Ransomware como WannaCry es una amenaza creciente y global que amenaza su información.

Verifique este Check List para prevenir un ataque de RANSOMWARE en su empresa.

Ransomware es un malware malicioso que encripta archivos en su computadora y servidores y puede infectar una red completa en cuestión de minutos. Una vez que sus archivos han sido encriptados, Hackers o Cyber criminales mantienen sus archivos secuestrados, requiriendo el pago correspondiente para des encriptarlos y devolverle su información. El último ataque, llamado WannaCry, infectó más de 200,000 sistemas en 150 paises en cuestión de pocos días. Usted necesita tomar los pasos necesarios para proteger su ambiente ahora, ésta es una amenaza global que obliga acción inmediata.

Administración Del Inventario

- ☐ Catalogar todo el software que se despliega a través de la red
- ☐ No hay sistemas operativos no compatibles (Windows XP o 2003) que se ejecutan en mi red
- ☐ Nadie está ejecutando software no autorizado (dropbox / icloud / etc, servicios de streaming, etc.)
- ☐ No hay computadoras desconocidas / no administradas, puntos de acceso u otros dispositivos en la red

Gestión de Parches

- ☐ Todos los servidores han gestionado los parches de Windows y están actualizados
- ☐ Todas las estaciones de trabajo han gestionado los parches de Windows y están actualizadas
- ☐ Todos los demás sistemas operativos cuentan con un mantenimiento de parches regular y están actualizados
- ☐ Todas las aplicaciones y sus parches se mantienen y su actualización es monitoreada

Firewall - Cortafuegos

- ☐ Estamos ejecutando un firewall o cortafuegos de grado empresarial, no un cortafuegos para consumidores
- ☐ El filtrado avanzado, la detección de intrusos, la clasificación de tráfico de la capa 7 y el cortafuegos están totalmente administrados
- ☐ Ejecutándose la última versión del software de firewall y actualizaciones administradas
- ☐ Monitoreo de alertas de firewall

Software de Antivirus (AV)

- ☐ Estamos ejecutando un software de antivirus de grado empresarial, no un software de antivirus para consumidor
- ☐ Todos los servidores y estaciones de trabajo están ejecutando AV con escaneo en tiempo real
- ☐ Gestionado de forma centralizada y actualizado
- ☐ Configuración de políticas en AV para bloquear la ejecución de ejecutables dañinos, junto con alertas.
- ☐ Las alertas del AV son monitoreadas

Respaldos

- ☐ Todas las máquinas que tienen datos críticos en ellas se respaldan
- ☐ Las imágenes de los servidores se realizan al menos mensualmente
- ☐ Copias de seguridad de archivos se ejecutan diariamente
- ☐ Siguiendo la regla de copia de seguridad 3-2-1 (3 copias de seguridad, almacenadas en 2 medios diferentes, con 1 fuera del sitio)
- ☐ Prueba de restauraciones de copias de seguridad al menos una vez al mes
- ☐ Supervisión de informes de fallos de copia de seguridad

Filtrado

- ☐ Antispam/anti-phishing implementado
- ☐ Filtrado de archivos adjuntos en el correo electrónico (.exe, scr, .com, etc.)
- ☐ Filtrado de DNS implementado
- ☐ Mostrar extensiones de nombre de archivo en Windows
- ☐ No habilitar macros (para documentos de Microsoft Office)

Búsquedas en la Web

☐ Deshabilitar todos los scripts / plugins innecesarios

☐ Los navegadores están actualizados y ejecutan las últimas versiones de los complementos necesarios

Permisos

☐ Aplicar el principio de los privilegios mínimos en los sistemas y datos

☐ Políticas de restricción de software establecidas para evitar que los programas se ejecuten desde ubicaciones de ransomware comunes (carpetas temporales, etc.)

Prevención avanzada

☐ Políticas de grupo

☐ Exploraciones periódicas de vulnerabilidad / puerto

☐ Inspecciones periódicas de la red para desactivar cualquier servicio innecesario / vulnerable

☐ Segmentación de la Red para servidores, backup, datos, puntos finales

☐ Deshabilitar puertos USB para unidades flash, etc.

Capacitación

☐ Entrenamiento de concientización de aspecto de seguridad: Ofrezca ejemplos de qué evitar

☐ Ataques simulados (phishing, etc.) con plan de acción (por ejemplo, desconectar de la red / Wi-Fi)