Preparación 1

Objetivo: Establecer contactos, definir procedimientos, reunir información para ahorrar tiempo durante un ataque.

Cree una lista de todos los dominios legítimos que pertenecen a su organización. Esto le ayudará a analizar la situación y evitar que se inicie un procedimiento de baja de un sitio web olvidado pero legítimo.

Prepare una página web alojada en su infraestructura, alístela para ser publicada en cualquier momento para advertir a sus clientes sobre un ataque de phishing en curso. Prepare y pruebe un procedimiento claro de implementación.

Prepare un texto o formato de pedido de baja, si es posible en varios idiomas. Lo va a utilizar para todos los casos de phishing. Esto acelerará las cosas cuando se trate de llegar a la empresa de hosting durante el proceso de baja del sitio fraudulento.

Contactos internos
Mantenga una lista de todas las personas involucradas en los registros de nombres de dominio de su organización.

Mantenga una lista de todas las personas acreditadas para tomar decisiones sobre la ciberdelincuencia y la eventual acción sobre phishing. Si es posible, tener un contrato de mencionar que usted puede tomar decisiones.

Contactos externos
Tenga varias maneras de ser contactados de manera oportuna (24/7 si es posible):

- Dirección de email fácil de recordar por todos (por ejemplo: seguridad @ suorganizacion)
- Un formulario web en el sitio web de su organización (la ubicación del formulario es importante, no más de 2 clics de distancia de la página principal)
- Cuenta Twitter visible

Establezca y mantenga una lista de contactos para pedir bajas con:

- Proveedores de hosting
- Registadores de dominios
- Proveedores de correo electrónico

Establezca y mantenga contactos en los CERT a nivel mundial, ellos estarán siempre dispuestos a ayudar si es necesario.

Sensibilice al cliente
No espere que sucedan incidentes de phishing para comunicarse con sus usuarios. Cree conciencia sobre el fraude de phishing, explique qué es el phishing y asegúrese de que sus usuarios sepan que usted nunca va a pedirles credenciales / información sensible por e-mail o por teléfono.

Identificación 2

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

Detección de Phishing

- Controle de cerca todos los puntos de contacto (e-mail, formularios web, etc.)
- Implemente trampas de spam y trate de reunir el spam desde asociados o terceros.
- Implemente vigilancia activa de repositorios de phishing, como por ejemplo AA419 o PhishTank.
- Monitoree cualquier lista de correo especializadas a la que tenga acceso, o algún “feed” RSS / Twitter, que le informe sobre casos de phishing.
- Utilice sistemas automatizados de control de todas estas fuentes, de modo que cada detección active una alarma para tener reacción inmediata.
- Controle los logs de web. Compruebe que no hay referentes sospechosos que traen visitantes a su sitio web. Este suele ser el caso cuando los sitios web de phishing dirigen al usuario a la página web legítima después de haber sido engañado.

Involucre a las partes correspondientes
Tan pronto como detecte una página web de phishing, póngase en contacto con las personas en su empresa que estén acreditados para tomar una decisión, si no es usted.
La decisión de actuar en la página web o e-mail fraudulentos debe tomarse tan pronto como sea posible, en cuestión de minutos.

Reuna evidencia
Haga una copia con fecha y hora de las páginas web de phishing. Utilice una herramienta eficaz para hacer eso, como por ejemplo HTTrack. No olvide de tomar todas las páginas del sistema de phishing, no sólo la primera, si hay varias. Si es necesario, haga capturas de pantalla de las páginas.

Contención 3

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

- Difunda la URL de ataque en el caso de un sitio web de phishing.
  Utilice todos las formas que tenga de difundir la URL fraudulenta en todos los navegadores web: utilice las opciones de Internet Explorer, Chrome, Safari, Firefox, la barra de herramientas Netcraft, Phishing-Initiative, etc.
  Esto evitará que sus usuarios accedan a la página web mientras se trabaja en la fase de rehabilitación.
- Difunda el contenido del correo electrónico fraudulento en sitios web / asociados informe de spam.
- Comuníquese con sus clientes.

Despliegue la página de advertencia/alerta con la información sobre el ataque de phishing en curso.
En caso de que se vea afectado varias veces a la semana, no solamente despliegue un mensaje de alerta, sino una página de alerta de phishing muy informativa para aumentar la concienciación.

Revise el código fuente del sitio web de phishing.

- Vea hacia donde se envían los datos: ya sea a otro contenido de la web que no se puede acceder (un script PHP por lo general), o si se envia por correo electrónico a los autores del fraude.
  - Mire cómo se ha construído la página de phishing. ¿Los gráficos vienen de una de su sitio web legítimo, o se almacenan localmente?
  - Si es posible, en el caso de que se estén tomando los gráficos de uno de sus propios sitios web, puede cambiar los gráficos para mostrar un logotipo de "sitio de phishing" en la página del defraudador.

Remedio 4

Objetivo: Adoptar medidas para detener el fraude.

En caso que las páginas de phishing fraudulentas estén alojadas en un sitio web comprometido, trate de ponerse en contacto con el propietario del sitio web. Explíquele claramente el fraude al propietario, de manera que él tome las acciones adecuadas: eliminar el contenido fraudulento, y sobre todo mejora la seguridad del sitio, para que el estafador no pueda volver la misma vulnerabilidad.

En todo caso, contacte también a la empresa de alojamiento de la página web. Envíe mensajes de correo electrónico a las direcciones de contacto de la empresa de alojamiento (generalmente hay una abuse @ empresaalojamiento) luego trate de contactar a 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 información de tarjetas de crédito (ya sea un caso de phishing de “sólo e-mail" o uno habitual, si usted consiguió averiguar la dirección de email destino).

En caso de redirección, (el enlace en el e-mail va a menudo redirigida a una URL) baje la redirección poniéndose en contacto con la empresa responsable del servicio.
En caso de que no obtenga respuesta, o no toman medidas, no dude en llamar y enviar mensajes de correo electrónico regularmente, cada dos horas, por ejemplo.

Si la baja de servicio es demasiado lenta, póngase en contacto con un CERT local en el país en cuestión, lo que podría ayudar a desarmar el fraude.

Recuperación 5

Objetivo: Volver al estado previo de funcionamiento.

- Evalúe el final del caso de phishing
- Asegúrese que las páginas fraudulentas y/o dirección de correo electrónico no funcionen.
- Mantenga el control de la URL fraudulenta. A veces un sitio web de phishing puede aparecer varias horas después. En caso que se haya utilizado una redirección y no la hayan bajado, vigílela muy de cerca.
- Al final de una campaña de phishing, retire la página de advertencia asociada desde su sitio web.

Repercusiones 6

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

- Considere qué pasos de preparación podría haber dado para responder al incidente más rápida o eficientemente.
- Actualice sus listas de contactos y agregue notas sobre la forma más eficaz de comunicarse con cada parte implicada.
- Considere cuáles relaciones dentro y fuera de la organización que podrían ayudar en futuros incidentes.
- Si se requiere una acción legal, colabore con los equipos jurídicos.

Un aporte para:

Organización de los Estados Americanos

CICTE

IRM # 13

Respuesta ante incidentes de phishing

Directrices para el manejo de incidentes de phishing

Autor IRM: CERT SG / Cedric PERNET
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