



4Geeks Academy

Plan de Respuesta a Incidente de Ransomware basado en NIST

Por: Juan Cervantes Simón

Introducción

Para el desarrollo de este ejercicio se ha expuesto un ataque de ransomware hacia la empresa **TechCo**, que, a causa de una seguridad laxa e insuficiente, ha provocado pérdidas a nivel de archivos y credenciales, así como de los sistemas de copias de seguridad, por lo que fué imposible realizar tareas de recuperación.

Para esta tarea se requiere elaborar un plan de respuesta para estas situaciones que se alinee con el marco general del esquema nacional de ciberseguridad.

Activos Afectados

En el ataque sufrieron el cifrado de archivos tanto el servidor general como el sistema de copias de seguridad como la base de datos con información de clientes.

Asimismo la infraestructura de red débil y mal configurada fué fácilmente afectada por el ataque, permitiendo la propagación del mismo al resto de áreas de la empresa.

El ataque a estos activos ha provocado la pérdida de documentación operativa, información privada de los clientes, contratos, copias de seguridad y registros confidenciales entre otros datos identificativos, tanto del personal como de los clientes y socios de la empresa.

Vulnerabilidades Presentes

- **Infraestructura de red**

La falta de segmentación y gestión de las áreas de difusión de la red ha jugado un importante papel para el desarrollo del ataque, siendo que, al no existir segmentación alguna entre departamentos, permitiendo el movimiento lateral del ransomware.

- **Falta de conciencia**

El ataque inició porque un empleado descargó y ejecutó un archivo inconscientemente, sin verificación de su origen ni comprobaciones con figuras de responsabilidad, eso denota una formación insuficiente contra el phishing y falta de instrucción en buenas prácticas en el manejo de información empresarial.

- **Falta de monitoreo**

En la empresa no existía ningún tipo de sistema de detección de anomalías, lo cual permitió que el ransomware se desarrollara en los primeros instantes del ataque.

- **Falta de resiliencia de copias de seguridad**

Aunque la empresa sí contaba con un sistema de copias de seguridad, el hecho de que estuviera en la misma red en la que estaban los ordenadores infectados provocó la pérdida de las copias de respaldo, destruyendo por completo la posibilidad de mitigar el ataque con rapidez.

Medidas de Protección Propuestas

Segmentación de Red

- Es altamente recomendable aplicar configuraciones más sólidas en lo que a la infraestructura de red se refiere, lo más recomendado es realizar una división por áreas/departamentos para poder frenar el avance de futuras amenazas con objeto de mitigar su impacto y, consecuentemente, reducir el tiempo de recuperación de los servicios.

Protección de dispositivos finales

- Para prevenir la ejecución de este tipo de programas en la medida de lo posible, lo más recomendable es instalar programas EDR, así como configurar políticas de ejecución de aplicaciones basadas en firmas para evitar ejecuciones de aplicaciones desconocidas, como por ejemplo **CrowdStrike Falcon**.

Protección de correo electrónico

- Implementar filtrado anti-spam y de phishing, así como la eliminación de correos electrónicos que contengan archivos ejecutables, con esto se conseguiría reducir drásticamente las probabilidades de que los empleados, como por ejemplo **StrongestLayer**.

Gestión de las copias de seguridad

- Para optar por una configuración de copias de seguridad se recomienda, además de tener un servidor adicional, aislado, en el que almacenar los respaldos, añadir una política de verificación de funcionamiento de las copias generadas, para aportar resiliencia adicional al sistema de copias de seguridad.

Controles de acceso

- Con objetivo de impedir accesos no autorizados se recomienda implementar la autenticación de múltiple factor para los inicios de sesión corporativos, así como añadir el principio de mínimo privilegio para los inicios de sesión, de esta forma se pueden prevenir escaladas de privilegios por parte de los atacantes.

Concienciación del personal

- Con el objetivo de que la plantilla sea capaz de detectar esta clase de amenazas es necesario instaurar formaciones periódicas, así como realizar simulaciones de phishing con objetivo de aumentar la conciencia de los usuarios al respecto y que sea más difícil para los empleados caer en este tipo de amenazas.

Medidas de Detección Recomendadas

Herramientas de Monitoreo

- Soluciones SIEM para la recolección y correlación de los logs.
- Programas EDR con capacidad de detección de Ransomware.
- Agregar sistemas NDR para el análisis del tráfico de red.

Indicadores de Compromiso

- Monitoreo de cambios de configuración y/o extensiones de archivos en poco tiempo.
- Alertas de red a dominios del tipo *command and control*.

