arcserve®

Estudio de caso de cliente

Arcserve ayuda a los MSP a proteger a los clientes contra el ransomware

TruTech ofrece servicios de administración de TI a pequeñas y medianas empresas del norte de California. Sus servicios van desde la administración de escritorios, servidores y redes hasta el soporte de seguridad de TI y la administración antivirus.

Tru Technical Partners

INDUSTRIA: Proveedor de servicios administrados de TI
UBICACIÓN: Campbell, CA

SOLUCIÓN: Arcserve UDP Cloud Direct BaaS

PROBLEMA

El virus ransomware infecta los servidores de los clientes y bloquea el acceso a los datos críticos para el negocio.

SOLUCIÓN

El cliente se recupera de forma rápida y evita el tiempo de inactividad prolongado.

RESULTADOS

TruTech demuestra valor como MSP al cliente.

EL PROBLEMA

El ransomware infecta el servidor de la oficina

Cuando uno de los clientes de TruTech fue a trabajar y no pudo acceder a ninguno de sus archivos, sabía que algo estaba muy mal. No podía resolver el problema por su cuenta, así que sabía que era hora de ponerse en contacto con su MSP. Después de investigar un poco, se dieron cuenta de que sus sistemas estaban infectados por el temible virus de ransomware CryptoLocker.

La investigación de TruTech sobre la infección por ransomware reveló cómo se propagó al sistema de su cliente. Un empleado de la empresa había recibido un correo electrónico de una fuente que creía que era de confianza, ya que los scripts lo hacían parecer legítimo. Cuando ese empleado descargó el archivo adjunto del correo electrónico, su computadora y sus archivos se infectaron. Así, el virus se extendió al servidor de 160 GB de la oficina, lo que resultó en la pérdida total de acceso a los archivos y en un prolongado tiempo de inactividad en la compañía.

LA SOLUCIÓN

TruTech recupera los datos de los clientes desde Arcserve UDP Cloud Direct BaaS rápidamente

Afortunadamente para el cliente de TruTech, se había hecho un backup del servidor infectado con ransomware a través de la solución Arcserve UDP Cloud Direct BaaS. TruTech se puso en contacto con el equipo de soporte de Arcserve para ayudar a recuperar los datos críticos del cliente.

Tan pronto como se recuperaron los datos del cliente desde Arcserve UDP Cloud, el equipo de TruTech entró en acción inmediatamente. La política de retención del cliente se remontaba a siete días, y los archivos con ransomware no estaban presentes en su backup de Arcserve. El equipo luego copió sus datos de Arcserve en una unidad externa. El cliente pudo acceder a sus archivos desde Arcserve UDP Cloud. Como resultado de la infección por ransomware, el cliente estuvo inactivo durante tres días hábiles. La recuperación de todos sus datos tomó un total de ocho horas.

¿Qué es el ransomware?

Los virus de ransomware suelen llegar a través de mensajes de correo electrónico e infectan los archivos de una computadora, sistemas e, incluso, servidores. Permanecen inactivos e indetectables durante meses, por lo que un usuario ni siquiera sabe que su sistema está infectado hasta que es demasiado tarde. El virus cifra los archivos de un sistema y bloquea el acceso al usuario. Los archivos son retenidos como rehenes por los hackers hasta que el usuario acepta pagar el rescate con el objetivo de volver a acceder a sus datos mediante una clave de descifrado.

Los ataques de ransomware están en aumento

Los ataques de ransomware están aumentando en frecuencia cada año.

- **Se informaron al FBI 2.500 ataques de ransomware en 2015, con un costo de USD 24 millones.**
- **Los hackers recolectaron USD 209 millones tan sólo en los primeros meses de 2016.**

Desde hospitales y negocios hasta organizaciones gubernamentales, cualquiera puede convertirse en una víctima del ransomware. Y los criminales cibernéticos son muy difíciles de detectar o, incluso, localizar. Los correos electrónicos que contienen el virus también se envían automáticamente como spam de a miles, por lo que, para los criminales cibernéticos, es muy fácil aumentar las posibilidades de retener los archivos de alguien.

El envío diario de backups a un sitio remoto es una capa esencial de seguridad que puede ayudar a proteger los datos críticos de su negocio contra ataques cibernéticos tan devastadores. Es por eso que tener una solución de protección de datos sólida es fundamental para ayudar a prevenir la pérdida de datos, ya sea por un desastre natural, un error de los empleados o por hackers que mantienen a sus datos como rehenes.

LOS RESULTADOS

TruTech demuestra valor como MSP al cliente

Al ponerse en contacto con TruTech, la empresa fue capaz de iniciar el proceso de recuperación casi de inmediato. El valor y la principal diferencia entre ser un cliente con soporte de servicio administrado frente a uno con soporte reactivo se hizo evidente debido al rápido soporte de emergencia proporcionado por TruTech. Y gracias a la solución de Arcserve optimizada para WAN, pudieron recuperar todos los datos del servidor en menos de 8 horas. “Pudimos recuperar todos los datos que necesitábamos”, dijo Ben Rombaoa, gerente de TI de TruTech.

> La recuperación de desastres se vuelve más importante a medida que los ataques cibernéticos siguen aumentando.
>
> – **Ben Rombaoa,** gerente de TI

Los backups en un sitio remoto mantienen a los datos fuera del alcance del ransomware

Dado que el ransomware se propaga infectando servidores locales, una solución como Arcserve UDP Cloud Direct BaaS, que envía datos a un sitio en la nube, es fundamental para mantenerlos a salvo de esos ataques. De acuerdo con Víctor Cruz, Ingeniero Principal de Sistemas y Redes, “algo muy importante para el backup en la nube es tener una ubicación de backup confiable fuera de la oficina. La recuperación de desastres se vuelve más importante a medida que los ataques cibernéticos siguen aumentando”.

Para obtener más información sobre Arcserve, **visite** arcserve.com/la