La clave está en formular las preguntas correctas

Un análisis del riesgo cibernético en las pequeñas y medianas empresas

La digitalización de la economía y de la sociedad ofrece muchas ventajas. Vivimos en un mundo en el que casi todas las personas poseen un teléfono inteligente, compran productos por Internet y utilizan servicios de streaming. Bajo el lema de la "Industria 4.0", las empresas se están beneficiando con la aceleración y la eficiencia mejorada prometida por la digitalización de los procesos operativos. Por otro lado, los puestos de trabajo que funcionan con computadoras personales (PC) y conexiones a Internet veloces también se han vuelto fundamentales para las actividades comerciales de pequeñas y medianas empresas (PYMES). Sin embargo, la creciente digitalización e interconectividad también están generando un alto grado de dependencia en sistemas de TI funcionales y seguros, así como la necesidad de contar con empleados correctamente capacitados.

Durante varios años, las fallas de los sistemas y los ataques de hackers han dado origen a un número cada vez mayor de casos de interrupción en los negocios, con filtraciones de datos que resultaron costosos para empresas de todos los tamaños. En la publicación anual del "Barómetro de riesgos" de Allianz para 2018, la interrupción del negocio y los incidentes cibernéticos se describen como los dos riesgos principales para las empresas. En la mayoría de los países todavía no se ha establecido la obligación de reportar incidentes cibernéticos, por lo que solo podemos estimar las pérdidas anuales mundiales en alrededor de 400.000 millones de dólares.

Las Pymes son más conscientes de los riesgos cibernéticos y de su impacto negativo sobre las operaciones comerciales habituales. Esto fue impulsado en cierta medida por la introducción de normativas de protección de datos en muchos países, lo que a su vez ha conducido a las Pymes a interesarse más por analizar sus riesgos de TI, protegerse a sí mismas y trasladar una parte de sus riesgos cibernéticos a las aseguradoras.

Muchas aseguradoras de daños contra bienes patrimoniales y de responsabilidad civil han reconocido este riesgo y ofrecen seguros cibernéticos para proteger a las empresas de los elevados costos de los incidentes cibernéticos. Los elementos de cobertura más habituales para daños propios comprenden la interrupción del negocio, la recuperación de datos y la extorsión cibernética. Para daños ocasionados a terceros, existe una cobertura de responsabilidad civil hacia terceros en caso de pérdida de datos personales, sanciones contractuales de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y responsabilidad civil de redes/multimedia. También es importante el "componente de servicios" que ofrecen las aseguradoras, como los análisis de seguridad, las medidas preventivas, la capacitación y la mediación con expertos en casos de siniestros.

Para calcular las primas apropiadas para la cobertura cibernética, las aseguradoras deben procurar entender el riesgo cibernético de sus clientes. Los analistas de riesgos cibernéticos asisten a los suscriptores en el proceso de toma de decisiones al analizar la exposición al riesgo cibernético y la pertinencia de las medidas de protección. Para ello, necesitan obtener información exhaustiva de los posibles titulares de póliza a través de cuestionarios, documentación de respaldo y diálogos sobre riesgos. Es necesario aclarar el enfoque de gestión de riesgos informáticos del solicitante y comprender los sistemas complejos, las redes y la organización de

seguridad involucrados. Esta clase de análisis a menudo se asemeja a una auditoría de seguridad cibernética externa, que puede durar varios días o incluso semanas, por lo que solo puede utilizarse para determinar riesgos importantes.

En el caso de las Pymes, debido a los bajos montos de seguros y primas, las aseguradoras no pueden darse el lujo de llevar a cabo análisis de riesgos cibernéticos que requieran mucho tiempo y costos. Por lo tanto, la mayoría de las aseguradoras trabajan, actualmente, con cuestionarios de riesgo convencionales, que incluyen una parte todavía en papel, pero que podrán, con el tiempo, también completarse en línea. El modelo de cuestionario de la German Insurance Association, por ejemplo, consta en su versión básica de diez preguntas, además de otras que pueden añadirse según el potencial de riesgo. Así pues, las empresas con una facturación anual de entre 5 y 10 millones de EUR, que procesan datos confidenciales, deben responder 35 preguntas. En función de los montos del seguro y de los elementos de la cobertura considerados, algunas aseguradoras incluso reducen sus cuestionarios cibernéticos a menos de cinco preguntas y hacen referencia a requisitos de seguridad informática adicionales, establecidos en sus condiciones generales de seguro.

En general, los cuestionarios sobre riesgos cubren dos áreas diferentes: exposición al riesgo y calidad del riesgo. En el caso de la exposición al riesgo, es importante que las aseguradoras conozcan el tamaño y la facturación anual exactos de la empresa, así como el sector en el que operan. Otras preguntas fundamentales tienen que ver con la cantidad de datos personales almacenados y procesados por la empresa y su dependencia de los sistemas informáticos operativos.

