¿Quién es CrowdStrike? Análisis del precio de las acciones, impacto de Microsoft y pronóstico futuro

https://www.btcc.com/es-ES/academy/financial-investment/who-is-crowdstrike-stock-price-analysis-microsoft-impact-and-future-forecast

La actualización del software de CrowdStrike el jueves pasado provocó una gran caída en Microsoft Windows en todo el mundo. El mercado reaccionó rápidamente, haciendo caer las acciones de CrowdStrike. El viernes 19 de julio, las acciones cayeron unos asombrosos 38,09 dólares, o un 11,10%, cerrando a 304,96 dólares por acción, lo que supone un mínimo de tres meses. Esto marcó el tercer día consecutivo de pérdidas, lo que se suma a una caída del 3,4% con respecto al día anterior.

Entonces, ¿qué impacto tendrá este incidente en CrowdStrike? ¿Cuál es el futuro del precio de las acciones de CrowdStrike?

Interrupción de TI de CrowdStrike: soluciones

En la tarde del 18 de julio, hora del Este, Microsoft estalló repentinamente y colapsó, afectando a alrededor de 8,5 millones de dispositivos Windows en todo el mundo, y resultó que el culpable era el gigante de la seguridad de la información de la red CrowdStrike, que provocó la actualización del software a nivel mundial. retrasos en vuelos, más de 5.000 cancelaciones de vuelos e interrupciones en el transporte, instituciones médicas, agencias administrativas y operaciones bancarias.

Las repercusiones de la interrupción de TI de CrowdStrike se sintieron en una amplia gama de empresas, muchas de las cuales todavía luchan por recuperarse de la interrupción. Microsoft, en un comunicado emitido el sábado, evaluó el impacto y estimó que 8,5 millones de dispositivos Windows se vieron afectados por la interrupción. Esto representa menos del uno por ciento de todas las máquinas con Windows a nivel mundial; sin embargo, los impactos económicos y sociales fueron significativos debido a los servicios cruciales administrados por las empresas que utilizan las soluciones de CrowdStrike.
La interrupción de TI de CrowdStrike sirve como un claro recordatorio de la importancia de las pruebas rigurosas y el control de calidad en las actualizaciones de software. Si bien las actualizaciones de software son cruciales para mantener la seguridad y la funcionalidad del sistema, los defectos o errores en estas actualizaciones pueden tener consecuencias de gran alcance. Las empresas dependen de proveedores de ciberseguridad como CrowdStrike para proteger sus sistemas y datos críticos, y cualquier interrupción en estos servicios puede tener implicaciones significativas para sus operaciones.
CrowdStrike ha tomado medidas rápidas para abordar el problema y minimizar el impacto en sus clientes. La compañía implementó una solución para la actualización defectuosa y está trabajando en estrecha colaboración con sus clientes para garantizar una recuperación sin problemas. Si bien la interrupción ha causado algunas interrupciones a corto plazo, la rápida respuesta y el compromiso de CrowdStrike para resolver el problema demuestran su compromiso de brindar soluciones de ciberseguridad confiables y seguras.

Impacto financiero y consecuencias de las acciones de

CrowdStrike

Raj Joshi, vicepresidente senior de Moody's Ratings, emitió una declaración destacando el riesgo de importantes reclamaciones de responsabilidad derivadas de los clientes afectados. "Las interrupciones no sólo han planteado dudas sobre las prácticas de ingeniería de software de CrowdStrike, sino que también han subrayado las crecientes vulnerabilidades en la infraestructura global de la nube, con un número cada vez mayor de posibles puntos de falla", dijo.

Esta situación podría tener ramificaciones significativas para el precio de las acciones de CrowdStrike, ya que los inversores evalúan el impacto potencial de la insatisfacción del cliente y las acciones legales. La seguridad de los endpoints es un aspecto crucial de la postura de ciberseguridad de cualquier organización, y cualquier debilidad percibida en las ofertas de CrowdStrike podría erosionar la confianza de los inversores.

Además, dado que el segundo trimestre de la compañía finaliza el 31 de julio, es probable que los inversores examinen los resultados financieros en busca de signos del impacto de los cortes. Cualquier indicador financiero negativo o comentario de la dirección de la empresa podría exacerbar aún más la trayectoria descendente de la acción.

En medio de los últimos acontecimientos en torno a CrowdStrike, los analistas financieros advierten sobre posibles consecuencias para las acciones de la empresa. Keith Bachman, analista de BMO Capital Markets, afirmó recientemente en un informe: "Creemos que este problema tendrá consecuencias financieras". Bachman citó la probabilidad de que los clientes busquen alivio y compensación por daños, incluyendo potencialmente descuentos o créditos para nuevos contratos y renovaciones, lo que sugiere un impacto potencial en las tasas de crecimiento y el flujo de caja.

La situación se intensificó el viernes cuando el director ejecutivo de Tesla, SpaceX y X, Elon Musk, recurrió a las redes sociales para anunciar: "Acabamos de eliminar CrowdStrike de todos nuestros sistemas". Musk no especificó si esta acción fue tomada por una o todas sus empresas, lo que alimentó aún más las especulaciones sobre la gravedad del problema.

El analista de Jefferies, Joseph Gallo, se hizo eco de estas preocupaciones con una visión sombría de la situación. La evaluación de Gallo subraya el potencial de importantes repercusiones financieras para CrowdStrike, especialmente dada la naturaleza de alto perfil del anuncio de Musk y los posibles efectos dominó que podría tener en la reputación y la base de clientes de la empresa.

