



mexis[®]

Managed secure IT | no matter what

Cómo convencer a tu CFO que la seguridad informática es más una inversión que un gasto

m·Network



Para llegarle al corazón a un Director de Finanzas hay que hablarle con números y en un lenguaje que atrape su atención.

Por eso, si no quieres saturar su cabeza de información digital, sistemas y detalles técnicos para convencerlo de invertir en seguridad para tus redes, comienza por plantear un escenario en el cual las redes de tu empresa son afectadas y enlista cuáles serían las consecuencias monetarias de ello.

A lo largo de los últimos años, las empresas han invertido millones de dólares en contratar a expertos en seguridad informática para fortalecer sus sistemas de protección contra hackers, piratas cibernéticos, fallas en el sistema, accidentes y cibercriminales.

Cómo convencer a tu CFO que la seguridad informática es más una inversión que un gasto

Sin embargo, esta suma es mínima si consideramos los miles de millones de dólares que algunas empresas como Bloomberg, Amazon o Google podrían perder como consecuencia de no haber atendido la seguridad de sus redes, mismas que intercambian una cantidad cada vez más grande de datos e información de miles de empleados, socios y usuarios.

Eso, claro, sin contar la abismal pérdida de respeto y confianza por parte de aliados y clientes que llega como consecuencia de la pérdida de datos esenciales para la operación de una empresa, sin importar su tamaño o facturación anual.

Todas las compañías, sin excepción alguna, son susceptibles a sufrir ataques cibernéticos, por lo tanto una de las inversiones más necesarias que hay que hacer es la contratación de un experto en seguridad informática que pueda preparar los sistemas de una compañía para lo peor, y así evitar que no solo se pierda dinero, sino también prestigio.

En cambio, si el CFO continúa renuente, plantea esta situación y háblale en su idioma:

Dile que organice un ALE o Expectativa de Pérdida Anualizada, que en términos básicos, es un balance entre la probabilidad de que tu empresa sea atacada por hackers, el valor de la inversión en seguridad informática y la pérdida generada por dicho ataque.

Si las medidas de protección digital resultan más costosas que las consecuencias de un probable ataque que sucede, por ejemplo, cada diez años, quizá no vale la pena invertir en un experto en seguridad informática, pero ¿qué pasa cuando se pierde la confianza de un cliente o socio? La escala ALE no toma en cuenta ese factor, y si lo cuantificáramos, el costo de un ataque cibernético se triplicaría.

Actualmente las empresas toman actitudes reactivas, en lugar de adoptar una filosofía preventiva, lo que al final genera el ambiente perfecto para que un ataque contra los sistemas de una compañía suceda, generando pérdidas millonarias y promoviendo la inevitable inversión en un sistema de seguridad digital.

Con estas razones, el CFO no sólo entenderá la importancia de fortalecer la seguridad informática de una empresa, sino también la de ver a esa inversión como los cimientos de un futuro mucho más sólido.