Simulacro de Phishing en instituciones académicas

Estado: Propuesta
Jesus Sanz de las Heras
Fecha: Octubre 2009

1. Problema

El Phishing es una técnica que empleando mensajes de correo electrónico intenta engañar al receptor para que le proporcione datos confidenciales. Estos datos generalmente suelen ser claves bancarias, en el caso de las universidades son las claves de acceso al correo. Estos mensajes dicen ser originados por los responsables del Servicio de comunicaciones o informática de la universidad argumentando cualquier motivo para crear necesidad de modificar las claves y enviárselas al delincuente. Los mensajes enviados en este engaño en apariencia están diseñados para que sean idénticos a los que podrían enviar cualquier departamento de la institución , lo que provoca que el receptor no se de cuenta del verdadero origen del mensaje y envíen las claves al usurpador o delincuente. Muchas veces estos mensajes están muy mal redactados y a pesar de ellos los usuarios siguen confiando en ellos y enviando las claves a pesar de los reiterados anuncios de la universidad para que no se fíen de estos mensajes.

El objetivo fundamental del delincuente al recolectar esas claves es poder usar los servidores de la universidades para distribuir spam de forma delictiva. Por supuesto con esas credenciales también podría acceder a otros servicios. La distribución de spam desde los servidores de la universidad se realiza en remoto y automáticamente por parte del delincuente, suele ser masiva y puede provocar graves daños en los servidores de correo dejándolos inservibles durante un tiempo. Ocasionan una gran perdida de tiempo en la resolución de los problemas (revisar claves, servidores, usuarios etc), pero sobre todo genera una gran sensación de impotencia e inseguridad en los Servicios de Informática y comunicaciones de la universidad, donde parte de la seguridad (claves) se escapan por el eslabón mas débil, nuestros propios usuarios.

Las universidades toman diferentes medidas para evitar que los usuarios no envíen las claves, a pesar de lo cual los usuarios siguen picando, confiando en los mensajes y enviando las claves. La mejor forma de evitarlo es la formación e información del usuario, pero es tarea ardua y continua en el tiempo, además es suficiente con que un solo usuario sean engañado. También hay soluciones técnicas algo mas complejas y efectivas que podrían afectar el correcto uso del correo a otros usuarios, como es limitar el número de correos en un periodo determinado de tiempo.

En definitiva nos enfrentamos a un problema con graves repercusiones técnicas pero cuyo origen no es técnico sino de índole social. Debemos remarcar primero que los usuarios que envían las claves lo hacen sin malicia y segundo que la conservación de claves de acceso al correo y otros servicios de a institución debería ser incluido en las normas de uso interno y por tanto responsabilidad suya.

2. Objetivo del simulacro

En primer lugar somos conscientes de la importancia de informar a los usuarios en la seguridad en la Red y en concreto en la custodia de claves para que no sean engañados por mensajes que les solicitan sus claves aunque digan proceder de la propia universidad. Pero la experiencia nos está demostrando que siempre hay y habrá usuarios que no hayan leído la información o que no la recuerden si la leyeron hace tiempo y que por tanto pican en este tipo de engaños enviando las claves a una dirección aparentemente del servicio de informática de su universidad, sin ser conscientes que se las están enviado a otras personas ni los daños que pueden causar en los servicios de la institución.

Para evitar en un futuro estos problemas podemos poner en marcha **Simulacros de Phishing** que es el objetivo de esta propuesta**.** Entendemos por Simulacro de Phishing a la planificación de envíos masivos a los usuarios de la universidad solicitándoles sus claves para que las envíen a un buzón gestionado por los propios responsables del simulacro. En definitiva imitar los ataques de Phishing pero controlados por los responsables del servicio. El objetivo es detectar cuales usuarios de la universidad han (nos han) enviado las claves para ponerse en contacto con ellos y reeducarlos. Consideramos que será mejor informales después de un phishing controlado (simulacro) que después de un phishing real cuando ya han enviado las credenciales a algún indeseable.

3. Recomendaciones a tener en cuenta en el procedimiento de simulacros de phishing

3.1. Planificación técnica del simulacro

Debemos disponer de una herramienta automática que envíe los mensajes a los todos o al subgrupo de usuarios que consideremos. Esta herramienta deberá automáticamente:

- Chequear la base de datos de usuarios
- Componer el mensaje de Phishing
- Generar cabeceras (*header*) falsas
- Generar campos *reply-to: From: y* Sender redireccionados a un buzón recolector externo, controlado por los responsables de la universidad.
- Distribución masiva a los usuarios

Aspectos a tener en cuenta

- El contenido del mensaje debe ser lo mas parecido a los mensajes de phishing que se suele recibir en su universidad. Sobre todos los relacionados con solicitud de claves ya que son lo que mas problemas ocasionan.

- El *buzón recolector* debe esperar recoger la información de claves que envíen los usuarios. Si no se recogen claves es que los usuarios empiezan a estar concienciados del tema.

- La distribución de los correos del simulacro puede ser realizada por:
  - Servidores de la propia institución, lo que implicaría que se distribuyera desde una IP local
  - Servidores (¿uno de RedIRIS?) para que la IP fuera externa.
- El buzón recolector será abierto por las personas asignadas para ello

3.2. Otros aspectos del simulacro

El simulacro debe ser realizado y conocido por pocas personas. Si lo conociera mucha gente y se corriera la voz perdería su efectividad.

Periodicidad. Los simulacros puede ser realizados con una periodicidad superior a 6 meses.

El simulacro debe ser consentido por el responsable de los servicios comunicaciones de la Universidad.

Es muy recomendable incluir información publica en la web de la institución, acerca del tema del Phishing para que puede ser considerado como una forma de aviso del simulacro y respalde legalmente el simulacro.

Nos podemos encontrar con el problema del uso que se de a las claves recogidas, es decir, debemos articular alguna idea para de garantizar que nadie va a abusar de esas claves recogidas. Por ejemplo un idea podría generar el mensaje solicitando el primer y último

carácter de la clave del usuario, de esta forma no se podría imputar al servicio de informática que está “robando” claves.

4. Resultados esperados

4.1. ¿Qué sucederá cuando se reciba un phishing real?

Los usuarios que estén correctamente informados serán conscientes y lo borrarán. Habrá usuarios que hayan sido reeducados en algún caso de phishing simulado (simulacro) y lo borrarán. Es difícil (no imposible) que haya usuarios que con la información de las páginas web y con los simulacros que haya recibido envíen las claves.

4.2. ¿Qué sucederá cuando se reciba un mensaje real de los servicios de informática?

Los servicios de informática podrán enviar los mensajes informativos que consideren pero debe estar anunciado con algo así como “Los servicios de informática nunca solicitarán su clave por correo electrónico”