



Ciberseguridad para pequeñas y medianas empresas

Una nueva oportunidad para los proveedores de servicios

Introducción

La ciberseguridad es una necesidad imperiosa para las pequeñas y medianas empresas (pymes). En [2021 Cyber Readiness Report](#), Hiscox explica que "la proporción de empresas víctimas de ataques ha aumentado del 38 % [en 2020] al 43 % [en 2021]. Hay muchas empresas que han sufrido varios ataques". La seguridad es un problema global: la investigación [Cyber Security Breaches Survey](#) realizada por el gobierno del Reino Unido en 2021 reveló que el 37 % de las microempresas (entre 1 y 9 empleados), el 39 % de las pequeñas empresas (entre 10 y 49 empleados) y el 65 % de las medianas empresas (entre 50 y 249 empleados) habían identificado infracciones o ataques en los últimos 12 meses. Teniendo en cuenta la similitud en las respuestas, no es descabellado afirmar que las pequeñas empresas de todo el mundo con activos importantes están en el punto de mira. En este white paper se analizará:

- La exposición de las pymes en Internet y los desafíos únicos a los que se enfrentan en lo que respecta a las amenazas para la seguridad
- Cómo pueden ayudar los ISP a las pymes a afrontar su exposición a los riesgos de seguridad
- La oportunidad de mercado que representa la seguridad de las pymes y cómo pueden preparar los proveedores un caso de negocio

Desafíos de ciberseguridad a los que se enfrentan las pequeñas empresas

Las pymes se enfrentan a amenazas de seguridad a diario. Son objetivos atractivos porque, en conjunto, tienen un valor económico considerable y a menudo carecen de experiencia en cuestiones de seguridad. Las pymes están expuestas al malware que se utiliza para robar y descargar información financiera, datos de clientes o propiedad intelectual valiosa. Se enfrentan a ataques de phishing que utilizan ingeniería social sofisticada para engañar a los usuarios a fin de que descarguen malware o compartan credenciales con las que acceder a activos rentables. El uso generalizado de dispositivos inteligentes (Internet de las cosas) entraña una exposición adicional que posiblemente ni siquiera los propietarios de negocios hayan tenido en cuenta. Para obtener más información, consulte una publicación de Akamai relacionada: [Panorama de amenazas para las pymes](#).

Para dar una idea del impacto en las pequeñas empresas:

- En el informe de Hiscox de 2021, se indicaba que "los costes de los ataques varían considerablemente. Una de cada seis empresas víctimas de un ataque afirma que su supervivencia se ha visto amenazada".
- En el informe del gobierno del Reino Unido de 2021 también se indicaba que "del 39 % de las empresas... que identifican filtraciones o ataques, una de cada cinco (21 %) pierde dinero, datos u otros activos. Un tercio de las empresas (35 %) afirma que se ha visto afectado negativamente".

Conclusión

La mayoría de las pymes no tiene la misma experiencia en seguridad que las organizaciones más grandes, y le resulta cada vez más difícil defenderse de forma adecuada.

Además de los riesgos a los que se ven expuestas las pymes, en la encuesta del Reino Unido también se observó que solo el 38 % de las empresas cuentan con políticas de seguridad oficiales, y solo el 14 % de las empresas dispone de formación en ciberseguridad para los empleados. Sin embargo, el 77 % afirma que la ciberseguridad es una prioridad clave para el equipo directivo. En conclusión: la mayoría de las pymes no tiene la misma experiencia en seguridad que las organizaciones más grandes, y le resulta cada vez más difícil defenderse de forma adecuada.

La oportunidad que representa la seguridad para las pymes

Los ISP gozan de una fantástica posición para ayudar a las pymes a abordar su exposición a los riesgos de seguridad. Ya tienen un papel de asesor con una relación continua con el equipo de TI, contactos definidos y conexiones de facturación, por lo que es probable que el asesoramiento por parte de una fuente fiable sea bien recibido. Hay disponibles soluciones de seguridad que se adaptan a los puntos fuertes del proveedor, al tiempo que cumplen los requisitos de las pymes en términos de facilidad de uso, gran cobertura de dispositivos y precios compatibles con presupuestos modestos. Los proveedores pueden crear una experiencia atractiva para los suscriptores con el fin de impulsar los ingresos y aumentar la afinidad por la oferta de servicios de acceso.

Si extrapolamos los datos publicados por [TeleGeography](#), empresa de análisis líder del mercado que hace un seguimiento de los ISP de todo el mundo, y de una encuesta a unidades de negocio de los proveedores dedicadas a pymes, Akamai considera que hay 65 millones de pymes en todo el mundo que utilizan servicios de acceso a Internet. Con tarifas de acceso en todo el mundo que van desde 50 hasta 125 dólares mensuales y un aumento de entre el 10 y el 20 % (entre 5 y 25 dólares al mes) por la seguridad básica incorporada en el servicio de acceso, el mercado total representa algo menos de 12 000 millones de dólares al año (promedio de estimaciones altas y bajas).

Akamai Secure Internet Access SMB transforma la seguridad de las pymes

Akamai permite a los proveedores aprovechar la oportunidad que representa la seguridad para las pymes. Akamai Secure Internet Access SMB es una nueva solución de seguridad web que proporciona defensas basadas en DNS ligeras y ampliables. De esta forma, los ISP pueden ofrecer a las pymes una capa de protección básica en redes fijas, móviles y convergentes. Secure Internet Access SMB se ha desarrollado desde cero para que los ISP lo utilicen como software con licencia dentro de la red gestionado por un proveedor o "como un servicio" gestionado por Akamai. Las defensas basadas en DNS pueden cubrir todos los dispositivos de una pyme y responder perfectamente a las amenazas dinámicas actuales.

