La importancia de la ciberseguridad en el sector farmacéutico

Los grandes avances tecnológicos acarrean grandes riesgos en materia de seguridad de la información. Estos deben ser gestionados adecuadamente con el fin de mantener la confidencialidad, integridad, disponibilidad y resiliencia de información. La ciberseguridad es la práctica mediante la cual defendemos los dispositivos electrónicos de almacenamiento de información a fin de salvaguradarla de ataques maliciosos o accesos no autorizados.

LILLIAM VALENZUELA
SOCIA EN UMBRA ABOGADOS, DELEGADA DE PROTECCIÓN DE DATOS CERTIFICADA

Aquellos sectores que traten información sensible o que posea un gran valor en el mercado como parte de su actividad, estarán siempre el punto de mira de los ciberatacantes. La sofisticación que ha alcanzado en los últimos años el cibercrimen complica las laborares de prevención, detección y respuesta de las compañías para hacer frente a estas grandes amenazas.

La información que maneja el sector farmacéutico es altamente sensible y muy apetecible para el mercado negro de la ciberdelincuencia, ya que es de las más valiosas y mejor pagadas. El espionaje industrial y la piratería informática han alcanzado cifras alarmantes, lo que resulta trascendental en este sector, donde la investigación, desarrollo e inversión financiera son claves para su posicionamiento en el mercado. Algunas estadísticas de seguridad informática indican que el coste de un ciberataque exitoso es de más de 5 millones de dólares (1). Asimismo, otras fuentes estiman que el daño relacionado con ciberataques llegará a los 6 trillones de dólares anuales para 2021. A inicios del año 2019 se estimaba que habría un ataque de ransomware cada 14 segundos para los últimos meses del año (2). A pesar de estos datos, no existe suficiente concienciación en el sector farmacéutico sobre el alto riesgo al que se exponen estas compañías, lo que a menudo deriva en una deficiente inversión en cuanto a recursos y tiempo para la prevención de incidentes de seguridad.

¿Están las compañías farmacéuticas legalmente obligadas a invertir en ciberseguridad?

Los ataques informáticos pueden estar dirigidos al robo de datos personales o de secretos empresariales.

En lo que se refiere a los datos que puedan identificar a personas físicas, resulta de aplicación el Reglamento General de Protección de Datos (RGPD) y la Ley 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPGDD). La primera norma se aplica a nivel europeo, mientras que la segunda tiene un alcance estrictamente nacional. Estas normas imponen una serie de obligaciones a las empresas que deben ser implantadas con el fin de preservar la seguridad de la información relativa a las personas físicas. Las compañías farmacéuticas generalmente tratan datos de empleados, de clientes, de proveedores, de candidatos a procesos de selección e, incluso, tratan datos de salud relacionados con estudios de investigación, fases de prueba de medicamentos, control de los efectos adversos reportados y datos de pacientes.

La información que maneja el sector farmacéutico es altamente sensible y muy apetecible para el mercado negro de la ciberdelincuencia, ya que es de las más valiosas y mejor pagadas

Las medidas que deben ser implantadas de acuerdo con la normativa de Protección de Datos abarcan tanto el ámbito legal y organizativo como el tecnológico. Ni el RGPD ni la LOPGDD ofrecen al sujeto obligado un catálogo detallado de medidas tecnológicas, sino que dejan el balón en manos de las compañías cuando refieren que estas deberán ser aplicadas con enfoque de riesgo. Ello supone la necesaria realización de un análisis de riesgos para determinar cuáles son las medidas técnicas que resultan adecuadas al riesgo identificado.

El RGPD establece sanciones de hasta 20 millones de euros o del 4% de la facturación anual del ejercicio anterior por el incumplimiento de las obligaciones mencionadas.

Los secretos empresariales, por su parte, se refieren a aquella información que no sea generalmente conocida por las personas pertenecientes a los círculos en que se utilice, ni fácilmente accesible para ellas. Además, se considerará secreto cuando tenga un valor empresarial, ya sea real o potencial, y haya sido objeto de medidas razonables por parte de su titular para mantenerlo en secreto.

A diferencia de lo que sucede con los datos personales, no existe una obligación legal de la compañía relativa a la protección de sus secretos empresariales, sino que será la propia naturaleza del negocio la que exija un determinado nivel de salvaguarda. Habitualmente son considerados, y en consecuencia protegidos como secretos empresariales, los datos relativos a cualquier información o conocimiento, incluido el tecnológico, científico, industrial, comercial, organizativo o financiero, los planes comerciales, informes de farmacovigilancia,

investigaciones y fases de prueba de nuevos fármacos, patentes y know how. La Ley 1/2019 de Secretos Empresariales dispensa al titular del secreto una protección legal frente a cualquier modalidad ilícita de obtención, utilización o revelación de la información. Esta norma no establece una obligación de protección, así como tampoco establece sanciones para el titular del secreto por ausencia de medidas, sino que ofrece respaldo legal a posteriori a modo de respuesta, castigo e indemnización frente a los actos ilícitos que atentan contra el secreto el secreto. Es importante señalar que solo será posible emprender acciones legales con base a la mencionada ley si previamente esta información ha sido objeto de medidas para mantener su condición de secreto por parte de la empresa.

