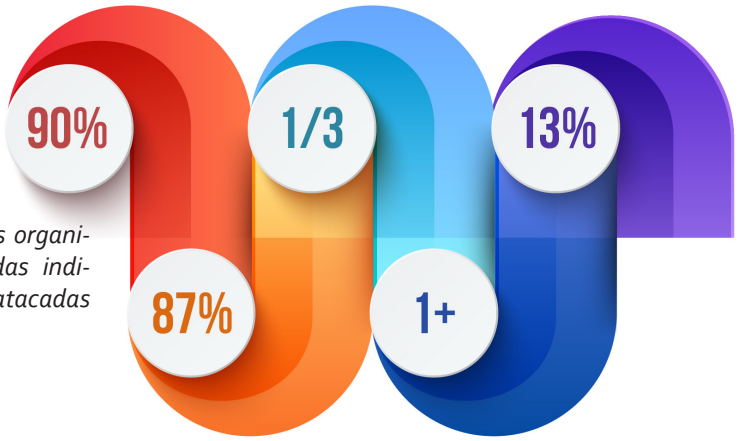
La cinta LTO Ultrium, el mejor escudo contra ransomware

La cinta magnética es una tecnología multiherramienta que respalda las 5 mejores prácticas para proteger y recuperar los datos de un ataque de ransomware. Una de las principales preocupaciones de los líderes empresariales debido a las graves consecuencias de un ataque exitoso.

Ataques de ransomware en cifras

La investigación realizada recientemente por IDC* a empresas de todo el mundo revela que:

1/3 de las organizaciones había sufrido un ataque de ransomware o una brecha de seguridad que había bloqueado el acceso a sus sistemas o datos en los últimos 12 meses.



Más del 90% de las organizaciones encuestadas indicaron haber sido atacadas por malware.

Sólo el 13% de las organizaciones que habían sido víctimas de un ataque de ransomware no habían pagado un rescate.

87% de ellas haber sido víctimas de un ataque exitoso.

No es raro que las organizaciones sean atacadas más de una vez por ransomware.

Además, los ataques de ransomware se han duplicado con creces desde principios de la década de 2020, impulsados por el aumento del teletrabajo a raíz de la pandemia y, desde la invasión de Ucrania, se hacen todavía más frecuentes, diversos y complejos.

*Informe titulado "Proactive Defense Strategies Provide the Best Chance to Defeat Ransomware", enero 2022, esponsorizado por el programa LTO y escrito por Phil Goodwin, Research Vice President de IDC.

Las graves consecuencias de ser víctima de un ransomware

Las consecuencias de un ataque exitoso de ransomware a los datos pueden llegar a ser devastadoras para una empresa, con múltiples efectos a corto y largo plazo.
El impacto inmediato del ransomware en las organizaciones es la pérdida de productividad de los empleados, la interrupción de las operaciones, la concentración de todos los recursos de la empresa para minimizar el tiempo de respuesta a la catástrofe y el pago de rescates desorbitados que pueden llegar a alcanzar los millones de euros.

Mientras que las consecuencias a largo plazo incluyen la pérdida de ingresos, la pérdida permanente de clientes, la pérdida irrecuperable de datos, las sanciones reglamentarias por violaciones a la protección de datos, la pérdida permanente de la reputación de la organización y las demandas de los accionistas y otros colectivos por negligencia.
Por eso es sumamente importante que las organizaciones tomen las buenas medidas para estar bien protegidas ante este peligroso malware.

LA CINTA LTO ULTRIUM RESPALDA LAS 5 MEJORES PRÁCTICAS DE PREVENCIÓN Y RESPUESTA ANTE RANSOMWARE

Podemos afirmar que la mayoría de las organizaciones serán atacadas tarde o temprano, la cuestión radica en saber si están preparadas para responder de forma eficiente a minimizar el impacto y reducir la probabilidad de pagar un rescate.
Las empresas deben adoptar las 5 mejores prácticas para poder defenderse contra el ransomware y garantizar la recuperación de los datos sin tener que pagar el rescate.

1. Cifrado de datos.

Los datos deben estar encriptados en reposo en el almacenamiento primario, cuando se envían a través de una red y cuando se almacenan en copias de seguridad. El cifrado es la mejor defensa contra el robo y la exfiltración de datos, ya sea por amenazas externas o internas, porque los ciberdelincuentes no pueden utilizar los datos. Por supuesto, las organizaciones deben prestar mucha atención a los sistemas de gestión de claves para que los infiltrados no puedan acceder fácilmente a las claves de cifrado.

Las unidades de cinta LTO permiten implementar el cifrado de datos, a nivel de hardware, sin penalización de rendimiento. Las cintas encriptadas serán inútiles para cualquiera sin la clave de cifrado.

2. Inmutabilidad.

Las copias inmutables impiden que nadie cambie o borre una copia de datos. Las organizaciones deben tener copias de seguridad en formatos inmutables para garantizar la integridad de los datos cuando sea necesario recuperarlos. Estas copias inmutables pueden protegerse aún más mediante el cifrado. Los equipos de TI deben asegurarse de que la inmutabilidad no pueda ser eludida mediante métodos sencillos, como el restablecimiento del reloj del sistema o los cambios de políticas.

