



Cyber MSME



Ciberseguridad para PYMES

Presupuesto para ciberseguridad

Como proteger su negocio cuando cada euro cuenta

Creado por CTS Customized Training Solutions &
CASE



The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Antecedentes

Esta herramienta se ajusta sobre todo para PYMES (así como para uso personal) que quieran reforzar su ciberseguridad, pero que cuentan con un presupuesto ajustado o escaso.

Recomendaremos algunos programas concretos y opciones de hardware para ayudarle a identificar herramientas interesantes, pero siéntese libre (y le animamos a ello) de hacer su propia investigación sobre los temas que veremos.

Introducción

Cuando hablamos de ciberseguridad, piratería informática, servidores y similares, nos las imaginamos como se suelen mostrar en la películas de Hollywood. Imaginamos tecnologías futuristas, empresas multimillonarias, piratas informáticos envueltos en la oscuridad escribiendo como locos en el teclado, grandísimas habitaciones llenas de servidores, e interfaces de líneas de texto (esto último es verdadero). Esto nos lleva a pensar que todas estas cosas son para empresas grandes con millones de fondos para respaldarles. Pero, ¿podemos implementar herramientas de ciberseguridad en una PYME trabajando con una presupuesto ajustado? Por supuesto, veamos como.



Soluciones de terceros vs soluciones auto-alojadas

Antes de empezar a hablar sobre VPNs y Ad-blockers (bloqueadores de anuncios) vamos a explicar el vocabulario que usaremos al recomendar determinadas soluciones:

Terceros

Esto significa que alguien (otra empresa) lo hará por usted. Por lo general, todo lo que tiene que hacer es instalar una aplicación o realizar los pasos básicos: la configuración y el alojamiento los realiza una empresa externa.

Pros:

Facilidad de configuración y acceso; no se requieren habilidades ni conocimientos adicionales;

Un mercado altamente competitivo hace que diferentes empresas ofrezcan muchos servicios adicionales.



Contras:

Es posible que los planes de pago no se adapten a sus necesidades, lo que le hará pagar por cosas que no necesita o usa; está confiando sus datos a una tercera empresa; Los precios de las suscripciones pueden aumentar rápidamente.

Auto-alojamiento:

Esto significa que usted es responsable de alojar sus herramientas de ciberseguridad. Además de un dispositivo para alojarlo, también necesita el software adecuado, así como el conocimiento para instalarlo y configurarlo correctamente.

Pros:

Obtienes exactamente lo que quieres; puede ser divertido y desafiante aprender cosas nuevas; gran cantidad de software de código abierto disponible de forma gratuita con un gran apoyo de la comunidad; Puede sentirse como un hacker de películas de repente usando Linux y líneas de comando :)



Contras:

Se requieren conocimientos informáticos básicos / intermedios; Se necesita servidor, lo cual es un coste en sí mismo;

Auto-alojamiento con presupuesto limitado

Cuando terminó de leer sobre el auto alojamiento, posiblemente se preguntó: "¿Quién elegiría esa opción? ¡No sé nada sobre servidores y no quiero gastar miles de euros en infraestructura!".

Lo que pasa es que no es necesario gastar miles de euros en infraestructura. Para ser justos, ¡ni siquiera es necesario hacerlo!

En primer lugar, el alojamiento en la nube es muy importante. Todos los grandes del mundo de las tecnologías de la información (Amazon, Google, Microsoft) ofrecen plataformas en la nube, mientras que hay docenas más ofrecidas por empresas más pequeñas (DigitalOcean y Heroku, por nombrar algunas). Todos ofrecen una prueba gratuita (de 1 a 3 meses según la plataforma), por lo que hay tiempo para aprender e intentar hacer las cosas uno mismo (en lugar de pagar por adelantado).



Una vez finalizada la prueba gratuita, el pago por una máquina virtual capaz de alojar el software mencionado en este kit de herramientas ascendería a entre 5 y 10 euros al mes, lo que puede ser menos que las suscripciones de terceros combinadas.

Pero, ¿qué pasa con tener un servidor? ¿No sería rentable y eficiente en espacio, no?

¡Todo lo contrario! Un dispositivo adecuado para su PYME puede costarle menos de 100 euros y caber en la palma de su mano. Conozca [Raspberry Pi](#), un pequeño ordenador completísimo.



La Raspberry Pi con una mandarina para ver la escala. La mandarina estaba deliciosa.



