Ciber

Algunas respuesta a preguntas sobre la protección frente a los ciberataques

1. El mundo digitalizado.

Todo el mundo habla de “ciber-riesgo”, pero ¿qué significa?

Ciber es un prefijo utilizado para relacionar todo lo que tenga que ver con Internet, ciberespacio, mundo digital y ordenadores en general. El ciber-riesgo es la posibilidad de sufrir un ataque informático que cause daños y problemas

¿Cuáles son las actuales tendencias y evoluciones en el mundo digitalizado?

La revolución digital ya está aquí – el progreso tecnológico es cada vez más rápido.

Todas las personas, empresas e instituciones usan internet, ordenadores, máquinas y herramientas conectadas con el mundo digital.

En el último año los ciberataques han aumentado un 59%.

Estudios internacionales (Múnich RE) consideran que el ciberataque es una de las 5 principales amenazas tenidas en cuenta por los Gerentes de Riesgo de las empresas.

En los últimos años, ha crecido un 50% el número de empresas y sociedades que disponen de este seguro.

¿Qué significa ‘Seguro de Ciber Riesgo’?

Es un seguro específicamente diseñado para cubrir las pérdidas ocasionadas por incidentes que afecten a los sistemas informáticos del asegurado (ordenadores, móviles, portátiles, servidores,...).

Normalmente se cubren las pérdidas del asegurado y los daños a terceros., incluyendo gastos de defensa y judiciales. También se incluyen garantías que ayudan a minimizar las consecuencias de los ciberataques.

¿Qué impacto tiene la nueva GDPR en el ciber riesgo para la compañía?

Existe un gran impacto en todas las compañías y organizaciones que almacenan y trabajan con datos personales. Nos enfrentamos a una rigurosa exigencia legal para procesar dichos datos (ya no existe consentimiento implícito).

Las compañías pueden enfrentarse a grandes costes y obligaciones (responsabilidad de notificación en las primeras 72h, multas de 20M€ o 4% de la facturación global).

El ámbito global de aplicabilidad es muy amplio (ciudadanos de la UE).

Además, existen Derechos de reclamación por daño inmaterial.

Datos de interés:

Los ciberataques para secuestrar datos se han multiplicado por dos en 2022

Contacta con un experto:
91 266 70 52 - Colegios@aon.es

2. “La duda no es si voy a ser ciberatacado, sino cuándo”

Todas las empresas y sociedades, aunque no manejen datos ‘interesantes’ pueden ser objetivo de hackers y ciber ataques ya que la mayoría de las actividades dependen de la existencia de sistemas informáticos conectados.

La Ciber Extorsión está enfocada sobre todo en compañías y organizaciones pequeñas. Al tener sistemas informáticos menos sofisticados sufren daños más severos y son más fáciles de hackear.

¿Cuál es el tamaño medio de las compañías que contratan Seguro de Ciber Riesgo’?

¡Todas las empresas demandan este seguro! Cualquier entidad, tenga el tamaño que tenga, cuenta con operaciones que dependen de sistemas informáticos y manejan datos personales sensibles.

Nuestro departamento de IT tiene protecciones suficientes. ¿No deberíamos incrementar la inversión en este punto antes que contratar un seguro?

La prevención es importante. Las organizaciones invierten en extintores, rociadores y sistemas de detección de incendios, pero también se contrata la cobertura de Daños Materiales correspondiente. En ciber la situación es similar. Es importante prevenir pero también aminorar las consecuencias de los siniestros. Cualquier organización puede sufrir un ciberataque.

¿Cuál podría ser un ejemplo de siniestro?

A. Publicación no autorizada de datos personales.

Una newsletter es enviada a todos los colegiados o clientes.

Un empleado olvida ocultar las direcciones de email, por lo que nombre y apellidos son visibles para todo el mundo (publicación no autorizada de datos personales).

Consecuencias:

- Todos los colegiados/clientes deben ser notificados de que sus datos han sido publicados.
- Colegiados y clientes pueden reclamar compensaciones debido a una infracción de la GDPR.
- Se causa un daño reputacional a la propia compañía / institución debido a que colegiados y clientes han hecho público el incidente en las RRSS.

B. Fuga de datos confidenciales

Un empleado deja la oficina sin apagar el ordenador con más de 1.000 datos de clientes.

Un empleado de la limpieza roba el ordenador y vende los datos en internet.

Consecuencias:

- Colegiados y clientes reclaman compensaciones contra el asegurado.
- Costes de notificación a colegiados y clientes de la fuga de datos.
- Daños reputacionales del asegurado.
- Reclamación de terceros por violación de secretos profesionales / industriales.

Datos de interés:

El 47% de los ciberataques a empresas comienzan por una vulnerabilidad de software

Contacta con un experto:
91 266 70 52 - Colegios@aon.es

C. Intrusión maliciosa en los sistemas informáticos con la consecuente destrucción de datos, violación de copyright y extorsión.