¿Qué consecuencias puede acarrear la escasa o nula protección de la información?

Los daños derivados de la ausencia de medidas de seguridad pueden clasificarse en daños económicos y reputacionales.

- Daños económicos: Como se ha mencionado, el RGPD establece sanciones millonarias por infracciones de protección de datos, cuyo impacto económico puede afectar gravemente a la organización. Téngase en cuenta que el mero hecho de no implantar las medidas de seguridad organizativas y técnicas adecuadas al riesgo ya supone una infracción grave.

  El robo, secuestro o pérdida de información clasificada como secreto empresarial podría paralizar el negocio, devaluar la información, mermar el propio valor de la compañía o incluso provocar el cierre definitivo de la empresa.

  Cuando un ciberdelincuente aprovecha una vulnerabilidad en los sistemas de una compañía y logra sustraer datos, sabe que la competencia pagará a precio de oro la oportunidad de arrebatarle una patente millonaria a sus rivales. Es posible que el competidor no utilice la información adquirida ilícitamente tal cual está diseñada, pero podrá marcar una hoja de ruta para hacer desarrollos o invenciones similares, con lo que la empresa afectada, tras años de inversión en su investigación, verá cómo su competencia crece de manera inmediata.

Si bien la mayoría de los riesgos tecnológicos no pueden ser eliminados, debe trabajarse en su reducción hasta un nivel aceptable para el negocio

  El ciberdelincuente también sabe que puede optar por el secuestro de información y solicitar un rescate pactando un precio descomunal, ya que la compañía afectada podría llegar a pagar elevadas sumas de dinero por la devolución de la información sustraída si esta resulta ser crítica para el negocio. Es necesario apuntar que el pago de los rescates en ningún caso garantiza la recuperación de la información.

  Por último, si en el mejor de los casos la información puede ser recuperada, la mera paralización temporal de la actividad puede suponer daños económicos de elevadas cuantías.

- Daños reputacionales: Las sanciones de protección de datos no solo suponen un daño económico sino que además, al ser públicas, pueden acarrear daños reputaciones, pérdida de confianza de clientes y de posición en el mercado. Los daños reputacionales podrían ser irreversibles o requerir de una importante inversión en comunicación para recuperación de la imagen corporativa y reputación.

Recomendaciones en materia de ciberseguridad

Si bien la mayoría de los riesgos tecnológicos no pueden ser eliminados, debe trabajarse en su reducción hasta un nivel aceptable para el negocio. Para ello se recomienda, en primer lugar, realizar un análisis de los riesgos existentes con el fin de diseñar las medidas técnicas adecuadas que busquen reducir la probabilidad de que las amenazas identificadas se materialicen, así como reducir el impacto de los posibles incidentes de seguridad.

Desarrollar un Plan Director de Seguridad puede ser una herramienta idónea para los reducir riesgos mediante un profundo y detallado estudio de la empresa, principalmente de sus fortalezas y vulnerabilidades. El Plan Director tendrá que estar alineado con los intereses estratégicos de la entidad e incluir las obligaciones y buenas prácticas que deberán cumplir todos los empleados.

Es imposible garantizar la seguridad total por lo que las compañías deben estar preparadas para recuperarse ante posibles desastres tecnológicos. Por ello, es conveniente también confeccionar un Plan de Continuidad de Negocio que contenga las pautas de actuación en caso de que haya un fallo que comprometa la continuidad de la actividad empresarial. Estos planes son fundamentales para poder recuperar, en un plazo razonable, la operativa habitual de las empresas.

Se recomienda, además, contar con un Plan de Protección de Datos efectivo que documente todos los procedimientos implementados puesto que, en caso de denuncia ante la Agencia Española de Protección de Datos, será preciso acreditar el nivel de cumplimiento previo al incidente como base para una buena defensa legal.

Deberá prestarse especial atención a la formación de los empleados, ya que una gran parte de los incidentes de seguridad se producen por fallos humanos como resultado de su falta de concienciación y escasa formación. El entrenamiento constante de la plantilla y el desarrollo de planes de formación permitirá mantener un nivel de alerta para aquellas cuestiones que no pueden ser resueltas técnicamente, en especial cuando los ciberdelincuentes acuden a la ingeniería social para entrar en los sistemas, engañando o manipulando a los empleados para lograr sus objetivos.

Las compañías farmacéuticas deberán, en definitiva, desarrollar proyectos a nivel técnico que garanticen la seguridad, porque es un sector donde la información es un activo clave para la continuidad y, precisamente por esto, son el blanco perfecto del cibercrimen y el espionaje industrial. No debe olvidarse que solo existen dos tipos de empresas: las que han sido atacadas y las que no saben que han sido atacadas ◂◂

Referencias

- Ponemon Institut: https://www.ponemon.org/blog/the-2017-state-of-endpoint-security-risk-report
- CyberSecurity Ventures: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/