Desde la perspectiva de los proveedores, Secure Internet Access SMB se ha diseñado para proporcionarles un control total. Pueden personalizar el servicio en función de sus objetivos y su identidad corporativa. Además, definen la experiencia del usuario y especifican los niveles de servicio a través de las API. También determinan el modelo de negocio (oferta premium, paquete, servicio por niveles, etc.) y definen precios acordes a las condiciones regionales. Akamai ayuda a los proveedores a poner en marcha iniciativas de marketing con un paquete "Go to Market" que incluye asesoramiento y ejemplos.



Secure Internet Access SMB se ha diseñado específicamente para las pymes y la experiencia de usuario se ha concebido para clientes que cuentan con conocimientos, tiempo y recursos limitados. No es necesario instalar ningún software y todos los dispositivos que encontramos en una empresa normal están protegidos. Los responsables empresariales pueden "configurarlo y olvidarse". El servicio identifica y bloquea la actividad maliciosa o el contenido no deseado sin que sea necesario ningún tipo de intervención. Todas estas ventajas contrastan con las soluciones de seguridad tradicionales para pymes, normalmente productos reempaquetados y con el precio ajustado que incluyen funciones que la mayoría de las pymes no puede usar y, por lo tanto, no puede beneficiarse de ellas.

Como se muestra en los siguientes ejemplos, los proveedores barajan diversos modelos de negocio para Secure Internet Access SMB. También investigan ofertas basadas en comisiones de servicios complementarios, como herramientas antivirus, para clientes que quieren ampliar aún más su protección de seguridad.

Caso de negocio 1

Un importante proveedor estadounidense con aproximadamente 2 500 000 suscriptores de pymes creó dos niveles de servicio de seguridad que añadiría a su servicio de acceso como parte de un paquete: la opción básica bloquea el malware y el phishing por 9,95 dólares al mes y la opción premium (29,95 dólares al mes) incluye las mismas funciones que la opción básica, además de filtros sencillos que pueden configurar los propietarios de negocios para bloquear contenido no deseado en los lugares de trabajo (políticas de uso aceptable [PUA]). El proveedor utilizó Secure Internet Access SMB para reducir el tiempo de comercialización y la sobrecarga operativa interna. Inicialmente, se dirigen a clientes nuevos y pretenden ampliar las ofertas a todos sus clientes de pymes. Se ofrecen descuentos en el paquete premium si los suscriptores se inscriben durante tres años. Esperan que el servicio sea rentable en el segundo año.

Caso de negocio 2

Otro importante proveedor estadounidense con 500 000 clientes de pymes ha desarrollado dos niveles de servicio de seguridad como parte de su servicio de acceso: un producto básico por 19 dólares al mes y un producto premium por 29 dólares al mes. También pretenden crear un servicio basado en la tecnología SD-WAN dirigido a cadenas de retail y de restaurantes regionales. Debido al enfoque combinado, la seguridad será fundamental para el servicio en sí y, por lo tanto, Secure Internet Access SMB será un elemento básico de su cartera. Estas innovaciones son factibles porque Secure Internet Access SMB no depende en absoluto del tipo de red y es ampliable.

Conclusiones

La presión que genera la competencia anima a los ISP a evolucionar más allá de la conectividad y a ofrecer más servicios con valor añadido para lograr un aumento de los ingresos. Los servicios de seguridad son una opción obvia, puesto que los usuarios son conscientes de la necesidad de protegerse. La presencia y la posición fiable en los segmentos del mercado de las pymes crean una oportunidad para que los ISP ofrezcan una capa básica de protección web con el fin de reducir el riesgo de sus clientes. Las pymes suelen ser un segmento de mercado desatendido y las limitaciones de recursos pueden predisponerlas a externalizar servicios como la seguridad.

Akamai Secure Internet Access SMB se ha diseñado para implantarse como servicio de ISP desarrollado específicamente para pymes. El servicio "simplemente funciona" y no supone una carga de configuración ni gestión a los responsables de los negocios.

Un portal gráfico facilita la comprensión del estado de la amenaza y la configuración de filtros opcionales de contenido web para implantar políticas de uso aceptable. Las opciones de implantación (con licencia y "como servicio") ayudan a los proveedores a coordinar los requisitos empresariales y operativos.

Secure Internet Access SMB permite a los proveedores controlar la estrategia de precios y el modelo de negocio, así como definir la marca y la experiencia del usuario según las aptitudes y los requisitos regionales. Para generar interés, los proveedores pueden informar a los suscriptores de las pymes del panorama de amenazas e incluso ofrecer información sobre las condiciones locales. Un paquete "Go to Market" de Akamai ayuda a poner en marcha iniciativas de marketing de los proveedores.

Para obtener más información sobre la ciberseguridad para pymes, visite akamai.com.



Akamai potencia y protege la vida online. Las empresas líderes de todo el mundo eligen Akamai para crear, proteger y ofrecer sus experiencias digitales, ayudando así a millones de personas a vivir, trabajar y jugar cada día. Gracias a la plataforma informática más distribuida del mundo, de la nube al Edge, nuestros clientes pueden desarrollar y ejecutar las aplicaciones con facilidad, mientras acercamos las experiencias a los usuarios y mantenemos las amenazas a raya. Para obtener más información acerca de las soluciones de seguridad, informática y distribución de Akamai, visite akamai.com y akamai.com/blog, o siga a Akamai Technologies en [Twitter](https://twitter.com/Akamai) y [LinkedIn](https://www.linkedin.com/company/akamai). Publicado en junio de 2022.