Servicios Centrales:
Avda. Presidente Carrero Blanco, 10 B - 4º B
41011 Sevilla
Teléfono: 95.499 03 80 Fax: 95.427 66 43

Servicio Técnico y Centro Logístico:
C/ Juan Sebastián Elcano, 31 bajo
41011 Sevilla
E-mail: microsa@microsa.es

Soluciones Informáticas

Asunto: <u>SEGURIDAD DE LA INFORMACIÓN</u>
<u>Métodos de protección</u>

Estimado Sr./Sra.,

En los últimos años hemos sido testigos de un espectacular crecimiento en la implantación de los accesos Internet de banda ancha como el ADSL y el cable, enfrentándonos a un gravísimo problema de seguridad, ya que **"la banda ancha se puede similar a vivir todos en la misma casa y con las ventanas abiertas"**.

Y al mismo tiempo los usuarios durante este período "han bajado la guardia" sobre precauciones en el uso de Internet y se ha pasado de un cierto temor y respeto a una **situación actual en la que se realizan conexiones a Internet sin ninguna protección ni medida de seguridad ni asesoramiento por ningún experto en seguridad**.

Adjunto le enviamos informe que hemos desarrollado sobre esta gravísima situación actual de inseguridad en la protección de nuestros sistemas y de la información en ellos contenida y le dejamos planteada las siguientes preguntas para su reflexión:

¿Está su empresa protegida contra la fuga de información?

¿Es consciente de la pérdida de productividad con su correspondiente coste económico que para su empresa supone un mal uso de Internet?

¿Tiene sentido en una empresa hacer uso de una herramienta de tan alto riesgo como Internet sin ningún plan previo de seguridad de la información?

¿Sabe que Internet y el correo electrónico son las principales vías de contagio de los nuevos virus como los troyanos que nos provocan un agujero de seguridad siendo su PC controlado desde el exterior por un pirata informático?

Con el auge del ADSL y del cable, ¿es conocedor del riesgo actual de sufrir intrusiones en su ordenador y ser víctima de cualquier internauta malintencionado que con pocos conocimientos informáticos puede fácilmente coger, borrar y modificar la información de su ordenador?

En definitiva, **para una empresa la información es su activo fundamental** que debe protegerse de ataques externos e internos y pensamos que la empresa debe de tener en todo momento un control de todo el tráfico desde y hacia Internet.

... / ...

Aunque **la seguridad total es imposible**, se puede controlar un conjunto de vulnerabilidades y no sólo prevenir ataques sino ser capaces de detectar y responder a los mismos.

Para ello, **nuestras recomendaciones básicas** son:

1) Tener instalado un buen **antivirus** y mantenerlo permanentemente actualizado.
2) Realizar el acceso a Internet a través de un **router** bien configurado y jamás a través de modem o de tarjeta RDSI.
3) Instalar un **Sistema de Seguridad**.

Los Sistemas de Seguridad profesionales suelen ser sistemas muy costosos y muy complejos tanto de instalación como de mantenimiento; y a pesar de ello le ofrecemos dos soluciones a diferente nivel a precio muy especial:

1) **Solución ISA** que consiste en la instalación de un servidor con **Microsoft ISA Server 2000** y de un antivirus gateway Internet.
   Microsoft ISA Server 2000 proporciona conectividad a Internet segura y rápida, debido a que integra un cortafuegos (firewall) empresarial de varias capas y un caché web escalable y de alto rendimiento. Utiliza como base la seguridad y el directorio de **Microsoft Windows 2000** para ofrecer sus funcionalidades basadas en perfiles de grupos y usuarios.
   El antivirus **InterScan** de **Trend Micro** filtra los virus desde/hacia Internet antes de infectar nuestros PCs y servidores.

2) **Solución 3COM** que consiste en la instalación de un aparato cortafuegos entre nuestro router y nuestra red local.

Con ambas soluciones cubrimos el objetivo marcado de impedir las conexiones externas no deseadas y de tener un control de todo el tráfico desde y hacia Internet:

- Complementa la seguridad realizada por el router de **cerrar todos los puertos desde Internet** cuando éste plantea problemas de agujeros de seguridad.
- **Limita el acceso por PC y protocolo hacia Internet**, por lo que sólo accederán a Internet aquellos PCs permitidos y con los protocolos que se le permitan (web, correo, FTP...)
- Permite **denegar el acceso a determinadas páginas de Internet** y configurar que sólo se acceda a determinados dominios, impidiendo por ello la fuga de información vía troyano.
- **Se registran todos los intentos de accesos y accesos válidos hacia Internet** con información del nombre de la página visitada y la cantidad de información enviada o recibida. Los intentos de ataques externos de intrusos son notificados inmediatamente por correo electrónico.

... / ...

Las principales diferencias entre ambas soluciones son las siguientes:

- La **Solución ISA** la forma un servidor al que se le puede dar este uso de seguridad o cualquier otro en función del software que se le instale, por lo tanto no tiene ninguna limitación, en contra de la **Solución 3COM** que está limitada al diseño del producto.
- En la **Solución ISA** la seguridad está implementada por usuario y no por PC como en el caso de la **Solución 3COM**.
- En la **Solución ISA** se puede implementar un antivirus en el propio cortafuegos impidiendo el contagio de nuestros PCs y servidores.
- La **Solución ISA** no es sólo un cortafuegos como la segunda solución, sino que es un proxy con caché web y utiliza como base la seguridad y el directorio de **Microsoft Windows 2000**.
- La **Solución ISA** es mucho más profesional incluyendo múltiples informes y estando abierta a multitud de software creado para esta plataforma.

Para un mayor control por parte de la dirección de la empresa hemos creado un **Visor de Informes Microsa** de accesos a Internet en donde podemos generar informes ordenados por:

- usuario y web
- usuario y protocolo
- usuario, fecha y web
- usuario, fecha y protocolo
- protocolo y usuario

con información del usuario, fecha, destino, protocolo, tiempo, bytes enviados y bytes recibidos.

Desagraciadamente tenemos conocimiento de continuos ataques de hackers que estamos sufriendo y por otro lado por la enorme proliferación de troyanos que pueden controlar nuestro PC desde fuera, hacen **necesario que se tomen medidas de seguridad antes de que sea demasiado tarde**. Por lo que **el sufrir intrusiones no es un riesgo remoto sino una triste realidad**.

Partiendo de la base de que la información es el activo fundamental de una empresa, proponemos estas soluciones para tener en todo momento un control de todo el tráfico desde y hacia Internet, aunque debemos de mentalizarnos que toda implementación de seguridad que se realice, requiere de su conveniente monitorización y actualización, ya que de no ser así a corto plazo no nos servirá de nada. Y sobre todo **es importante entender la seguridad como un proceso y no como un producto**.

En la confianza de que podamos asesorarle en la solución de seguridad más acorde con sus necesidades, aprovechamos la ocasión para saludarle muy cordialmente,

Francisco Martelo
Director