



Soluciones McAfee System Protection

Diez cosas que las empresas de pequeño y medio porte precisan saber para mantener un ambiente tecnológico seguro

Protección tecnológica total es esencial para empresas de todos los portes





¿Qué es lo que usted debe saber? Tener una SMB (Empresa de Pequeño o Medio Porte)* significa tener que enfrentar 100% de sus propios problemas de TI. La mayoría de las empresas de pequeño y medio porte carecen de información sobre cómo protegerse contra virus, *hackers* y *spam*. Sabemos por experiencia propia que las empresas de pequeño y medio porte están enfrentando los mismos desafíos y necesidades.

Desafíos

- Equipo de TI y conocimiento sobre la seguridad interna limitados
- Los dueños de empresa están cada vez más conscientes de las amenazas de virus y *hackers*
- Presupuesto limitado para seguridad tecnológica

Necesidades

- Soluciones de seguridad comprobadas, fáciles de instalar y de mantener actualizadas
- Soluciones accesibles y económicas
- Protección proactiva del patrimonio de la empresa - como archivos, aplicaciones y datos de clientes
- Tiempo de actividad y disponibilidad máximos de la red, del servidor y de los recursos de *desktop*



Algunas cosas que precisa saber para proteger a su empresa

Nº1

Las soluciones para SMB no deben versiones reducidas de las soluciones para las grandes empresas.

Una misma solución no sirve para todos. Una solución que sirve para una empresa global no es ideal para una SMB. Su empresa precisa de una solución comprobada, creada con sus necesidades en mente -como tamaño, presupuesto y desafíos. Aumentar la seguridad de TI es un elemento esencial para la estrategia tecnológica de toda SMB. Tratar de administrar su empresa en esta época de sofisticadas amenazas virtuales sin una seguridad central ideal es como dirigir un auto sin seguro -¡es preciso estar protegido todos los días!

- Cerciórese de que sus soluciones de seguridad protegen las vulnerabilidades de su empresa
- Comprenda e implante todos los recursos de sus soluciones de seguridad
- Manténgase informado acerca de las amenazas de seguridad, nuevas o mutantes, que pueden afectar a su empresa

Nº2

Una buena protección no precisa ser complicada.

Usted precisa contar con una solución simple de instalar y fácil de mantener actualizada. Su tiempo debe ser dedicado al éxito de su empresa, y no a la protección constante de la red.

- Por lo menos, cree una política de seguridad para su empresa y entrene a sus empleados para aplicarla
- Obtenga los *patches* de seguridad más recientes, los cuales le proporcionarán una protección más actualizada
- Suscríbase a boletines informativos de seguridad, notificaciones de actualización de software, AVERT™ Virus News, etc.
- Establezca prácticas para una correcta administración de contraseñas y cuentas
- Si no las está usando, ¡desactívelas!

Nº3

La protección de la seguridad debe ser proactiva, y no, reactiva.

El secreto es encontrar una solución de seguridad proactiva que haga mucho más que apenas detectar y reaccionar a los virus. La solución apropiada monitorea constantemente toda su red, administra políticas de seguridad en todos los niveles y toma medidas para mantenerlo protegido contra virus de última generación.

- Su software de seguridad debe ser fácil de administrar y de mantener actualizado
- El sistema debe alertarlo sobre problemas de seguridad y ayudarlo a resolverlos fácilmente
- El software de seguridad debe tener una consola de administración fácil de comprender, hasta para los miembros del equipo que no tengan conocimiento técnico

Nº4

Soluciones económicas no siempre significan protección de baja calidad.

No siempre las empresas de pequeño y medio porte pueden mantener un equipo de TI especializado, o gastar el tiempo y los recursos destinados a cuestiones prioritarias críticas para los negocios, para garantizar la seguridad de la red.

- La solución ideal es la que se ajusta a sus límites presupuestarios sin sacrificar la calidad de la protección
- Adquiera un *firewall* de perímetro
- Instale y use un antivirus para *desktop* -procure hallar soluciones proactivas en la identificación y exclusión de virus conocidos y desconocidos
- Protección para *desktop* y servidor -procure hallar soluciones que protegen sus datos y sus aplicaciones críticas para los negocios
- Cuento con varias capas de protección -antivirus, *firewalls*, protección de email, anti-spam, servicios administrados, etc.



Nº5

Los usuarios son los peores enemigos de sí mismos—su red está cada vez más vulnerable.

