Lo que quieren las PYMES: cómo implementar la ciberseguridad para satisfacer las necesidades de una empresa

AUTOR
Ivan Bulaev

Infraestructura, Ciberseguridad

Artista: Script & Seal

Implementar la ciberseguridad es como comprar ropa, todo debe quedarle bien. Como proveedor de servicios administrados, ¿cómo puede garantizar la mejor opción para su cliente?

Se ve muy bien en el estante, pero cuando se la prueba, ¡ay! El estilo, el color y la tela están bien, pero cuando se trata del ajuste, se siente como si estuviera hecho para el cuerpo equivocado. Mangas tan largas que cuelgan a los lados, hombros tan estrechos que no puede moverse y la cintura en el lugar equivocado. En el mundo de los negocios, esto mismo sucede cuando una empresa ocupa un espacio para oficinas que no corresponde con su tamaño o sus necesidades. Puede ser demasiado pequeño o demasiado grande, carecer de salas de reuniones o incluso no tener baños para el personal en el turno de la noche. Posiblemente la empresa tenga que pagar por un estacionamiento que es demasiado grande o no haya una red con capacidad suficiente para las tareas empresariales.

Al mismo tiempo, una empresa también puede enfrentarse a estos problemas respecto a cómo se encarga de la ciberseguridad. Quizás sea difícil reconocer lo que se necesita para mantenerla segura y que entonces se utilice un servicio o una solución que no sean adecuados para este propósito. En este escenario, es primordial que los proveedores de servicios de seguridad comprendan y respondan a las demandas empresariales específicas cuando ofrezcan protección a sus clientes.

¿Cuál es el nivel de protección que funciona mejor?

Con las pequeñas empresas, integradas por varias docenas de empleados, y las grandes empresas, donde ambas cuentan con funciones principales de ciberseguridad similares, es posible confundirse acerca de cuál es el nivel de protección que funcionaría mejor. La única manera de comprender cuáles son las necesidades de ciberseguridad que requiere una empresa, cuando ella misma no tiene claro lo que quiere, es evaluar cómo funciona dicha empresa y qué tan consolidadas están sus TI. Esto permitirá identificar específicamente las herramientas y el nivel de personalización que sean más adecuados para ella.

Imagine una compañía pequeña que fabrica y vende de manera local su propia marca de ropa, y que tiene una oficina con 50 personas. La empresa está creciendo rápidamente: en los últimos dos años el número de empleados casi se ha duplicado. Muchas personas se encargan de comprar telas, así como de la ropa confeccionada que se vende en las tiendas, pero casi nunca están en la oficina ya que trabajan de forma remota o en diferentes lugares.

En una empresa de este tipo, las TI con frecuencia se subcontratan a un administrador de TI externo quien proporciona este servicio y da mantenimiento a los sistemas de ciberseguridad de forma remota. Junto con la instalación de las aplicaciones que se utilizan en la oficina y la compra de equipos PC para la empresa, también se encarga de administrar la protección mediante la instalación de una solución de seguridad para los nuevos dispositivos, realiza la verificación de las actualizaciones del programa y se asegura de que la protección esté siempre activa. La empresa no necesita un análisis profundo de los incidentes y adapta los permisos de acceso de los usuarios para diferentes servicios. Su infraestructura puede incluir un gabinete de servidores o incluso no contar con ningún servidor local, y tener todo almacenado en la nube.

Aunque existen muchas otras razones para que los clientes cambien su suministro de TI por los proveedores de servicios administrados (MSP). Según Forrester, el 28 por ciento de las empresas que cuentan con 100 o más empleados y compraron SaaS (software como servicio) a partir de un MSP indican que "el servicio al cliente, el soporte y la experiencia" fueron su principal motivación durante la compra para elegir esta opción (Fuente: Forrester Analytics, "Encuesta sobre la seguridad realizada por Global Business Technographics®", 2019).

Cómo encontrar la solución correcta

Esta marca local de ropa podría ser una empresa pequeña o mediana de cualquier otro tipo: una agencia de publicidad, una consultora o una pequeña editorial. Independientemente del rubro al que se dediquen, el enfoque es el mismo: para administrar la ciberseguridad en dichas empresas, los proveedores de servicios deben ofrecer una solución que sea económica y compacta desde la nube, la cual requiera recursos mínimos para su instalación y administración, pero que al mismo tiempo brinde protección a todos los dispositivos: desde los equipos de escritorio que se encuentran en la oficina hasta las tabletas y teléfonos móviles de los empleados que trabajan a distancia.

Analicemos lo que una empresa más grande, con una infraestructura de TI bien establecida, espera y necesita de la ciberseguridad. Por ejemplo, una tienda en línea almacena y procesa una gran cantidad información confidencial, y utiliza diversos CRM, ERP y sistemas de servicio al cliente. Para darle servicio a un entorno tan complejo, debe haber un departamento interno de TI y un administrador dedicado a la ciberseguridad, o un equipo completo, ya sea interno o de un proveedor de servicios, para protegerlo.

