Avast Business

Informe técnico

5 pasos para proteger a los negocios del ransomware

28 Noviembre 2023

Avast Business

Sobre el autor

Rob Krug, Arquitecto de Seguridad Senior, Avast Business

Rob lleva más de 30 años en el ámbito de la ingeniería de redes y la seguridad. Su experiencia incluye un amplio trabajo en telecomunicaciones, diseño y gestión de redes y, sobre todo, en seguridad de redes.

Especializado en vulnerabilidades de seguridad, Rob tiene una amplia experiencia en criptografía, hacking ético e ingeniería inversa de malware. Rob sirvió en la Marina de Estados Unidos, y también trabajó como analista de seguridad de datos y director de ingeniería para varios distribuidores y proveedores de servicios internacionales. Rob ha diseñado, implantado y mantenido algunas de las redes más complejas y seguras imaginables.

Introducción

l ransomware está en aumento y no muestra signos de desaceleración. Se prevé que el coste global de los daños debidos a los ataques de ransomware alcance los 20.000 millones de dólares a finales de 2021, según Cybersecurity Ventures.

No es una exageración decir que el ransomware representa una amenaza existencial para el sustento de las empresas estadounidenses y mundiales en sectores como el educativo, financiero, gubernamental, sanitario, policial y de telecomunicaciones. Las víctimas del ransomware —así como ciudadanos, clientes, inversores y pacientes a los que estas organizaciones deben atender— tienen mucho que perder.

En el primer semestre de 2020, las empresas, las instituciones de educación superior y los gobiernos locales dedicaron casi 145 millones de dólares para aplacar a los hackers, y restaurar los datos y las redes después de ser golpeados por grandes ataques de ransomware. Y el pago del rescate no garantizaba —ni lo hace ahora— que esas organizaciones recuperen sus datos. Como si pagar un rescate por tus propios datos no fuera lo suficientemente degradante y agotador, los impactos financieros y otros impactos negativos del ransomware se extienden mucho más allá del rescate. Las víctimas del ransomware también tienen que hacer frente a los costes de TI añadidos, la pérdida de productividad, el aumento de los costes legales, la necesidad de modificar la red y/o las cuotas de suscripción a nuevos servicios de control de crédito para empleados o clientes.

Afortunadamente, las empresas pueden protegerse de la amenaza del ransomware. Una de las mejores maneras de hacerlo es con una solución de copia de seguridad y recuperación en la nube eficaz y protegida, que evite el evento del ransomware y devuelva una copia no infectada de sus datos. Sin embargo, para los que no tienen esa solución, hay otras formas de contrarrestar el impacto.

A continuación, se ofrecen varios consejos sobre cómo las PYMES pueden mitigar el ransomware. Pero, primero, evaluemos el panorama general.

Avast Business

Por qué aumentan los ataques de ransomware

Las nuevas opciones de pago digital que proporcionan a los delincuentes un alto grado de anonimato, el creciente ecosistema de hackers de ransomware y la desaparición del perímetro de la red empresarial (en medio de una plantilla cada vez más distribuida) han contribuido al aumento del ransomware. El bitcoin y otras criptomonedas han hecho que los ciberladrones puedan exigir y recibir pagos y transferir dinero anónimamente de forma segura y sencilla.

El hecho de que el ransomware no sólo sea explotado por empresas criminales sofisticadas y bien financiadas añade más leña al fuego del ransomware. Los hackers respaldados por el Estado y los particulares, que buscan sacar provecho de lo que perciben como dinero fácil, también están lanzando ataques de ransomware.

La pandemia también ha contribuido a alimentar el aumento del ransomware. Los ciberdelincuentes están aprovechando la pandemia en su beneficio, intensificando sus ataques a organizaciones y consumidores individuales para obtener beneficios financieros y políticos.

El gran aumento del trabajo desde cualquier lugar hace que más trabajadores utilicen sus propios dispositivos, como ordenadores portátiles, de sobremesa y móviles. Las redes domésticas no son tan seguras como las empresariales; los departamentos de TI tienen mucho menos control sobre la seguridad y la configuración de los dispositivos de los trabajadores remotos y la infraestructura que protege esos puntos finales. Por desgracia, los malhechores también lo saben, ya que hemos visto un crecimiento de ransomware de casi un 400% en los últimos dos años como resultado.

