NOTA DE PRENSA
14 / 12 / 2020

Cómo evitar el hackeo a documentación confidencial sobre la vacuna contra el Covid-19

> ¿Qué pueden hacer las farmacéuticas para evitar los ciberataques a la información más preciada en estos momentos?

La industria farmacéutica, así como los organismos oficiales de Sanidad, tienen estos días que enfrentarse no sólo a una batalla contrarreloj para tener lista la vacuna contra el Covid-19 lo antes posible, sino también para impedir el hackeo de documentos confidenciales sobre la preciada vacuna.

Poco después de darse a conocer que Pfizer ya dispone de una vacuna para hacer frente al coronavirus aprobada por el Reino Unido, y tras haber comenzado los trámites para su aprobación por parte de la Agencia Europea del Medicamento, han saltado las alarmas por el hackeo a documentos confidenciales sobre la vacuna sufrido por la citada Agencia. De momento, se ha dado a conocer que el pasado miércoles, la European Medicines Agency confirmaba en su página web haber sido objeto de un ciberataque y anunciaba la apertura de una investigación para aclarar lo sucedido.

¿Qué pueden hacer las farmacéuticas para evitar los ciberataques a la información más preciada en estos momentos? Inicialmente, aplicar un modelo de seguridad centrado en los datos, teniendo en cuenta que el objetivo último de las organizaciones no es proteger la red, ni los sistemas o los dispositivos, sino proteger su bien más valioso, es decir, los datos sensibles, y además hacerlo tanto dentro como fuera de la entidad y estando la información tanto en reposo, como en tránsito o en uso.

El primer paso a dar es que las organizaciones cifren los datos con tecnología IRM (Information Rights Management) para determinar en todo momento quién accede a la información, a qué datos, con qué permisos y desde dónde, es decir, tanto dentro como fuera de la compañía.

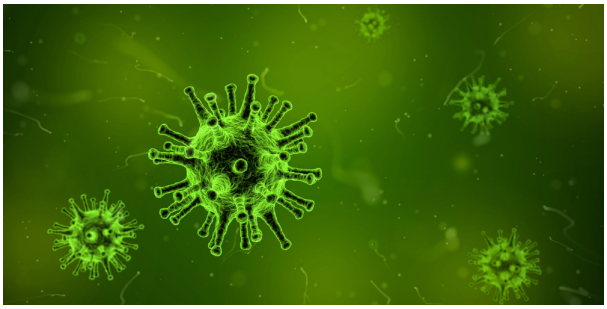
Adicionalmente, hay que evitar la fuga de información accidental o por exfiltración con una solución de DLP (Data Loss Prevention) que prevenga la pérdida de datos detectando potenciales brechas de

datos o transmisión de los mismos mediante el monitoreo (dando visibilidad del dato en toda la red), detección y bloqueo de información sensible mientras está en uso, en movimiento y en reposo.

Finalmente, para garantizar la seguridad de la información, necesitamos también implementar una solución de seguridad XDR (NDR + EDR), que evite y de respuesta a los incidentes de seguridad maliciosos que quieren robar la información, tipo ransomware o ataques dirigidos.

Javier Modúbar, CEO de Ingecom, advierte que: “En los últimos ransomwares, se ha visto que los atacantes realizan un doble chantaje que ocasiona un daño reputacional y un daño económico. Extraen los datos de las organizaciones y si éstas se niegan a pagar, les amenazan con publicar en Internet su información crítica”.

Ingecom, como Value Added Distributor (VAD) especializado en soluciones de ciberseguridad y ciberinteligencia, cuenta con este tipo de soluciones de fabricantes como SealPath, Forcepoint y Bitdefender, entre otros, para prevenir que la información sensible de las vacunas sea hackeada.



Contacto de prensa:

JAVIER MODUBAR ALVAREZ
info@ingecom.net
944395678
http://www.ingecom.net