¿Estáis preparados?

Descripción del Reto 2: phishing

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

Reto 2

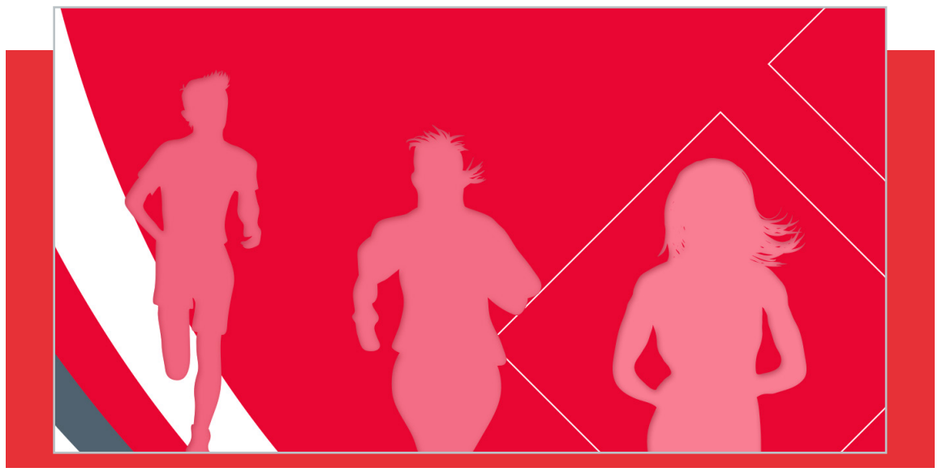
Phishing

R.2 Descripción del incidente de phishing alojado en nuestra página web

Este es el material que se ha de entregar al equipo para debatir sobre el incidente con ayuda de la presentación.

1.1 Escenario

- Formáis parte de una pequeña empresa que tiene una página web o una tienda online para interactuar con clientes. Los clientes tienen la posibilidad de darse de alta en la web para recibir información periódica y acceso a los servicios.
- Para vuestra actividad tenéis contratada la conexión a internet, el alojamiento web y el soporte informático.
- Publicáis y modificáis los contenidos de vuestra web conectándoos al gestor de contenidos alojado en el proveedor.
- En vuestra oficina hay varias personas que actualizan la web, entre ellas una persona de reciente ingreso.
- Vuestros clientes contactan por teléfono, email o a través de la web.



Reto 2

¿Respuesta a incidentes?

1.2 ¿Qúe ha pasado?

- Una llamada de un cliente, os pone sobre aviso de que cuando intenta acceder a vuestra página web aparece la de un conocido banco (o una muy parecida). También aparece un mensaje en su navegador indicándole que tu página está en una lista negra de *phishing*.
- Alguien ha conseguido entrar en tu servidor web y ha cambiado los contenidos de tu web por otros que parecen los de un banco muy conocido.
- El cambio de los contenidos está siendo utilizado para realizar *PHISHING*, es decir para «pescar usuarios y contraseñas» de los usuarios de ese banco. Seguro que también han enviado correos o mensajes para engañarles y que visiten la página.
- Preguntando a los empleados si habían notado algo extraño, una de las personas que administran la web, confesó avergonzada que el día anterior recibió una llamada urgente de alguien que decía ser el proveedor tecnológico pidiendo las contraseñas de administración de la web, con la excusa de realizar unas actualizaciones imprescindibles. Hace poco que trabaja aquí y no conoce al proveedor. Se las dio sin dudar pues le pareció honrado y creíble.
- Esta vez ha sido un ataque de ingeniería social, pero con el software de nuestra web desactualizado, podrían haber aprovechado algún agujero de seguridad para realizar cualquier otro tipo de ataque.