Cómo monitorear, responder y recuperarse de amenazas

Los atacantes están en todas partes. El **ransomware** ya es una prioridad para nuestros clientes y también para nosotros.

Las organizaciones de todo el mundo se enfrentan a una proliferación de datos multigeneracionales.

Las cargas de trabajo se crean en entornos locales, dispositivos de usuario y en la nube, y a medida que los clientes avanzan hacia aplicaciones modernas y las empresas se transforman, la seguridad es un tema cada vez más crítico.

> Los usuarios quieren saber: ¿Cómo me aseguro de que mis entornos son seguros y mis datos están protegidos si mi centro de datos se ve afectado por una amenaza, no sólo por el ransomware, sino por cualquier amenaza?

Las organizaciones deben asegurar sus entornos, garantizar que los datos estén seguros y protegidos, y devolver la agilidad al negocio, es necesario que los clientes tengan una sólida estrategia de defensa contra el ransomware. Pero, ¿cómo proporcionar una estrategia de defensa reforzada de seguridad en múltiples capas?
Cada centro de datos y cada entorno de datos es diferente. Hay que entender cuáles son las amenazas, dónde están, cómo es el panorama de las amenazas, qué hay que hacer para endurecer las medidas de protección y definir un perímetro de seguridad. Esto permitirá comenzar a proteger los datos, asegurarlos y garantizar que no saldrán del centro de datos y que no están infectados con malware. Es necesario supervisar el estado de lo que ocurre en ese entorno, independientemente de dónde residan los datos. La supervisión desde la nube es una capacidad importante que permite responder a una amenaza y luego volver a la normalidad, con la confianza de que todo está funcionando adecuadamente.

Medidas de protección

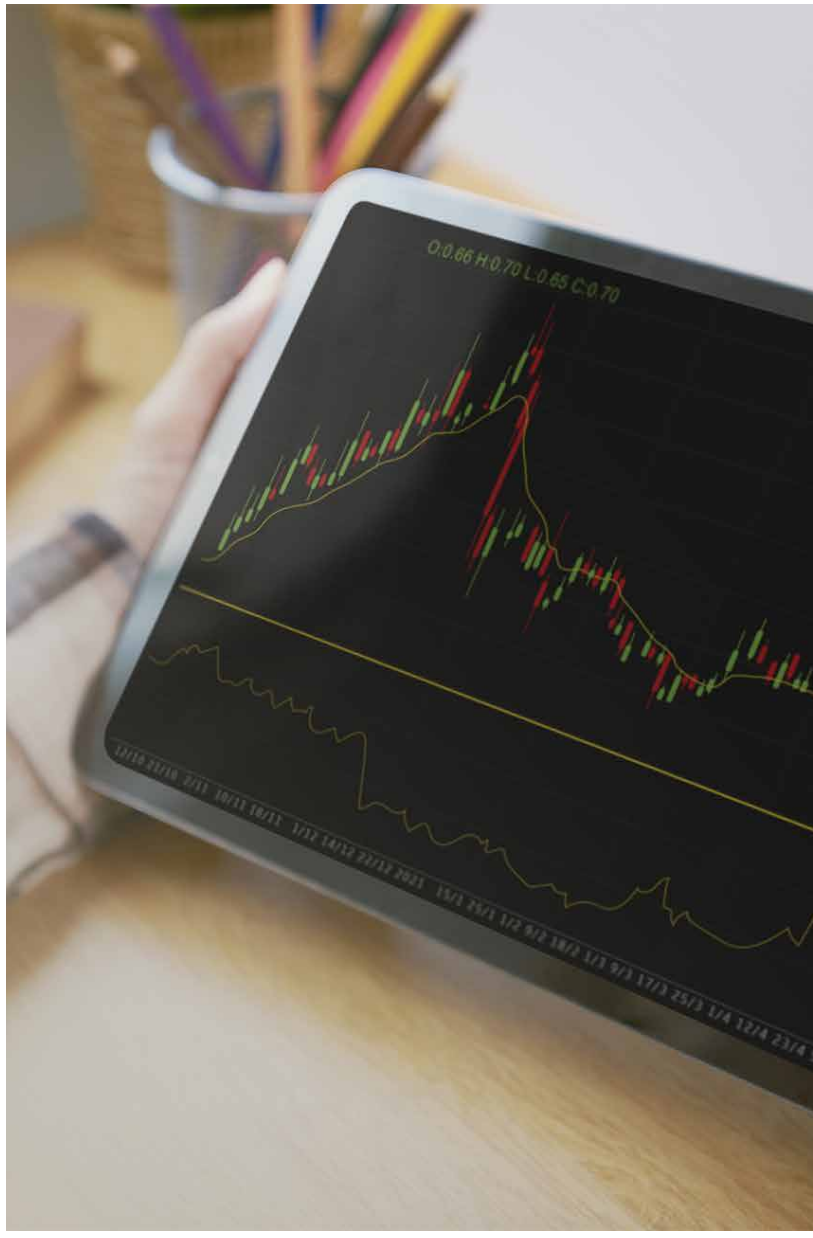
Proteger los datos mediante una serie de medidas que resume así: ante todo, es necesario hacer una evaluación de riesgos del perfil de seguridad de su entorno de datos, evaluando la seguridad de todo el entorno integrado. En seguida, se aconseja evaluar qué controles están habilitados y qué necesita para habilitarlos, dónde y por qué, administrado a través de un único panel de control.
Es necesario definir la estrategia de defensa de la seguridad, es decir, proteger el patrimonio de datos, y establecer arquitecturas inmutables para garantizar la autenticación adecuada.
También se requiere fortalecer los CIS y otros protocolos que minimizan el área de amenaza, y poner en marcha una autenticación de confianza cero, la cual consisten en una autenticación doble para que los procesos y los usuarios sean exactamente quienes se espera que sean. Estas tres capacidades, junto con la capacidad de air gap y de proporcionar redes aisladas, proporcionan seguridad para el patrimonio de datos.
Otra de las medidas consiste en aislar diferentes entornos de almacenamiento mediante la gestión y el mantenimiento de la infraestructura para abrir y cerrar los entornos de almacenamiento y asegurarnos de que están aislados, ya sea en on-premise o en la nube.

En seguida, hay que supervisar los datos mediante una evaluación del estado desde cualquier lugar, donde se aproveche el aprendizaje automático para proporcionar análisis de datos en todos los entornos. Esto puede incluir el uso de honeypots, que actúan como señuelo para el malware e identificarán una posible amenaza que pueda estar activa.

El siguiente proceso es la capacidad de respuesta, que consiste en proporcionar la capacidad de restaurar muy rápidamente al punto anterior al evento, y luego podemos automatizar la validación de las piezas recuperadas.

En esa respuesta, se pueden eliminar quirúrgicamente las amenazas de su entorno. Si hay archivos infectados, se puede actuar contra ellos para que la amenaza no vuelva a infectar el sistema en el futuro.

Y, por último, está la recuperación, "en la cual es necesario volver a un estado competente y normal en el que todo funcione como se espera".



Fuente de información: cio.com.mx