En este tipo de organizaciones, la superficie de ataque es mucho más amplia. Utilizan más aplicaciones que las empresas de menor tamaño, incrementando la probabilidad de que se vuelvan vulnerables, así como más dispositivos que podrían verse comprometidos debido al software malicioso que infecta la red. Trabajar con muchos contratistas y socios también propicia que la infraestructura se vuelva más vulnerable a los ataques en la cadena de suministros. La tarea de un administrador de ciberseguridad, ya sea un especialista interno o un proveedor de servicios, es habilitar la protección contra el malware en cada dispositivo. También deben configurarlo de una manera que garantice que todos los empleados tengan acceso a los servicios necesarios, según su función. Finalmente, los administradores necesitan informes detallados sobre el estado del sistema y, en caso de que se produzca un incidente, deberían ser capaces de detectarlo, analizarlo y responder rápidamente.

¿Cuáles son los riesgos de las vulneraciones a los datos?

Cualquier tiempo de inactividad causado por un incidente o una vulneración a los datos puede costarle dinero, la fidelidad de sus clientes y la reputación de su empresa. Las compañías de tamaño mediano corren el riesgo de perder hasta $120,000 USD como resultado de una vulneración de los datos, gran parte de este dinero se destinará a reparar daños a la reputación, así como a pagar indemnizaciones y multas. Si bien ninguna empresa de seguridad de la información puede garantizar una protección del 100 por ciento contra ciberincidentes, el uso de herramientas de protección especializadas puede minimizar el daño y las consecuencias de un incidente.

451 Research realizó un estudio independiente, encargado por Kaspersky, para analizar los aspectos que determinan la seguridad de la información desde la perspectiva del líder de seguridad empresarial.

Podemos suponer que muy probablemente una empresa pequeña no pagará de más por un servicio de seguridad más costoso. Pero una empresa grande que busca ahorrar dinero y utiliza un producto que no satisface sus necesidades se dará cuenta rápidamente de sus errores. Para elegir correctamente cuál es la mejor opción de servicio para sus clientes, los proveedores deben buscar que la función de ciberseguridad de los clientes ya esté consolidada, lo cual frecuentemente se correlaciona con el tamaño y el nivel de consolidación que tenga toda la empresa.

Weodeo se adapta a nuestras necesidades

Hablamos de ello con Weodeo, una empresa con sede en Francia que se dedica a la administración de servicios. Su propietario, Philippe Aymonod, dijo lo siguiente: "Las empresas más pequeñas son conscientes de lo importante que es la seguridad de TI y se enfrentan a muchas de las mismas ciberamenazas que las grandes empresas. Pero no tienen los mismos recursos para lidiar con ellas. En consecuencia, esperan que su socio actúe como un asesor de seguridad que podrá ofrecerles protección de una manera simple y eficiente, sin afectar su productividad".

"Nosotros evaluamos el nivel de protección de nuestros clientes de acuerdo con varios parámetros: el nivel de conciencia de la empresa con respecto a la seguridad y el panorama de amenazas, la complejidad en la infraestructura de los clientes, cualquier característica particular que esté relacionada con su empresa, el equipo y los posibles ajustes estratégicos que deban hacerse en el futuro".

> "Las pequeñas empresas esperan que su socio actúe como un asesor de seguridad que podrá ofrecerles protección de una manera simple y eficiente, sin afectar su productividad."
>
> Philippe Aymonod
> Weodeo

También es muy importante que los proveedores de servicios identifiquen sus propios objetivos y recursos, como su infraestructura, recursos humanos y habilidades técnicas. Por ejemplo, si los proveedores trabajan solamente con servicios en la nube (los MSP "nacidos en la nube") o buscan acelerar su implementación para nuevos clientes y administrar fácilmente a todos los clientes mediante una sola consola, estos funcionarán mejor si la ciberseguridad se proporciona como un servicio que puede supervisarse a través de una consola alojada en la nube.

Por otro lado, los proveedores que ya han desarrollado su propia infraestructura pueden elegir una solución administrada en entornos locales y centrarse en los clientes cuyas infraestructuras de TI están más consolidadas y requieren una protección más granular. Esta es una buena oportunidad para proporcionar servicios flexibles a los clientes más exigentes, mantener acuerdos de nivel de servicio (SLA) y ser un experto según la opinión del cliente. En este caso, la empresa que proporciona el servicio también debe tener la capacidad adecuada en el equipo para administrar la protección avanzada.

¿Cuál es el mejor enfoque?

Ambos enfoques tienen ventajas. Los proveedores que proporcionan seguridad en la nube pueden centrarse en ofrecer un mayor número de servicios en la nube y en ampliar su cartera para incluir PYMES que usen los servicios SaaS a un ritmo cada vez mayor. Los MSP que trabajan con empresas medianas y cuentan con una infraestructura propia pueden utilizar sus recursos para desarrollar servicios de seguridad avanzados y escalarlos.

Aunque podría decir que cualquier tipo de protección de ciberseguridad es mejor que nada, si esta no satisface las necesidades de la compañía, ¿tiene sentido cambiar a una solución que se adapte perfectamente a la empresa?