Para garantizar la inmutabilidad de las copias se aconseja utilizar cintas LTO Ultrium WORM (Write Once Read Many), es decir, cintas LTO Ultrium que permiten "Grabar una vez, leer varias veces" para que los datos puedan ser leídos, pero no puedan ser modificados o borrados por nadie una vez escritos. Cuando la unidad de lectura/grabación LTO detecta un cartucho WORM, el firmware prohíbe modificar o alterar los datos del usuario que ya están grabados en la cinta.

3. Air Gap.

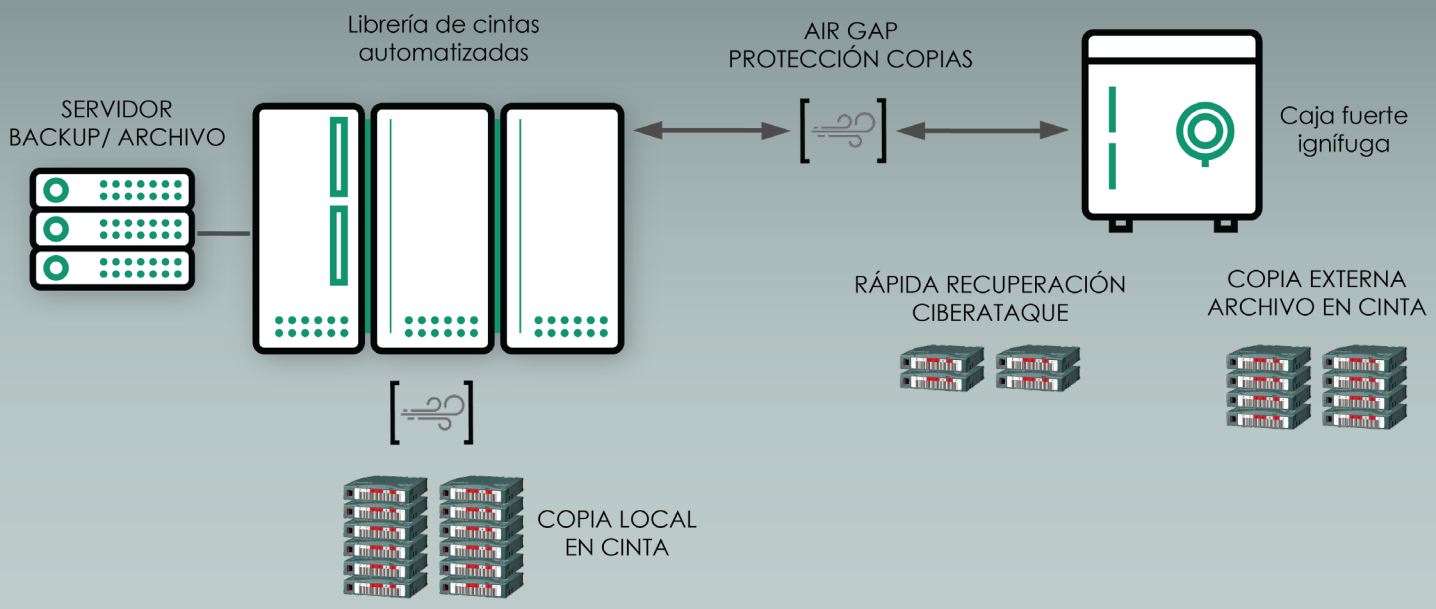
El llamado "air gap" permite desconectar físicamente las copias de datos de cualquier red consiguiendo que las copias de seguridad sean inaccesibles para los ciberdelincuentes. Una copia con air gap debe ser inmutable y encriptada para impedir las amenazas internas que puedan tener acceso físico a la copia desacoplada de la red. Es importante señalar que tener una copia de datos en la nube no es necesariamente un air gap. Los sistemas accesibles a través de una red deben garantizar que la ruta de control y la ruta de datos estén separadas por métodos de acceso y credenciales diferentes.

La cinta es posiblemente el medio más simple, de menor coste y más seguro para garantizar que los datos almacenados quedan desconectados de la red. Sin acceso físico, los delincuentes no pueden comprometer la copia de seguridad.

4. Estrategia de respaldo 3-2-1-1.

La estrategia 3-2-1-1 es una actualización de la antigua estrategia 3-2-1. Esto significa realizar tres copias de datos en dos tipos de soportes diferentes, con una copia local y desconectada de la red, y otra copia en una distinta ubicación, también desacoplada de la red.

La naturaleza amovible de la cinta permite generar tantas copias de datos como se desee y conservarlas en distintas ubicaciones desconectadas de la red, pudiendo servir como segundo tipo de soporte, copia "onsite/offline" así como copia "offsite/offline" de los datos, la parte 2-1-1 de la estrategia. Cuando se combinan con el cifrado y la inmutabilidad, estas copias son posiblemente la opción más segura que tiene una organización para asegurar la supervivencia de sus datos en caso de un ataque de malware.



