

Newsletter



MARZO 2024, NÚMERO 8

CUIDADO NO SÓLO CON LOS HACKERS; OJO CON LOS EMPLEADOS

UN 40% de las empresas mexicanas consideran que el mayor riesgo que enfrentan con empleados manejando información sensible de las organizaciones es al ataque potencial de hackers frente a un 29% que estima que son los propios empleados, desleales y resentidos, el mayor peligro, nos reporta el monitoreo de percepciones empresariales de VESTIGA.

Lo relevante aquí es que casi un tercio de las empresas ya han, correctamente, ubicado la mayor fuente de riesgo para la información y, en realidad, los activos en general de las empresas, como también lo identificó el monitoreo de VESTIGA.

Durante los últimos dos años (2022 y 2023), 18% de las empresas mexicanas sufrieron robo de información por parte de sus propios empleados en contraste con sólo 5% que fueron víctimas de algún hackeo o ataque externo.

De este modo, como coinciden la gran mayoría de las agencias de inteligencia y firmas globales de manejo de riesgos, sabemos que las organizaciones están más expuestas a un daño patrimonial (incluyendo el reputacional) más grande frente a la acción o inacción, por error, negligencia o acto deliberado, por parte de sus propios empleados.

A este respecto, debemos decir que las empresas tienen que considerar que, si se alinean ciertas circunstancias, es potencialmente mucho más peligroso para sus activos y reputación un empleado decepcionado, resentido, idealista y con urgencia económica, que un hacker integrante de una sofisticada banda ubicada en algún país de Asia, Europa del Este o Sudamérica.

Todos tenemos en mente a un Edward Snowden, cuya célebre filtración de documentos confidenciales nos permitieron enterarnos de que el gobierno estadounidense cometía abusos y espionaje a sus ciudadanos en el curso de su defensa de la seguridad nacional de ese país. Y más allá de lo loable del resultado de dicha filtración, si estamos de acuerdo en que lo fue, agreguemos una dimensión en la que casi nadie repara: **la del inmenso daño que puede materializar, cualesquiera sus motivos, un solo empleado con acceso irrestricto y no vigilado a información clave de su organización.**

Por eso es muy importante que las áreas de recursos humanos establezcan mecanismos eficaces no sólo para filtrar a los perfiles adecuados para cada puesto, sino sistemas de monitoreo del desempeño laboral y personal de los empleados, especialmente de aquéllos en cargos de **alta responsabilidad y/o manejo de información sensible**. Como puntos de atención, sugerimos revisar los factores o razones que están presentes, uno o más de ellos, en quienes roban y/o filtran información de organizaciones:

- 1- **LUCRO** (el que roba la información para venderla, sólo por codicia)
- 2- **EXTORSIÓN** (el que roba porque lo chantajejan terceros)
- 3- **IDEALISMO** (el que roba porque se cree justiciero y/o por una causa)
- 4- **EGO** (el que roba porque quiere demostrar que puede, pura vanidad)
- 5- **REVANCHA** (el resentido que sólo quiere desquite, al costo que sea)

En el próximo número de este NEWSLETTER, profundizaremos en estos cinco factores.

Contacto

☎ 55 91 83 82 16 CDMX
814 777 38 93 Monterrey
✉ atencion.clientes@vestigaconsultores.com

vestigaconsultores.com