Una justificativa importante para la adquisición de seguridad tecnológica en empresas de pequeño y medio porte es el creciente número de opciones para conectividad remota a aplicaciones de misión crítica - eso tornó a las SMB más conscientes y vulnerables al acceso no autorizado. Con una solución de detección de invasión proactiva y basada en la red, usted puede bloquear ataques a la red, deteniendo las amenazas antes que entren.

- Proteger a los usuarios remotos es un gran desafío: generalmente utilizan conexiones con poco ancho de banda, son inaccesibles a los administradores de la red y su antivirus puede no estar actualizado
- La infección por virus puede suceder siempre que un documento o archivo ejecutable sea transferido por el FTP o por los archivos compartidos del usuario.
- Las amenazas internas (por ejemplo, empleados) están entre las principales fuentes de actividad mal intencionada
- Una defensa verdaderamente sólida exige amplia protección integrada que abarque toda su empresa, y que llegue al *desktop*
- Use un *firewall* como McAfee® Desktop Firewall™

Nº6

Su caja de entrada es un riesgo potencial.

Gartner Research** afirma, "La amenaza a la seguridad que puede presentarse con más probabilidad en empresas de pequeño y medio porte es un virus llegando por email". Lo

ideal es identificar reglas específicas para los negocios para que sean aplicadas a los emails que entren en la red - determinando lo que es seguro y lo que es una amenaza potencial, lo que llegará al usuario final y lo que permanecerá en cuarentena.

- Cree para los usuarios finales una política de uso del email
- No comparta su dirección de email
- No abra emails de origen desconocido
- No haga clic dos veces en los adjuntos, a menos que sepa lo que son; no abra ningún archivo con extensión doble (por ejemplo, hello.txt.vbs)
- Protéjase contra el *spam* con soluciones como McAfee Security SpamKiller® powered by McAfee SpamAssassin™ - una suite de ofertas para proteger su empresa del *desktop* al *gateway*

Nº7

Su caja de salida es un riesgo potencial.

Los mensajes que contienen comentarios ofensivos sobre raza, sexo, edad, orientación sexual, pornografía, credos religiosos o políticos, origen nacional o discapacidad física deja su empresa legalmente vulnerable. La fuga de informaciones confidenciales sobre la empresa, los clientes o los aliados también imponen gastos y penalidades. Enviar un email es como enviar una tarjeta postal -muchas personas pueden leerlo en el camino.

- Cree para los usuarios finales una política de uso del email
- Protéjase contra un eventual contenido inadecuado adicionando automáticamente un mensaje de exención de responsabilidad a todos los emails de salida

• Prevéngase contra mensajes y archivos inapropiados, no solicitados u hostiles, por medio de filtración de contenido

- McAfee GroupShield® — ofrece protección amplia contra contenido inadecuado para sus servidores de email

Nº8

Las amenazas mixtas de hoy llegan hasta usted rápidamente, replicándose e inundando su red.

Elas combinan los peores aspectos de los *worms*, virus y caballos de Troya, y son complementadas con sofisticadas técnicas de invasión. Probablemente, nunca sabrá qué es lo que lo afectó. Tales amenazas se diseminan tan rápidamente que pueden interrumpir las actividades comerciales en cuestión de minutos. El ataque Nimda, que causó un perjuicio de por lo menos \$600 millones***, tenía cuatro métodos de propagación. Y se prevé que en el futuro los virus sean todavía más perjudiciales.

- Monitorar una red es un gran desafío -por su naturaleza, la red debe ser accesible a varios usuarios, ejecutando varias aplicaciones simultáneamente; el monitoreo de tales actividades exige tiempo y recursos significativos, así como un programa de monitoreo proactivo -y no, reactivo
- Cerciórese de que sus empleados conozcan los peligros de los virus y de otros archivos mal intencionados y cómo pueden afectar a los negocios
- Configure el antivirus para que barra emails, *downloads* de Internet, disquetes, unidades Zip y CD-ROM antes del uso



Las Soluciones McAfee System Protection fueron creadas para su empresa

- **McAfee SAV (Active VirusScan Suite) Small Business Edition**
- **McAfee AVD (Active Virus Defense Suite) Small Business Edition**—

Protección antivirus premiada, integrada y económica, que abarca toda la red y ofrece actualizaciones automáticas

- **McAfee WebShield® e250 e e500** -Hardware y software integrados, que detienen los virus antes que entren en la red

- **McAfee VirusScan® ASaP** - El único servicio antivirus 24x7 administrado, actualizado automáticamente todos los días

- **McAfee Desktop Firewall** - Impide que los clientes envíen o reciban amenazas hostiles de aplicaciones no autorizadas en la red, ofreciendo recursos de *firewall* amplios para la red y sus aplicaciones, combinados a la tecnología de detección de invasión

- **McAfee VirusScan**— Software antivirus líder para *desktop*, de McAfee

- **McAfee SpamKiller powered by McAfee SpamAssassin** -Viene listo para uso, detecta 95% del *spam* y lo detiene antes que llegue a los usuarios finales

Nº9

Los usuarios finales bajan software no relacionado con el trabajo.