5. Escaneo de respaldo.

El malware puede permanecer latente en los sistemas durante muchos meses antes de activarse. Por lo tanto, sería como una bomba de acción retardada ya que podría no detectarse inicialmente y ser respaldado con el resto de datos. Por consiguiente, es fundamental escanear todos los datos de las copias de seguridad en busca de malware antes de restaurarlos para evitar cualquier reinfección.

La tecnología LTO permite escanear las cintas al restaurarlas para detectar y eliminar el malware.

Otras ventajas de la tecnología de cinta:

- **Longevidad de archivo**. Con el cuidado adecuado, las cintas pueden preservar los datos almacenados durante más de 30 años. Las últimas generaciones de cinta ofrecen una longevidad de archivo todavía mayor, superando los 50 años. Para las colecciones digitales, esto significa integridad y estabilidad de los datos almacenados durante varias décadas.

- **Simplicidad de escalado**. La tecnología de cinta ofrece una gran flexibilidad para crecer fácilmente, pudiendo alcanzar grandes capacidades. Y los departamentos de TI pueden ampliar su almacenamiento añadiendo nuevas unidades de lectura y grabación y/o nuevas cintas a su librería de cintas.

- **Reducido coste (TCO)**. El coste de almacenar datos en soluciones de cinta es extremadamente bajo porque no requiere energía ni refrigeración para el almacenamiento de datos, a diferencia de las soluciones de disco. Las soluciones de almacenamiento en cinta son, objetivamente, la forma más rentable de almacenar datos durante extensos periodos de tiempo.

- **Rápida restauración de datos**. La generación LTO Ultrium9 tiene una velocidad de restauración de hasta 1.000 MBps (asumiendo una compresión de datos de 2,5:1) por unidad, 8 veces superior a la tasa de rendimiento de un enlace Ethernet de 1 Gbps. Las organizaciones pueden escalar la solución de cinta para que coincida con la tasa de ingesta de los sistemas de destino, lo que hace que las operaciones de datos a gran escala sean más eficientes cuando la recuperación de datos desde la nube simplemente no es viable.

- **Almacenamiento sostenible**. El almacenamiento en cinta puede reducir las emisiones de carbono hasta un 95 % y los residuos electrónicos hasta un 80%, respecto a soluciones equivalentes basadas en disco, al poder conservar los datos durante más de 5 décadas sin consumir electricidad.

- **Hoja de ruta**. La hoja de ruta LTO está marcada hasta la catorceava generación con capacidades que se han ido duplicando entre generaciones, desde su introducción hace 20 años, y que superarán los 100TB nativos en 2030.

Cintas LTO9 en un datacentre

Beneficios de adoptar una actitud de defensa proactiva ante ransomware

Constantemente surgen nuevos ataques de ransomware, siendo el comando y control de dispositivos uno de los más recientes métodos.

El ransomware y el malware forman parte de la carrera armamentística continua de los ciberdelincuentes. Atacar a las organizaciones es una ocupación a tiempo completo en el que los delincuentes dedican todo su esfuerzo a detectar posibles brechas de seguridad y nuevas formas de éxito. A medida que las organizaciones de TI erigen políticas de defensa contra determinados ataques, los delincuentes encuentran formas cada vez más creativas de burlarlas.

De hecho, las organizaciones de TI están intrínsecamente a la defensiva, pero deben tomar medidas proactivas para frustrar los ataques y garantizar que la recuperación sea una prioridad.

Sin embargo, dado que los datos son esenciales para la supervivencia de las organizaciones, siguen siendo el objetivo más común de los delincuentes. Por desgracia, los ciberdelincuentes han aprendido a atacar primero las copias de seguridad, ya sea mediante el borrado o el cifrado, porque al eliminar la posibilidad de restaurar los datos aumentan las posibilidades de que las organizaciones se vean obligadas a pagar el rescate para recuperar sus datos.

Ninguna tecnología o estrategia puede garantizar que se pueda evitar un ataque de ransomware. Por lo tanto, aunque las herramientas de identificación de puntos vulnerables son importantes, simplemente no son suficientes.

La buena noticia, si es que puede llamarse así, es que los piratas informáticos operan de forma muy parecida a un negocio. Es decir, buscan maximizar beneficio con el menor esfuerzo posible.

Los ciberdelincuentes, buscan objetivos vulnerables y rentables. Las organizaciones que se convierten en objetivos difíciles tienen más posibilidades de librarse de ellos para que busquen otras presas más fáciles de atacar.

> La mejor defensa contra ransomware es la garantía de recuperabilidad mediante la supervivencia de los datos como la que ofrece la tecnología de cinta LTO Ultrium. Aunque no es disuasoria contra los ataques, ya que los delincuentes desconocen la capacidad de supervivencia de los datos, permitirá que las organizaciones puedan pasar inmediatamente al modo de recuperación sin tener que pagar el rescate.

No dude en contactarme para recibir cualquier información complementaria sobre el contenido tratado en este documento.

Un cordial saludo.

FUJIFILM
Business Development Recording Media Iberia
Móv: +34 674 312 793
Email: anna.baldris@fujifilm.com