arcserve®

EL INCREÍBLE IMPACTO DEL RANSOMWARE EN LA FIDELIDAD DEL CONSUMIDOR Y SU COMPORTAMIENTO A LA HORA DE COMPRAR

Si crees que tu empresa es inmune, piénsalo dos veces. Estudios recientes revelan que los consumidores no son tan piadosos como crees. Descubre cuánto tardarán en decir basta... y buscar otro proveedor.

Índice

ACERCA DE ESTE ESTUDIO

Los ataques cibernéticos paralizaron a las organizaciones. Los medios han informado muchas de sus consecuencias devastadoras y, en la actualidad, la mayoría de los miembros de la comunidad de TI entienden los riesgos. Lo que no se entiende —lo que las organizaciones casi nunca discuten o tienen en cuenta— son las consecuencias cuantificables a corto y largo plazo de los ataques de ransomware sobre el comportamiento del consumidor a la hora de comprar y su fidelidad de marca.

Después de un sufrir un ataque cibernético, ¿cuánto tardan los consumidores en decir basta? ¿En qué momento saldrán a buscar el producto o servicio de un competidor? Para averiguarlo, encuestamos a 1.998 consumidores de Norteamérica, Reino Unido, Francia y Alemania.

Acerca de los participantes de nuestra encuesta

Más de la mitad de los encuestados realiza negocios en línea; tres cuartos de ellos usan cuentas para la banca en línea y casi el 80%, para las comunicaciones digitales. Un hecho interesante es que no solo la mayoría está al tanto de las amenazas para la seguridad de los datos, sino que también respetan activamente las mejores prácticas en materia de protección de datos. Usan software antivirus, instalan actualizaciones y usan la autenticación de dos factores. También resguardan sus contraseñas y las cambian periódicamente.

¿Las organizaciones están cumpliendo su parte del trato? Los consumidores creen que no. Casi el 70 % de los encuestados cree que las empresas no están haciendo lo suficiente para proteger su información de manera adecuada y supone que sus datos han sido comprometidos sin su conocimiento.

Esto representa una fuerte advertencia para los líderes empresariales y de TI, en particular porque casi nueve de cada diez encuestados tienen en cuenta la confiabilidad de una organización antes de adquirir un producto o un servicio. ¿Cuántos clientes podrías estar perdiendo?

PRINCIPALES HALLAZGOS

Los consumidores a los que encuestamos lo dejaron muy claro: si no proteges sus datos frente a ataques de ransomware o si no garantizas el acceso a la información —aunque ocurra solo una vez— se irán sin pensarlo dos veces en busca de un competidor que pueda hacerlo.

70 %

de los encuestados cree que las empresas no están haciendo lo suficiente para proteger su información de manera adecuada y supone que sus datos han sido comprometidos sin su conocimiento

39 %

afirmó que la preocupación por la seguridad de su información de identificación personal (PII) era la única razón por la que optó por no abrir una cuenta o hacer transacciones con una empresa

85 %

tiene en cuenta la confiabilidad de una organización antes de hacer una compra

59 %

declaró que probablemente evitaría hacer negocios con una organización que haya sufrido un ataque cibernético en los últimos 12 meses y que su nivel de tolerancia no aumentaría mucho con el tiempo

28 %

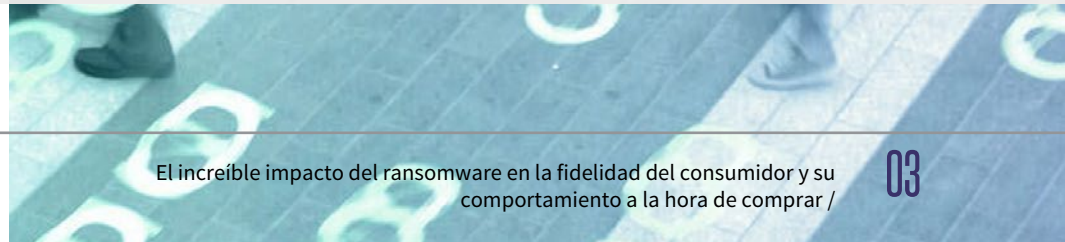
afirmó que llevaría sus negocios a un competidor si sufriera una mínima interrupción del servicio, una transacción fallida o una instancia de información inaccesible, y casi el 60% sostuvo que lo haría si sufriera dos incidentes de este tipo o menos

