

Los 8 Factores que pueden afectar a su Seguridad Informática Corporativa en las próximas dos horas

Una guía diseñada para ayudar a las pequeñas empresas a comprender las amenazas web y lo que significa

Introducción

Los empresarios deben trabajar muy duro para mantener el negocio e intentar aumentar las ventas. Se pueden buscar empleados y publicidad que le aseguren la expansión pero cerciorarse de que la seguridad informática no suponga un obstáculo a sus esfuerzos es igualmente importante.

Así que el objetivo de este informe es no es atemorizarle para que compre algo. La idea es que en cinco minutos usted conocerá más sobre los temas de seguridad a los que se enfrenta en una empresa pequeña y entenderá que hay que estar preparado para afrontarlos y de ese modo poder acelerar su crecimiento.

¿Qué puede conseguir?

Pero primero, ¿porqué debería molestarse en leer sobre seguridad informática? Hay una respuesta obvia: protección. Hay algunas cosas ahí fuera que pueden causar bloqueos del sistema, parones, pérdida de información y mucho más. Pero también existe otro beneficio para las pequeñas empresas: productividad. Las buenas prácticas informáticas que se detallan en este informe pueden ayudarle a recuperar el ancho de banda perdido, además de mantener la productividad de los empleados y el personal. No es sólo sobre cómo prevenir un “Armageddon”, es sobre cómo hacer que cada día de trabajo sea tan productivo como sea posible impidiendo que las amenazas externas que le hagan ir más lento. Usted paga mucho por su ancho de banda, ¿por qué no utilizarlo de la forma más efectiva posible?

Los 8 factores que debería saber (y qué suponen para su negocio)

1. Las empresas utilizan más aplicaciones basadas en Web que nunca

Hace algunos años, la mayoría de las aplicaciones corporativas estaban en tu ordenador o portátil, o en un servidor en tu oficina. Pero las empresas de software se dieron cuenta de las ventajas de poder acceder a esas aplicaciones vía Web, lo que quería decir que esas aplicaciones realizaban una pequeña parte del proceso en su ordenador mientras que la mayor parte del proceso se realizaba en un granja de servidores en algún lugar del mundo. Es la forma más barata de hacerlo. Es más flexible. Es más escalable. Y casi seguro que su negocio se aprovecha de las ventajas de alguna de estas aplicaciones basadas en Web ya sea para sus cuentas, su CRM o cualquier otra aplicación corporativa.

Pero el problema con las aplicaciones basadas en Web es que necesitan gran cantidad de código para que se ejecuten y no sólo en el servidor a través de la Web que también su ordenador. Y a mayor cantidad de código más impactos en la Web y mayor índice potencial de infección. Así que los empresarios deben ser conscientes de que el margen de exposición a riesgos, puede aumentar en caso de usar aplicaciones basadas en Web.

2. Los medios sociales pueden ser buenos y malos para su negocio

Los medios sociales es algo más que Facebook. Las redes sociales ayudan a que la gente sea productiva en su trabajo, ofreciéndoles respuestas a problemas, permitiéndoles comunicarse de forma rápida y sencilla, y encontrando la información que necesitan. Algunas de las empresas más eficientes y mejor gestionadas del mundo se aprovechan del uso de los medios sociales a través de la empresa.

Pero no todas las redes sociales están bien reguladas. Algunas son notorios criaderos de malware. De la misma forma que las aplicaciones basadas en Web representan una oportunidad de amenaza vía Web, el uso sin restricción de las aplicaciones sociales acarrea peligro. Se deben tomar precauciones para que los usuarios sólo puedan tener acceso a redes de confianza, que es algo que la mayoría de las soluciones firewall deberían realizar de forma automática.

3. En cuestión de segundos se pueden ahorrar horas

Ya que los medios sociales se han convertido en parte de la vida diaria del empleado, su utilización en el trabajo puede causar un descenso significativo de la productividad. Esto no es una amenaza Web directa pero sí una amenaza directa a la eficacia de su negocio. Algunas empresas prohíben la utilización de móviles para uso personal durante las horas de oficina mientras otras son más relajadas en ese aspecto. Lo mismo se podría aplicar al uso Web, particularmente para los medios sociales.

La misma funcionalidad que protege contra amenazas Web permite restringir el accesos a redes de medios sociales o a cualquier otro recurso online inapropiado. Es un proceso sencillo que puede aportar dividendos en términos de ahorro de tiempo. Puede que no le haga popular pero ¿al fin y al cabo quién paga las facturas?