Hay cinco criterios clave para entender lo bien que una empresa se protege a sí misma contra atacantes y el impacto de los incidentes de seguridad informática: la identificación de información y los recursos que deben protegerse, la adecuada protección de estos, el reconocimiento de ataques e incidentes, la respuesta correcta a estos y la recuperación ordenada de los sistemas informáticos, procesos y datos con posterioridad a un incidente.

Para las Pymes, las preguntas sobre las medidas de seguridad básicas esenciales son particularmente importantes:

- ¿Existe un sistema de gestión de accesos establecido, así como una capacitación periódica en seguridad informática para el personal?
- ¿El software se actualiza regularmente y existen sistemas antiguos en uso?
- ¿Las computadoras, computadoras portátiles y redes están adecuadamente protegidas y separadas entre sí?
- ¿Se llevan a cabo copias de seguridad de manera periódica?

Los cuestionarios sobre cibernética para Pymes son relativamente fáciles de implementar para las aseguradoras y, en general, no les toma a los titulares de pólizas demasiado tiempo para completarlos. Los cuestionarios en línea posibilitan evaluar las respuestas y emitir ofertas con rapidez. No obstante, los resultados de encuestas señalan que los cuestionarios sobre seguros son diligenciados por los mismos directores, lo cual supone un cierto peligro, pues ellos no siempre están correctamente familiarizados con este conjunto de problemáticas relativamente nuevas, sumamente complejas y que cambian rápidamente. Suelen subestimar la situación de amenaza de la propia compañía y sobrestimar su nivel de seguridad informática.

Otro enfoque posible para la evaluación de riesgos es el uso de análisis externos. Estos consisten en la evaluación externa del nivel de seguridad de una empresa, empleando datos y mediciones de acceso público, sin la participación activa de la empresa analizada. En este proceso, se recaban datos de los sistemas vulnerables y en peligro, las configuraciones no seguras y la filtración de datos de las empresas. Además de los factores tecnológicos, se tienen en cuenta los factores económicos y conductuales extraídos de múltiples fuentes para establecer un perfil de riesgo integral.

Estos análisis imitan el enfoque utilizado por los atacantes maliciosos, cuyo primer paso consiste en recabar información sobre las víctimas vulnerables. Sin embargo, a diferencia de los atacantes, los sistemas de la empresa solo se escanean sin acceder a los mismos. Algunos proveedores de estos servicios son BitSight, Cyence, Security Scorecard y diversas compañías de reciente creación. Este tipo de evaluación posee muchas ventajas: se realiza de manera automática en intervalos periódicos, lleva a cabo análisis objetivos y comparativos y puede rápidamente identificar nuevas fallas y fuentes de datos. No obstante, dado que estas tales mediciones no analizan el funcionamiento interno de una empresa, solo posibilitan una externa y, por lo tanto, limitada evaluación de las vulnerabilidades técnicas. En el caso de las Pymes, este enfoque puede ser acotado, debido a la tendencia de estas empresas a tener una menor presencia digital, según el sector.

En el futuro, la combinación de enfoques probablemente ofrecerá el mejor análisis posible de los riesgos cibernéticos de una Pyme. Un ejemplo podría ser un escaneo externo automatizado que se ejecute paralelamente a un cuestionario resuelto en línea, y que verifique las páginas web indicadas por la compañía. Ello permitiría un análisis directo de la información en la gestión de correcciones y de configuraciones seguras. Las amenazas cibernéticas están en constante evolución, por lo que una " toma instantánea" del riesgo de una compañía no resulta suficiente. Por el contrario, las aseguradoras y los titulares de pólizas deben medir y calcular la exposición informática de su cartera de manera permanente. Una alternativa para ello podría ser integrar los resultados de los análisis del software y el hardware, que se utilizan dentro de una red interna de una Pyme, para examinar los sistemas, las debilidades y configuraciones de seguridad.

El sector de seguros ha desarrollado métodos iniciales y procedimientos estructurados para el análisis de riesgos cibernéticos de las Pymes. La situación de las amenazas que cambian de forma constante, las nuevas experiencias en la tramitación de casos de siniestros cibernéticos y los avances tecnológicos tendrán un impacto en la evolución de los métodos de análisis de riesgos. Las aseguradoras de delitos cibernéticos deben determinar sus primas de seguros, en función de los resultados de los análisis de riesgos objetivos y de las medidas de protección empleadas por los titulares de pólizas. De esta manera, el sector de seguros podrá desempeñar un papel importante en impulsar la madurez cibernética de una economía en su conjunto y ayudar a mejorar la resiliencia cibernética de cada empresa.

Autor
Thomas Schnitzer – Senior Cyber Risk Analyst – Swiss Re

Swiss Reinsurance Company Ltd
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2121
Fax +41 43 285 2999
www.swissre.com

7/30/18