GUÍA BÁSICA

SEGURIDAD PARA PYMES

INTRODUCCIÓN

El cibercrimen se sigue extendiendo día a día a una velocidad de vértigo, y cada día inventan nuevas artimañas para conseguir víctimas de las que conseguir un beneficio económico. Esto complica bastante el panorama de la seguridad, sobre todo si se tiene en cuenta de que cada dispositivo que esté conectado a Internet es un potencial foco de riesgos.

Conocer todo lo que tenemos que saber acerca de la seguridad es complicado si no te dedicas a este mundo de manera profesional. Al final, un autónomo o un empresario debe concentrarse en su actividad, en lo que sabe hacer, y conseguir que la seguridad de su vida digital empresarial sea lo más saludable posible como para no tener que estar preocupándose de todos los riesgos de Internet.

Además, hoy en día no basta con tener un antivirus instalado, medida de seguridad totalmente necesaria. Hay que contar con más herramientas y tomar más precauciones, porque incluso viendo un vídeo o utilizando las redes sociales podemos estar poniendo en peligro la integridad de nuestros sistemas.

A medida que una compañía crece, también crecen con ella sus riesgos. En este documento intentamos brindar una herramienta de trabajo, de educación y de concienciación básica para autónomos y pequeñas y medianas empresas que se tienen que enfrentar al duro trabajo de implementar la seguridad de sus ordenadores, sus dispositivos móviles, sus redes internas, sus servidores, etc.

El documento está dividido en tres grandes bloques: seguridad básica para autónomos, seguridad para empresas hasta 25 empleados y seguridad para empresas que cuentan hasta con 250 trabajadores. A partir de este tamaño, entendemos que se cuenta (o se debería contar) con personal especializado en seguridad y sistemas.

Recomendamos, de todas las maneras, una lectura desde el principio, para tener bien claros y sólidos los conceptos más básicos y así poder avanzar hacia los más complejos.

Esperamos que esta guía te sirva de ayuda.

Equipo de ESET España

Autónomos

Si eres autónomo, la seguridad es sencilla de implementar y de administrar y depende única y exclusivamente de ti. Seguramente tendrás un ordenador (de sobremesa o portátil), un smartphone y una tablet, y todo tu trabajo lo desarrollarás con este equipo informático.

Si es así, todos los consejos para usuarios domésticos también se pueden aplicar a ti en cuanto a seguridad se refiere. Preservar tu información y tus datos es el objetivo prioritario que perseguir y cumplir.

Existen tres aspectos que debemos cuidar si queremos preservar nuestra seguridad online:

- La seguridad de la información entendida como la preservación de nuestros datos personales y la integridad de nuestros dispositivos y aplicaciones
- El secreto de nuestra información
- Nuestra reputación online

¿Qué deberías tener en cuenta?

- Instala un buen antivirus tanto en tu ordenador como en tus dispositivos móviles.
- Toma medidas adicionales de seguridad en tus dispositivos móviles.
- Cuida las conexiones a Internet que utilizas.
- Elige contraseñas fuertes.
- Haz copias de seguridad.
- Cifra toda la información de tu empresa.

- **Instala un buen antivirus tanto en tu ordenador como en tus dispositivos móviles**

Idealmente, debería ser una suite de seguridad completa que te ofrezca todo tipo de protección, no solo contra amenazas informáticas, sino que cuente con cortafuegos personal, con antispam y con protección avanzada contra los engaños y timos en Internet, como el phishing, o anti-botnets, para evitar que tu ordenador sea controlado remotamente.

Además, para todos tus dispositivos pero sobre todo para los móviles, busca una buena protección que te ofrezca la posibilidad de reaccionar frente a robos y pérdidas, ya que suele ser el problema más frecuente hoy en día.

