¿Estáis preparados?

Descripción del Reto 1: ransomware

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice

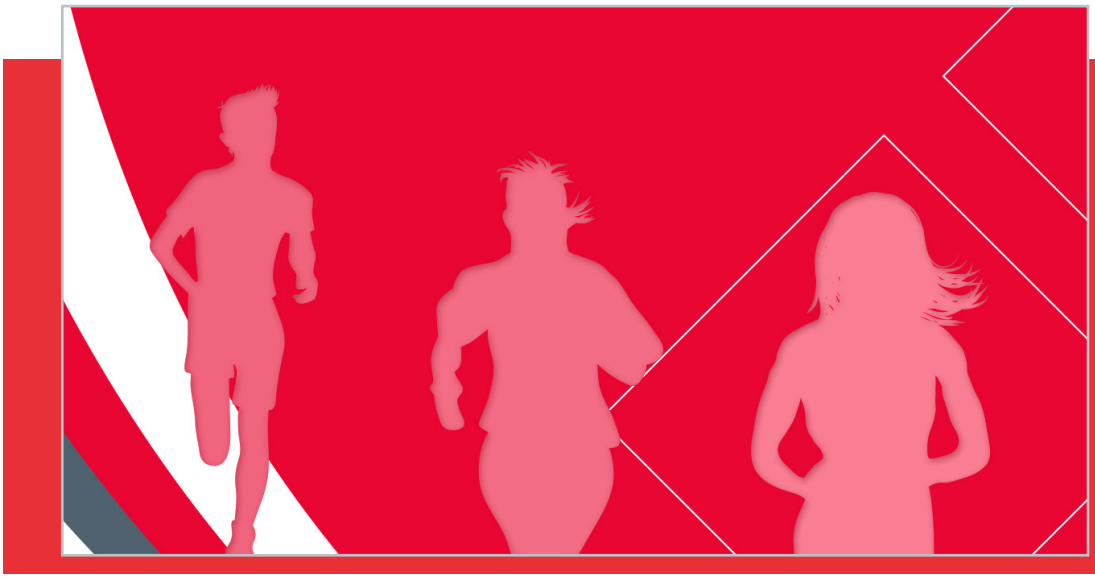
Ransomware

R.1 Descripción del incidente de ransomware

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 pyme que tiene una oficina con algunos ordenadores, una red con wifi y conexión a internet.
- En vuestra empresa la información se emplea para contactar con clientes y proveedores, mantener una modesta página web, elaborar las facturas e intercambiar datos con la gestoría (RRHH, impuestos,...).
- Para vuestra actividad tenéis contratada una conexión a internet, un alojamiento web con una página sencilla, los servicios de una gestoría y el soporte informático.
- Los empleados tienen un horario comercial.
- Los clientes contactan por teléfono, email, a través de la web o presencialmente.



1.2 ¿Qúe ha pasado?

- Un martes uno de los comerciales, descubre que no puede acceder a su ordenador, donde le aparece un mensaje reclamando dinero para permitirle acceso. En menos de una hora, a la mayoría de los comerciales, les pasa lo mismo.
- Es un RANSOMWARE, un malware que cifra el ordenador a cambio de un rescate. Parece que el origen está en el PC de ese comercial.
- Preguntándole si había sentido algo raro, comenta que ayer, a última hora, recibió un mensaje de un cliente (del que no se acordaba) con un fichero adjunto que descargó y que no tenía nada. Pensó que era una equivocación. Se lo envió a otros compañeros para ver si podían abrirlo desde sus ordenadores.
- Ya tenemos a la mitad de la oficina parada, los teléfonos no paran de sonar y ya no sabemos que escusas dar a los clientes.
- No podemos tramitar más pedidos, hasta que no se restablezca la situación.
- Todos los discos que el comercial tiene conectados al ordenador están cifrados por el ransomware. Afortunadamente las copias de seguridad están en un disco externo que no está pinchado al ordenador.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL