**Acciones para prevenir y mitigar un ataque cibernético**

Cuando se habla de ataques informáticos es importante resaltar que no siempre suceden por las mismas razones ni se percibe un patrón específico que los asocie. Ya sea por un tema de malas prácticas en la configuración de los servidores o una falta de medidas de seguridad apropiadas, toda empresa o persona es propensa a delitos cibernéticos.

Durante el 2017, México, Colombia y Brasil fueron los países de Latinoamérica con más ciberataques, dejando en la región una pérdida por más de 184 mil millones de dólares, según cifras de un estudio realizado por una compañía de seguridad informática.

La preocupación de que los datos de una empresa sean expuestos es preponderante; aún más después de los recientes casos en los que la red social Facebooko el Sistema de Pagos Electrónicos Interbancarios (SPEI) fueran vulnerados, afectando no sólo a las finanzas sino a la reputación de estas organizaciones.

“Las empresas solían percibir un ciberataque como algo lejano, que ocurría en otros países, pero cuando vieron que sucedió en México*,* se tomaron más en serio el asunto de la ciberseguridad, fungió casi como una labor de concientización que llevó a las compañías a preocuparse por buscar ayuda para fortalecerse en ese ámbito”, comentó Jazmín Rodríguez, Gerente de Proyecto de Ciberseguridad de Mer Group.

Una táctica sencilla que se puede implementar es el cambiar las contraseñas al menos cada tres meses. Una compañía puede no darse cuenta que hackearon sus sistemas hasta 90 días después.

Ya sea que cambiemos las contraseñas de forma tradicional o por medio de un gestor, es fundamental que sean claves que incluyan números, letras mayúsculas y minúsculas, símbolos, etcétera; siempre fáciles de recordar pero difíciles de adivinar.

Además del cambio constante de los accesos de seguridad, hay otras consideraciones que las empresas deben tomar en cuenta para protegerse como blindajes y, aún más vital, conocer perfectamente cada proceso de la compañía.

Cada una de las tácticas que se aplican para evitar y mitigar los efectos de un ciberataque suman. No obstante, no existe como tal una práctica que asegure al 100% la información, pero sí se pueden tomar acciones para disminuir considerablemente la probabilidad de que se pierda o se filtre.

Por ejemplo, es recomendable realizar un análisis constante de los sistemas para comprobar que todo está en orden. También, asegurarse de que no sólo la empresa esté protegida, sino que nuestros proveedores, clientes, socios, aplicaciones; todos los módulos que estén relacionados, directa o indirectamente con la organización, cuenten con los métodos necesarios para resguardar la información.

“Si conocemos y entendemos el proceso, por dónde viaja la información desde que se crea hasta que se destruye, entonces podremos saber qué saldrá del perímetro de seguridad y así establecer medidas adicionales”, aseguró Jazmín Rodríguez.

Aún existen muchas áreas de oportunidad en el sector de seguridad cibernética, pero los sistemas que se tienen hoy en día son altamente efectivos y las empresas deben considerarlos, no como un gasto adicional, sino como una inversión que necesitan para mantenerlas a flote. En cuanto estén conscientes de esto, ya se podrá hablar de un avance relevante en la materia.