www.segu-info.com.ar agradece especialmente a FAM por la realización de este documento.

PHISHING – Contraatacando al enemigo

El PHISHING es uno de los pocos ataques que sufren las empresas en los cuales como responsables de la seguridad de la información de las mismas, no podemos hacer mucho para evitarlo.

Al ser notificados de un incidente de este tipo debemos estar preparados para comenzar a aplicar un procedimiento adecuado para la gestión del incidente. Es necesario que cada uno de los pasos estén escritos detalladamente y debemos tener preparados modelos de informes, en lo que solo haya que completar la información del caso.

Los mensajes de aviso iniciales a las áreas involucradas también deben estar preescritos, para evitar perdida tiempo, y acá esta el punto. La batalla que comenzamos al aplicar el procedimiento, es contra el tiempo de vida del sitio de PHISHING. Eliminar el sitio en el menor tiempo posible es el objetivo.

Mientras el sitio esta activo, los clientes están recibiendo mensajes en nombre de nuestra organización, invitándolos a ingresar sus datos personales para que después les vacíen sus cuentas.

El tiempo de vida del sitio de PHISHING lo podemos contabilizar desde el momento que nos notificamos, hasta su baja. Ahora bien, es probable que el sitio haya estado vigente bastante tiempo antes de que fuéramos notificados. Para ajustar más este dato y teniendo en cuenta que el atacante utiliza cuentas de correo con nuestro dominio, podemos hacer lo siguiente:

1) Si la cuenta utilizada existe (seguridad@nuestraempresa.com.ar, por ejemplo), revisar aquellos mensajes entrantes de gente desconocida, dado que probablemente se trate de alguien que a respondido a un mensaje de PHISHING. Se deben apartar estas respuestas para analizarlas y detectar aquellas de fecha más temprana. No se debe mirar la respuesta del "cliente" sino el mensaje al que el hace referencia.
2) Si las cuentas utilizadas no existen, crearla para recepción de respuestas, dado que estas nunca van a ir al atacante sino a nosotros, dado que son de nuestro dominio.

IMPORTANTE: Nunca responder a esos mensajes, recuerden que el origen del intercambio no fue generado por nosotros, por lo tanto no se debería dar respuesta por este medio. Es solo para monitoreo.

Esto también puede ser útil para detectar ataques. Si creamos cuentas del tipo administrador@xxxxx, sistemas@xxxxxx, servicoalcliente@xxxxxx, etc. (basta con revisar casos de PHISHING en general para ver que cuentas se suelen usar, para ir agregando), podemos revisar estas cuentas frecuentemente o configurar una regla que nos avise ante un mensaje sospechoso.

El procedimiento de gestión del incidente no debe ser complicado, debe ser ágil. Puede estar dividido en tres etapas:

Etapa 1 – Informe preliminar

Comienza a partir de que los responsables de seguridad informática son notificados del incidente. El coordinador del incidente, debe realizar un informe preliminar para poder comenzar a trabajar con el equipo de investigación, para los niveles gerenciales, y enviar instrucciones precisas al personal de centro de contactos o de mesa de ayuda a fin de informar a los clientes de forma adecuada. En este caso es donde hay que poner especial cuidado:

1) Deben informar en forma clara que la organización no es responsable de los mensajes enviados.
2) Si el reclamo viene de un cliente "real", deberá recabarse la información necesaria para su seguimiento, y si fue victima del engaño solicitarles que renueve inmediatamente sus claves de acceso, con el método de práctica.
3) El reclamo puede provenir (suelen ser los "mas") de personas que se sienten invadidas por que le estamos enviando "SPAM", a pesar de que ellos no tienen relación con la organización. Una de las preocupaciones es "de donde sacaron mis datos!!!??", a pesar de que el único dato que esta involucrado en este tema es la cuenta de correo electrónico.

En todos los casos hay que dar información clara y precisa, dado que esta en juego la imagen de la organización.