84 %

admitió que compartió sus experiencias negativas relativas al ransomware con familiares, amigos o colegas, escribió sobre sus experiencias en Internet o envió correos electrónicos relatando los incidentes

43 %

afirmó que la seguridad de sus datos es tan importante que estaría dispuesto a pagar más por los productos y servicios de una organización que creyera fiable y segura, porcentaje que se eleva a 50 % o más en muchas industrias



EL RANSOMWARE ES UNA AMENAZA PARA TI

Al igual que los saqueadores que se llevan televisores de pantalla grande de las tiendas en pleno caos, los atacantes cibernéticos aprovechan las grandes interrupciones y toman de rehenes a las organizaciones cuando son más vulnerables.

¿Estás preparado? Muchos no lo están.

Debido a una amplia gama de amenazas —desde la COVID-19 e incendios hasta huracanes y los típicos empleados descontentos—, las organizaciones están sufriendo fallas sistémicas con cada vez más frecuencia.

Los ataques de ransomware serán cada vez más graves y frecuentes

En 2019, el 78 % de organizaciones como la tuya fueron víctimas de un ataque de ransomware exitoso, según CyberEdge Group. Anticipamos que estos ataques se volverán cada vez más feroces. ¿Por qué?

Porque las organizaciones suelen adoptar un enfoque fragmentado hacia la protección y la seguridad de sus datos. Después de una transformación hecha con prisa, los entornos fragmentados —montados con parches durante años— revelan sus puntos débiles. Y no solo eso: cada computadora remota se transforma en un nuevo centro de datos que hay que proteger. Además, las máquinas que quedaron sin atención de los trabajadores remotos se transforman en los principales blancos de la minería ilícita de criptomonedas. En medio del caos y la confusión, muchas veces la seguridad avanzada de los datos, el backup y la recuperación de desastres (DR) quedan en el olvido.

Las brechas empiezan a estar fuera de control.

Y si hay algo de lo que puedes estar seguro, es esto: los atacantes cibernéticos aprovecharán la oportunidad de explotar las vulnerabilidades de tu organización. Multiplicarán tus problemas y lucrarán con eso.

Las personas son más propensas que nunca a caer en los trucos de los atacantes cibernéticos

Naturalmente, a medida que transcurre la jornada laboral, la fuerza de voluntad de las personas se debilita, según la Dra. Kathleen Vohs. Además, un desastre —natural, causado por el ser humano o digital— las deja exhaustas y hace que se dejen llevar por sus emociones. Su «respuesta inmunológica» a los ataques de suplantación de identidad (phishing) y las descargas involuntarias se deteriora cada vez más.

