¿Estáis preparados?

Solución del Reto 2: phishing

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

R.2 Solución al RETO 2: phishing alojado en nuestra página web

Este es el material que se ha de entregar al equipo cuando hayan debatido sobre el incidente.

1.1 ¿Qué puedes hacer?

- Llamar al proveedor del alojamiento web, contarle lo ocurrido y confirmar que él no ha llamado ayer.
- Solicitar al proveedor de alojamiento web que ponga *offline* la web.
- Cambiar las contraseñas de la página web de todos los administradores y pedir a los usuarios que cambien las suyas por precaución.
- Ponerse en contacto con la policía y con Incibe para saber cómo actuar.
- Hacer, o pedírselo al soporte informático, una copia cifrada de nuestra web con el *phishing* para enviársela a la policía junto con la denuncia.
- Hacer una copia cifrada (para enviársela a la policía junto con la denuncia) de los registros del servidor donde se puedan ver los accesos de los ciberdelincuentes y de las víctimas que hubieran ingresado sus credenciales del banco, para protegernos de posibles denuncias y tener evidencias de que nuestra empresa ha sido una víctima más.
- Por precaución, pasar un antivirus a los equipos que alojan la web en el proveedor. Si alguien ha tenido acceso al servidor web, podría haber alojado algún malware. Por precaución, también pasar el antivirus a los ordenadores de todos los administradores de la web en nuestras oficinas.
- Actualizar el software del gestor de contenidos para evitar tener software vulnerable, es decir, con agujeros de seguridad. Esta es otra forma en la que podrían haber accedido a la web, aunque esta vez se lo servimos en bandeja, dándoles las credenciales.

R.2 Phishing

- Restaurar nuestra página web con la copia de seguridad más reciente. Posiblemente tengamos que volver a cargar los contenidos que hemos modificado desde el último *backup*.
- Con ayuda de nuestro soporte informático y el proveedor de alojamiento web, solicitar que nos eliminen de las listas negras siguiendo (por ejemplo) los pasos indicados en: *Google Safe Browsing*.
- Adoptar una política de uso del gestor de contenidos web (revisión de usuarios y permisos, uso y cambio de contraseñas, ordenadores y redes confiables para actualizar la web,...) para evitar ataques como el que sufrió la responsable de la web.
- Establecer charlas para enseñar a los nuevos empleados, y a los no tan nuevos, cómo han de hacer en estos casos y como evitar caer en los ataques de ingeniería social.
- Establecer una política de contraseñas robustas que se cambien con cierta periodicidad.
- Dar permisos de administración de la web solamente a los empleados que realmente van a realizar esta labor y están formados para ello.

1.2 ¿Qué no debes hacer?

- Ocultar que conoces cómo se ha originado el incidente.
- No formar a los nuevos empleados para que sepan cómo actuar en caso de incidente y cómo identificar un ataque de ingeniería social.
- Destruir las pruebas del problema. Pueden servirnos como evidencias ante una posible denuncia.
- Dar permisos de actualización de la web, de manera indiscriminada, a todos los usuarios.
- No actualizar el software de tu web y los equipos con los que actualizas los contenidos.

1.3 Lecciones aprendidas: ¿cómo podrías evitarlo?

- Es importante formar a todo el personal para identificar técnicas de ingeniería social.
- También hay que estar preparado por si ocurre un incidente, es decir tener un procedimiento de gestión de incidencias que todo el mundo conozca para saber cómo actuar. Hemos informado a todo el personal de cómo actuar ante este tipo de incidentes.
- Las copias de seguridad han servido para solucionar el problema con rapidez. Hay que hacerlas regularmente, conservarlas en un lugar externo y separado (no conectado) y probar que funcionan y sabemos recuperarlas.
- Tenemos que tener a mano la lista de contactos de apoyo y de denuncia para estos casos.
- Debemos analizar bien nuestros riesgos pues está claro que esto puede ocurrir pero no debe volver a pasar, tenemos que poner medidas (cambiaremos de antimalware y revisaremos los procedimientos de correo electrónico).
- Planificar sesiones de concienciación para identificar este tipo de amenazas y no dejarnos engañar.
- Realizar auditorías de seguridad periódicas a la web, o contratarlas con nuestro proveedor, para aseguramos que los servicios web están actualizados y que no tienen vulnerabilidades.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL