

PLAN DE RESPUESTA

Nicolás Oriol Sengáriz
4Geeks

Índice

Plan de respuesta según NIST	2
Detección	2
Contención	2
Eliminación	2
Recuperación	3
Respuesta a un ataque	3
Protección de datos	4

Plan de respuesta según NIST

Detección

El mejor método para detectar el ataque es tener EDR en cada endpoint, todos conectados a un SIEM con alertas de detección de comportamientos anómalos y modificación de archivos importantes y realizar

También se pueden usar IDS o IPS para monitorear si no se desea tener EDRs.

Es necesario validar el incidente para descartar falsos positivos.

Debe haber monitoreo del estado de la red y de los sistemas 24/7.

Contención

Lo primero que se tiene que hacer al detectar un ataque es identificar el equipo o equipos infectados y aislarlos para evitar que el ataque se propague.

También es recomendable aislar los servidores con información crítica o con los backups, de esta manera si no se puede contener el ciberataque en un equipo o varios nos aseguramos que no afecte a la información más sensible.

Es recomendable realizar una adquisición en caliente para investigar con más calma el ataque luego.

Eliminación

Se realiza un escaneo profundo para encontrar los componentes del ataque y se procede a eliminar los componentes y las tareas programadas dejadas por el atacante, si es que hay.

Se realiza un cambio de contraseña en todas las cuentas.

Recuperación

Después de verificar que el sistema está “limpio”, es decir, se han eliminado los componentes del ataque se procede a restaurar desde los backups.

Una vez verificada la limpieza del sistema, se procede a la restauración de los equipos y servidores afectados desde la última copia de seguridad considerada " limpia".

Una vez restaurado todo hay que realizar pruebas de integridad que consisten en verificar que los sistemas restaurados funcionan correctamente antes de reconectarlos a la red productiva.

Respuesta a un ataque

La empresa al contar con EDRs conectados a un SIEM y con monitoreo continuo 24/7 hubiera detectado rápidamente el ataque.

Al detectar el equipo o equipos afectados se pueden aislar para evitar la propagación.

Una vez controlado el ataque en un equipo o varios equipos, se procede a realizar un escaneo profundo para saber encontrar el vector de entrada, si es un archivo descargado de un correo, una vulnerabilidad sin parchear...

El CISO es el encargado de hablar con las autoridades pertinentes, con los seguros, con los dueños, accionistas, con quien sea.

Para prevenir la recurrencia se debe mejorar la ciberseguridad:

- Se debe educar a los empleados en la cultura de ciberseguridad
- Se deben realizar escaneos periódicos para detectar vulnerabilidades y corregirlas
- Se deben realizar pruebas de pentesting periódica para ver cómo de efectiva es la seguridad
- Se debe tener todos los servicios y programas lo más actualizado que se pueda para que sean lo más seguros posible.
- Se debe configurar todo de forma robusta
- Se deben segmentar las redes para evitar el movimiento lateral y si es posible crear DMZs para los servidores o equipos críticos

Protección de datos

Se realizarán copias de seguridad periódicas (backups).

Se usará la regla **3-2-1** que significa: tres copias de seguridad, en dos soportes distintos, con una copia fuera de línea (offline).

Se cifrarán todos los datos sensibles, tanto en reposo como en movimiento.

En reposo se cifrarán bases de datos y discos duros mediante algoritmos robustos como AES-256.

En movimiento existirá un uso obligatorio de protocolos seguros (TLS/SSL) para toda comunicación de red.

Además, habrá controles de acceso.

Los usuarios solo tendrán acceso a la información mínima necesaria para sus labores, basándose en el principio de menor privilegio.

Para todos los accesos a aplicaciones críticas o de forma remota se pedirá una segunda forma de verificación, en este caso es la Autenticación Multifactor (MFA).