- **Toma medidas adicionales de seguridad en tus dispositivos móviles**

Seguimos sin tomar conciencia de la importancia real y del valor de nuestros smartphones y tablets, y no tanto desde el punto de vista de la cuantía económica del terminal –que también-, sino de la información que contiene. Por eso, y como es muy frecuente la pérdida o el robo de estos dispositivos, te sugerimos que implementes simples medidas de precaución:

- Coloca una contraseña de acceso al teléfono. De esta manera, si te lo roban, dificultarás el acceso a la información que contiene.

- Descarga aplicaciones solo desde sitios oficiales y de confianza. Sigue siempre la normativa corporativa y averigua si puedes hacerlo.

- Por último, cifra la información almacenada en tu dispositivo. Existen muchas aplicaciones para hacerlo.

- **Cuida las conexiones a Internet que utilizas**

Es común utilizar el equipo portátil de trabajo para conectarse a redes WiFi públicas como, por ejemplo, redes de bares, cafés, aeropuertos, etc. En estos casos debe considerarse que la seguridad estará ligada a los controles existentes en dicha red. En muchos casos, estos controles son inexistentes, tales como la ausencia de contraseña para realizar la conexión WiFi, o permitir que los dispositivos se vean entre sí.

Por ello, recomendamos no realizar conexiones importantes, como por ejemplo acceder al correo corporativo, ya que la red puede estar expuesta y que la información viaje sin ningún tipo de cifrado, haciendo que muchos de los datos enviados puedan ser vistos por otra persona que esté conectada a la misma red.

En el caso de que utilices un equipo público para conectarte con tu empresa, evita abrir archivos con información confidencial de forma local, ya que estos archivos pueden quedar accesibles en ese equipo y ser vistos por cualquier persona que utilice el mismo equipo en un futuro.

- **Elige contraseñas fuertes para todos tus servicios online**

Dada la cantidad de sistemas, plataformas, correos electrónicos y otros servicios de la empresa existentes, cada integrante de la compañía suele tener varias contraseñas. Sin embargo, una única contraseña débil puede significar el acceso a información confidencial o a un sistema por parte de un atacante o un código malicioso.

Entendemos como contraseñas débiles aquellas que no combinan letras, números, símbolos y mayúsculas y minúsculas, como mínimo, y que son de menos de 10 caracteres. Una contraseña débil es, por ejemplo, 1111111.

Teniendo en cuenta esto, es importante que las contraseñas que se utilizan dentro de la empresa (y también a nivel personal) sean fuertes: es decir, fáciles de recordar y difíciles de descifrar.

Muchas veces la motivación de crear contraseñas fuertes contrae el riesgo de que sean olvidadas. Debido a esto, la utilización de un software para la gestión de contraseñas es la alternativa más adecuada, no siendo así la utilización de cuadernos o papeles pegados en el escritorio para anotarlas. Además, la utilización de contraseñas diferentes para los distintos servicios es también muy importante.

- **Haz copias de seguridad**

No dejes ningún día de hacer una copia de seguridad de la información de tu empresa. Hay distintas formas de organizar las copias, pero una bastante sencilla y eficiente es tener un disco por cada día laborable de la semana, de este modo, si la copia más reciente fallara, puedes utilizar otra hecha sólo 24 horas antes. Guarda el disco del último día de la semana en un lugar distinto a tu sitio de trabajo habitual, porque si no en caso de robo o incendio puedes perder toda la información.

- **Cifra toda la información de tu empresa**

Las empresas se enfrentan a un desafío cada vez más importante al tener que combatir el cibercrimen y asegurar la información y los datos corporativos –principal activo de cualquier compañía- no solo en los ordenadores del parque informático, sino también en dispositivos portátiles que trabajan de forma independiente y deslocalizada y que en muchos casos son objeto de robos y/o pérdidas.

Además, esta nueva forma de trabajo provoca que, en muchas ocasiones, la información viaje por correo electrónico a través de conexiones WiFi sin protección o a través de otros medios. Es en estos casos en los que las políticas de seguridad de la compañía intentan asegurar al máximo la información más crítica. Por eso es muy recomendable instalar, configurar y mantener alguna solución de cifrado para todo el disco, el correo, los dispositivos extraíbles y las carpetas y archivos.