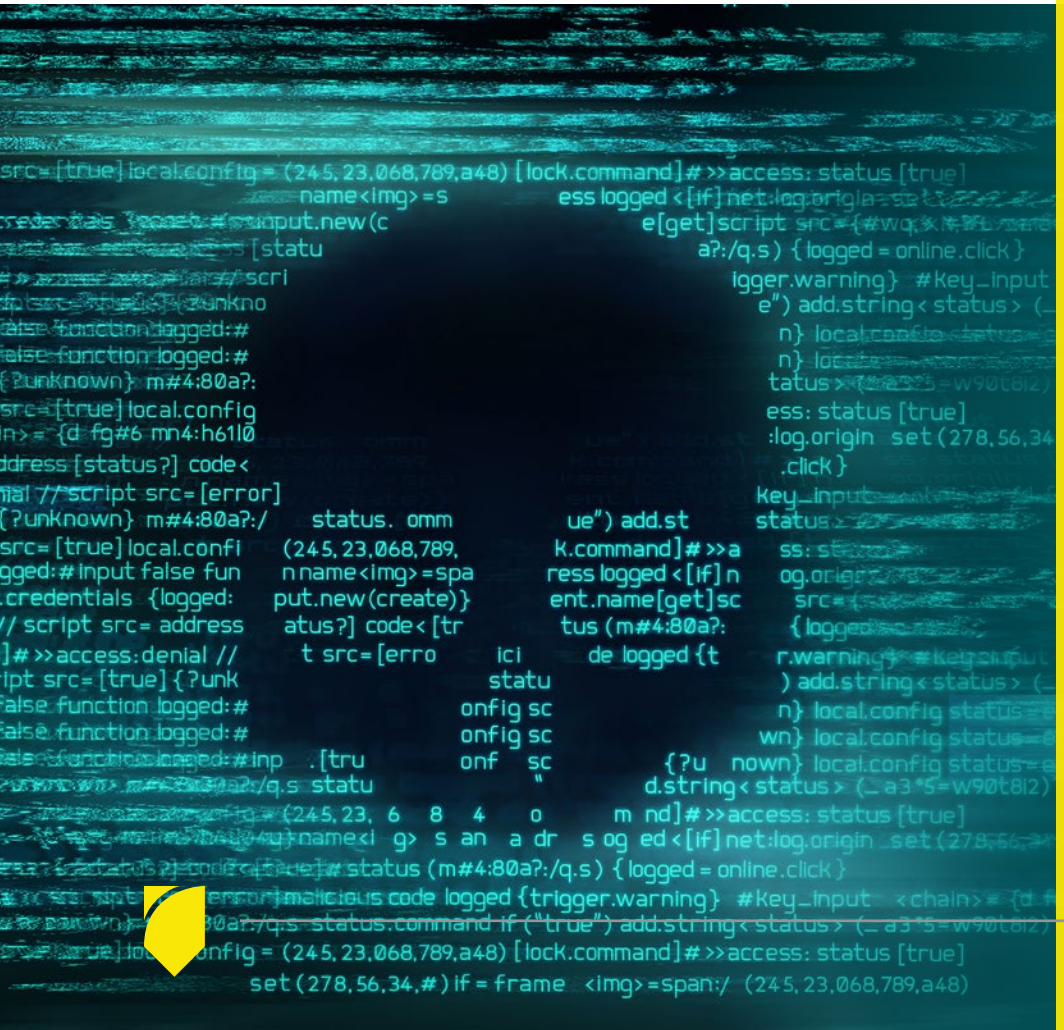
Cuando buscan información crítica, motivadas por el altruismo, las personas abrirán archivos, harán clics en enlaces y transferirán datos y dinero, cosas que no habrían hecho en circunstancias normales.

Tu trabajo nunca fue tan fundamental.

LOS ATAQUES DE RANSOMWARE DEVASTARÁN TUS FINANZAS

Movidos por el deseo de gratificación instantánea, los consumidores hacen cada vez más negocios en línea. Pero son cautelosos. De hecho, casi tres cuartos de los consumidores a los que encuestamos dijeron que no creían que las organizaciones estuvieran protegiendo sus datos de manera adecuada.

Esa inquietud los llevará a hacer negocios contigo... o con tus competidores.



Los consumidores son impiadosos con las empresas incapaces de proteger sus datos

85 %

evalúa la fiabilidad de tu organización o tu sitio web antes de decidir hacer negocios contigo

39 %

menciona la preocupación por la seguridad como la única razón por la que no hizo negocios con una organización

59 %

tenderá a evitar hacer negocios contigo si sufriste un ataque cibernético en los últimos 12 meses

45 %

no hará negocios contigo si has sido víctima de atacantes cibernéticos en los últimos tres años, prueba de que los malos recuerdos no se borran fácilmente

Los ataques de ransomware ya no se pueden disimular

Antes, las organizaciones podían pagar el rescate y evitar que el ataque cibernético saliera a la luz, pero esto ya no es así. Hoy los atacantes cibernéticos divulgan sus ataques aunque reciban el pago por el rescate.

Dada la importancia de la confianza y la seguridad de los datos para los consumidores, es necesario que te hagas esta pregunta: ¿estás haciendo todo lo posible para ganarte su fidelidad?

SI QUEDAS INACTIVO, LOS CONSUMIDORES LLEVARÁN SUS NEGOCIOS A OTRA PARTE

Si tu organización registra tiempos de inactividad vinculados con el ransomware, puedes dar por perdido a uno de cada cuatro consumidores. Sucede que en la economía a demanda de hoy, una sola interrupción de servicio, transacción fallida o instancia de información inaccesible parece eterna.