Etapa 2 – Análisis detallado

Aquí debe dispararse el procedimiento para conocer más en detalle las características del sitio. Esta etapa debe comenzar luego del análisis preliminar realizado en la etapa 1, es decir que se solapan en el tiempo y para ello es necesario que la realice otra persona o equipo. Se debe obtener información del sitio, y del hosting. Recordemos que generalmente el PHISHG se hace desde sitios legales a los cuales, aprovechando alguna vulnerabilidad del mismo, se les "cuelga" la página utilizada para el fraude. Esto a veces es una ventaja, dado que de poder contactar a los responsables del sitio afectado, la eliminación del sitio suele ser más sencilla (nadie que se considere legal quiere verse involucrado en algo ilegal).

Se debe obtener toda la información posible sobre el dominio. Datos del "webmaster" y teléfonos que hayan sido consignados al registrar el dominio, suelen ser muy útiles. Hay que intentar por todos los medios a nuestro alcance hacer llegar el reclamo y la solicitud de baja de la página en cuestión.
A partir de aquí solo queda comenzar a monitorear el sitio en cuestión y detectar su cese de actividad.

Etapa 3 – Informe final

Aquí, mientras esperamos, rogamos y rezamos que el sitio sea dado de baja, es donde se deben comenzar a darle forma al informe final. Este debe incluir todo el detalle de lo actuado, con anexos que incluyan los mensajes, notas y otra evidencia de lo que se haya realizado. Debe incluirse el informe de "daños", es decir, si hubo reclamos o denuncias de clientes que hayan sido victimas. Debe tenerse en cuenta que el informe de daños es parcial. Los efectos del PHISHING no suelen verse de inmediato. Muchas veces los clientes ingresaron al sitio de

PHISHING, y luego de dar sus datos personales, son redirigidos al sitio real, y luego de volver a ingresar sus datos e ingresar satisfactoriamente, asumen que en el primer ingreso, pusieron mal algún dato. Días o meses después se dan cuenta que hay algo raro en sus movimientos.

Una buena práctica, mientras seguimos esperando, es revisar que tan bien se aplico el procedimiento, tomando nota de los puntos donde debemos mejorar. Puede ocurrir que al momento del ataque, no tengamos ningún procedimiento, entonces ese es el momento de comenzar a documentar, lo más detalladamente posible.

La etapa 3 puede llevarnos unas pocas horas de trabajo intenso, dependiendo de nuestra experiencia. Después, parece que nuestra suerte esta en manos de terceros, que solo resta esperar. Mientras tanto nos llegan correos de nuestro jefe, o peor, del jefe de nuestro jefe, preguntando que estamos haciendo, y generalmente es difícil decir "nada, esperando… no hay nada por hacer."

Por eso vamos a incorporar una 4ta etapa.

Etapa 4 – Contraataque

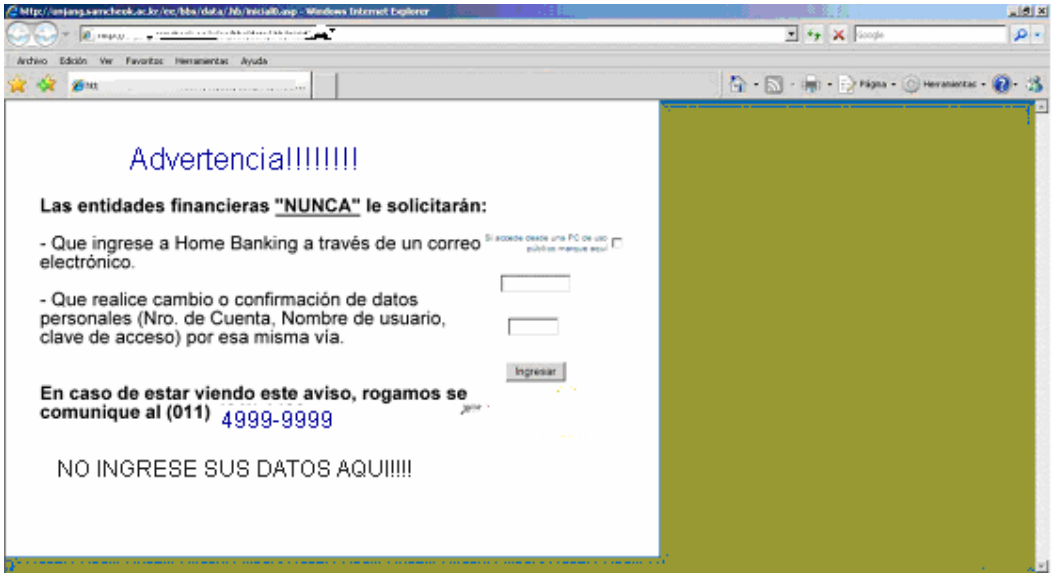
Aquí es donde debemos poner toda nuestra imaginación, usar la experiencia de otros casos y de otros colegas. Pueden pasar horas y hasta días hasta que se realice la baja de la página.

