AVG Business

Mantenga el control de su propia empresa

Ransomware: hechos, cifras y características

Una creciente cantidad de pequeñas y medianas empresas están siendo víctimas del ransomware, un software malicioso que chantajea a sus víctimas secuestrando PC y datos. Sin embargo, no todas las pymes son conscientes de los riesgos y las consecuencias para su empresa.

El ransomware está ganando territorio

400.000.000
de muestras de ransomware en total, 1.200.000 nuevas muestras en 2015

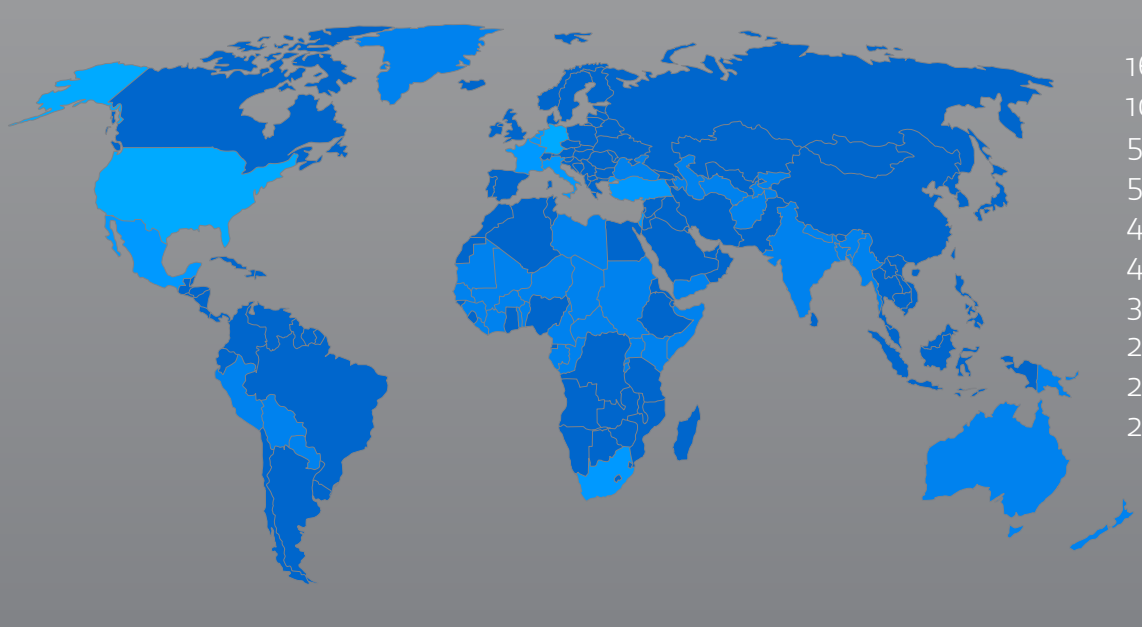
60.000
PC recientemente infectadas por Locky en un período de 24 horas

$325.000.000
daños causados por una forma de ransomware (CryptoWall) en todo el mundo

$200-10.000
el monto de rescate solicitado

$27.000.000
rescates pagados estimados en la ilocalizable moneda BitCoin

Expansión global de PC infectadas por Locky



16500 en Alemania
10900 en Estados Unidos
5200 en Italia
5000 en Países Bajos
4300 en Sudáfrica
4100 en Francia
3200 en Bélgica
2900 en Israel
2800 en Turquía
2300 en México

«Esto no afecta a mi empresa, ¿no?»

Claro que sí. Las pymes son un blanco importante.

80%
De acuerdo a una investigación global, el 80% de las pymes no utilizan protección de datos

50%
Sólo la mitad de las pymes utiliza protección del correo electrónico, mientras que el ransomware se propaga mayormente a través del correo electrónico

4/10
Es 4 veces más probable que los empleados en las pymes hagan clic en vínculos maliciosos dentro de un correo electrónico

Los ataques de ransomware pueden tener un impacto negativo significativo en las pequeñas y medianas empresas, ya que estas no siempre son capaces de lidiar con el rescate o los costos para resolver el daño después del ataque.

Una amenaza al tiempo de actividad de la empresa

En el entorno empresarial actual, el tiempo es dinero. Una investigación entre 300 encuestados dentro de empresas de todos los tamaños mostró que el tiempo de inactividad durante y después de un ataque puede ser más dañino que el ataque real en sí.

72 horas
cantidad promedio de horas en que la víctima tiene que pagar el rescate

72%
de empresas infectadas no pueden acceder a sus datos por al menos dos días después de un ataque de ransomware

32%
de acceso perdido por cinco días o más

¿Cómo funciona el ransomware?

El siguiente diagrama muestra cómo el ransomware se comporta y se las arregla para chantajear a su empresa. Este diagrama se basa en el famoso ransomware «Locky».

Mantenga el control de su propia empresa

Diríjase a www.antivirusavg.es o comuníquese con su socio de seguridad para empresas de AVG autorizado

#securitysimplified

Sources:
http://bit.ly/1Wx0wRw
http://bit.ly/207ZAoV
http://bit.ly/23NGDOb
http://on.wsj.com/1FOVvu0
http://bit.ly/1jdOzCI
http://bit.ly/1TmJc12
http://bit.ly/1SgbXh9

The Online Security Company™
Devices. Data. People.™