

## **Análisis Detallado de Seguridad PYMES versus Corporaciones**

## Introducción

Uno de los acrónimos más utilizados hoy en día es “PYME”. La mayoría de los proveedores que dan servicio a las pequeñas y medianas empresas y grandes empresas hacen diferenciación entre ambas por sus ingresos anuales o por el número de empleados. Sin embargo en temas de Seguridad Informática, ninguna de estas formas de medida son las apropiadas. En vez de etiquetarlas, los proveedores deberían gastar su tiempo y energía en los requerimientos de seguridad y los recursos disponibles de cada una, para poder ofrecer la solución de seguridad que se adapte más a sus necesidades específicas.

En cuestión de dotar de seguridad a la red de una empresa, las PYMES y las corporaciones necesitan la misma cobertura de seguridad, aunque el nivel de experiencia, personal y presupuesto disponibles de las PYMES sean muy diferentes a los de las corporaciones. A los proveedores de seguridad les gusta destacar “enterprise-class” como una característica de venta para sus clientes PYMES y aunque lo que le ofrezcan tenga carencias en la cobertura, rendimiento y características comparado con lo que ofrecen a las grandes compañías.

## Mismas Necesidades de Seguridad

Las amenazas de red se propagan de forma indiscriminada vía Internet, sin hacer diferenciación entre PYMES y corporaciones. Así que en cuanto a su tamaño, cualquier empresa conectada a Internet va a hacer frente a las mismas amenazas. Las empresas de todos los tamaños harán frente a las amenazas que entren y salgan mediante el tráfico HTTP. De igual forma, casi todas las empresas utilizan el e-mail diariamente para comunicarse, tanto desde dentro como desde fuera de la empresa. Así que deben afrontar el alto y siempre creciente número de amenazas vía e-mail. Si estas empresas tienen su propio servidor de e-mail y página Web, se necesitarán unas medidas de seguridad adicionales dentro de la empresa para proteger estos servidores de e-mail y Web.

Lo mismo podríamos decir para los servidores de aplicaciones, bases de datos o cualquier otro componente de la infraestructura de red de una empresa. En cuanto a su tamaño, todas las empresas tendrán que hacer frente a las mismas amenazas contra estos recursos vitales. La única diferencia significativa entre ellas es su nivel de operaciones.

## Fundamentalmente Recursos Diferentes

El principal punto de diferenciación entre una PYME y una corporación tiene que ver con los recursos humanos y financieros de la compañía. Mientras que las PYMES tienen globalmente la misma necesidad de seguridad que las corporaciones, éstas disponen de menos recursos y mucho menos ancho de banda para tratar de forma efectiva estas necesidades.

Una gran compañía suele tener un completo Departamento de Seguridad Informática para gestionar las necesidades de seguridad de la empresa. Esto significa la implementación de sistemas complejos para asegurar de forma efectiva todos los componentes de la red de la empresa en cada una de sus ubicaciones. También significa que se mantienen al día de los cambios que se suceden en el campo de las amenazas y modifican la política de seguridad de la compañía cuando sea necesario para hacer frente a las nuevas amenazas. Y lo más importante, significa que están controlando constantemente el tráfico de la red de la compañía, incluyendo un análisis de los ficheros log para determinar si hay algún patrón inusual en el tráfico de la red. Una corporación tendrá los medios para comprar esos sistemas, y el personal cualificado para utilizarlos.

En cambio una PYME puede o no tener un Departamento de Informática a tiempo completo y seguro que no contará con un experto en seguridad a tiempo completo. Muchas de estas PYMES suelen tener un empleado que se dedica a todas las necesidades informáticas incluyendo la seguridad. Y otras simplemente subcontratan sus necesidades de informática a terceros.

Las PYMES normalmente carecen del tiempo y de los recursos financieros necesarios para implementar una solución de seguridad compleja a nivel de gran empresa. Mientras que un precio considerable y una implementación de 6 meses resulta normal para una compañía grande, la mayoría de las PYMES no están dispuestas o son incapaces de asumir con este gasto y necesitan resultados prácticamente inmediatos.

## Diferentes Decisiones de Seguridad

Dados estos problemas de recursos, las PYMES deben tomar decisiones de seguridad más complicadas. Mientras que algunas grandes empresas tienen la capacidad de gastar enormes cantidades de tiempo y dinero implementando un sistema de seguridad multi-capas, proactivo y detallado para conseguir la máxima eficacia, las PYMES deben aceptar lo que puedan permitirse adquirir y mantener.

El mejor sistema del mundo no sirve de nada a una PYME si necesita constantemente intervención manual en su rutina diaria. Con sólo una parte del tiempo de uno o más empleados de informática dedicados a la seguridad, un sistema complejo que ofrece información, de por ejemplo anomalía en el tráfico SMTP y HTTP en ficheros log, no sirve de nada si el empleado informático carece de tiempo para revisar dichos logs. De igual manera, un sistema complejo que necesite meses para su implantación completa no beneficia a una PYME que necesita una solución de seguridad instalada y funcionando en días disponiendo además de personal de informática limitado.

Con estos problemas aparentemente insalvables asociados a un nivel de conciencia de seguridad notablemente inferior, muchas PYMES seleccionarán sus soluciones de seguridad basándose en el coste, simplicidad y automatización en vez de en la eficacia y robustez de las mismas.

