Protégete contra WannaCry, un «arma de destrucción masiva» en forma de ransomware

Enorme. Sin precedentes. Un arma de destrucción masiva. Así han descrito los expertos en ciberseguridad el gusano de ransomware WannaCry que ha sacudido a organizaciones de todo el mundo. Hasta este momento se han paralizado centenares de miles de ordenadores de 150 países, desde sistemas sanitarios del Reino Unido hasta universidades de toda Asia. Y la amenaza no ha remitido. Ya se están detectando nuevas variantes de WannaCry. Variantes a las que les falta el kill switch que mitigaba los daños del original.

¿Cómo se puede afrontar la amenaza de WannaCry?

Resuelve de inmediato tu vulnerabilidad de Windows

Algunos agentes malintencionados han aprovechado la conocida vulnerabilidad de Windows, EternalBlue. Este hecho reafirma la importancia de instalar parches de seguridad cuanto antes y realizar un mantenimiento del software y los sistemas operativos soportados.

Por ello, recomendamos que las empresas:

- Sigan instalando parches de seguridad
- Actualicen el sistema operativo de Microsoft a una versión con soporte
- Instalen parches en las aplicaciones de Arcserve UDP y los servidores RPS
- Bloqueen los protocolos heredados, como SMBv1, para protegerse contra las evoluciones futuras del malware
- Instalen cuanto antes la actualización de seguridad MS17-010 de Microsoft

No pagues el rescate

En el caso de WannaCry, los atacantes necesitan realizar un descifrado manual. Teniendo en cuenta la intensidad con la que se busca a los responsables, se espera que los pagos de los rescates permanezcan intactos en direcciones de Bitcoin y que las solicitudes de descifrado queden sin respuesta.

Dicho esto, es posible que los archivos almacenados fuera del Escritorio, de la carpeta Documentos o de los dispositivos extraíbles se puedan reponer mediante la herramienta de recuperación.

Evalúa tu estrategia de copia de seguridad y recuperación ante desastres

WannaCry ha situado en el punto de mira la necesidad fundamental de acabar con el ransomware. Por ello, recomendamos que todas las empresas tomen medidas de inmediato para asegurarse de poder hacer copias de seguridad y recuperar sus datos correctamente:

- **Examina tus RPO y RTO**
  Asegúrate de realizar copias de seguridad de tus sistemas críticos con la mayor frecuencia posible y de que la recuperación del sistema se efectúe de acuerdo con las necesidades de tu negocio.
- **Confirma que se ha realizado una copia de seguridad de todas las fuentes de datos**
  Identifica los servidores o fuentes de datos que se hayan quedado fuera de tu plan de protección de datos y aplica el nivel correcto de disponibilidad de datos para asegurarte de que sean recuperables.

- **Accede al servidor de copia de seguridad como usuario**
  Al iniciar sesión en tu servidor seguro, asegúrate de hacerlo como usuario, no como administrador. No uses nunca tu cuenta de administrador al abrir correo electrónico o navegar por Internet.
- **Protege el elemento de protección**
  Asegúrate de que tus archivos de copia de seguridad se almacenen en un servidor seguro con un acceso limitado solo a quienes definitivamente lo necesiten. Estos archivos son tu mejor oportunidad para solucionar problemas, así que cerciórate de que están seguros.
- **La regla 3-2-1**
  Guarda al menos tres copias diferentes de tus datos en dos soportes distintos, y almacena al menos una copia fuera de las instalaciones. Es fundamental que tu estrategia de copia de seguridad incluya redundancias y aproveche las opciones de almacenamiento invulnerables a los ataques, como cintas, discos offline y la nube.
- **Sigue el principio de los privilegios mínimos**
  Al configurar cuentas, concede solo el grado de privilegios de acceso que sea absolutamente necesario para cada rol.

Recuperación de ransomware en el mundo real

«El último ataque de ransomware fue increíblemente importante. Afectó a 45 servidores diferentes, se extendió por sí mismo y simplemente se desbordó. De hecho, el equipo directivo se mudó a mi oficina por un tiempo; ya sabéis lo que eso significa.»

Gracias a Arcserve UDP, el administrador de la red de IT pudo restaurar con rapidez la copia de seguridad de la noche anterior, con lo que evitó un rescate de 30.000 dólares.

Elude los rescates con Arcserve Unified Data Protection

La galardonada aplicación Arcserve UDP, la cual goza de la confianza de más de 48.000 clientes de 150 países de todo el mundo, proporciona las capacidades de nivel empresarial y la facilidad de uso que requieren los desbordados y reducidos equipos de IT.

Consigue la flexibilidad que necesitas para recuperarte tanto de ataques masivos de ransomware como de desastres habituales y cotidianos, a la vez que cubres las necesidades específicas de tu negocio:

- Despliega Arcserve como software, aplicación o solución en la nube, sin ningún esfuerzo
- Protege los datos físicos y virtuales sin importar dónde estén: en las instalaciones, fuera de ellas, offline y en la nube
- Identifica con facilidad RPO y RTO reales, configura pruebas automáticas e identifica las máquinas desprotegidas con capacidades de recuperación asegurada
- Redimensiona sin interrupciones tu cobertura de copias de seguridad y recuperación a medida que crece tu empresa: de 1 TB a 1 PB, y más allá
- Pon en marcha al instante aplicaciones críticas con el modo de espera virtual o Instant Virtual Machine
- Recupera tus datos a partir de copias de seguridad basadas en archivos y en imágenes o soluciones disponibles en todo momento

Y hazlo todo desde una sola consola de gestión elegantemente sencilla

Asegura tu protección

Ponte en contacto con tu representante de Arcserve o llama al +34 935484134 para empezar hoy mismo

Para obtener más información sobre Arcserve, visita **arcserve.com**