Trabajo Seguridad informática

Francisco Espejo Carretero
Diego Pertiñez Cabo
Manuel Jesús Orozco

INDICE

INTRODUCCIÓN

Este trabajo consta de un escenario e incidente, y que haríamos si nos ocurriera a nosotros. Vamos a valorar los daños, los pasos que seguiremos para mitigarlo, lo que no se debe hacer y cómo podríamos evitar.

Francisco Espejo: Puntos 3 - 4
Diego Pertiñez: Puntos 1 - 5
Manuel Jesús Orozco: Puntos 2 y parte del 3

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.

INCIDENTE

- 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.

1

¿Cuáles son los activos?

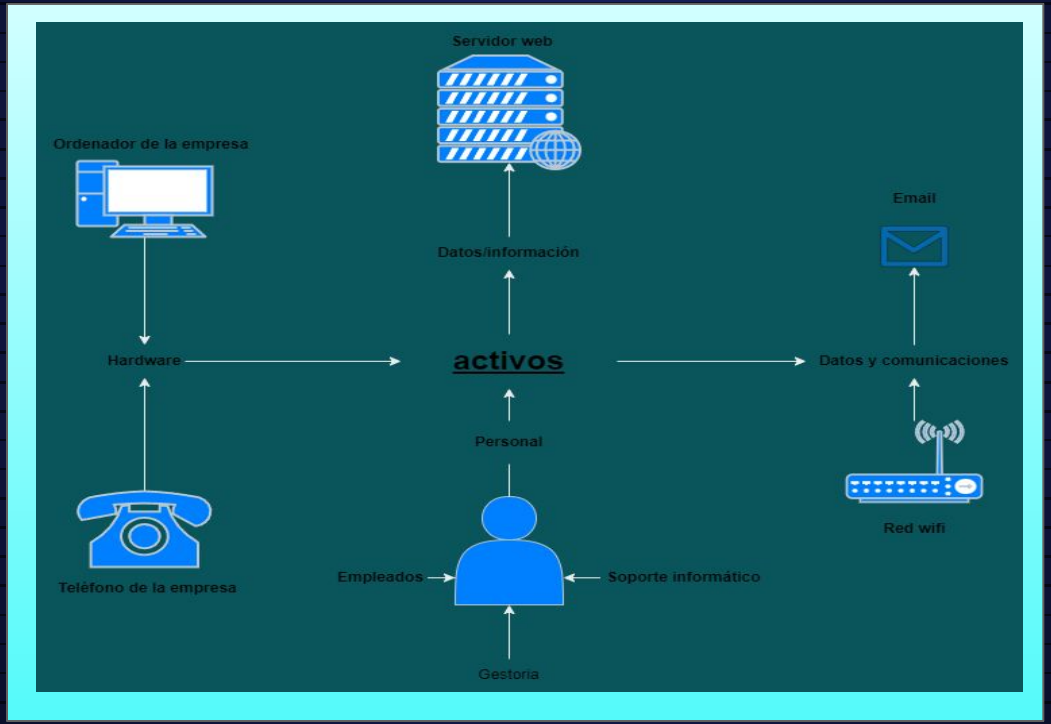
Cuáles son los activos

Los activos son los recursos que se utilizan en un sistema de gestión de seguridad,para que las organizaciones funcionen.

En este ejemplo los activos son:

- La red wifi
- Pagina Web
- Ordenadores de la empresa
- Teléfonos de la empresa
- Empleados
- Soporte informatico
- La gestoria
- Email

Cuáles son los activos



2

Valoración del incidente

Valoración del incidente

La página web no se verían daños causados pero si habría un problema el cual la gente que esté interesada en algún producto o servicio no se le podría atender. En los ordenadores si habría un grave problema debido a que estarían encriptados y por lo cual habría que desencriptarlos y esto significa que al ver tantos ordenadores con problemas habrá más dificultad a la hora de atender al cliente debido a la disponibilidad de los mencionados anteriormente. En los Teléfonos tendríamos problemas porque iríamos más lentos por la falta de equipos de trabajo. Los empleados dependen de los departamentos de dicha empresa pero en general todo estarí más colapsado. El soporte informático estaría estancado ya que todos estarían centrados arreglando el problema, pero debido a esto se verían menos atendidos si hay más problemas en la empresa. La gestoría se vería muy afectada puesto que se pararía la mayor parte de la transferencia de datos. El email se vería colapsado debido a que la demanda seguiría igual pero con este problema hay menos equipos disponibles.