Esta intolerancia a la interrupción del servicio es, posiblemente, la consecuencia más devastadora del ransomware que revela nuestra encuesta. Las consecuencias van mucho más allá del impacto inmediato de un ataque.

Los consumidores no tolerarán interrupciones del servicio por ataques de ransomware

58 %
recurrirá a un competidor si sufre dos interrupciones o menos

28 %
abandonará a una empresa si sufre una sola interrupción

46 %
abandonará a un banco o una empresa de valores si sufre una sola interrupción

45 %
abandonará a un minorista si sufre una sola interrupción

43 %
abandonará a un proveedor de comunicaciones y seguros si sufre una sola interrupción

Los consumidores no esperarán a que te recuperes del ransomware

Tras sufrir un ataque cibernético, muchas organizaciones detienen por completo sus operaciones: desconectan sus sistemas y aplicaciones mientras calculan los daños y recuperan los datos de los backups. Pero, para muchos consumidores, el tiempo es dinero.

37 %
recurrirá a un competidor si tus sistemas y aplicaciones no vuelven a conectarse dentro de las 24 horas

41 %
abandonará a una empresa si no puede acceder a los sistemas y aplicaciones en dos o tres días

49 %
recurrirá a un competidor si sus sistemas y aplicaciones de bancos o empresas de valores no vuelven a conectarse dentro de las 24 horas

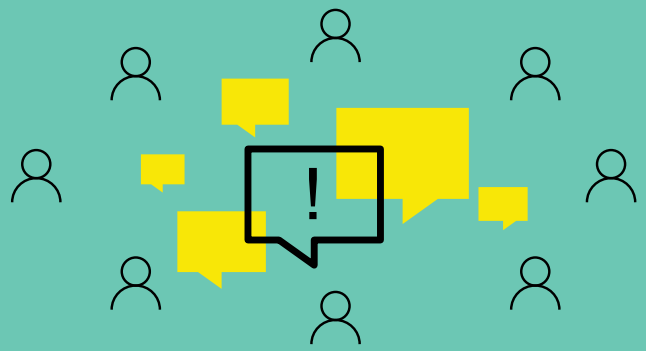
45 %
cambiará de productos o servicios de comunicaciones si no recupera el acceso dentro de las 24 horas

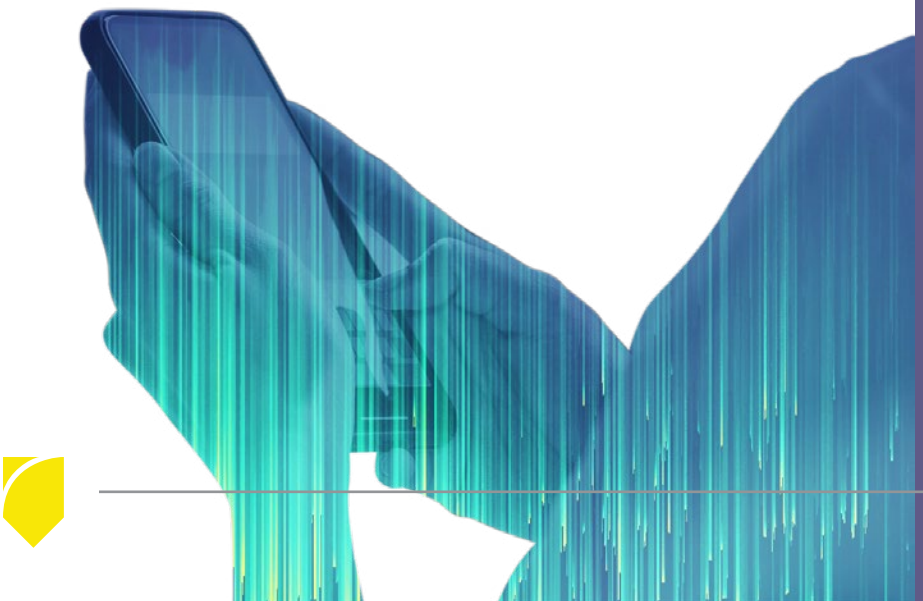
16 %
abandonará inmediatamente a bancos o empresas de valores o comunicaciones

LOS CONSUMIDORES EXPRESARÁN SU FRUSTRACIÓN

Puede que los efectos residuales de los ciberataques te sorprendan. De hecho, la mayoría de los consumidores compartió sus experiencias de ransomware con familiares, amigos y colegas. Un cuarto de ellos lo hizo por Internet.

