Los crÃ-menes cibernÃ©ticos aumentan cuando la economÃ-a va en picada

March 3, 2009

IN THIS PRESS RELEASE

- Las pÃ³lizas tradicionales de cobertura para negocios pueden no incluir la protecciÃ³n adecuada para los riesgos de los crÃ-menes cibernÃ©ticos, dice el I.I.I.

SHARE THIS

- IN ENGLISH
- DOWNLOAD TO PDF

SPONSORED BY

Las pÃ³lizas tradicionales de cobertura para negocios pueden no incluir la protecciÃ³n adecuada para los riesgos de los crÃ-menes cibernÃ©ticos, dice el I.I.I.

INSURANCE INFORMATION INSTITUTE
Oficina de Prensa
New York: 212-346-5500; media@iii.org
Elianne Gonzalez, Florida: 954-389-9517 o 305-407-4305

NEW YORK, 3 de marzo de 2009 â€" La dÃ©bil economÃ-a ha disparado los problemas relacionados con el crimen tecnolÃ³gico o cibernÃ©tico, causando millones de dÃ³lares en pÃ©rdidas en todo tipo de negocios. El envÃ-o de correos electrÃ³nicos basura (*spamming*), la entrada no autorizada en las bases de datos de los negocios (*hacking*), el robo de las claves de acceso a lugares privados (*pinging*) y el acceso denegado de los usuarios a una pÃ¡gina Web especÃ-fica objeto de un ataque cibernÃ©tico, son solo algunos de los ejemplos de fraudes relacionados a los servicios cibernÃ©ticos que pueden paralizar un negocio. Basarse solo en los sistemas de seguridad y los seguros tradicionales para protegerse de estos riesgos no es suficiente, lo que hace obtener protecciÃ³n contra estos en la forma de un seguro contra ataques cibernÃ©ticos una necesidad crÃ-tica para cuidar de su negocio, segÃºn indica el *Insurance Information Institute* (I.I.I.).

â€œEl incremento del crimen cibernÃ©tico es enormeâ€•, dijo Loretta Worters, vicepresidente del I.I.I. â€œVan desde correos electrÃ³nicos que tratan de pescar informaciÃ³n privada del usuario (*phishing*) engaÃ±Ã¡ndoles para que usen pÃ¡ginas Web ficticias, hasta lo que se conoce como secuestro cibernÃ©tico, en el que los criminales se roban los nombres de usuarios y las claves para obtener acceso a cuentas en lÃ-nea, muchas veces destruyendo sistemas de redes (*network*) y sus bases de datos, o simplemente robando estas, lo que expone a los negocios a demandas de tercerosâ€•.

La industria de los seguros ha desarrollado un seguro para riesgos cibernÃ©ticos que ayuda a los negocios a hacerle frente a los riesgos de seguridad que tienen el potencial de desconectar o destruir la red, destruir la

data almacenada o causar otros daÃ±os que pueden afectar los negocios a travÃ©s del robo de la informaciÃ³n de sus clientes.

Ahora que el pÃºblico estÃ¡ cada vez mas preocupado e interesado en lo concerniente a mantener su informaciÃ³n lo mÃ¡s privada posible, los negocios pueden estar mas expuestos a demandas de los clientes en casos en los que la informaciÃ³n privada de estos se vea comprometida. El grave problema es que la mayorÃ-a de los negocios no estÃ¡n preparados o asegurados apropiadamente para estos riesgos.

SegÃºn una reciente encuesta producida por Ernst & Young en la que se entrevistaron 1,400 organizaciones, en el informe *2008 Global Information Security Survey*, sÃ³lo un 13% de los que respondieron tienen un seguro que cubra las pÃ©rdidas resultantes de un ataque cibernÃ©tico. Lo que es mÃ¡s, sÃ³lo un 20% de los que respondieron a la encuesta tienen una estrategia documentada para proveer de informaciÃ³n de seguridad, y menos de la mitad realizan alguna actividad directamente relacionada con la seguridad de la informaciÃ³n almacenada.