Valoración del incidente

En resumen debido a los daños localizados la conclusión es que perdemos dinero debido a que hay menos equipos disponibles y si tenemos que contratar a más informáticos para solucionar el problema, el precio aumentaría considerablemente. Aparte perderemos clientes y lo más importante, su confianza, porque crearán que nuestra empresa no tiene ningún tipo de seguridad, y por tanto, perderemos su dinero.

3

¿Qué puedes hacer?

¿Qué puedes hacer?

El 50% determinaron que su organización no estaba preparada para repeler un ataque de ransomware. El costo promedio de un ataque de ransomware en las empresas fue de 133,000 $ en el año 2019.

Cree que no están preparadas

Cree que sí están preparadas

¿Qué puedes hacer?

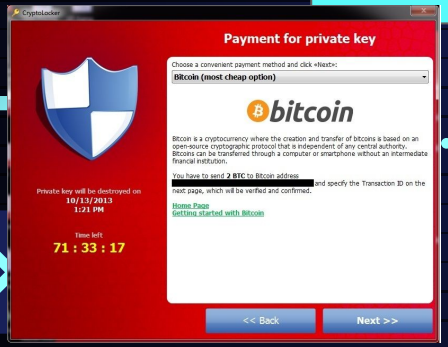
El ransomware es un software malicioso que infecta el ordenador, la red o el software y bloquea el acceso a información importante hasta que la víctima entrega el pago.

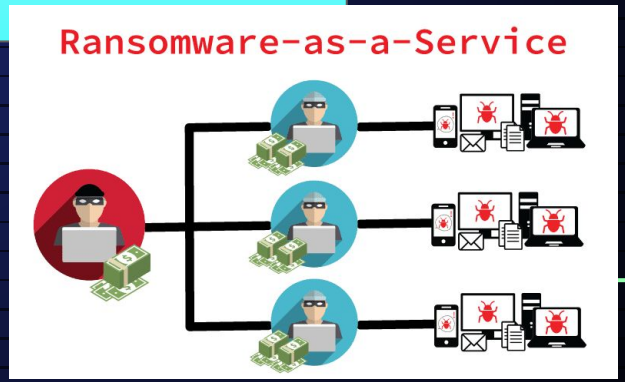
¿Qué puedes hacer?

Primero veremos los tipos de ransomware para identificar cual nos ha podido atacar.

Cryptoransomware, cifra los datos que se mantienen como rehenes y no pueden ser liberados sin una clave de descifrado. CryptoLocker

Ransomware como servicio (RaaS), en el que el autor se convierte en cliente del ciberdelincuente pagando por el acceso al ransomware como si se tratara de una suscripción.

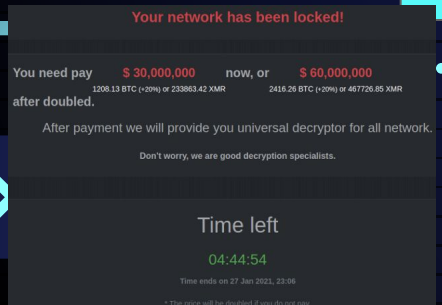




¿Qué puedes hacer?

Los filecoders cifran y bloquean los archivos en su PC. Los ciberdelincuentes tras este tipo de ransomware exigen un pago a cambio de las claves de descifrado, normalmente con un plazo límite, o los archivos podrían resultar dañados, destruidos o bloqueados de forma permanente. Alrededor del 90 % de las cepas de ransomware son filecoders.

Los screenlockers hacen exactamente lo que indica su nombre: bloquean la pantalla y así el acceso a la máquina. Suelen hacerse pasar por mensajes de una institución oficial como el FBI, e indican que ha incumplido la ley y que debe pagar una multa para poder desbloquear el PC. Los screenlockers son ya más comunes en dispositivos Android que en PC con Windows.