Podemos comenzar a analizar el código fuente de la página para ver que descubrimos. Intentar ver como se esta recolectando la información. Esta claro que no podemos atacar al dominio (aunque a veces tengamos ganas de tirarle con todo lo que podamos!). Definitivamente eso no se debe hacer!!!

Una posibilidad, es ver de donde toman las imágenes del sitio de PHISHING. Muchas veces para hacer el sitio lo mas idéntico posible, toman las imágenes desde el sitio original, poniendo la url completa. De ser así tenemos algo para hacer:

1) Relevar las imágenes utilizadas en nuestro sitio, y que estén referenciadas en la página falsa.
2) Relevar en nuestro sitio en que lugares se esta usando esa imagen.
3) Renombrar las imágenes originales, y realizar el cambio en nuestro código para que apunten a las nuevas.
4) Eliminar las imágenes originales.

Esto hará que el sitio de PHISHING se vea bastante feo. Pero mejor aún, podemos generar imágenes nuevas (con el nombre de las originales) y poner advertencias bien visibles que persuadan a la posible víctima de ingresar al sitio. Eliminar aquellas imágenes que haga referencia a nuestra entidad. Por ejemplo luego de realizar los cambios podría quedar algo así:



También es posible intentar llenarle la base de datos al malhechor con información falsa, usuarios y contraseñas. Esto le llenaría la base de "basura" haciéndole más difícil su tarea.

Todo lo que se haga en esta etapa debe estar dentro de un marco de ética y legal, nunca olvidar que nosotros somos los buenos!

Por último, es fundamental concientizar al cliente. Informarle en forma permanente sobre el PHISHING. Capacitar al personal del centro de contactos o de la mesa de ayuda, para que informen correctamente y para que los clientes encuentren apoyo y no se sientan desamparados.

A continuación se detalla el tratamiento de la gestión de incidentes en caso de Phishing.

Gestión de incidentes - PHISHING

Generalidades

Objetivo

Describir las acciones a seguir ante un incidente de PHISHING

Introducción

El PHISHING es una técnica de fraude informático que tiene por objetivo el robo de la identidad de los usuarios de Banca Hogareña u otros sitios similares.

Se realiza mediante un mensaje de correo electrónico enviado en forma masiva, con técnicas de distribución de SPAM (correo no deseado o "basura")

El mensaje es enviado aprovechando vulnerabilidades del protocolo de correos (SMTP), mediante el cual se pueden utilizar nombres cuentas de remitentes simulando ser, por ejemplo, una unidad de servicios de la entidad.

Algunos clientes, sorprendidos o intimidados por el mensaje, podrían seguir las instrucciones del mismo que lo llevan a un sitio apócrifo, similar o igual, al sitio original de Banca Hogareña, para solicitarle sus datos de ingreso (usuario y contraseña) y capturarlos con el objetivo de cometer un fraude.

Ante la detección de un incidente de este tipo deben tomarse los recaudos pertinentes a fin de minimizar el impacto, el cual afecta fundamentalmente a la imagen de la institución.

Consideraciones generales

Detección del incidente

Los incidentes se detectan al tomar conocimiento con la denuncia de que en Internet circula un mail que en apariencia fue enviado por la organización.

La detección puede provenir de:

- ☐ Un cliente que realiza un reclamo en alguno de los canales habilitados
- ☐ Mesa de Ayuda
- ☐ Sucursales
- ☐ Usuarios en general
- ☐ Organismos relacionados
- ☐ Colegas

Factores a tener en cuenta para la resolución de un incidente

La resolución del incidente se considera cumplida cuando se logra deshabilitar el sitio "simulado" de Banca Hogareña.

El impacto del incidente esta directamente relacionado con el tiempo de actividad del sitio "simulado".

La ventana de tiempo transcurrida desde la detección del sitio hasta su deshabilitación debe reducirse al máximo posible. Esto depende de la eficiencia de la aplicación de las acciones previstas en presente documento.

