RESUMEN DE LA SOLUCIÓN

Cinco medidas para combatir el ransomware en el sector sanitario

Proteja a sus pacientes y su empresa con la protección de datos moderna de Pure Storage®.

Los recientes ataques de ransomware han paralizado diversos hospitales en todo el mundo. Las agencias gubernamentales de los EE.UU. han advertido al sector sanitario de que se espera un aumento de los ataques en los próximos meses. A finales de 2021, se prevé que cada 11 segundos una nueva organización será víctima de un ataque de ransomware, según Cybersecurity Ventures. Por otro lado, aunque los hospitales tienen pólizas de seguros que les cubren una parte de los costes de desbloqueo y descifrado de los datos, estas pólizas no ofrecen una garantía o una red de protección completa. Además, el pago de los rescates aún fomenta más la actividad de los ciberdelincuentes. En respuesta a ello, el Departamento del Tesoro de los EE.UU. está planeando imponer sanciones civiles a los hospitales o a sus representantes que paguen los rescates.

El tiempo de recuperación tras un ataque de ransomware afecta a la atención al paciente

Cuando un ataque de ransomware inutiliza la solución de historia clínica electrónica (HCE) de un hospital, la disrupción puede ser generalizada. La interrupción en el funcionamiento de la HCE causada por un ataque de ransomware dificulta la toma de decisiones, hace que puedan producirse errores médicos e incluso puede ser un factor que contribuya al fallecimiento de un paciente.

Los ataques de ransomware contra las organizaciones sanitarias no solo cifran las bases de datos de producción de la HCE, sino que también afectan a las copias de seguridad que se usan para recuperarse de los ataques. A medida que aumenta la sofisticación de estos ataques, las organizaciones sanitarias deben abordar la mitigación y la recuperación tras el ransomware con una estrategia moderna de ciberprotección.

Mejore su nivel de ciberprotección con una estrategia con cinco medidas

Recuperación tras el ransomware

FlashBlade™ con los Snapshots SafeMode™ de Pure Storage acelera la recuperación tras un ataque de ransomware al aumentar las estrategias de protección de los datos.

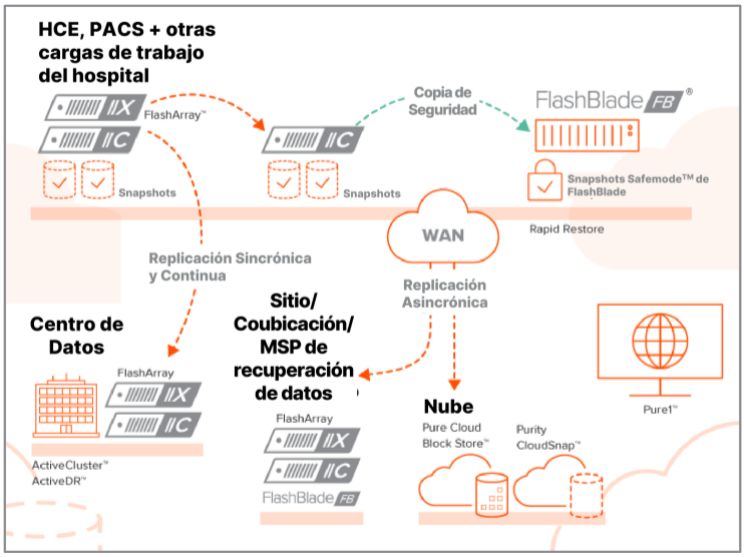
Protección de los Datos

Implante la protección de datos moderna en su organización y diga adiós a las soluciones tradicionales en silos.

Copias de seguridad y Restauración

La arquitectura moderna de Pure realiza rápidamente copias de seguridad y restauraciones de datos cuando más falta hacen.

Le presentamos cinco medidas que puede tomar para proteger sus datos de un ataque y el modo en que Pure Storage puede ayudarle:



Medida 1: aumente la visibilidad. Esta medida consiste en saber qué equipamiento tiene y por qué lo tiene. Ese servidor que se conserva en el sótano del hospital y del que nadie se acuerda puede ser el eslabón más vulnerable de su defensa. Es fundamental hacer un inventario de los recursos y los puntos de entrada y también lo es monitorizar cada recurso para detectar las anomalías que pueden ser un indicio de la existencia de una intrusión.

- La plataforma de análisis Pure1 Meta™ sintetiza la inteligencia procedente de miles de dispositivos.
- La combinación de FlashBlade con Splunk o Elasticsearch permite crear una potente plataforma de análisis y protección de los datos.

Medida 2: garantice el control. Ponga una barrera virtual alrededor de su infraestructura para controlar el acceso. El aumento de las plantillas distribuidas y de las políticas de teletrabajo exige un nuevo enfoque de la ciberprotección. Pure Storage ha creado FlashArray™ desde cero para ejecutar las VDI más rápidamente y con más densidad que cualquier otro producto del mercado.

Medida 3: reduzca la exposición al riesgo. Esta medida no consiste solo en detectar. También conlleva el desarrollo de un entorno con un mantenimiento y una supervisión constantes, para lo que hay que recoger enormes cantidades de datos con el fin de realizar complejos análisis. Por ello, es importante tener una infraestructura desarrollada para proporcionar unos resultados rápidos.

- Haga una evaluación para ver si su organización está preparada para el próximo ataque de ransomware.

Medida 4: dificulte el ataque. Los Snapshots SafeMode de Pure Storage proporcionan resiliencia gracias a unas copias de seguridad inmutables, ya que impiden que un atacante o un trabajador deshonesto borren las copias de seguridad, incluso en caso de que se hayan vulnerado las credenciales de administrador. Además, los Snapshots SafeMode protegen los datos si se produce un ataque. Por otro lado, la incorporación del cifrado hace que las cosas sean aún más difíciles y costosas para el atacante. En la Conferencia RSA de 2019, Pure Storage y Thales presentaron el Cifrado Transparente Vormetric para el Almacenamiento Eficiente, el primer sistema de cifrado de datos de extremo a extremo del sector TI y seguridad que logra la reducción de los datos de la cabina.

Medida 5: responda y evolucione. Su capacidad para responder, recuperarse y evolucionar lo más rápidamente posible después de un ataque es fundamental. FlashRecover™ de Pure Storage, con tecnología de Cohesity®, es la primera solución de protección de datos del sector que es moderna, all-flash y tiene una arquitectura desarrollada de manera conjunta y ofrece una copia de seguridad aceleradas y una restauración rápida a escala.

- Purity ActiveDR™ proporciona unas potentes funcionalidades de replicación de los datos que garantizan unas copias de seguridad rápidas y FlashBlade ofrece una capacidad de restauración rápida de hasta 270 TB/hora.
- Para los usuarios de MEDITECH, Pure se ha asociado con BridgeHead Software, Amazon Web Services (AWS) y Healthcare Triangle, para proporcionar copias de seguridad como servicio (BaaS), lo que permite automatizar la creación, el almacenamiento y la replicación de las copias de seguridad de MEDITECH en Pure Cloud Block Store™ en AWS.

PS1946-02-es 02/23