¿Qué puedes hacer?

Ahora vamos a seguir unos pasos, contando que ya hemos sido atacados, y vamos a aprender a mitigarlo:

1. Apagar y desconectar los dispositivos afectados de la red.
2. Informar a la policía del ataque (el número es el 017)
3. Reunir empleados y hacer encuesta de como ha sucedido
4. Pensar en la distribución de nuestros servidores y pensar en la recuperación de datos.
5. No pensar en pagar ningún tipo de rescate
6. Analizar qué tipo de ransomware es
7. mantener copias de seguridad cifradas de los datos fuera de línea
8. Clona los discos duros de los equipos infectados, pues pueden servir de evidencia si vamos a denunciar a la policía
9. Aislar los equipos que hayan sido infectados ransomware inmediatamente desconectándolos de la red para evitar que este virus se expanda y ataque otros equipos o servicios compartidos. Aisla o apaga los equipos que no estén aún del todo afectados para contener los daños. Si fuera posible cambia todas las contraseñas de red y de cuentas online.
10. Ayudarte de herramientas como el programa Crypto Sheriff para identificar el tipo de ransomware
11. Es muy probable que el ransomware en el PC se elimine a sí mismo después de cifrar los archivos para no dejar rastros del atacante

¿Qué puedes hacer?

Si el ransomware pasado un tiempo no se ha eliminado a sí mismo y no queremos perder más el tiempo podemos hacer lo siguiente:

Reiniciar el ordenador pulsando la tecla F8 mientras tenga lugar el arranque

1. Seleccionar Modo seguro ayudándote de la línea de comandos
2. Escribir 'cd restore' y después pulsa sobre la tecla 'Intro'
3. Escribir 'exe' y vuelve a pulsar nuevamente la tecla 'Intro'
4. Escoger la fecha en la cual deseas restaurar el sistema. No olvides elegir una fecha que sea antes de que el ordenador se infectase y después debes pulsar 'Intro'

En el supuesto de que este método no te ayude a recuperar el control de tu ordenador puedes hacer uso de un software externo anti-Ransomware, el cual podrá tanto descargarse como comprarse desde otro ordenador y cargarse en una memoria USB, un CD u otros sistema de almacenamiento.

¿Qué puedes hacer?

Para inciar el anti-ransomware realizaremos los siguientes pasos:

1. Reiniciar el ordenador pulsando la tecla F8 mientras tenga lugar el arranque
2. Seleccionar el Modo a prueba de fallos con Network Media
3. Después, se deberá iniciar Windows
4. Insertar en el ordenador la memoria USB o cualquier otro medio que hayas utilizado
5. Instalar el software para eliminar el Ransomware, utilizar Malwarebytes Anti-Malware para eliminar la infección, utilizar HitmanPro como segunda opción, u otra opción como el programa Emsisoft Emergency Kit.
6. Por último, utilizar la herramienta de descifrado

4

¿Qué no debes hacer?

¿Qué no debes hacer?

1. No pague el rescate. Si el ciberdelincuente siente que puede seguir engañando a la víctima, es posible que le pida que pague una y otra vez y asi sucesivamente. Pero, supongamos que el ladrón es sincero y está dispuesto a descifrar los archivos si la víctima paga. ¿ Le darías dinero a un ladrón?. Ese ciberdelincuente usará el dinero para seguir dañando a otras personas y con esto haciendo negocio.. Hay múltiples estudios que muestran que los archivos probablemente no se desbloquearán a pesar de pagar lo que el atacante pida.

¿Qué no debes hacer?

2. Proporcionar información personal al responder mensajes de texto, mensajes instantáneos, llamadas telefónicas o correos electrónicos. No solo puede ser un intento de phishing (incluso viniendo de una fuente de confianza), este correo electrónico puede ser utilizado para obtener información para un ataque futuro. Hay muchas bandas o grupos diferentes que realizan estafas de ransomware y usan distintos métodos para intentar infectar su equipo. Una de las más populares es el uso de spam. Puede ser un correo electrónico en el que se le diga que un paquete no pudo entregarse. Jamás dar click en estos enlaces, si no algo malo podría ocurrir.

