
mexus®
Managed secure IT | no matter what
Ransomware, ¿Cuánto le costaría a tu empresa ser víctima de esta estafa?
m·Security

Managed secure IT | no matter what

Ransomware, ¿Cuánto le costaría a tu empresa ser víctima de esta estafa?

De acuerdo a un informe reciente sobre los estragos que el ransomware deja en las empresas, **63% de las organizaciones afectadas** indicó que sufrieron un largo periodo de inactividad que puso en riesgo su negocio y las acercó a la bancarrota.

Otro 48% dijo que perdieron datos y software esencial para continuar operando aun cuando se ya se había pagado un rescate a cambio de poder recuperar sus datos.

De hecho, de acuerdo a diferentes fuentes, el ransomware NotPetya no había sido diseñado para secuestrar información, como se había pensado en un principio, sino para dañarla, lo que revela que hoy este tipo de estafa tiene más posibilidades de arruinar un negocio que nunca.

El costo de mantenerse inactivos durante unas horas o días se mide en millones de dólares, pues dependiendo la actividad y escala de cada negocio, cada minuto puede significar la interrupción de operaciones millonarias.

Managed secure IT | no matter what

Ransomware, ¿Cuánto le costaría a tu empresa ser víctima de esta estafa?

Durante el ataque de ransomware WannaCry, **una de cada cuatro empresas nunca recuperó sus datos**, lo que significa que dejó de ganar dinero durante los días o semanas que demoró en restablecer todo nuevamente y reanudar sus actividades.

El año pasado, el número de ataques de ransomware aumentó más del doble, pasando de 2 mil incidencias diarias a más de 4 mil.

Dependiendo la escala de cada ataque, **el costo de cada ransomware va de los 250 a los 800 mil dólares**, una suma que muy pocas empresas estarían dispuestas a perder, y menos cuando no existe garantía de que los criminales vayan a cumplir su parte del trato.

Cuando NotPetya atacó a miles de empresas de Europa, Asia y América, se supo que sus autores habían pedido 250 mil dólares en criptomoneda Bitcoin para cesar su encriptación de datos, pero esta es una cifra mínima comparada con lo que otros hackers han pedido a cambio de la información que secuestran.

Existe una manera de disminuir el riesgo de ser afectados por este fenómeno, y que no requiere un gasto que afecte las operaciones de un negocio. Se trata de la contratación de servicios de ciberseguridad que, además de permitir un ahorro significativo a mediano y largo plazo, evita que un ataque de ransomware nos haga perder millones de dólares en tan solo unas horas.