Hasta 25 empleados

Cuando la empresa crece, se necesita incorporar más personal, y dotarle de las herramientas necesarias para que desarrollen su trabajo de la forma más adecuada. Al principio, lo normal es que los dispositivos móviles que se utilizan sean los personales de cada empleado, pero esta "ventaja" puede convertirse en un inconveniente si no se tienen en cuenta otros factores.

Además, suele ser normal instalar en las oficinas un servidor de ficheros, es decir, un servidor dedicado a tener documentos y aplicaciones compartidas: un punto más estratégico a proteger.

Y el acceso a Internet seguro que se realiza a través de un router con una buena conexión y con banda ancha. Conexión a través de la cual los empleados realizarán diferentes tareas, tanto personales como profesionales, pueden descargar cosas de la Red e incluso conectarse a servicios en la nube.

¿Qué deberías tener en cuenta?

- Instala antivirus a todos tus empleados y a tu servidor de ficheros.
- Establece normas de conexión segura.
- Asegura tu red interna.
- Dicta una política de contraseñas seguras.
- Utiliza sistemas de alimentación ininterrumpida (SAI)
- Utiliza firma electrónica y certificados de seguridad. Cuida la LOPD.
- Normaliza un uso seguro de Internet.

- **Instala la misma protección antivirus que tienes en tu equipo a todos tus empleados**

Es mucho mejor contar con una solución de protección antivirus corporativa que te permita tener un control de forma centralizada sobre todas las protecciones y mantenerlas actualizadas que tener productos individuales que después tengas que controlar uno o a uno o confiar en que tus empleados van a hacerlo.

Además, así evitarás que tus empleados manipulen la configuración por defecto del programa que hayas elegido, llevando a cabo acciones que pueden poner en riesgo la seguridad de la empresa, como desactivar el cortafuegos, por ejemplo.

También es conveniente que cuenten con todas las protecciones: antivirus, antispam, anti-phishing, cortafuegos personal, etc.

- **Implementa las mismas medidas de seguridad y la prevención en sus dispositivos móviles, que preferiblemente deberían ser de empresa**

Al principio, es más barato para el empresario que un empleado pueda utilizar su propio smartphone para trabajar, pero puede suponer un riesgo de seguridad. Es mucho mejor proporcionar a los trabajadores los dispositivos que creas que pueden llegar a utilizar, instalarles la protección y educarlos y concienciarlos sobre la necesidad de tomar medidas de prevención, como el uso de contraseñas, entre otras.

- **Instala un buen antivirus que proteja también tu servidor de ficheros**

Si tienes un servidor de ficheros que es utilizado por todos los empleados, es necesario que también lo protejas de la forma adecuada. Es otra de las ventajas de los antivirus para empresa, que te permiten instalar la mejor protección para estos dispositivos, estén o no conectados a la Red, y además podrás gestionarlo todo desde una única consola.

- **Establece normas de conexión segura para tus trabajadores si acceden a la información de tu empresa desde fuera de sus instalaciones**

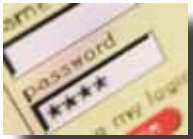
Si vas a permitir que los empleados se conecten desde fuera de la oficina al servidor de esta, ten en cuenta que pueden hacerlo desde cualquier sitio, también desde una red WiFi. Así que nuestra recomendación es que instales y habilites una red VPN (Virtual Private Network o red privada virtual). De esta manera, cada vez que cualquiera se conecte a la empresa, estará navegando de forma segura y con la información protegida.

- **Asegura tu red interna**

Con ese número de trabajadores y conectándose a recursos compartidos, como el servidor o impresoras, por ejemplo, lo más normal es que hayas configurado una red interna. Protegerla con una buena contraseña implica un blindaje, de forma que no pueda haber intrusiones externas.

De la misma manera, es conveniente instalar un buen cortafuegos corporativo, que evite precisamente el aprovechamiento de agujeros de seguridad para colarse en la Red y acceder a los mismos recursos que el resto.

- **Proporciona a tus empleados contraseñas robustas y establece una política de mantenimiento para cambiarlas cada poco tiempo**



Lo mismo que hemos comentado anteriormente sobre establecer contraseñas robustas se debe aplicar para todos los trabajadores. Además, es necesario concienciarlos acerca de la necesidad de no compartirlas, no escribirlas en post-it o llevarlas guardadas en las notas del teléfono, etc.

Una correcta identificación de usuarios para acceder a la red interna, a los servidores o recursos compartidos o a los servicios online que utilices no solo te asegurará que nadie pueda colarse para poner en riesgo tu información, sino que también te servirá para controlar posibles robos o fugas de información internas. Eso sí, recuerda no solo cambiarlas cada cierto tiempo, sino dar de baja aquellos usuarios que ya no trabajen en la empresa, por ejemplo, que suele ser el ejemplo más común y fuente de problemas.

- **Utiliza sistemas de alimentación ininterrumpida (SAI)**

Aunque no es una medida de seguridad en sí misma, indirectamente sí puede ayudarnos. Para evitar que los procesos en curso se interrumpan bruscamente en caso de corte del suministro eléctrico y para filtrar los "microcortes" y picos de intensidad, que resultan imperceptibles pero que pueden provocar averías en los equipos, es muy aconsejable disponer de sistemas de alimentación ininterrumpida, al menos para los servidores y equipos más importantes.

El tiempo de autonomía depende de la potencia de la unidad y de los equipos conectados. En general es suficiente con unos 10-15 minutos, plazo que permite terminar de forma ordenada los trabajos en curso, cerrar de la forma adecuada las aplicaciones y salir de los servicios online que estemos utilizando.

- **Uso seguro de Internet**

Cualquier ordenador, teléfono o tableta entraña un riesgo de seguridad. Cada día se crean más de 250.000 códigos maliciosos (virus, troyanos, ataques de phishing, etc.) para conseguir engañar a los usuarios. Por lo tanto, utilicemos las herramientas que utilicemos, vamos a estar expuestos a dichos riesgos. Y estos son más altos si estamos conectados a Internet y navegamos, utilizamos redes sociales, etc.

Conociendo los riesgos, la probabilidad se reduce un 50% de ser víctimas de un fraude, un engaño o una infección, porque aprenderemos a reconocerlos y a evitarlos. Y si completamos nuestras buenas prácticas con la instalación de herramientas de seguridad, no estaremos exentos, pero al menos reduciremos el umbral de riesgos significativamente.

Cuando hablamos de navegación web, vamos a referirnos a tres aspectos diferentes:

a) Correo electrónico

Con este tamaño de empleados, lo normal es no tener un servidor de correo, ya que en la mayoría de las ocasiones se utilizará el que nos proporciona nuestro proveedor de hosting o bien uno gratuito.

Sea como fuere, el uso de un correo electrónico corporativo supone someterse a una serie de normas de actuación para preservar su seguridad. Aunque la empresa tenga instaladas herramientas de seguridad, muchas veces, sin darnos cuenta, estamos exponiendo la integridad de nuestro correo a un riesgo innecesario al darnos de alta con él en redes sociales u otros servicios para un uso personal.

Al hacerlo, no solo estaremos exponiendo nuestra dirección a riesgos, sino al envío de spam, newsletters o incluso ataques de phishing que no hacen más que mermar la productividad.

Por lo tanto, es recomendable concienciar a todos los empleados e indicarles que sigan las recomendaciones para preservar la seguridad del correo electrónico corporativo y no utilizarlo para fines personales. Existen multitud de servicios gratuitos, como Gmail o Yahoo!, en los que podemos crearnos una dirección de correo personal y utilizarla para darnos de alta en cuantos sitios queramos.

Si alguno de tus empleados ya ha utilizado el correo electrónico para darse de alta en estos sitios, todas las redes sociales y los sitios online dan la posibilidad de cambiarlo, así que están a tiempo de hacerlo.

Si ves que recibes muchos correos o intentos de ataques de phishing, solicita a tus empleados que se den de baja en los newsletters que reciban y configura el antivirus para que bloquee este tipo de mensajes, si no lo hace ya.

Si te preguntas qué es el phishing, es una amenaza que en la mayoría de las ocasiones viene en un correo electrónico simulando ser tu banco o tu red social e invitándote a que introduzcas tus datos de acceso en el sistema porque se han detectado problemas de seguridad. Cuando accedes, probablemente el sitio que veas sea igual que Amazon, Facebook o tu banco, pero fíjate en la barra de dirección de tu navegador, porque casi siempre es una página clonada pero alojada en otro sitio diferente. Si introduces tus datos, éstos caerán en manos indeseadas que pueden hacer un uso indebido de ellos.

b) Navegación web

El permitir o no que tus empleados naveguen en Internet es tu decisión. Muchas empresas tienen bloqueada la posibilidad de navegación de sus empleados, más por precaución que por distracción de sus obligaciones. Pero esta medida termina siendo contraproducente a la larga, porque es indudable que Internet es una gran herramienta de trabajo con la que un comercial puede localizar nuevos clientes o una central de compras, a nuevos proveedores.

También existen muchas empresas que establecen una forma de navegación restringida, donde el usuario puede utilizar Internet pero no entrar a determinados sitios, como a redes sociales, por ejemplo. En otras ocasiones, no existe ninguna restricción.

Sea cual sea tu decisión, debes pensar que hay que buscar el equilibrio entre la productividad y la permisividad, y siempre tener presente –y que lo tengan tus empleados- que utilizar Internet en el trabajo es recomendable con un uso profesional, y no personal, para evitar problemas laborales. Pero además, también debes saber que tienes entre manos una gran herramienta con algunos riesgos, entre los que se incluyen infectar el parque de ordenadores de tu empresa por navegar por sitios inadecuados, por ejemplo.

Así que nuestra recomendación es que apliques el sentido común, recomiendes hacer un uso profesional de la navegación, que eviten ir a sitios de contenido dudoso y que hagan caso de los avisos que algunos navegadores muestran cuando se intenta visitar un sitio que pudiera contener algún tipo de amenaza.

c) Redes sociales

Tal y como hemos comentado anteriormente, algunas empresas tienen restringido el uso de redes sociales en el trabajo con el objetivo de que la productividad no disminuya. Sin embargo, otras muchas han descubierto el gran potencial que desde el punto de vista de marketing y promoción tiene el que los trabajadores hablen en nombre de la empresa en las redes sociales, promocionen sus productos y servicios, etc. A fin de cuentas, pueden más 10 voces que 1.

Si este fuera el caso, elabora un código de conducta en las redes sociales donde se normalice de qué se puede hablar y de qué no, o cuándo se solicita la ayuda y cooperación de los trabajadores para la promoción de un determinado producto o servicio.

Por último, si alguno de tus trabajadores es el encargado de gestionar las redes sociales de la empresa, tienes que tener en consideración otra serie de buenas prácticas:

- Protege el usuario y la contraseña de tus canales oficiales y encárgate de cambiarlo al menos cada tres meses. No delegues esta tarea.

- Ante cualquier sospecha de que la cuenta haya sido secuestrada o vulnerada procede a intentar recuperar la cuenta. Si ves actividad sospechosa en la cuenta, avisa a tu comunidad (desde el blog corporativo, por ejemplo).

- Recomienda seguir siempre las normas en cuanto al lenguaje corporativo a aplicar y el tipo de información que puedes compartir con tus comunidades.

Hasta 250 empleados

Cuando alcanzas el volumen de 250 empleados o más, además de todo lo anterior, seguramente estás utilizando ya un servidor de correo corporativo en tus propias instalaciones. Puede que también tengas un servidor web donde alojas tu página o tu tienda online.

Además, las posibilidades de que cualquier empleado tome decisiones por su cuenta que pudieran poner en riesgo la seguridad también son factibles. Así que, además de todo lo anterior, te recomendamos tener en cuenta otros factores más especializados que hagan que tu seguridad sea lo más robusta posible.

Por otro lado, y conforme más grande va siendo la empresa, más necesaria es tener tanto una estrategia informática bien pensada de acuerdo a las necesidades de cada uno e implementada y mantenida, así como contar con los suficientes conocimientos de seguridad informática de forma que todos los posibles agujeros queden bien tapados y asegurados.

Por eso, siempre recomendaremos contar con buen personal especializado no solo en administración de sistemas, sino en seguridad informática, que entienda los conceptos –cada vez más complejos cuanto más grande es el parque informático-, conozca las diferentes soluciones del mercado y se ocupe de implementarlas y mantenerlas. Además, también sería muy recomendable contar con un documento de Políticas de Seguridad empresarial, de forma que todos y cada uno de los miembros de la empresa sepan, en cada momento, qué tienen que hacer, cómo actuar ante una emergencia, qué medidas tomar en caso de riesgos, etc.

¿Qué deberías tener en cuenta?

- Asegura tu servidor de correo.
- Asegura tu web seguro.
- Instala un Gateway seguro.
- Implementa un sistema de detección de intrusiones.
- Instala un firewall perimetral.
- Ten una sólida política de seguridad de empresa.
- Cuenta con personal especializado en administración de sistemas y en segurida.

- **Servidor de correo**

Un servidor de correo en las instalaciones corporativas entraña algunos riesgos:

- La inundación (tipo de ataque de negativa de servicio) se produce cuando un sistema se sobrecarga con multitud de mensajes de correo electrónico. Para un atacante es relativamente fácil crear un programa sencillo que envíe millones de mensajes de correo electrónico (incluidos mensajes vacíos) a un único servidor de correo para intentar inundarlo. Sin la seguridad adecuada, el servidor de destino puede experimentar una negativa de servidor, debido a que el disco de almacenamiento del servidor se colapsa con mensajes inútiles. O bien, el servidor deja de responder porque todos los recursos del servidor están ocupados procesando el correo del ataque.

- Correo masivo (spam o correo basura) es otro tipo de ataque común al correo electrónico. Con el aumento del número de empresas que practican el comercio electrónico en Internet, se ha producido una invasión de mensajes comerciales de correo electrónico indeseados o no solicitados. Esto es lo que se llama correo basura, y se envía a una amplia lista de distribución de usuarios de correo electrónico, colapsando el buzón de correo de todos los usuarios.

- La confidencialidad es un riesgo asociado con el envío de correo electrónico a otra persona a través de Internet. Este mensaje de correo pasa a través de muchos servidores antes de llegar al destinatario. Si no se cifra el mensaje, cualquier hacker podría interceptarlo y leerlo en cualquier punto de la ruta de entrega.

Para prevenir los riesgos de inundaciones y el correo masivo (spam), debes instalar una adecuada protección de seguridad y configurar el servidor de correo electrónico correctamente. La mayoría de aplicaciones de servidor proporcionan métodos para enfrentarse a este tipo de ataques. Asimismo, puedes trabajar con tu proveedor de servicios de Internet (IPS) para que aporte algún tipo de protección adicional contra estos ataques.

Las medidas de seguridad adicionales necesarias dependerán del nivel de confidencialidad que desees mantener, así como de las características de seguridad que ofrezcan las aplicaciones de correo electrónico. Por ejemplo, ¿es suficiente con mantener la confidencialidad del contenido del mensaje de correo? ¿O deseas que sea confidencial toda la información asociada con el correo electrónico, como las direcciones IP de origen y destino? Algunas aplicaciones tienen características de seguridad integradas que ofrecen la protección que necesitas.

- **Servidor web**

Lo más normal con un tamaño de empresa considerable es que su página web, o su tienda online, la tengas alojada en tu propio servidor. De hecho, los servidores web se han convertido en el escaparate de salida de muchas compañías, desde las empresas más pequeñas hasta grandes corporaciones.

Con todo esto, los servidores web donde se alojan cada una de estas páginas, han pasado a ser un blanco fácil para cualquier tipo de atacante.

Los ataques a estos servidores normalmente son los más llamativos, debido en gran medida a la necesidad que tenemos todos los usuarios de Internet de depender de él, por lo que es muy fácil divulgar un ataque, ya que en cuestión de segundos una gran mayoría de la población mundial se dará cuenta de que hay algo que se ha modificado en el servidor comprometido.

Hoy en día, los servidores web tienen que estar protegidos frente a cualquier tipo de amenazas, tienen que estar preparados para ser el primer punto de entrada a cualquier compañía y, sobre todo, tienen que estar bien securizados.

La mayor parte de estos ataques, en la actualidad, vienen como consecuencia de una mala configuración del servidor o un mal diseño, así como de fallos de programación derivados de los ajustados Service Level Agreement (SLA) al que se enfrentan los desarrolladores de los portales web.

Las grandes corporaciones tienen sistemas más complejos y, por lo tanto, más difíciles de administrar; y las pequeñas empresas tienen servidores simples y con una configuración paupérrima, lo que hace que, en su gran mayoría, estos servidores sean susceptibles de ser atacados.

En este punto tenemos dos opciones para actuar: por un lado, intentar realizar una configuración correcta de los servidores web y de los elementos que lo componen y, por otro, contar con herramientas de seguridad dedicadas exclusivamente a la securizacion de estos servidores.

En el mercado, existen herramientas dedicadas para proteger servidores web, dispositivos de seguridad capaces de ofrecer multitud de funcionalidades que, sin lugar a dudas, nos serán de gran utilidad a la hora de proteger nuestro entorno web.

Estos dispositivos son capaces de realizar funciones que van desde firewall de aplicación web (Web Application Firewall -WAF-), aceleración de las propias aplicaciones, balanceo de carga entre los servidores e IPS. Son muchas las posibilidades que ofrecen este tipo de herramientas, que cada vez más se están imponiendo en las compañías con el fin de proteger la parte más importante de la empresa de cara al exterior.

Entre los beneficios que nos ofrecen este tipo de dispositivos, podemos destacar:

1. Protección de firewall e IPS sobre aplicaciones web.
2. Firewall de aplicaciones XML, implementando las capacidades IPS, sobre el código XML.
3. Balanceo de carga entre los servidores web, con el fin de conseguir su descongestión.
4. Bloqueo de amenazas sobre las aplicaciones que corren en el servidor web como cross site, inyección SQL o ataques de buffer overflow.
5. Soporte para comunicaciones SSL y procesamiento de cifrado XML.
6. Cumplimiento de normativas de seguridad.
7. Reducción de la complejidad en la administración.

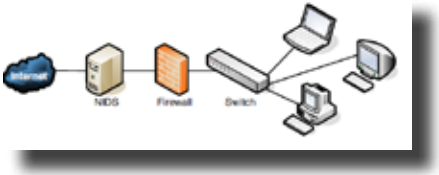
- **Gateway**

Una pasarela, puerta de enlace o gateway es un dispositivo que permite interconectar redes con protocolos y arquitecturas diferentes a todos los niveles de comunicación. Su propósito es traducir la información del protocolo utilizado en una red inicial al protocolo usado en la red de destino.

El gateway o «puerta de enlace» es normalmente un equipo informático configurado para dotar a las máquinas de una red local (LAN) conectadas a él de un acceso hacia una red exterior, generalmente realizando para ello operaciones de traducción de direcciones IP (NAT: Network Address Translation). Esta capacidad de traducción de direcciones permite aplicar una técnica llamada IP Masquerading (enmascaramiento de IP), usada muy a menudo para dar acceso a Internet a los equipos de una red de área local compartiendo una única conexión a Internet, y por tanto, una única dirección IP externa.