Las perdidas por ataques cibernÃ©ticos pueden ser bien cuantiosas y ademÃ¡s van en aumento. El informe llamado *Computer Crime and Security Survey* de 2007 del Computer Security Institute, indica que un 46% de las empresas han sufrido uno o mÃ¡s incidentes de seguridad en los previos 12 meses y el promedio de las pÃ©rdidas sufridas ha incrementado de $168 mil en el aÃ±o anterior, a $350,424.

â€œSin importar la lÃ-nea de negocios, virtualmente todas las empresas dependen en una u otra medida de los sistemas computarizados para funcionarâ€•, enfatizÃ³ Worters. â€œEs necesario que las empresas vean que el riesgo de sus sistemas de conexiones son diferentes de los riesgos fÃ-sicos tradicionales como serÃ-a un incendio. Si un criminal o un virus cibernÃ©tico logra desactivar sus sistemas computarizados o destruir sus equipos de computadoras, data o programas (*software*), la mayorÃ-a no tiene cobertura o si tienen, esta es muy limitada. Las aseguradoras han excluido estos riesgos de las pÃ³lizas comerciales estÃ¡ndares y son ofrecidas por separado. Ya sea que su empresa conduzca negocios usando Internet, archive datos de los clientes en sus servidores o simplemente use el correo electrÃ³nico, estÃ¡n expuestas a este riesgoâ€•.

Las coberturas de riesgos cibernÃ©ticos estÃ¡n disponibles en una pÃ³liza separada. Cada pÃ³liza esta diseÃ±ada segÃºn las necesidades de la compaÃ±Ã-a, incluyendo la tecnologÃ-a que se estÃ© usando y el nivel de riesgo al que estÃ© expuesta. Estas suelen incluir tanto cobertura para daÃ±os a la propiedad propia de la empresa asegurada como a la de terceras personas.

Tipos de cobertura disponibles

- **DaÃ±os o pÃ©rdida a archivos y data** (*loss/corruption of data*) â€“ Provee de cobertura por daÃ±os o la destrucciÃ³n causada a las bases de datos e informaciÃ³n valiosa, sean resultado del efecto de virus, cÃ³digos maliciosos o los programas conocidos como caballos de Troya (*Trojan horses*).
- **InterrupciÃ³n de negocios** (*business interruption*) â€“ Cubre la perdida de ingresos como resultado de un ataque a los servicios computarizados de la compaÃ±Ã-a que puedan limitar la habilidad de la empresa en conducir sus negocios, por ejemplo, el ataque que se conoce en inglÃ©s como â€œdenial-of-serviceâ€• que es un ataque a los sitios Web que imposibilita que los usuarios acceden el sitio y por tanto no pueden conducir transacciones. Esta cobertura tambiÃ©n incluye gastos extras, servicios de estudios forÃ©nsicos para determinar los daÃ±os e interrupciÃ³n de los servicios dependientes de estos sistemas.
- **Responsabilidad civil** (*liability*) â€“ Da protecciÃ³n a la empresa por costos de defensa, montos asignados en una sentencia de corte, gastos de juicios y en ocasiones demandas punitivas por daÃ±os causados por la compaÃ±Ã-a como resultado de una de estas situaciones: -Uso inapropiado de los datos privados debido al robo de la data (por ejemplo, tarjetas de crÃ©dito, informaciÃ³n financiera o mÃ©dica privada, etc.). -Re-transmision de virus de computadoras y de otras consecuencias resultado del uso de los sistemas computarizados de la empresa por los atacantes y que puedan causar daÃ±os a terceros. -Fallos de seguridad que previenen a terceros el uso de los sistemas de computarizados. -Servicios provistos por profesionales especializados en Internet. -Demandas alegando el uso no

autorizado de materiales con derechos de autor (*copyright/trademark infringement*), difamaciÃ³n o calumnias ya sea por el material usado en el sitio de la compaÃ±Ã-a, como por las contribuciones a Ã©ste de visitantes en boletines pÃºblicos (*bulletin boards*) y lugares de conversaciÃ³n en lÃ-nea (*chat rooms*). Este tambiÃ©n cubre responsabilidades asociadas con la publicaciÃ³n de promociones y propaganda digital (*banner ads*) de otros, en el sitio Web.

