

El ransomware en el punto de mira

Lo que los CISO tienen que decir

Con el fin de dejar de lado todo el revuelo y la confusión que rodean al tema, hemos encuestado a más de 250 directores de Seguridad de la Información (CISO) en agosto de 2021 para conocer de primera mano sus experiencias con el ransomware, sus preocupaciones y sus planes para proteger sus organizaciones en el futuro.

No hay descanso a la vista

Total

53 %

Ha sufrido al menos una vez un ataque de ransomware en los últimos 12 meses

Organizaciones de tamaño medio

(de 1000 a 10 000 empleados)

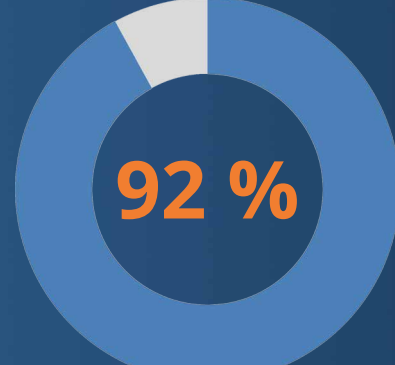
66 %

69 %

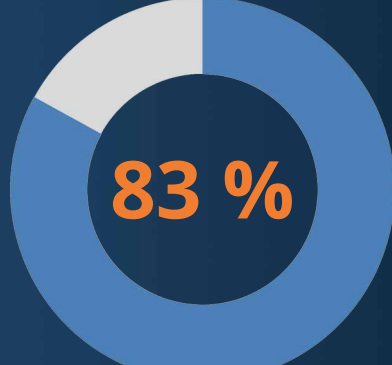
Espera sufrir al menos un ataque de ransomware en los próximos 12 meses

80 %

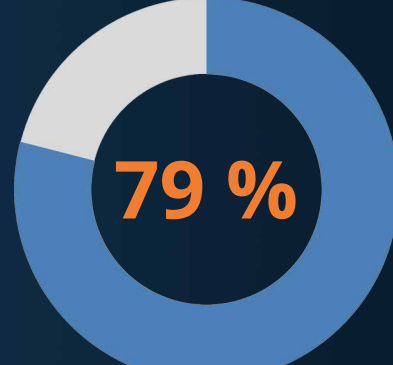
Los 3 sectores que se espera que se vean más afectados por el ransomware en los próximos 12 meses



Construcción y maquinaria



Venta al por menor y bienes de consumo duraderos



Fabricación

El valor del rescate NO supone gran preocupación

Impactos del ransomware que suponen una **mayor** preocupación

#1

Exposición de datos confidenciales o de propiedad exclusiva

#2

Valor de recuperación/restauración de la operatividad normal

#3

Pérdidas de ingresos debidas a interrupciones operativas

Impactos del ransomware que suponen una **menor** preocupación

#9

Pérdida de productividad de los empleados

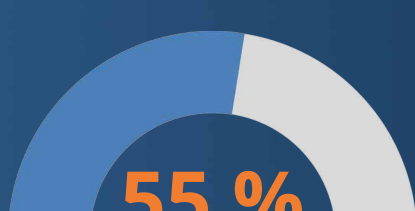
#10

Valor del pago del rescate

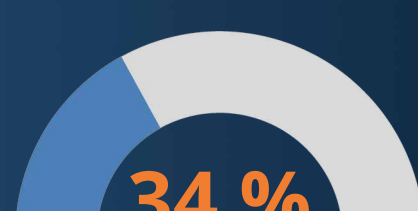
#11

Valor de las multas por incumplimiento regulatorio

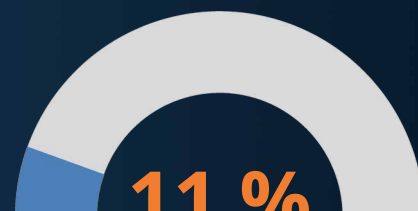
Ruleta de ransomware



El pago del rescate condujo a la recuperación COMPLETA de los datos



El pago del rescate condujo a la recuperación PARCIAL de datos



El pago del rescate NO condujo a NINGUNA recuperación de datos

1 de cada 5

1 de cada 20

víctimas del ransomware sufrieron un impacto de

Más de 5 millones de dólares

Más de 50 millones de dólares

Vigilantes en la puerta

Contramedidas técnicas de gran importancia para aminorar ataques de ransomware



Copia de seguridad y recuperación de datos



Plataforma de protección de puntos finales (EPP)



Seguridad del correo electrónico (con detección de phishing)



Sensibilización y formación de los usuarios

Principales contramedidas técnicas que se añadirán a las defensas contra el ransomware en los próximos 12 meses



Análisis de comportamiento de usuarios y entidades (UEBA)



Segmentación de la red / acceso de confianza cero



Prevención de pérdida / fuga de datos (DLP)

Un rayo de esperanza en la oscuridad...

Se diría que la naturaleza de alto perfil y alto impacto del ransomware está ayudando a que la cuestión de la ciberseguridad se trate en la junta directiva.

Los obstáculos más importantes para lograr defensas eficaces contra el ransomware



Dificultad para aplicar herramientas/tecnologías



Falta de personal cualificado para aplicar las soluciones



Otras prioridades en conflicto

Los obstáculos menos importantes para lograr defensas eficaces contra el ransomware



Resulta difícil justificar las solicitudes de presupuesto respectivas



Falta de apoyo de la junta directiva

Haga clic para descargar el informe completo >>>>

