Ciberseguridad en el sector Seguros,

¿cuáles son los retos?

Los últimos ciberataques sufridos en importantes compañías del sector asegurador han puesto de manifiesto la debilidad de sus sistemas de protección digital. Estos ataques, cada vez más sofisticados y diseñados con un objetivo específico, provocan en las aseguradoras importantes **pérdidas económicas, reputacionales o de información confidencial.**

De acuerdo con diferentes estudios, el riesgo de ciberseguridad ha ido creciendo en los últimos años colocándose en el

TOP 10 de riesgos de las entidades aseguradoras, incluso por encima de riesgos tan delicados como el riesgo operacional o riesgo de crédito.

Dada la naturaleza de este sector, los retos que se plantean son muy variados, ya que suelen convivir negocio **B2C y B2B,** multiproducto y multisector, con el añadido del carácter distribuido de las oficinas, bien sean de gestión, de atención directa al cliente o mediante agentes especializados.

Frente al desafío del teletrabajo.

La puesta en marcha del teletrabajo como operativa de larga duración supone hacer frente a todas las amenazas que derivan de esta modalidad de trabajo no presencial. Además de tener que contar con las herramientas suficientes sin que ello repercuta de manera negativa en el trabajo, como puede ser una caída de las telecomunicaciones, las compañías deben estar preparadas las posibles amenazas que hay en el mercado.

Trabajar desde el domicilio particular significa que el empleado pueda hacer uso de su equipo personal en vez de del equipo corporativo, además de conectarse a la red doméstica. Este hecho puede suponer un riesgo, ya que puede contar con versiones desactualizadas de parches de Windows o de antivirus, y de los sistemas operativos que en ciertos casos han dejado de recibir soporte en enero de 2020, lo que agrava aún más la amenaza.

Impacto en cliente y usuario.

Desde el sector seguros existe una gran preocupación sobre estas amenazas. De hecho, algunas compañías ya han sido ampliamente alcanzadas por los ataques, mientras que muchas de ellas ya han ido invirtiendo en diferentes recursos para evitar este tipo de situaciones.

Son de especial riesgo aquellas que ofrecen servicios sanitarios directos a clientes, por el impacto general de los datos de salud y el impacto especifico derivado de la situación de pandemia. En este caso, no sólo estaríamos hablando de una perdida de datos, sino también de un retraso en realizar pruebas médicas que pudieran ser de alta importancia.

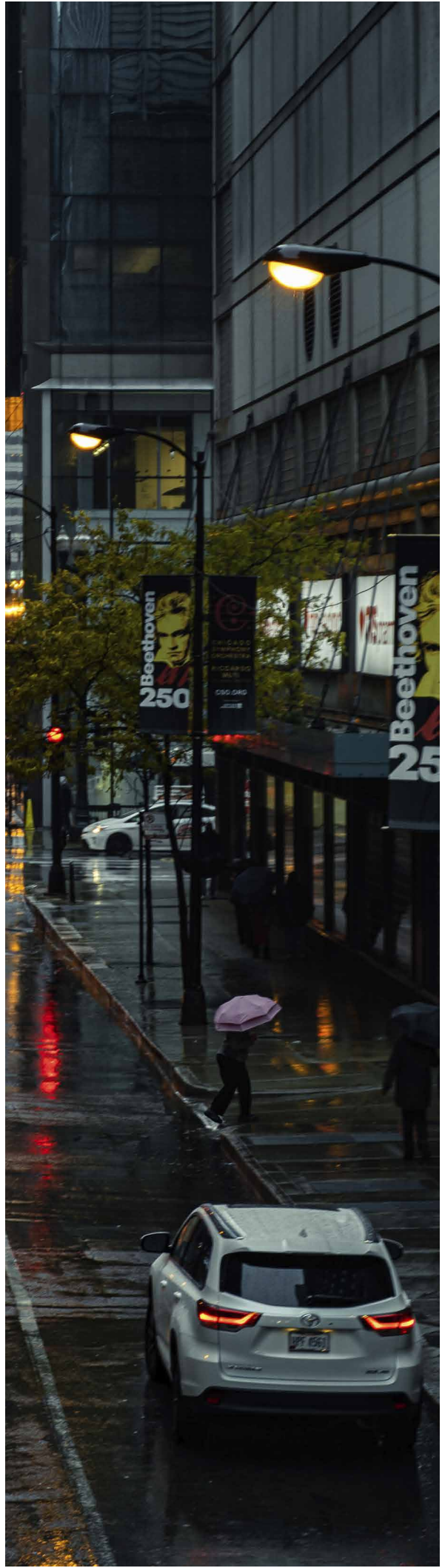
Por último, es importante reseñar que un ciberataque de alto impacto, aunque sea contra una aseguradora en concreto, pone en tela de juicio la confianza digital del ciudadano con respecto a todas en conjunto a la hora de consumir servicios de este sector.

