Política

Plan de respuesta a incidentes

Checklist de seguridad para tu empresa

Checklist

Checklist

Checklist

Introducción

El ransomware está dirigido a usuarios domésticos, empresas y redes gubernamentales y puede provocar la pérdida temporal o permanente de información confidencial o de propiedad exclusiva, la interrupción de las operaciones regulares, las pérdidas financieras incurridas para restaurar los sistemas y archivos, y el daño potencial a la reputación de una organización.

Nuestro Checklist de seguridad le permitirá tener una guía paso a paso para poder actuar ante posibles incidentes informáticos que sucedan en su organización, aunque este documento esté enfocado hacia la posible materialización de una infección de ransomware, es completamente funcional en caso de cualquier otro tipo de incidente que tenga la posibilidad de poner en riesgo la operación de su empresa al momento de afectar la disponibilidad de los recursos de la misma, sin importar si el incidente es por desastres naturales, aplicaciones maliciosas, desgaste normal o mecánico u ocasionado por acciones humanas.

Dentro de este Checklist usted encontrará una guía práctica para prevenir, contener, reaccionar y recuperar su organización de incidentes informáticos.

Checklist

Prevención

Objetivo: Implementar la triada preventiva (Usuarios, tecnología y políticas) cuya única finalidad es minimizar el área de impacto para reducir la posibilidad de sufrir un incidente con Ransomware hasta en un 90%. La prevención es tu mejor arma.

Procesos

Asegúrate de cumplir con las políticas de seguridad que se te han entregado, o con las que ya cuentas en tu organización, lo importante es darle seguimiento, no es lo mismo que digamos que contamos con políticas a que realmente las llevemos a cabo, esto va a ser una gran diferencia en la prevención de incidentes.

☐ **Inventariado de activos:** El inventario de tus equipos o activos informáticos y de información es importante, ya que nos permitirá el saber ¿a qué? ¿quién? ¿por qué? y ¿cómo? Tiene acceso a nuestros activos.
☐ **Relación con proveedores:** Controlar la relación con proveedores te ayudará a mantener nuestra información segura a través de acuerdos y contratos correspondientes.
☐ **Copias de seguridad**: Las copias de seguridad van a ser tu columna vertebral de seguridad en materia de prevención. Ver anexo Política Backup y Regla 3R
☐ **Culturización de usuarios**: los usuarios forman parte de la estrategia de seguridad informática en la organización, es necesario no sólo educarlos en temas de seguridad, sino generar un ambiente de cultura organizacional en el que la seguridad esté incluida. Ver anexo Culturización.

Tecnología

☐ **Anti-Malware**: las soluciones antimalware son vitales para que podamos controlar nuestra organización en ambientes potencialmente hostiles. Léase el anexo Soluciones antimalware.
☐ **Respaldos**: Las soluciones de respaldos son de vital importancia a la hora de llevar a cabo nuestra política de copias de seguridad. Ver anexo Política Backup.
☐ **Configuraciones**: Las configuraciones por defecto pueden ser catastróficas al momento de no atenderse. Ver anexo Carpeta Hardening.
☐ **Deshabilitar SMB1**
☐ **Bloquear scripts Powershell Ej.** (powershell Set-ExecutionPolicy -ExecutionPolicy Restricted)
☐ **Bloquear Macros de documentos**
☐ **Deshabilitar, cambiar Puerto o uso de VPN para uso de servicio RDP**
☐ **Aplicación de mínimo privilegio**
☐ **Aplicación de 2FA**
☐ **Segmentación de redes**
☐ **Gestión de vulnerabilidades**

Checklist

Personas

☐ **Culturización:** La culturización lleva a los usuarios a no sólo conocer de posibles amenazas, sino a nosotros como personal de IT a detectar comportamientos maliciosos y poder atacarlos, convirtiendo a los usuarios en nuestra primera línea de defensa. Ver anexo culturización.

Contención

Si algo ha salido mal o no planeado, esta guía de contención de incidentes te dará la oportunidad de identificar qué es lo que tienes que hacer.
Mantener la calma: Es momento de pensar con cabeza fría y nervios de acero, caso contrario sólo vamos a equivocarnos en algún proceso u omitir alguno.

Paso 1: Aislar la infección

☐ Es necesario cortar toda comunicación de nuestro paciente cero con el resto de nuestra red empresarial, por ello desconecta:

- Redes inalámbricas (Bluethoot, NFC)
- Red ethernet

Paso 2: Asegura tus respaldos

☐ Aísla de la red los dispositivos o medios donde se encuentran tus copias de seguridad, esto por lo menos hasta que tengamos garantizado que la infección ha sido controlada.

Paso 3: Comunicar el incidente

☐ En base a los planes de contingencia realizados, es necesario poner en práctica el plan de comunicación de incidentes, para que el resto de la organización realice sus procesos necesarios de contención.