A raíz de los recientes cortes y posibles pérdidas de clientes, las implicaciones financieras para las acciones de CrowdStrike son cada vez más evidentes. El analista Gallo ha expresado su preocupación por la carga de gastos que enfrenta CrowdStrike mientras trabaja para abordar los problemas y potencialmente otorgar créditos a los clientes afectados, lo que podría afectar significativamente sus márgenes. Si bien el alcance exacto de los créditos, descuentos o productos gratuitos adicionales aún no está claro, Gallo predice que CrowdStrike necesitará tomar medidas importantes para apaciguar a sus clientes y mitigar el daño.

El daño a la reputación resultante de estas interrupciones es particularmente preocupante para CrowdStrike, particularmente entre los clientes gubernamentales y de infraestructura de misión crítica. Es probable que este daño alargue los ciclos de negociación y limite aún más el potencial de crecimiento de CrowdStrike a medida que los nuevos clientes esperan garantías de que la situación se ha manejado adecuadamente. El momento de estas interrupciones, que ocurrieron en las últimas dos semanas del trimestre, no podría haber sido peor para CrowdStrike, ya que este suele ser el período más crucial para los resultados financieros.

Hoy, las acciones de CrowdStrike cayeron bruscamente, un 11,1% para cerrar en 304,96. Esta caída sigue a un fuerte aumento en 2024, con las acciones de CrowdStrike ganando un 34% hasta el cierre del mercado del jueves. Sin embargo, los recientes apagones y las pérdidas de clientes han ensombrecido las perspectivas de la empresa, y los inversores están empezando a preguntarse si la valoración de las acciones podrá mantenerse.

Por el contrario, las acciones de SentinelOne subieron un 7,9% a 21,72, mientras que las acciones de Palo Alto Networks subieron un 2,2% a 330,89. Estas ganancias sugieren que los inversores pueden

estar cambiando su atención hacia otras acciones de ciberseguridad, al menos en el corto plazo. Sin embargo, queda por ver si estos avances se mantendrán, dada la volatilidad general en la industria de la ciberseguridad.
La plataforma XDR de CrowdStrike, que significa detección y respuesta extendidas, ha sido una parte clave de la estrategia de la empresa. Esta plataforma proporciona una amplia solución de ciberseguridad de detección de amenazas que monitorea puntos finales, puertas de enlace web/de correo electrónico, firewalls de aplicaciones web y cargas de trabajo empresariales en la nube. Sin embargo, las recientes interrupciones han puesto en duda la fiabilidad y eficacia de esta plataforma, lo que podría erosionar aún más la confianza de los inversores.

CrowdStrike: definición y descripción general

CrowdStrike se erige como la fuerza pionera e incomparable en el panorama de la ciberseguridad, siendo pionera en la integración de antivirus (AV) de próxima generación, detección y respuesta de endpoints (EDR) y ofreciendo servicios de detección de amenazas las 24 horas. Fundada en 2011, esta empresa con sede en California se ha establecido como líder mundial en seguridad de terminales, aprovechando tecnología de vanguardia para proteger a las empresas y agencias gubernamentales contra las amenazas cibernéticas en constante evolución.
En el corazón de las ofertas de CrowdStrike se encuentra la plataforma Falcon, una solución integral de ciberseguridad que detecta, previene y defiende contra amenazas cibernéticas para los sistemas informáticos de los clientes, incluido Microsoft. A través de operaciones remotas, Falcon proporciona un sólido mecanismo de defensa que ayuda a los sistemas informáticos a resistir las intrusiones de piratas informáticos, garantizando la integridad y seguridad de los datos y sistemas críticos.
Sin embargo, un incidente reciente que involucró al software Falcon Sensor de CrowdStrike resalta las complejidades y desafíos en el ámbito de la ciberseguridad. Según informes de expertos en sistemas informáticos, el incidente se debió a la implementación de la última versión del software Falcon Sensor, cuyo objetivo era mejorar la capacidad de los sistemas informáticos de los clientes para resistir las intrusiones de piratas informáticos. Desafortunadamente, se sospechaba que un código de programa defectuoso interactuaba con los sistemas de Microsoft, provocando inestabilidad y eventuales fallos.
CrowdStrike respondió rápidamente y lanzó una solución remota para solucionar el problema. Sin embargo, volver a poner en línea los sistemas afectados requiere una limpieza manual del código defectuoso, lo que puede ser un proceso que requiere mucho tiempo. Si bien algunos sistemas informáticos con niveles de protección más bajos se pueden restaurar en un día, aquellos con niveles de seguridad más altos pueden tardar varios días en recuperarse por completo.
A pesar de este revés, la posición de CrowdStrike como proveedor líder de ciberseguridad sigue siendo inquebrantable. Más de la mitad de las empresas Fortune 500 y numerosas agencias gubernamentales, incluida la principal agencia de ciberseguridad de EE. UU. y la Agencia de Seguridad de Infraestructura, confían en el software de la empresa. Esta adopción generalizada refleja la capacidad de CrowdStrike para proporcionar soluciones de ciberseguridad confiables y efectivas que cumplan con los estrictos requisitos de empresas y gobiernos de todo el mundo.
Además, el compromiso de CrowdStrike con la innovación y la excelencia es evidente en su continua inversión en investigación y desarrollo. El equipo de expertos de la empresa trabaja constantemente para mantenerse a la vanguardia, identificando y mitigando las amenazas emergentes para garantizar que los sistemas de los clientes permanezcan seguros.