A pesar de todas las prevenciones de seguridad del departamento de IT un hacker consigue introducirse en el servidor de la compañía.

El hacker destruye datos sensibles de un colegiado /cliente, manipula su sitio web e infringe derechos de copyright de terceros.

Datos sensibles son encriptados y se pide un rescate de 10.000€.

Consecuencias:

- Reclamación de terceros por violación de derechos de copyright.
- Coste de contratación de expertos en gestión de crisis para negociar el secuestro de datos.
- El pago del rescate de los datos encriptados.

3. Necesitamos un seguro de ciber riesgos

¿Las amenazas son solo externas o también internas?

Los empleados pueden, intencionadamente o no, perjudicar a la compañía (Venta de secretos, manipulación del sitio web, etc.) pueden producir daños reputacionales difícilmente recuperables.

Los ataques internos son potencialmente más peligrosos que los externos.

Algunos sistemas de prevención:

- Tener control de acceso de los empleados y cambiar contraseñas frecuentemente.
- Cambiar contraseñas de manera inmediata una vez el empleado abandona la compañía.

¿Por qué no estamos cubiertos por nuestro seguro de Daños y RC?

La póliza de Ciber es específica para incidentes de Ciber Seguridad.

Las pólizas de Daños y RC no están diseñadas para proporcionar una cobertura adecuada a este tipo de pérdidas. Existen ciertas exclusiones relativas a este tipo de daños, tales como Daños Inmateriales, Perjuicios Patrimoniales Puros, etc.

Las pólizas de Ciber cubren ambas situaciones; Daños Propios y Daños a Terceros (todo en una sola póliza).

Hay coberturas especiales que se encuentran únicamente en las pólizas de Ciber: Daño Reputacional, Responsabilidad derivada de Seguridad y Privacidad, Servicios de respuesta por incidencias, Responsabilidad civil derivada de contenido de páginas web, Extorsión, etc.

Las pólizas de Ciber proporcionan atención de emergencia 24/7 en caso de incidentes de ciber seguridad.

Estos seguros evitan la implicación de varios aseguradores diferentes al tener Daños Materiales y RC contemplados en la póliza.

¿Cuáles son los requisitos mínimos de seguridad requeridos para una póliza de ciber?

- Firewall
- Protección anti-malware
- Backups regulares.
- Gestión de contraseñas.
- Gestión de soluciones iniciales.

Contacta con un experto:
91 266 70 52 - Colegios@aon.es

¿Cuáles son las coberturas más comunes en una póliza de Ciber?

- RC derivada de seguridad y privacidad.
- Servicios de respuesta por incidencias en seguridad y privacidad.
- Defensa y sanciones en procedimientos sancionadores.
- Fianzas
- Incumplimiento de estándares de seguridad PCI.
- Pérdida de Beneficios por interrupción de sistema informático.
- Amenazas de extorsión.
- Gastos de reconstrucción.
- Gastos de gestión de crisis y gastos de relaciones públicas..

Datos de interés:

La pérdida media por ciberataques en negocios profesionales es de 65.000€.

4. Mucho más que un seguro

Hemos contratado un almacenaje de datos y procesador externo. ¿Pueden terceros proveedores ser incluidos en una póliza de ciber?

Actualmente la mayoría de las compañías externalizan los servicios de IT, por lo que terceros pueden ser incluidos en la póliza.

Almacenamos todo en la nube y tenemos externalizado el servicio de IT. Si hay una brecha en la seguridad, es problema del proveedor.

Con la GDPR el asegurado es responsable de los datos perdidos y de la brecha sucedida ya que es el asegurado quien debe asegurarse de que el proveedor de servicios de IT cumpla con los requerimientos del GDPR.

¿Qué hacer en caso de un incidente? ¿Existe servicio de atención 24h? ¿Qué servicios se ofrecen?

- Asistencia técnica (incluyendo investigaciones forenses).
- Asistencia legal.
- Gestión de crisis.
- Negociación de extorsiones.
- Servicio de relaciones públicas.

¿Cómo es de importante formar a los empleados?

Que los empleados sean conscientes del riesgo de un ciber ataque es prácticamente la medida más importante que una compañía puede tomar para salvaguardar su negocio.

5. ¿Tenemos respuesta a todas estas preguntas?

- ¿Cuántos días de interrupción de la actividad puedo asumir?
- ¿Mi sistema informático es 100% seguro?
- ¿Tengo la seguridad de que ningún hacker o virus puede afectar a mis sistemas?
- ¿Qué haría en caso de que secuestren mis datos y necesite asistencia rápida y especializada?
- En caso de un ciber ataque, ¿seré capaz de asumir los costes de una asistencia legal, gestión de crisis y defensa reputacional especializada?
- ¿Podré asumir los costes de notificación en caso de que haya una fuga de datos?
- ¿Cómo puedo prevenir que un empleado no pierda un ordenador con información confidencial de clientes?
- ¿Podré asumir los costes que suponen que un empleado dañe gravemente los sistemas de IT?