LLOYD'S

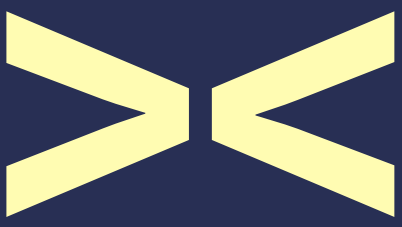
Cerrando la brecha

Asegurar su negocio frente a las cambiantes ciberamenazas

Junio de 2017

Resumen ejecutivo

En colaboración con
KPMG y DAC Beachcroft



KPMG

DAC beachcroft

Resumen ejecutivo

1.1 Visión general

Durante las últimas décadas, internet ha permitido que se produzca una extraordinaria innovación, creando nuevos modelos de negocio, dando lugar a compañías que cambiarán el mundo y generando millones de puestos de trabajo.

Pero este progreso tiene un precio. Dada su naturaleza, los sistemas digitales son susceptibles de sufrir ciberataques por parte de personas o grupos malintencionados con repercusiones cada vez más graves para las empresas de todo el mundo. La naturaleza de esta amenaza cambia a una velocidad tal que cada vez es más difícil que las empresas puedan contrarrestarla.

Sin embargo, pese a que la amenaza cada vez es más compleja, muchos líderes empresariales todavía no son conscientes de esta ciberamenaza. Una encuesta realizada recientemente por Lloyd's a más de 350 ejecutivos senior de empresas europeas reveló que, aunque el 92% de las empresas había sufrido alguna forma de ciberataque en los últimos cinco años, únicamente al 42% le preocupaba sufrir otro incidente en el futuro.

Este informe de Lloyd's, realizado en colaboración con KPMG en el Reino Unido, la firma legal internacional DAC Beachcroft y los aseguradores de Lloyd's, ayuda a las empresas a comprender mejor las ciberamenazas.

La primera parte del informe ofrece una evaluación única de las diversas ciberamenazas a las que se enfrentan las empresas hoy en día, desglosadas por sector (aquí se muestra un ejemplo para los servicios financieros), y busca formas de mitigarlas. Además, se detalla el impacto financiero total de las violaciones de datos y analiza algunos de los costes asociados con recientes y notorios ciberataques.

La segunda parte contempla cuatro motivos por los que las empresas deben aumentar sus esfuerzos a la hora de abordar el ciberriesgo y ofrece el punto de vista experto de los aseguradores de Lloyd's de ciberriesgos sobre algunas formas de llevarlo a cabo.

Riesgos del sector de servicios financieros

- Objetivo principal
- Objetivo frecuente
- Objetivo ocasional
- Objetivo inusual

(El orden de los círculos en la misma categoría no indica frecuencia relativa.)

Para consultar por completo el exclusivo análisis por sectores del informe sobre las ciberamenazas a las que se enfrentan las empresas en la actualidad, visite lloyds.com/cyberriskinsight.

Entre los sectores cubiertos se incluyen los siguientes:
- Educación
- Servicios financieros
- Sanidad
- Hostelería
- Tecnología de la información
- Industria
- Medios de comunicación y entretenimiento
- Petróleo y gas
- Servicios profesionales
- Sector público
- Venta al por menor
- Telecomunicaciones
- Transporte
- Servicios

Para más información sobre estas amenazas, lea el informe completo de Lloyd's «Cerrando la brecha» en lloyds.com/closingthegap

1.2 Conclusiones principales

Los tipos de ciberataques contra las empresas varían de sector en sector y están en constante evolución. Por ejemplo:

- Ha habido un gran crecimiento en los ataques a empresas mediante el fraude del CEO, que provoca importantes pérdidas económicas.
- El sector de servicios financieros se encuentra en primera línea en lo que respecta a ataques del cibercrimen organizado, pero la venta al por menor está siendo atacada cada vez con más frecuencia.
- Las empresas de servicios profesionales, como abogados o contables, sufren cada vez más ataques como vía de acceso a sus clientes, que a menudo son grandes empresas.
- El ransomware y los ataques de Denegación de Servicio Distribuido (DDoS) cada vez son más utilizados contra empresas, especialmente en el sector de la sanidad, medios de comunicación y entretenimiento.
- El sector público y el de las telecomunicaciones son muy susceptibles de sufrir ciberataques centrados en el espionaje.

Las empresas tienen que ser conscientes del coste total de un ciberataque, especialmente los costes a largo plazo (es decir, los costes asociados al impacto a largo plazo de un ciberataque, tales como la pérdida de ventaja competitiva y la pérdida de clientes). Cuando estos se suman a los costes inmediatos (como son los honorarios legales, los costes de investigación forense o el pago de extorsiones) los costes a largo plazo pueden aumentar la factura final drásticamente.

Existen cuatro factores que agravan el daño causado por los ciberataques, haciendo aún más importante que las empresas mitiguen sus ciberriesgos y mejoren su ciberseguridad:

- Multas cada vez más altas para las empresas que incumplen la normativa de ciberseguridad, tal y como se contempla en la futura legislación europea.
- Víctimas de ciberataques con una mayor disposición a demandar a las empresas que han perdido sus datos.
- Incremento de la responsabilidad por ciberseguridad en la cadena de suministro.
- Mayor vulnerabilidad debido a un mayor uso de dispositivos conectados (el Internet de las cosas).

1.3 Siguientes pasos

Lloyd's es el hogar de más de 70 aseguradores que ofrecen cobertura aseguradora frente al ciberriesgo. Basándose en los conocimientos especializados y únicos del mercado de Lloyd's, el informe destaca cuatro maneras fundamentales mediante las cuales las empresas pueden prepararse frente a una ciberamenaza y mitigarla:

1. Comprender las amenazas específicas para su empresa, incluidos los costes inmediatos y a largo plazo; todas, desde la reputación tal y como se perciba por los clientes y el valor de los datos guardados a las vulnerabilidades de la cadena de suministros y los perfiles de los líderes empresariales.

2. Evaluar tanto las amenazas actuales como las futuras: los suscriptores evaluarán ambas para poder ofrecerle la cobertura de seguro que mejor satisfaga sus necesidades.

3. Garantizar que los empleados, incluida la dirección, comprenden perfectamente las ciberamenazas a las que se enfrenta su empresa y promover una cultura de gestión del ciberriesgo.

4. Solicitar asesoramiento experto en lo que concierne a ciberseguros para garantizar que sus riesgos se cubren adecuadamente.

1.4 Conclusión

Las ciberamenazas evolucionan cada día, por lo que las empresas deben estar mejor preparadas para las consecuencias de un ciberataque. No solo es probable que los costes aumenten con la implantación de la nueva legislación europea, sino que el número de maneras en que las que las empresas pueden verse atacadas está aumentando.

A pesar de no ser posible estar seguro al 100% frente a un ciberataque, existen diversas medidas que las empresas pueden adoptar para reducir el riesgo de que ocurra y de garantizar que minimizan las consecuencias y se recuperan más rápido en el caso de que suceda.

El seguro es parte de esta solución. Cada día, los suscriptores de Lloyd's expertos en ciberriesgos trabajan con miles de compañías en todo el mundo, desde multinacionales a PYMES, para comprender mejor sus riesgos y ofrecerles el asesoramiento experto y la cobertura aseguradora que necesitan.

Si desea leer el informe completo de Lloyd's «Cerrando la brecha», visite **lloyds.com/closingthegap**

Si desea saber cómo los aseguradores de Lloyd's pueden ayudarle, visite **lloyds.com/cybercover**