En pocas palabras, un consumidor descontento dará a conocer su frustración. Por eso, si sufres un ataque cibernético, prepárate para una avalancha de malas noticias.





Los consumidores comparten sus experiencias de ransomware

45 %
compartió sus experiencias negativas con familiares, amigos o colegas

25 %
publicó sus experiencias en el foro de una comunidad, un blog o un sitio web

24 %
compartió sus experiencias por correo electrónico

23 %
publicó reseñas negativas en Internet o compartió sus experiencias por redes sociales

Prepara a tu equipo de relaciones públicas

28 %
te considerará menos confiable

24 %
opinará que no invertiste suficiente dinero en la seguridad

17 %
creerá que eres incompetente y que te importan más tus ganancias que su seguridad

PROTEGER LOS DATOS DE LOS CONSUMIDORES FRENTE AL RANSOMWARE PUEDE MEJORAR TUS FINANZAS

Los ataques cibernéticos influyen mucho en las decisiones de compra de los consumidores, pero nuestra encuesta también reveló buenas noticias: la protección contra el ransomware es realmente buena para los negocios. De hecho, **más de 4 de cada 10 consumidores estarían dispuestos a pagar más por productos y servicios si creen que puedes proteger sus datos de manera confiable.** Esa cifra **aumenta a 5 de cada 10 o más en ciertas industrias, como los bancos y las empresas de valores.**

¿Podrías cobrar más por tus productos y servicios?

43 %
gastará más —en líneas generales— por productos y servicios de una empresa que consideren más confiable y segura

51 %
pagará más a bancos y empresas de valores

44 %
pagará más a proveedores de comunicaciones, almacenamiento de datos y proveedores de nubes públicas

39 %
pagará más a organizaciones de servicios de medios, educación y transporte

43 %
pagará más por servicios gubernamentales

45 %
pagará más por servicios de salud y seguros

42 %
pagará más por servicios públicos

41 %
pagará más por compras minoristas

PARA IMPULSAR LAS VENTAS DE TUS PRODUCTOS, HAZ QUE LA PROTECCIÓN DE DATOS Y PROTECCIÓN CONTRA EL RANSOMWARE SE UNAN A LAS FINANZAS DE TU ORGANIZACIÓN.

Sientes la presión. Sabes que eres responsable de proteger el sustento de tu organización —sus datos— y que no estás plenamente equipado. ¿Cómo ayudar a quienes toman las decisiones a ver más allá del precio de la protección de datos y contra el ransomware y tener en cuenta su valor para el negocio?

Ayuda a los encargados de tomar decisiones a tener una idea clara del riesgo que representa el ransomware para tu organización.

Explícales que los atacantes cibernéticos lograron atacar al 78 % de las organizaciones con ransomware el año pasado y destaca ejemplos recientes de la industria para plantear un caso convincente (ver columna derecha).

Evita los detalles técnicos específicos y enfócate en las consecuencias inmediatas para la continuidad del negocio.

Entra en la reunión listo para explicar cuánto perderá tu empresa si queda inactiva un minuto, una hora, un día o una semana. Comunica los impactos económicos, como posibles pedidos de rescate, la pérdida de datos e ingresos, la atención mediática no deseada, las multas de entes reguladores y el tiempo que los empleados pasarán sin hacer nada.

Describe los efectos inmediatos y a largo plazo del ransomware sobre la fidelidad del consumidor y sus decisiones de compra.

Calcula, por ejemplo, el impacto económico para tu empresa si perdieras al 28 % de tus clientes tras una sola interrupción del servicio a causa de un ataque de ransomware.

Demuestra que la protección contra el ransomware puede ser una ventaja competitiva.

Los consumidores aprecian que sus datos estén protegidos. Asegúrate de que quienes toman las decisiones también estén dispuestos a pagar más si puedes brindarles tranquilidad.

Entusiasma a los responsables de la toma de decisiones con la marca y no con el producto

A la mayoría no le importan las funcionalidades y las especificaciones técnicas. Lo que les interesa es la solidez de la reputación de una marca.

Comparte nuestro documento de una página, «¿Crees que tus consumidores perdonarán un ataque de ransomware?»