Pasos a seguir a partir de la detección de un incidente

Coordinador del incidente

- ☐ Recibir el aviso de un posible caso de PHISHING
- ☐ Notificar en forma inmediata y convocar al equipo de respuestas a incidentes.
- ☐ Realizar un análisis preliminar respecto al correo recibido y verificar que se trate de una ataque de PHISHING activo, es decir que el sitio simulado este funcionado.
- ☐ Dar instrucciones para comenzar el análisis técnico del caso a fin de detectar la ubicación del sitio de PHISHING, el servicio de Hosting que la soporta y proceder a solicitar su deshabilitación.
- ☐ Informar a los responsables del Centro de Contactos y Mesa de Ayuda respecto del incidente y de las recomendaciones de práctica según texto del Anexo I.
- ☐ Informar a la Superioridad del incidente, sus características y de las acciones realizadas hasta el momento.
- ☐ Solicitar el bloqueo de la dirección de Internet de la página de PHISHING para que los usuarios de la organización no ingresen a la misma.
- ☐ Bloquear la cuenta de correo utilizada para la distribución del mensaje para que no ingrese a los servidores de correo de la organización.
- ☐ Analizar posibles contramedidas que permitan minimizar el impacto del ataque.
- ☐ Documentar la evidencia recolectada, en orden cronológico y archivarla.
- ☐ Realizar un informe ejecutivo para los niveles superiores y el área de Prensa.
- ☐ Determinar métricas para evaluar el impacto del incidente:
    - o Llamados al Centro de Contactos
    - o Cantidad de clientes damnificados
    - o Cantidad de transacciones desconocidas en Home Banking
    - o Tiempo de "vida" del sitio de PHISHING
- ☐ Documentar las situaciones que se consideran podrían mejorar el nivel de respuesta.
- ☐ Dar por cerrado el incidente al comprobar fehacientemente que el sitio de PHISHING ha sido deshabilitado.

Análisis técnico del incidente

Equipo de respuesta ante incidentes

Recibir el informe preliminar

- ☐ Obtener información a través de herramientas pasivas, utilizando los siguientes sitios web, seleccionando la opción correspondiente:
  - o http://www.dnsstuff.com/
  - o Spam Database Lookup
  - o Reverse DNS lookup
  - o IPWHOIS Lookup
  - o IP Information

  - o http://www.ip-plus.net/tools/dig_dns_set.en.html
  - o Dig DNS Check

- ☐ La información obtenida deberá volcarse en un formularios a fin de ordenarla, resaltando aquellos datos que son relevantes.
- ☐ Realizar la gestión de la anulación de las plataformas de servicios implicados por e-mail y telefónicamente, a fin de lograr el objetivo ala brevedad posible.
- ☐ Deberá enviar correo al webmaster encontrado en el paso anterior, en la descripción "Ipwhois Lookup / e-mail ", en el idioma que corresponda, de no ser en español, al menos en ingles.
- ☐ Realizar la solicitud telefónicamente, los datos podrán encontrarse en ""Ipwhois Lookup / phone ".
- ☐ Enviar un informe de lo actuado al Coordinador del Incidente, incluyendo toda la información recolectada.
- ☐ Realizar un seguimiento del estado del sitio fraguado para verificar su desactivación.
- ☐ Informar al Coordinador del Incidente la desactivación del sitio.

Anexo I

Recomendaciones de práctica

Modelo para el centro de contactos

Se ha detectado un incidente de PHISHING. Esta técnica de ataque consiste en intimar a un destinatario de correo electrónico a ingresar a una página para actualizar sus datos personales, con el fin de capturarlos y utilizarlos posteriormente en forma fraudulenta.

Se recomienda recordar a los clientes y usuarios de Home Banking que:

- Las entidades financieras "NUNCA" le solicita que informe o confirme sus claves o datos a través de un correo electrónico.
- Tampoco lo invitará a operar en ningún sitio web ajeno a www.subanco.com.ar y/o por accesos que no sean los convencionales para operar.
- En caso de recibir este tipo de mensajes, el mismo debe ser eliminado inmediatamente.El texto del mensaje utilizado en este ataque es el siguiente:

< Copiar el texto en particular >