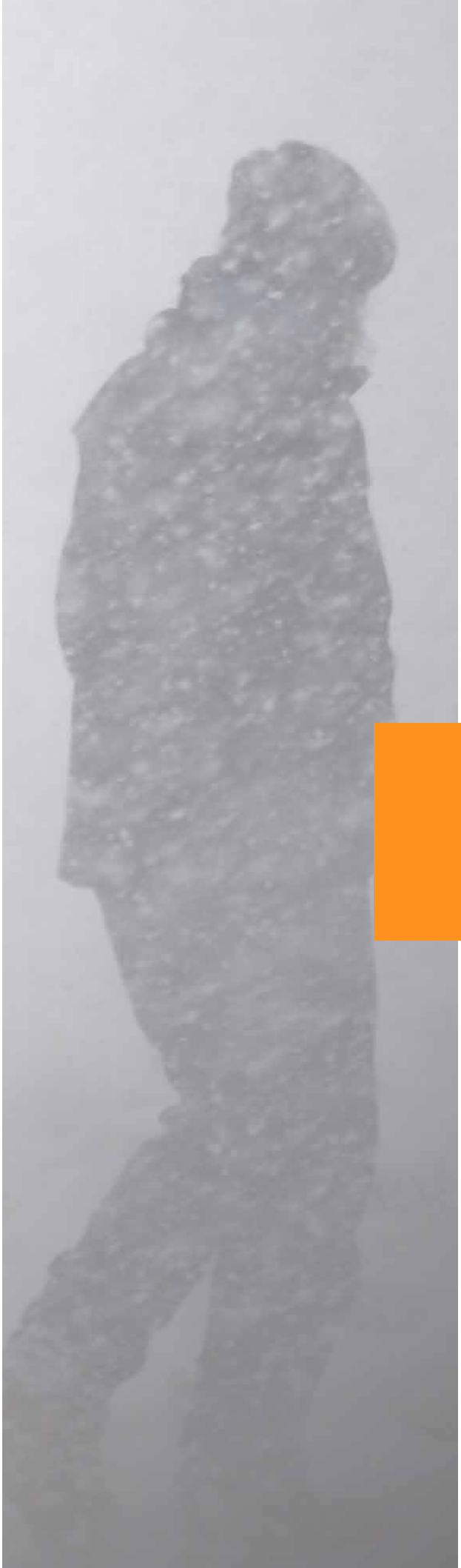
Una buena defensa es el mejor ataque.

Recomendamos una serie de acciones imprescindibles para minimizar estos riesgos:

• Es fundamental disponer de un programa de concienciación en seguridad para todos los empleados, ya que los ataques que se producen van dirigidos a cualquier usuario de cualquier área o departamento. Fortalecer este componente es muy necesario para hacer frente a este tipo de amenazas.

• Entender el perímetro de seguridad en sentido amplio, de manera que se abarque a proveedores, agentes externos, oficinas de atención al cliente, etc con medidas de protección adecuadas a los riesgos específicos de cada uno de estos. Merece especial atención lo referente a productos sanitarios **B2C,** que se suelen entregar de manera presencial en oficinas de atención directa y que implica tener en cuenta una infraestructura de seguridad mínima, backups locales, formación específica, entre otras acciones.





• Disponer de las últimas actualizaciones de antivirus, firewalls, sistemas operativos y disponer de las herramientas para poder interceptar un posible ataque es crucial para poder mantener la supervivencia de una compañía.
• Contar con herramientas de monitorización, recuperación y respuesta ante incidentes, así como un plan de continuidad del negocio testeado y efectivo, de cara a poder actuar ante situaciones de crisis. Los ataques son cada vez más devastadores, por lo que lograr un alto grado de resiliencia en materia de infraestructura IT es una de las claves para sobrevivir con éxito a cualquier incidente de estas características.

Como conclusión, podemos afirmar que el riesgo cero en ciberseguridad no existe, aunque si se toman medidas y acciones a tiempo, la probabilidad de que un ataque tenga éxito se puede reducir en consideración.

Fuente de información:
cio.com