Como tal, también es necesario configurar una seguridad específica para este tipo de servidores, que sea capaz no solo de detectar problemas generados por ficheros que viajan por la Red infectados, sino filtrar todas las comunicaciones en busca de riesgos de seguridad.

- **Sistema de detección de intrusiones**



El término IDS (Sistema de detección de intrusiones) hace referencia a un mecanismo que, sigilosamente, escucha el tráfico en la red para detectar actividades anormales o sospechosas, y de este modo, reducir el riesgo de intrusión.

Existen dos claras familias importantes de IDS:

- El grupo N-IDS (Sistema de detección de intrusiones de red), que garantiza la seguridad dentro de la red.
- El grupo H-IDS (Sistema de detección de intrusiones en el host), que garantiza la seguridad en el host.

Un N-IDS necesita un hardware exclusivo. Este forma un sistema que puede verificar paquetes de información que viajan por una o más líneas de la red para descubrir si se ha producido alguna actividad maliciosa o anormal. El N-IDS pone uno o más de los adaptadores de red exclusivos del sistema en modo promiscuo.

Éste es una especie de modo "invisible" en el que no tienen dirección IP. Tampoco tienen una serie de protocolos asignados. Es común encontrar diversos IDS en diferentes partes de la red. Por lo general, se colocan sondas fuera de la red para estudiar los posibles ataques, así como también se colocan sondas internas para analizar solicitudes que hayan pasado a través del firewall o que se han realizado desde dentro.

Las intrusiones se clasifican de la siguiente manera:

- Intrusiones por mal uso: son ataques en puntos débiles conocidos de un sistema. Pueden ser detectados observando y buscando ciertas acciones que se realizan a ciertos objetos.

- Intrusiones anómalas: se basa en la observación de desviaciones de los patrones de uso normales del sistema. Pueden ser descubiertos construyendo un perfil del sistema que se desea supervisar, y detectando desviaciones significantes del perfil creado.

Mientras las intrusiones de mal uso sigan patrones bien definidos pueden ser detectadas haciendo un análisis y chequeo en la información de auditoría y reportes del sistema. Por ejemplo, un intento de crear un archivo inválido puede ser descubierto examinando los mensajes en los logs que son resultado de las llamadas al sistema.

Los sistemas informáticos se apoyan en los Sistemas de Detección de Intrusiones (IDS -de sus siglas en inglés) para prepararse y ocuparse del mal manejo y del uso indebido de la información de una organización. Logran esta meta, recopilando la información de una gran variedad de fuentes del sistema y de la red y analizando la información que contribuye a los síntomas de sus problemas de seguridad, y permiten que el usuario especifique las respuestas en tiempo real a las violaciones.

Los productos de detección de intrusos son aplicaciones que monitorean activamente los sistemas operativos y el tráfico de red, con el objeto de detectar ataques y violaciones a la seguridad.

Es decir, los IDS son herramientas de seguridad en red que recopilan información de una variedad de fuentes del sistema, analizan la información de los parámetros que reflejan el uso erróneo o la actividad inusual, responden automáticamente a la actividad detectada, y finalmente informan el resultado del proceso de la detección.

- **Firewall perimetral**

El objetivo del Firewall perimetral es impedir que se realicen conexiones entre la red corporativa e Internet que estén fuera de la política de seguridad de la compañía. En un dispositivo perimetral el firewall es siempre la primera línea de protección.

El firewall de las protecciones perimetrales debe ser capaz de realizar diferentes tipos de filtrado:

- Filtrado estático a nivel de red, basado en reglas definidas por el administrador en base a los contenidos de las cabeceras de los paquetes IP, las direcciones IP de origen y destino, intervalo de tiempo, etc., tanto para tráfico entrante como saliente.

- Filtrado dinámico a nivel de aplicación con dos características.

GUÍA BÁSICA

SEGURIDAD PARA PYMES