Proporcionar a los usuarios finales privilegios para *download* en máquinas del local de trabajo puede dejar su red vulnerable a un ataque viral. Bloquear las PC con una configuración segura, implantando un *firewall* en cada máquina, permitirá una exposición mínima a aplicaciones perjudiciales.

- Si su empleado no precisa de un software para fines comerciales legítimos, no permita que sea cargado en la computadora
- Establezca políticas claras en la empresa sobre el *download* de música, pornografía, salas de charlas o juegos

Nº10

Usted y su empresa son la espina dorsal de la economía.

Su empresa y otras semejantes impulsan la economía nacional. Realmente, las empresas de pequeño y medio porte forman la gran mayoría de las empresas de los países. Lo que diferencia su empresa de las grandes corporaciones es que la suya puede ser más receptiva y flexible a los cambios en la tecnología. Usted tiene la ventaja del control, de la velocidad y de la agilidad a su lado al tomar decisiones sobre tecnología. Al adaptarse rápidamente a los cambios en la tecnología e implantar las mejores prácticas, usted puede tornarse un innovador en su ramo.

- De acuerdo con un estudio de Giga Information Group†, la inversión en las Soluciones McAfee Network Protection proporcionó a las empresas un ROI positivo de hasta 145% en tres años. El estudio reveló que las empresas que usan el *appliance* de prevención contra invasión, de McAfee, economizaron 23% en costos de capital, 41% en costos de operación y 33% en beneficios comerciales, de modo que la solución “se paga” en cuatro meses.

- Aumente la seguridad de la empresa para aumentar su lucratividad general. Tener una red segura disminuye las oportunidades de ser infectado por un virus, asegura que usted se mantenga en operación y que no haya inactividad del sistema interfiriendo en sus transacciones comerciales
- Usted no precisa ser especialista en operaciones de red para implantar medidas de seguridad en la red de su empresa. *Appliances* de seguridad viables y efectivos están disponibles por medio de revendedores entrenados para prestar consultoría e instalar el sistema necesario para proteger a su empresa

* Considerando que las empresas de pequeño porte tengan 100 empleados o menos, y las empresas de medio porte, de 101 a 999 empleados.

** Fuente: Computer Economics, Inc., una empresa de encuestas independiente, en Carlsbad, California, EE.UU., que atiende a 82% de las empresas Fortune 500.

*** Fuente: Computer Economics, Inc., 4 de enero de 2003.

† Fuente: Giga Information Group (subsidiaria de Forrester Research)—“The Total Economic Impact of IntruVert's IntruShield® Intrusion Detection and Prevention” (El impacto económico total de los recursos de detección y prevención de IntruShield®, de IntruVert), mayo de 2003.



McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054. 888.VIRUSNO (888.847.8766)

Los productos de Network Associates® cuentan con el respaldo de años de experiencia y compromiso con la satisfacción del cliente. Los miembros del equipo de PrimeSupport® son técnicos de soporte atentos y altamente cualificados, los cuales proveen soluciones personalizadas, y ofrecen asistencia técnica amplia para la administración del éxito de proyectos de misión crítica, todo ello con la calidad de servicio que atiende a las necesidades de todas las empresas que son clientes nuestras. McAfee® Research, líder mundial en seguridad y sistemas de información, continúa innovando en el desarrollo y la refinación de todas nuestras tecnologías.

Network Associates, McAfee, AVERT, GroupShield, SpamKiller, powered by SpamAssassin, Desktop Firewall, Protection-in-Depth, IntruShield, WebShield, VirusScan y PrimeSupport son marcas comerciales, registradas o no, de Network Associates, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. Los productos que llevan la marca Sniffer son producidos apenas por Network Associates, Inc. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. ©2004 Networks Associates Technology, Inc. Todos los derechos reservados. 4-sps-smb-002-0204