NTRSecurity

Seguridad corporativa

Nuestra propuesta

LA INVERSIÓN EN SEGURIDAD ORIENTADA AL NEGOCIO ES RENTABLE

UN PRODUCTO ADAPTADO A SUS NECESIDADES…

Todas las empresas independientemente de su tamaño necesitan seguridad para su información, protegerla de forma adecuada es un reto que debe abordarse, estudiando la empresa su dimensión, organización y necesidades, no importa si tiene uno o mil trabajadores, cada empresa es diferente, habla diferente, se mueve de forma diferente, prioriza de forma diferente y sobretodo dispone de medios diferentes.

El adaptar la seguridad a las necesidades reales es una obligación para que funcione bien y la empresa se beneficie de ello.

SUS OBJETIVOS SON NUESTROS OBJETIVOS

Digámoslo claro; un trabajador roba la base de datos de clientes y se la vende a la competencia o establece el negocio por su cuenta ¿consecuencias?

Un administrativo revela el estado de cuentas y los problemas internos de la empresa y le llega a un banco que toma medidas inmediatas como cortar el crédito ¿consecuencias?

Un técnico difunde sin mala intención el estado de desarrollo de un proyecto de investigación y lo acaba conociendo la competencia ¿consecuencias?

Un trabajador acumula toda la información que puede sobre actuaciones administrativas, legales etc. para, llegado el momento, denunciar a la empresa ¿consecuencias?

La estimación del impacto de un incidente de seguridad es difícil de cuantificar con exactitud, pues tiene, como cualquier impacto, consecuencias directas e indirectas sobre áreas muy diversas. Se puede estimar el impacto sobre el beneficio, sobre la imagen, sobre las personas, sobre la pérdida de un determinado activo, etc. Lo que es seguro es que, independientemente de la magnitud (y no para todos será igual), al que va a afectar, al final, es al negocio en su globalidad.

LA INFORMÁTICA TAMBIÉN

Cuando hablamos de seguridad de la información, rápidamente nos viene a la mente la informática, los equipos, las redes… y, por analogía, los hackers, los virus, los troyanos, las averías… y también aquello que hemos hecho para solucionarlo; el firewall, el antivirus, las copias de seguridad… para acabar diciendo, erróneamente, "**ya estamos cubiertos**".

Claro que Seguridad de la Información es también seguridad informática y medidas tecnológicas, pero como hemos señalado, son muchas más cosas y básicamente la principal afecta a la organización.

"Cuando hablamos de seguridad, Las empresas demasiadas veces son víctimas de su inconsciencia y falta de organización."

Son muchos los negocios que constantemente tienen incidentes de seguridad fácilmente previsibles y lo que hacen una y otra vez es actuar en el momento en que se producen, poniendo, en el mejor de los casos, "parches" que poco o nada ayudan a que ese suceso no se repita en el futuro. Casi nunca valoran el coste de esos incidentes en el beneficio y en el futuro de la empresa, a no ser que las consecuencias sean brutales.

Para cualquier empresa es imprescindible dotarse de una organización de la seguridad que sea rentable, acorde con su dimensión y presupuesto, que cubra aquellas áreas más críticas y sus vulnerabilidades, así como las amenazas más frecuentes, las que, posiblemente, serán diferentes para cada empresa. El fin que se persigue es único; el de preservar el negocio, es decir, el beneficio.

En el momento que analizamos, aunque solo sea intuitivamente, las consecuencias de la inseguridad, vemos que son cuantificables; ya sea en base a la falta de organización interna que impide el crecimiento, en la afectación a la cifra de negocio, en pérdida de imagen, en cumplimiento normativo, legal etc. y también podemos deducir, aunque solo sea de forma intuitiva de nuevo, que si el coste de analizar y corregir la seguridad es X euros, va a ser asumible y rentable o no para nuestra empresa.

Por pocos números que hagamos, si el presupuesto de seguridad está bien hecho y adaptado a nuestras necesidades, nos vamos a dar cuenta que solo con las ventajas directas que vamos a obtener, el retorno de la inversión será inmediato, y estamos hablando de dinero.

Es cierto que poner el discurso de seguridad en términos de coste-beneficio es extraño, pero facilita la comunicación con la empresa y acerca la misión de la seguridad al tipo de decisiones que la dirección entiende, puesto que las toma cada día.

EL BENEFICIO FRENTE AL MIEDO

Es cierto que muchas empresas de seguridad utilizan la estrategia de asustar, mediante amenazas muchas de ellas legales, mostrando escenarios y consecuencias negativas y preocupantes que raramente acaban produciéndose.

No es menos cierto, tampoco, que es un camino equivocado y muy poco profesional, por el que muchos de sus clientes, asustados, han acabado gastando poco o mucho dinero, para tener una documentación en el cajón que apenas les sirve para nada y con la sensación, pasado un tiempo, que han sido estafados. Si esas consecuencias negativas y temibles están, por supuesto que deben quedar cubiertas, se produzcan o no, pero el trabajo de seguridad debe aportar valor en terminos de beneficio real respecto a la inversión realizada.

"El desafío es triple: la protección de la Información (estratégica, sensible o vital), la continuidad de la actividad, pase lo que pase y cubrir la responsabilidad de los directivos y empresarios"

Contacto:

e-mail info@ntrs.es Telf. 936110817
www.ntrs.es