Este resumen general brinda una perspectiva novedosa y muy necesaria, fundamental para los cálculos de quienes toman las decisiones en tu organización.

Comienza el debate con tu director de TI o tu CIO.

Al reclutar desde el principio a un simpatizante que sepa de tecnología, contarás con un aliado que te puede ayudar a torcer el rumbo de la conversación para que ya no se trate del costo de inversión sino del valor que representa para tu empresa.

Casos de ataques de ransomware como estos pueden subrayar la necesidad de tomar medidas con urgencia

MUNSON HEALTHCARE

Cuando 29 empleados de esta organización de salud en el norte de Michigan fueron víctimas de una campaña de phishing, los atacantes cibernéticos obtuvieron discretamente acceso a los datos de los pacientes durante dos meses y medio, incluida información sobre tratamientos, datos bancarios y números de seguridad social.

Travelex

Tras emplear un ataque con REvil, los atacantes cibernéticos no solo exigieron 6 millones de dólares de esta institución financiera británica, también afirmaron que tenían datos personales y de las tarjetas de crédito de los consumidores. Travelex dejó inactivos sus sistemas de TI y sus sitios web por más de tres semanas con la excusa de que estaba haciendo "mantenimiento planificado".

MGM RESORTS INTERNATIONAL

A través de un ataque de ransomware, los atacantes lograron acceder al servidor en la nube de esta cadena de hoteles y a los datos personales de más de 10 millones de huéspedes, entre ellos el cantante pop Justin Bieber y el CEO de Twitter, Jack Dorsey.

SOLUCIONES DE ARCSERVE RESPALDADAS POR SOPHOS

Sabes que tus clientes no tolerarán tiempos de inactividad o violaciones de seguridad de los datos causados por ataques de ransomware. Por eso, acude a Arcserve.

Gracias a las tecnologías totalmente integradas de Sophos, te brindamos una protección completa contra ataques cibernéticos, grandes desastres, errores humanos y otras interrupciones no planificadas. Confía en los expertos: aprovecha el único conjunto de soluciones comprobado y diseñado por proveedores con más de 70 años de experiencia combinada.

- Potencia al área de TI y deja de hacer equilibrio entre varios proveedores, SLA y equipos de soporte
- Obtén protección total basada en SaaS para tus datos on-premise y en la nube de un solo proveedor que unifica el backup, la ciberseguridad, la recuperación de desastres y los servicios en la nube
- Garantiza operaciones ininterrumpidas y cumple los SLA con recuperación instantánea de máquinas virtuales y recuperación bare-metal (BMR), Virtual Standby local y remoto, backup que conserva la integridad de las aplicaciones y restauración granular, compatibilidad con instantáneas de hardware y extensiones que ofrecen alta disponibilidad y compatibilidad con cintas
- Asegúrate de no perder un segundo durante las interrupciones de los entornos on-premise con Virtual Standby remoto para conmutación de aplicaciones por error y por recuperación de emergencia, conmutación por error a recursos remotos de activación manual y recuperación instantánea de máquinas virtuales
- Olvídate de los problemas causados por la eliminación intencional o accidental, problemas programáticos y amenazas externas a la seguridad —problemas que no cubre Microsoft— con protección total para los datos de Exchange Online, OneDrive for Business y SharePoint Online
- Detecta el malware conocido y desconocido sin depender de firmas gracias a Sophos Intercept X Advanced, que viene totalmente integrado con tecnologías avanzadas de aprendizaje profundo (IA)
- Bloquea las principales técnicas de hacking, como la captura de credenciales, el movimiento lateral y el escalamiento de privilegios con prevención de exploits
- Detén ataques de ransomware contra datos respaldados con CryptoGuard y ataques de MBR con WipeGuard
- Garantiza la satisfacción de los requisitos de cumplimiento con cifrado AES y control de acceso basado en roles
- Crece junto con tus datos reduciendo drásticamente los requisitos de almacenamiento con la deduplicación global incorporada, que libera hasta 20 veces más capacidad

¿NECESITAS AYUDA?

Cuenta con Arcserve. Estamos siempre listos para poner manos a la obra y ayudarte.

arcserve®

arcserveayuda@arcserve.com
arcserve.com/la