Paso 4 (opcional): No reiniciar

☐**:** Si apagamos o reiniciamos el equipo, el ransomware puede interrumpir su proceso de cifrado, dañando así tus archivos de por vida, o eliminando algunos.

- Mantenlo en modo de ahorro de energía
- Mantenlo aislado de la red

Paso 5: Copia de seguridad

☐ Crea una copia de seguridad o imagen del equipo infectado, la mayoría de las veces los ransomware mantienen sus xploits en los equipos que le permitirán eliminar o sobrescribir los archivos cifrados después de cumplirse el tiempo del rescate.

Checklist

Paso 6: Cuarentena

☐ Si tu solución antimalware detectó el ransomware y lo puso en cuarentena, no lo elimines, con ello se puede encontrar la llave de eliminación de cifrado

Paso 7: Determinar el alcance de infección

☐ Basado en nuestro inventario de activos es necesario realizar los siguientes pasos:

- Identificar las unidades de red asignadas al equipo infectado.
- Identificar carpetas compartidas en el equipo infectado con otros equipos.
- Identificar dispositivos de almacenamiento (o de cualquier tipo) en red.
- Identifica dispositivos extraíbles, usb, discos duros, etc. Conectados al equipo.
- Identifica los servicios de almacenamiento en la nube (Dropbox, One drive, Google drive) con carpetas mapeadas en el equipo infectado.

Paso 8: Identificar cepa del ransomware

☐ basado en las herramientas de identificación de ransomware como lo es EMSISOFT o NO MORE RANSOMWARE.

Erradicación

Paso 1: Eliminar el malware

☐ para realizar la eliminación del malware es necesario haber realizado por lo menos la copia de seguridad con el equipo infectado, esto ayudará a tener la posibilidad de recuperar nuestra información en un futuro, y aplicar cualquiera herramienta de emergencia.

- Uso Kit de emergencia EMSISOFT
- Uso de herramienta Hitman Pro

Checklist

Recuperación

Si algo ha salido mal o no planeado, esta guía de contención de incidentes te dará la oportunidad de identificar qué es lo que tienes que hacer.

Mantener la calma: Es momento de pensar con cabeza fría y nervios de acero, caso contrario sólo vamos a equivocarnos en algún proceso u omitir alguno.

Opción 1: Copias de seguridad:

☐ **Restaurar copias de seguridad:** para restablecer tus copias de seguridad de forma correcta debes realizar lo siguiente:

- Localizar copias de seguridad
  - Hay que asegurar que están todos nuestros archivos
  - Verificar la integridad de las copias de seguridad

☐ Eliminar el ransomware de los sistemas infectados

☐ Restablecer tus operaciones con tus procesos previos.

Opción 2: Eliminar cifrado

☐ **Conocer el Ransomware:** Determine la cepa y la versión del ransomware si es posible.

☐ **Localizar un des-encriptador:** puede que no haya uno para las nuevas cepas de ransomware.

☐ **Reconectar:** Adjunte cualquier medio de almacenamiento que contenga archivos cifrados (discos duros, memorias USB, etc.).

☐ **Descifrar archivos.**

Opción 3: Clientes y proveedores

☐ **Localizar la última copia de seguridad:** es necesario localizar por lo menos la última copia de seguridad que se tenga, ya sea de hace unos meses o hace unos años.

☐ **Solicitar información:** Solicitar a nuestros clientes y proveedores que nos envíen información previamente compartida con ellos.

Checklist

Opción 4: Laboratorio de recuperación

☐ **Copia de seguridad:** Realizar una copia de seguridad del disco(s) duro(s) o dispositivo(s) afectado(s).

☐ **Enviar activos:** Realizar el envío de los activos para su análisis.

☐ **Recuperar información:** Solicitar de forma minuciosa qué información es la que se busca.

Opción 5: Pagar el rescate

Si no cree capaz de llevar el proceso usted mismo, puede contactar a especialistas para realizar el trabajo.

☐ **Contacto:** busque ponerse en contacto con las personas o responsables de su infección.

☐ **Negociar:** si es posible, puede intentar negociar un rescate más bajo y / o un período de pago más largo.

☐ **Métodos de pago:** determina los métodos de pago aceptables para el ransomware: Bitcoin, Cash Card, etc, y adquiera la moneda específica para realizar el mismo.

☐ **Validar dirección de pago:** esto se encuentra en la pantalla o notas del del equipo infectado con ransomware, normalmente se utiliza el explorador TOR, ya que se crea un sitio TOR que se ha configurado para este caso de rescate específico.

☐ **Reconectar:** Asegúrese de que todos los dispositivos que tienen archivos cifrados estén conectados a su computadora

☐ **Pague el rescate:** transfiera el pago a la billetera del rescate

☐ **Esperar:** A partir del pago será momento de esperar para que se pueda realizar la eliminación de cifrado y que no sean dañados los archivos al momento de tratar de revertir el mismo.