## **Ofertas actuales en cuestión de seguridad para PYMES**

La mayoría de los proveedores de seguridad que tradicionalmente han trabajado en el mercado de las grandes empresas, fallan cuando quieren cubrir de forma correcta las necesidades de seguridad en el mercado de las PYMES. Las ofertas de estos proveedores de seguridad para PYMES tienen menos componentes de hardware y son menos potentes que los utilizados por las corporaciones, por lo su rendimiento será más lento. La mayoría de estos proveedores simplemente quitan características y capacidades a sus productos dirigidos a grandes empresas, en un intento de crear una oferta a un precio reducido en el mercado de las PYMES. Por ejemplo, un producto de filtrado de URLs dirigido a una gran empresa contiene una lista negra de 50 millones de direcciones, para crear una versión para PYME puede que se recorte la lista, dejándolo en tan sólo 5 millones de direcciones. De igual manera, un motor de búsqueda de programas malignos dirigido a una corporación puede contener 500.000 firmas de programas malignos, en la versión para PYMES puede que sólo contenga 3.000 firmas, lo suficiente para cubrir el "wildlist", la lista oficial de virus distribuida por el mundo que utiliza la industria de seguridad. O un producto de filtrado de e-mail a nivel corporativo con capacidad de cazar spam y otros programas malignos basándose en el contenido o apariencia del mensaje, en una versión para PYMES puede verse reducido a una lista negra dinámica de los dominios spam conocidos.

Algunos proveedores de seguridad reducen incluso la potencia y funcionalidad de sus productos. Mientras que en una versión de Empresa un sistema de seguridad puede tener software y tecnología punteras, en un producto para PYMES puede que se utilice un software de seguridad de código abierto. En una versión para PYMES también pueden faltar características importantes que hagan que el producto sea menos robusto o menos intuitivo. Y lo más importante: todas estas reducciones hacen que las PYMES estén expuestas en cuanto a seguridad se refiere, haciendo que sus redes sean menos seguras que las de las grandes compañías.

## **Necesidades de las Pequeñas y Medianas Empresas**

El acceso al e-mail y Web son las aplicaciones más utilizadas por las PYMES para sus negocios. Las organizaciones deben buscar algunos atributos a la hora de seleccionar un sistema de seguridad que abarque e-mail.

## **Completa Protección para empresas de todos los tamaños**

Las pequeñas y medianas empresas hacen frente a los mismos ataques y problemas provenientes de amenazas basadas en Internet que las grandes empresas. Las corporaciones deben buscar proveedores de seguridad que tengan presencia internacional y que estén constantemente escaneando el contenido de Internet y e-mail para identificar nuevas amenazas. Cuando las empresas se acostumbran a buscar protección desde el "día cero" o protección para las amenazas por e-mail desde el primer día, identificarán los proveedores de seguridad adecuados. Hoy en día, empresas de todos los tamaños demandan protección desde la "hora cero".

## **Solución de Alto Rendimiento**

Para poder ser efectivo, el escaneado de seguridad del e-mail y Web debe ser rápido. A muchas de las soluciones de protección Gateway les lleva mucho tiempo procesar las comunicaciones entrantes y salientes, aumentando el tiempo de respuesta de la red y frustrando a sus usuarios.

## **Continuidad de Negocio**

Una solución Gateway efectiva debe no sólo vigilar amenazas identificadas, sino también proteger contra amenazas que no hayan sido identificadas todavía por los laboratorios de spam y programas malignos.

## **Administración Intuitiva**

Las pequeñas y medianas empresas no disponen de recursos informáticos para invertir en instalaciones complicadas, manteniendo varios paquetes de software de seguridad, pesadas actualizaciones o temas de licencia de usuarios. La solución debe ser intuitiva tanto en su implementación como en su mantenimiento. La solución también debe incluir un asistente de configuración intuitivo basado en Web y gráficos de resúmenes de estadísticas.

## **Conclusión**

Cuando está en juego la seguridad de los recursos de la red de la compañía, tanto las PYMES como las grandes empresas tienen las mismas necesidades de seguridad, pero cada una tiene sus diferencias en cuanto a nivel de experiencia y recursos tanto humanos como financieros. Así que "Enterprise-class" es algo bueno si se refiere a la potencia y una protección completa de la solución de seguridad. Sin embargo este término no debería significar que es una versión sacada de un producto realizado para corporaciones. Las soluciones de seguridad para PYMES deben ser construidas desde el principio y especialmente diseñadas para cubrir sus necesidades. Un producto para PYME debe ofrecer el mismo nivel de seguridad disponible en una versión para grandes compañías.

## Solución de Gestión ProSecure™ STM contra Amenazas Web y E-mail de NETGEAR®

El dispositivo ProSecure STM utiliza una tecnología única que detecta y bloquea las intrusiones basadas en un comportamiento de distribución rápido y a gran escala. De este modo se puede detectar intrusiones de spam y programas malignos tan pronto como se produzcan y bloquear todos los mensajes asociados en tiempo real.

El dispositivo ProSecure STM con tecnología Stream Scanning, está diseñado para escanear flujos de información a medida que van entrando en la red. NETGEAR STM con la tecnología Stream Scanning es capaz de procesar grandes volúmenes de información en tiempo real, utilizando un simple escáner para identificar spam, programas malignos, brechas de seguridad o aplicaciones innecesarias. Así se asegura que los usuarios de la red reciban su e-mail y los contenidos Web limpios y sin retrasos.

El dispositivo ProSecure STM utiliza un sistema de comportamiento de defensa proactivo que soluciona las vulnerabilidades. La solución NETGEAR utiliza un análisis forense para identificar características sospechosas tanto en el tráfico de entrada como de salida de la red y neutralizarlas hasta que puedan ser examinadas más detenidamente.