Además de ser capaz de ser una VPN y un bloqueador de anuncios (¡a la vez!), podría usarlo para docenas de cosas diferentes (servidores multimedia, almacenamiento en la nube, cabinas de juegos de arcade, espejos inteligentes, emuladores de consola retro; las posibilidades son enormes). Los últimos modelos también podrían usarse cómodamente como una PC para backup en caso de un fallo repentino al tener un sistema operativo Linux dedicado capaz de navegar por la web y reproducir multimedia con facilidad. Con un precio de entre 60 y 100 euros según el modelo, podría ser la solución más rentable a largo plazo.

VPN

Ya explicamos en detalle qué es una VPN y por qué deberíamos usarla (¡lo recomendamos encarecidamente!), pero para que sirva de recordatorio: VPN es una red virtual que protege nuestra privacidad escondiendo los datos que enviamos con una capa adicional de encriptación. Se usa principalmente como una capa de protección al usar redes públicas o inseguras, así los piratas informáticos no pueden hackear nuestros datos. Muchas empresas ofrecen servicios de VPN insistentemente (si frecuenta Youtube, seguro que más de una vez ha encontrado publicidad de VPN).



Opciones de VPN destacadas

Terceros:

No nombraremos ninguno en concreto, ya que el mercado es muy competitivo y las diferencias entre los principales proveedores son mínimas. Si escribe "mejor VPN + año actual" en su motor de búsqueda preferido, obtendrá resultados relevantes en segundos.

Coste: sobre 10euros/mes en plan mensual (comparando las ofertas de los principales proveedores), más económico si se compra en planes a largo plazo (3-5 euros al mes).

Auto-alojamiento:

OpenVPN (<https://openvpn.net/vpn-software-packages/>) **Coste:** Código abierto/gratuito

AlgoVPN (<https://github.com/trailofbits/algo>) **Coste:** Código abierto/gratuito



Ad-blockers (bloqueadores de publicidad)

Probablemente ya haya oído hablar de los ad-blockers. ¡Incluso existe una alta probabilidad de que esté usando uno ahora (y por una buena razón)! Los ad-blockers eran la respuesta largamente buscada a los anuncios intrusivos a página completa que plagaban Internet. Son los únicos responsables de un enfoque más fácil de usar para los anuncios en la web, pero también pueden ser un factor de seguridad enorme para su empresa. ¿Cómo es eso?

Los anuncios engañosos o maliciosos son una de las principales formas en que podemos comprometer la seguridad de nuestra PYME, ya sea haciendo clic en uno por error o siendo atraído por la promesa de una Tablet gratuita (que acaba de ganar). Aparte de eso, todos los anuncios se suman a su uso de Internet, lo que puede ser un factor importante cuando se encuentra en un lugar con acceso limitado a Internet o con un plan de datos. Cuando su camión de comida está en la carretera, desea que sus valiosos límites de datos de Internet se usen para su portal de entrega, no para anuncios de píldoras milagrosas. ¿Entonces cuales son nuestras opciones?



Primero, hablemos de dos tipos de bloqueadores de anuncios. El primero es el bloqueador de anuncios del lado del cliente que instalamos en nuestro navegador. El segundo es un bloqueador de anuncios basado en la resolución de DNS. Los bloqueadores del lado del cliente se instalan como un complemento de su navegador. Los solucionadores de DNS necesitan una máquina para operar. ¿Cuál es la mayor diferencia?

Imagina una película con una escena para adultos que no quieres ver. Los bloqueadores del lado del cliente serían como cubrirse los ojos con las manos. No podías verlo, pero todavía estaba allí. La película tardó más en terminar y nuestra factura de la luz fue más alta por eso. Podemos pensar que el coste no será alto durante un par de segundos, ¡pero imagine cubrirse los ojos cientos de veces al día! El coste eventualmente se incrementaría. El solucionador de DNS sería un televisor que corta la escena antes de que salga al aire, acorta la película y reduce la factura de la luz. Otro beneficio importante es que puede usar el solucionador de DNS a nivel de red, lo que hace que un dispositivo esté protegido de los anuncios simplemente conectándose a su red, sin la necesidad de instalar el bloqueador de clientes para cada navegador en cada computadora que use su empresa.



Opciones destacadas de bloqueo de anuncios de DNS:

Terceros:

NextDNS (<https://nextdns.io>) - Plan personal gratuito limitado a 300k solicitudes por mes, el plan Pro cuesta aproximadamente 2 euros al mes, el plan empresa inicia con aproximadamente 200EUR por año hasta un máximo de 50 empleados.

Precio: sobre 10euros/mes en plan mensual (comparando las ofertas de los principales proveedores), más económico si se compra en planes a largo plazo (3-5 euros al mes).

Auto-alojamiento:

Pi-hole (<https://pi-hole.net>) – La guía de instalación se puede encontrar en:

<https://github.com/pi-hole/>

Precio: Código abierto/gratuito



¡Gracias por su atención!