- **ExtorsiÃ³n cibernÃ©tica** (*cyber extortion*) â€“ Da cobertura para los pagos de rescate por extorsiÃ³n contra los sistemas computarizados de la compaÃ±Ã-a, asÃ- como los costos adicionales de contratar empresa o servicios privados especializados para encontrar y contrarrestar los efectos de los extorsionadores.
- **Manejo de emergencias** (*crisis management*) â€“ Provee de cobertura para contratar servicios de compaÃ±Ã-as especializadas en relaciones pÃºblicas o de publicidad que ayuden a reconstruir el buen nombre de la compaÃ±a despuÃ©s de un incidente. TambiÃ©n incluye reposiciÃ³n de los costos de notificar a los clientes sobre posibles efectos del uso no autorizado de sus datos personales, asÃ- como ofrecer servicios de monitoreo de crÃ©dito o cualquier otro mecanismo de mitigaciÃ³n de daÃ±os a aquellas personas afectadas por un evento cubierto en la pÃ³liza.
- **Pago de recompensas por captura de criminales** (*criminal rewards*) â€“ Da cobertura para ofrecer y pagar recompensas que conlleven a obtener informaciÃ³n pertinente a un crimen cibernÃ©tico y a la captura y convicciÃ³n de aquellos que hayan atacado a la empresa asegurada.
- **Cobertura de robo de identidad** (*identity theft*) â€“ Provee acceso a un centro especializado en robo de identidad para los clientes o empleados de la empresa que pudieran verse expuestos a este crimen a raÃ-z de un ataque a la empresa.

Â¿CuÃ¡nto cuesta el seguro para riesgos cibernÃ©ticos?

Dependiendo de la pÃ³liza, puede dar cobertura para ataques lanzados tanto desde afuera como dentro de la empresa, o por la implantaciÃ³n de un virus especÃ-ficamente dirigido contra la empresa o si Ã©ste virus es enviado masivamente por Internet. Las primas de este seguro pueden variar entre varios miles de dÃ³lares, basados en la facturaciÃ³n y considerÃ¡ndolos pequeÃ±os negocios (menos de $10 millones de ingresos anuales) hasta varios cientos de miles de dÃ³lares para corporaciones mayores que necesitan de una cobertura mÃ¡s extensiva.

Como parte del proceso de solicitud de la pÃ³liza, muchos proveedores de seguros ofrecen un anÃ¡lisis de los riesgos tanto en lÃ-nea como en las instalaciones fÃ-sicas de la empresa, generalmente sin costo para el asegurado ya sea que compren o no el seguro con esa empresa. Esto puede resultar sumamente Ãºtil no solo para el analista de riesgo de la aseguradora sino tambiÃ©n para el director de servicios tecnolÃ³gicos de la compaÃ±Ã-a, para los departamentos de riesgos y otros ejecutivos.

â€œAunque las compaÃ±Ã-as invierten millones de dÃ³lares anualmente en establecer barreras de protecciÃ³n (*firewalls*) y programas anti-virus, esto no es suficienteâ€•, indicÃ³ Worters. â€œAdquirir un seguro para los riesgos cibernÃ©ticos es otra capa mas de protecciÃ³n para cuidar de su negocioâ€•.

El I.I.I. es una organizaciÃ³n sin fines de lucro dedicada a la difusiÃ³n de informaciÃ³n y respaldada por la industria de seguros.

Back to top