Bitdefender

Añadir protecciones mejoradas fortalece el último frente: cifrado y administración de parches

Ante un ambiente cada vez más hostil, donde los grandes ataques informáticos saltan a los titulares casi todos los meses, las empresas han empezado a cambiar su paradigma de seguridad de cara a obtener más información sobre cómo se producen los ataques y cómo se convierten en objetivos. Tras reconocer que inevitablemente se acabará produciendo una violación de la seguridad y adoptar herramientas útiles de detección y respuesta en los endpoints, los CISO se centran en minimizar la superficie de ataque al tiempo que dotan de protección adicional a su infraestructura. Aquí es donde la administración de parches y el cifrado marcan la diferencia.

ESCONDER LO MÁS VALIOSO

Una encuesta de Bitdefender realizada a 1051 profesionales de compras de seguridad de TI en Estados Unidos y Europa puso de manifiesto que cuatro de cada cinco CISO opinan que el cifrado es el mecanismo más efectivo para proteger los datos, seguido por el software de seguridad y las copias de seguridad. Por países, el cifrado goza de la mayor confianza en Italia, el Reino Unido y Estados Unidos pero, de media, solo una empresa de cada seis cifra todos los datos.

Tres de cada cuatro responsables de la toma de decisiones sobre seguridad informática mencionan los costes económicos y el daño a la reputación empresarial como las peores consecuencias que podrían afrontar si una amenaza avanzada accediese a sus "joyas de la corona".

Los datos críticos relacionados con la propiedad intelectual deben almacenarse localmente, con acceso restringido y solo disponibles para el personal autorizado. Cualquier información almacenada localmente o en la nube debe también cifrarse para garantizar que los delincuentes informáticos no puedan leerla en caso de violación de la seguridad o acceso no autorizado.

Los CISO deben evitar el riesgo de perder datos, además de cumplir con las normativas cifrando completamente el disco duro de sus endpoints móviles.

El Cifrado de disco completo de GravityZone protege los datos de toda la unidad de disco duro del endpoint aprovechando los mecanismos de cifrado proporcionados por Windows (BitLocker) y Mac (FileVault). Se basa en el cifrado nativo de los dispositivos para garantizar la total compatibilidad y maximizar el rendimiento. El Cifrado de disco completo de GZ está integrado en la consola y en el agente de GravityZone, sin que haya que implementar un agente adicional ni instalar un servidor de administración de claves. El uso de la infraestructura de seguridad de endpoints existente para administrar el Cifrado de disco completo permite una implementación totalmente centralizada con un esfuerzo administrativo mínimo.

TAPAR LOS HUECOS DE LA MURALLA

Si bien los sistemas sin parchear dejan a las organizaciones a merced de brotes e incidentes de malware y vulneraciones de datos, la mitad de los CISO encuestados admite que la ampliación de la infraestructura ha aumentado la superficie de ataque de su empresa. Los especialistas en seguridad recomiendan encarecidamente a los CISO que tengan siempre el software actualizado con los últimos parches. Las herramientas de administración de parches facilitan esto y ayudan a las empresas a evitar eventos perjudiciales, como los infames brotes de WannaCry y GoldenEye.

El módulo de Administración de parches de GravityZone es compatible tanto con parches automáticos como manuales. Brinda a las organizaciones una mayor flexibilidad y eficiencia en la administración de parches, con la posibilidad de crear un inventario de parches, programar el análisis de parches, limitar el parcheado automático a las aplicaciones que decida el administrador y modificar la programación de parches, ya sean de seguridad o no, así como posponer los reinicios para parches que requieran esa acción. En el panorama actual de la seguridad informática, parchear el sistema operativo y las aplicaciones ha pasado a tener una alta prioridad para el equipo de TI, tanto de cara a la seguridad como para mantener el cumplimiento normativo. La Administración de parches de GravityZone permite la comprobación de los parches en toda la empresa para cumplir con las políticas y normativas.