4. Cualquier cosa es un ordenador

Otro desarrollo gradual que necesita saber es la proliferación de ordenadores, lo que quiere decir que ahora existen muchos más dispositivos que se pueden conectar a su red corporativa, pudiendo exponerla a posibles amenazas. Y con esto no sólo queremos decir que hay más ordenadores, servidores, Macs y portátiles. Muchos teléfonos son tan potentes como el ordenador que podría utilizar usted hace 10 años, y al incrementarse el uso de Web e email a través del móvil (tanto para negocio como para el tiempo de ocio), hay muchas mas oportunidades de ponerse en peligro.

A esta proliferación se añaden nuevos dispositivos como tablets, iPads, set-top boxes para televisión y dispositivos de almacenamiento de red. Todos ellos son ordenadores capaces de albergar código malicioso y su presencia significa que incluso una empresa pequeña tenga un complejo sistema de múltiples puntos de debilidad.

De nuevo, la idea no es sugerir que cada sistema está a punto de ser atacado por un virus o malware asesino. Pero todos necesitamos estar alerta y saber de dónde vienen las amenazas, cómo nos estamos exponiendo a ellas y cómo prevenir que entren en nuestros ordenadores.

5. El robo de información es un gran negocio

Hace veinte años, la mayoría de los virus se creaban por hackers quinceañeros en sus dormitorios llevados por la curiosidad y el aburrimiento. El problema de hoy en día es que la mayoría de ellos han crecido y tienen hipotecas que pagar, y el cibercrimen es una forma de pagar las facturas.

El crimen basado en Web en general y el robo de información en particular, es un gran negocio realizado por criminales altamente organizados. Y no discriminan sus objetivos, lo que quiere decir que cualquiera está en peligro no solamente las grandes empresas.

6. La compatibilidad importa

Algunas empresas se preocupan más de la seguridad informática que otras. Pero no servirá de nada si no es el propio dueño de la empresa el que se interese. Cada vez más proveedores, clientes, consejos de administración e incluso gobiernos se interesan en estrategias para la seguridad informática de las empresas con las que tratan. De hecho, muchas empresas se encuentran en una situación donde se requieren ciertos niveles de defensa para conseguir el nivel necesario de compatibilidad.

En algunos sectores como el legal, financiero y sanitario existe mayor preocupación en regulación y seguridad, mientras que los gobiernos locales suelen también insistir en cumplir con ciertos niveles de compatibilidad para proveedores.

Opere en estos sectores o no, cabe esperar que sus proveedores y clientes se tomarán mayor interés en la actitud que usted adopte hacia la seguridad. Ocuparse de una forma estructurada de la seguridad informática le etiquetará como una organización responsable y bien gestionada. También funciona hacia el otro lado: usted debe exigir la mejor práctica en seguridad informática por parte de sus proveedores porque cuanto más confíe en su red mayor será su defensa contra amenazas online en general.

7. El efecto exponencial

Se sabe muy bien cómo se desarrollan las amenazas. El problema no es sólo que los chicos malos cada vez son más sofisticados. Es que la forma de distribución ha cambiado completamente. Hace algún tiempo la única forma en la que el código malicioso podía abrirse paso hacia su ordenador era si usaba un programa infectado en un disco floppy. El riesgo era bajo.

Pero la reciente explosión de aplicaciones basadas en Web, incluyendo el email, la transferencia de ficheros y otras nuevas tecnologías basadas en Web, significan que hoy en día una única fuente puede transmitir de forma simultánea su malware a cientos de recipientes desconocidos.

8. Las empresas todavía no lo hacen bien

La conciencia de la necesidad de tener seguridad Web cada vez es más alta. De acuerdo con una encuesta realizada en Agosto de 2010 por CSI/FBI, el 98% de las empresas americanas tienen un producto firewall de alguna clase u otro diseñado para bloquear amenazas de Internet. Además el 97% de las empresas americanas tienen un software antivirus de ordenador de sobremesa cuyo objetivo es detener el malware que afecte a cada máquina. Sin embargo algo no funciona como debiera porque la misma encuesta predice que el 65% de esas empresas sufrirán una infección por virus en los próximos 12 meses.

El mensaje es claro. Sabemos lo que deberíamos estar haciendo. Sólo que no lo estamos haciendo bien del todo.

¿Qué puede hacer usted por su empresa?

Ya ha realizado la primera parte. Leyendo este informe esperamos que comprenda mejor los principales problemas a los que se enfrenta su pequeña empresa en lo que se refiere a seguridad informática.

El siguiente paso lógico sería buscar una solución que sea simple pero efectiva. No necesita gastar miles de euros comprando una solución compleja o contratando consultores para idear estrategias.

El dispositivo UTM de NETGEAR (Unified Threat Management) es simplemente un producto inteligente que puede ayudar a su empresa a mitigar todas esas amenazas online y mucho más.

Para saber más www.prosecure.netgear.com