Protocolos de Alerta

- Establecer alertas automáticas basadas en la edición de archivos.
- Notificación inmediata con el equipo de respuesta por medio de un canal con disponibilidad completa.

Análisis de Comportamiento

- Monitoreo de actividad de los equipos en horarios no laborables.
- Base de comportamiento y tráfico de red de los equipos de los empleados.

Plan de Respuesta a incidentes

Activación del protocolo - Equipo de respuesta (0 - 40 primeros minutos)

- ❖ En cuanto las alarmas de incidencia se disparan, es necesario que el equipo de respuesta se movilice para determinar el impacto y tipo de amenaza al que la empresa se enfrenta.

Contención de la amenaza (1 - 3 horas)

- ❖ El equipo procederá al aislamiento preventivo de los sistemas afectados, así como al bloqueo de los dominios, direcciones IP de todos los equipos participantes en los firewalls de la empresa y de las cuentas empresariales que hayan podido resultar comprometidas en el ataque.
Asimismo se deberán crear imágenes forenses de todos los equipos afectados para su posterior estudio, además de recopilar todos los registros a los que se tenga acceso, todo ello organizado y documentado cronológicamente.

Ánalisis e Investigación (3 - 24 horas)

- ❖ Una vez acotado y neutralizado el incidente, en las siguientes horas se analizará el software malicioso con objetivo de identificar el principio de cifrado usado para encriptar los archivos y así poder empezar a explorar opciones de descifrado,

asimismo analizar el comportamiento del malware para poder acotar con mayor precisión el alcance del ataque

Comunicación

- ❖ Habiendo completado el análisis se informará a los departamentos que han sido afectados en el ataque, así como al equipo ejecutivo.
Acto seguido se informará a las autoridades, y clientes afectados en caso de que en el análisis se hubiera identificado.

Toma de Decisiones

- ❖ Por último se intentará usar copias de seguridad, si estas no han resultado afectadas en el ataque de ninguna forma, adicionalmente y con objetivo de recuperar la información que no figuraba en las copias de seguridad, se valorarán las opciones de descifrado, por medio de herramientas gratuitas o por medio de entidades que ofrezcan servicios de descifrado.

Medidas de Recuperación

Eliminación de la Amenaza

- Para poder recuperar la cobertura de servicios a un estado lo más parecido posible a los momentos antes del ataque, se procederá con la limpieza de todos los equipos afectados, así como a la reinstalación de todos los sistemas y servicios en los equipos una vez se haya verificado que el ataque no ha dejado ninguna vulnerabilidad de tipo *puerta trasera* que pueda ser explotada posteriormente.

Restauración de sistemas

- Para dar paso al funcionamiento normal de la empresa se dispondrá a la restauración de los servicios y sistemas esenciales para el funcionamiento empresarial básico con la mayor prioridad a lo largo de los primeros días del ataque, siguiendo sucesivamente con los sistemas menos relevantes y servicios de funciones no-críticas para la empresa.
Una vez aplicada la restauración verificar todas las versiones de servicios, aplicando los parches de seguridad más actuales y estables, así como la consiguiente verificación del funcionamiento en un entorno saneado.

Plan de continuidad

- Para que la empresa pueda reanudar su actividad con normalidad se iniciará, como bien se ha comentado con anterioridad, con las funciones básicas y esenciales de la empresa, al tiempo que se informa de la anomalía en las gestiones a los clientes, informando sobre los plazos estimados de recuperación, adicionalmente el grupo ejecutivo ha de coordinarse con el departamento legal para emitir las notificaciones normativas según la regulación vigente.

Retorno a operaciones normales

- Una vez se valida la recuperación de la totalidad de los equipos con el equipo de seguridad, se procederá a la restauración completa de la estructura empresarial, junto con el consecuente monitoreo de los sistemas, verificando tiempos de respuesta y rendimientos aceptables

Plan de Mejora continua

- Trás la recuperación de las funciones empresariales, resta evaluar un plan de mejora con respecto a lo sucedido indicando todo lo que se ha aprendido en lo recabado durante el incidente, tiempos de detección, respuesta y recuperación que se ha percibido así como el coste del incidente con respecto a la información perdida y el tiempo en el que no se han prestado servicios a los clientes.
- Actualización del plan de respuesta en caso de que en las reuniones se hayan percibido aspectos a mejorar, así como aplicar las mejoras ya expuestas en el apartado de medidas de protección.
- Monitoreo y auditaje de la estructura empresarial, incluyendo revisiones trimestrales de los controles y eficacia de estos; así como una programación de auditorías anuales con una empresa de ciberseguridad externa a la empresa con objeto de encontrar nuevas formas de mejorar la seguridad y el plan descrito en este informe