominio específico fue autorizado por el propietario de ese dominio.
DMARC (Domain-based Message Authentication, Reporting, and Conformance)	Un protocolo de validación de correo electrónico que utiliza SPF y DKIM para determinar la autenticidad de un mensaje de correo electrónico.
SPF (Sender Policy Framework)	Un sistema de validación de correo electrónico diseñado para prevenir la suplantación de identidad (spoofing) del remitente.
Monitoreo de Dominios Cybersquatted	La vigilancia de dominios que han sido registrados de forma ilícita, a menudo con la intención de confundir a los usuarios y usarlos para phishing.
Repositorios de Phishing	Bases de datos y servicios que rastrean y almacenan información sobre sitios web de phishing activos o reportados.
IOCs (Indicadores de Compromiso)	Evidencias forenses, como hashes de archivos, direcciones IP o nombres de dominio, que indican que un sistema ha sido comprometido por un ataque o malware.
Entorno Sandbox	Un mecanismo de seguridad para ejecutar programas o analizar archivos adjuntos de correo electrónico maliciosos en un ambiente aislado y controlado, lo que previene que afecten al sistema operativo del usuario.

HTTrack	Se menciona como una herramienta para hacer una copia con marca de tiempo de las páginas web de phishing.
Análisis de Encabezados de Correo Electrónico (Email Headers)	La investigación de los metadatos detallados adjuntos a un correo electrónico para rastrear su origen y otra información del remitente, como el servidor de origen.
Bloqueo de IOCs de Red	La acción de configurar dispositivos de seguridad (como firewalls, proxies o DNS) para denegar el acceso a direcciones IP, dominios o URLs identificadas como maliciosas.
DNS Sinkhole	Una técnica de seguridad que redirige el tráfico de un nombre de dominio malicioso (como una URL de phishing o un servidor de Comando y Control) a una dirección IP segura o no enrutable controlada por el equipo de respuesta, lo que detiene la conexión maliciosa.