NUEVO RGPD DE LA UE:

# Relato de dos ataques de ransomware

Desde que el RGPD entró en vigor, el 25 de mayo de 2018, las consecuencias financieras y procesales de las violaciones de la seguridad de los datos personales son tan importantes que las empresas y proveedores de servicios intentarán evitarlas por todos los medios: o por lo menos, ese es el objetivo.

No espere a aprender por las malas; descubra cómo basta un poco más de protección para evitarle a su empresa las cuantiosas multas que supone el incumplimiento del RGPD.

## EMPRESA X

### RIESGO ALTO, CONSECUENCIAS GRAVES

Al prepararse para cumplir el RGPD, muchas empresas pasan por alto una de las violaciones de la seguridad de los datos personales que crecen más rápido: los ataques de ransomware.

Este es su proceso actual en caso de ataque:

### NO SE INSTALA PROTECCIÓN ANTIRANSOMWARE

### EL RANSOMWARE ATACA

Muchos servidores, ordenadores de sobremesa y portátiles se ven afectados.

### TI DETECTA EL ATAQUE

Se paralizan aplicaciones de producción esenciales.

### TI INTENTA CONTENER EL BROTE. COMIENZA LA CUENTA ATRÁS DE 72 HORAS PARA LA COMUNICACIÓN SEGÚN EL RGPD

Se empieza el diagnóstico de los datos personales que se han comprometido. ¡Aumenta la presión!

### LA EMPRESA CONTINÚA LA MITIGACIÓN Y EL ANÁLISIS DEL ATAQUE

Todo el mundo –desde el equipo jurídico a los ingenieros– se pone en marcha para paliar los daños.

### TI COMIENZA LA RECUPERACIÓN DE LOS ARCHIVOS CIFRADOS DESDE LA COPIA DE SEGURIDAD

TI empieza a restaurar los archivos dañados a partir de la última copia de seguridad.

### EL DELEGADO AVISA A LA AUTORIDAD DE SUPERVISIÓN DEL RGPD LOCAL

El delegado de protección de datos informa a la autoridad de supervisión local de la violación: el tipo de ataque, a cuántos datos personales ha afectado y qué medidas se van a tomar para la recuperación.

### LA EMPRESA COMIENZA A AVISAR A LOS CLIENTES

Si el ataque es serio, todos los interesados afectados deben saber lo que ha ocurrido, con quién ponerse en contacto, cuáles son las previsiones y las medidas que se han adoptado para la mitigación del problema.


### LA EMPRESA PAGA MULTAS POR INCUMPLIMIENTO

Puede que haya llegado el momento de pagar multas por incumplimiento del RGPD que van del 2 al 4 % de los ingresos anuales, o de 10 a 20 millones de euros, la cifra que sea superior.


### EMPRESA LIMPIA Y VUELTA A EMPEZAR

Si no se mejoran las defensas antiransomware, ¡con el próximo ataque de ransomware este ciclo inevitablemente se repetirá!

## EMPRESA Y

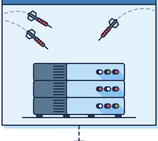
### CERO ATAQUES, CERO PROBLEMAS

Las empresas que se toman el RGPD en serio admiten que el ransomware es una amenaza importante para su cumplimiento y toman medidas para atajarla antes de que ataque.

Vea el proceso:

### LA EMPRESA INSTALA ACRONIS BACKUP CON ACTIVE PROTECTION PARA PREVENIR LOS ATAQUES DE RANSOMWARE

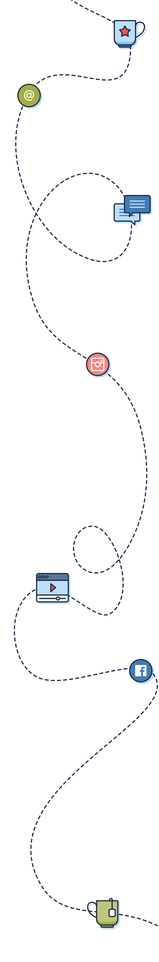
### EL RANSOMWARE ATACA



### ACRONIS ACTIVE PROTECTION LO DETECTA AUTOMÁTICAMENTE Y DETIENE ESTE PROCESO

### LA EMPRESA EVITA LA NECESIDAD DE NOTIFICAR LA VIOLACIÓN DE SEGURIDAD SEGÚN EL RGPD

(Gran suspiro de alivio)



## GARANTICE EL CUMPLIMIENTO DEL RGPD CON ACTIVE PROTECTION

Lidiar con las complejidades del RGPD no es nada fácil, pero si construye una defensa efectiva contra el ransomware, se puede librar de una enorme amenaza. Instale Acronis Backup y Acronis Backup Cloud con Active Protection y deje de preocuparse por las violaciones de la seguridad del RGPD.

Iniciar ya la prueba

Patrocinado por

Acronis