Publicado en Ciudad de México el 21/07/2021

Proteger los entornos cloud cuidando el presupuesto

El cambio impuesto por la pandemia es ahora la vida normal de las empresas. Así lo revela la encuesta de Statista de febrero de 2021, realizada a directivos de las 5,000 empresas más grandes de América Latina. Incluso el regreso a las oficinas seguirá basándose en la nube

La continuidad del acceso a la nube (pública, privada o híbrida) desde diversos puntos, desde el domicilio de los empleados hasta las sucursales y sedes de la empresa, hace que los datos críticos naveguen por la nube y no dentro del perímetro tradicional.

Esto requiere que la seguridad se mueva a lugares que anteriormente se consideraban secundarios en las demandas de seguridad y red. Según un reporte de IDC Latinoamérica de noviembre de 2020 se muestra que el 39% de todas las violaciones en la región ocurrieron a través de ataques a aplicaciones web a las que se accede a través de la nube.

Proteger el negocio en la nube también requiere que se haga frente a la realidad de los presupuestos cada vez más controlados. Hay dos estrategias que, utilizadas juntas, con discreción, pueden resolver los desafíos de presupuesto y protección de datos en la nube.

1 - El MSSP combina experiencia técnica y ahorros de costos de hasta el 25%. Según la investigación de IBM de 2013 (IDC), las empresas que contratan a un proveedor de servicios de seguridad gestionados (MSSP) pueden reducir sus costos de infraestructura de seguridad cibernética hasta en un 25%. Esta figura destaca varios gastos que ya no se realizan: adquisición de tecnologías, licencias de actualizaciones y servicios ofrecidos por proveedores de seguridad y gastos con servicios de soporte.

Otra ventaja que ofrecen los MSSP es la gran experiencia técnica de su equipo. Muchos MSSP han sido creados por expertos en seguridad convertidos en emprendedores - son profesionales que saben que el crecimiento de su negocio depende de inversiones constantes en la renovación de su centro de datos (on-premises o en la nube)- y de la formación de su equipo.

2 - Acceso remoto seguro: más accesible que SASE. Toda la seguridad está construida en capas, lo mismo ocurre con la seguridad en la nube. Siguiendo este enfoque, hay quienes posicionan Secure Access Service Edge (SASE, por sus siglas en inglés) como la solución de acceso seguro a la nube más conocida. Pero no todos los casos de uso justifican las inversiones en esta plataforma.

Existen también soluciones seguras de acceso remoto, que garantizan la conectividad del empleado a la nube en un modelo "cliente liviano", que no requiere la instalación de software en el PC, tableta o smartphone del usuario remoto.

Esta tecnología utiliza funciones de autenticación multifactor para comprobar, desde diferentes ángulos

(contraseña, biometría, token, etc.) la identidad real de la persona que busca entrar en aplicaciones críticas que se ejecutan en la nube. La inteligencia de esta oferta garantiza que la protección se base en la biometría de comportamiento, no en la firma.

En 2021 y en los próximos años, la nube continuará expandiéndose sin cesar, al igual que los recursos financieros de la organización. Aún así, nada justifica mantener esta infraestructura crítica y distribuida vulnerable a los ataques digitales.

Por Arley Brogiato, Director de SonicWall Latinoamérica y el Caribe

Datos de contacto:
Carlos Soto
5532322068

Nota de prensa publicada en: Ciudad de México

Categorías: Tecnología Digital Software Seguridad