¿Qué no debes hacer?

3. No dejar la conexión a Internet activa durante un ataque de ransomware.

4. No ejecutar copias de seguridad cuando el sistema esté infectado con ransomware. En el momento en que sospechemos que nuestros sistemas esten infectados, hemos de dejar de hacer copias de seguridad de nuestros datos de manera inmediata. Así evitaremos que el destino de nuestra copia de seguridad se vea infectado.

¿Qué no debes hacer?

5. No hacer nunca una copia de seguridad. Creemos que nunca sucederá nada malo, hasta que ocurre. Lo mejor, si tenemos un virus, si alguien borra accidendalmente algo, será tener una copia de respaldo para que así no perdamos tiempo, ni los datos, ni dinero, ni clientes ni nada relacionado.

6. No estar alerta por si llega un virus. La prevención es la mejor cura. Una estrategia de respaldo ha de ser el primer paso en nuestra lista de medidas para protegernos

¿Qué no debes hacer?

7. No mantenga el software actualizado. Los ciberdelincuentes saben las debilidades en el software del equipo antes que un usuario común. Cuando las descubren, intentan usarlas para acceder a estos sistemas. Esto se conoce como penetrar las vulnerabilidades. Los parches eliminan las vulnerabilidades. Lo mejor es tener a la última actualización todos nuestro softwares.

8. No usar software de seguridad. Lo mejor será tener antivirus que estén constantemente analizando los archivos y software. Algunos de estos pueden ser Norton Security o Kaspersky.

KASPERSKY lab

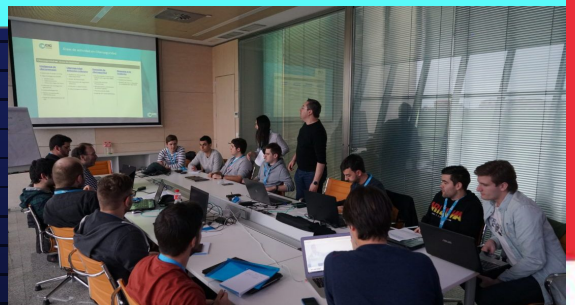
Norton™

5

¿Cómo podrías evitarlo?

¿Cómo podrías evitarlo?

La mayoría de los ciberdelitos son causados por empleados desprevenidos que no están lo suficientemente cualificados en ciberseguridad como para saber cuándo detectar las ciberamenazas en su camino. Por ello, la mejor manera de protegerse de los ataques de ransomware es invertir en una formación de concienciación sobre seguridad acreditada y rutinaria. Invertir en la formación del capital humano es la mejor manera de evitar los ataques de ransomware, ya que las bandas de ransomware son muy conscientes de que los empleados no están al día de las nuevas y mejores tácticas de ransomware. Lo ideal es que cuanta más formación práctica, simulacros de ciberataque y evaluaciones previas y posteriores a la formación ofrezca el personal, mejor preparado estará para detectar el ransomware y mejor informadas estarán las empresas sobre su nivel de riesgo de ransomware.



¿Cómo podrías evitarlo?

Algunos errores principales pueden ser abrir documentos que no vengan de una fuente fiable esto se puede solucionar con las firmas digitales las cuales hacen que sepamos al 100% con quien intercambiamos información.

Otro gran error puede ser el de reenviar el archivo, si este parece estar vacío deberíamos hablar con el que nos lo envió porque podría ser un virus. Una buena práctica es utilizar un antivirus actualizado el cual nos avisará antes de descargar el archivo y también realizar copias de seguridad regulares así la información perdida no fue demasiada. Otra buena práctica sería el de mirar los informes de seguridad en páginas como "Incibe" y estar al día con ellos para así enterarnos de campañas de phishing, nuevas vulnerabilidades...

Actualizar los sistemas automáticamente, así todas las máquinas tendrán el último parque y estarán más protegidas. Por último, ejecutar análisis programados regularmente con tu antivirus

Gracias!!