Según Infrascale, el **43%** de las PYMES encuestadas dijeron que han pagado de **$10,000** a **$50,000** a los atacantes de ransomware. Los precios eran aún más altos para otros: un **13% de las PYMES entregó más de $100,000.**

El ransomware tiene un precio elevado

Empresas de todos los tamaños y sectores de la industria son objeto de ataques de ransomware. Una reciente encuesta de Infrascale realizada a más de 500 ejecutivos de nivel C de PYMES reveló que el 46% ha sido víctima del ransomware.

El tiempo de inactividad es un enorme problema para las empresas, que pierden tiempo y dinero por cada hora, minuto o segundo que no tienen acceso a sus datos críticos y otros activos digitales. Esto ayuda a explicar por qué casi tres cuartas partes (73%) de las PYMES que se han enfrentado a ataques de ransomware han desembolsado dinero para pagar los rescates.

Avast Business

El pago de un rescate puede mermar considerablemente las finanzas de una organización. Según Infrascale, el 43% de las PYMES encuestadas afirma haber pagado de 10.000 a 50.000 dólares a los atacantes de ransomware. Las etiquetas de precio fueron incluso más altas para algunas otras: el 13% de las PYMES desembolsaron más de 100.000 dólares.

Según Coveware, la cantidad media pagada por un ataque de ransomware en el cuarto trimestre de 2019 fue de $84.116. Esta cifra es superior a la media de $6.733 de los 12 meses anteriores. El estudio de Coveware indica que esta cantidad está fuertemente sesgada por el ransomware Ryuk y Sodinokibi, empujando el pago medio en el cuarto trimestre de 2019 a 41.198 dólares. Las demandas de ambos pueden alcanzar normalmente seis o incluso siete cifras, lo que hace que un solo ataque exitoso sea extremadamente lucrativo. En junio de 2019, por ejemplo, los atacantes de Ryuk extorsionaron más de un millón de dólares en rescates de dos ciudades de Florida en solo una semana. Un solo afiliado de Sodinokibi apareció para hacerse con 287.000 dólares en tres días.

La cantidad de dinero que se canaliza hacia estos delincuentes para financiar futuros ataques es muy preocupante, y el tamaño y la cantidad de los rescates que se pagan está haciendo que los proveedores de seguros suban las tarifas de sus ciberseguros hasta un 25%.

Sin embargo, en la mayoría de los casos, el coste del rescate es trivial comparado con el coste del tiempo de inactividad del sistema, las ventas perdidas y la credibilidad perdida. Así, con la esperanza de restaurar rápidamente sus sistemas y recuperar sus datos, las víctimas del ransomware suelen pagar a los chantajistas anónimos.

Es probable que esta sea una tendencia continua, ya que la investigación de Infrascale muestra que más de una cuarta parte (26%) de las PYMES que informaron que nunca han pagado un rescate dijeron que considerarían hacerlo. De ese grupo, el 60% dijo que pagaría un rescate para recuperar sus archivos rápidamente, y el 53% dijo que pagaría un rescate para proteger la imagen pública de su empresa en torno a los esfuerzos de recuperación y protección de datos. Sin embargo, el 17% de los participantes en la encuesta que pagaron rescates a sus atacantes de ransomware indicaron que solo recuperaron parte de los datos de su organización a cambio.

La prevención del ransomware merece atención

El ransomware no es una amenaza que acaba de llegar a la escena. Este problema existe desde 1989. Sin embargo, muchas empresas todavía no se han preparado para los ataques de ransomware.

Casi una quinta parte (19%) de los encuestados por Infrascale dijeron que no creen que sus empresas estén adecuadamente preparadas para afrontar y prevenir tiempos de inactividad inesperados. Esto es interesante, teniendo en cuenta que más de un tercio (37%) ha perdido clientes y el 17% ha perdido ingresos debido al tiempo de inactividad.

El tiempo de inactividad puede costar a las empresas un buen dinero. Aproximadamente la mitad (48%) del grupo de encuestados informó de que su coste por hora de inactividad se situaba entre los 20.000 y los 50.000 dólares

El adagio de que el tiempo es oro parece aplicarse en este caso, aunque tal vez de una manera diferente a la que se podría pensar. La investigación de Infrascale indica que casi un tercio (32%) de las PYMES tiene poco tiempo para investigar soluciones de mitigación del ransomware. La misma cantidad dijo

que no cuentan con los recursos informáticos adecuados para hacer frente a las amenazas de ransomware. La cuestión es que las empresas que no se toman el tiempo necesario para prepararse adecuadamente para un ataque de ransomware pueden perder mucho dinero posiblemente pagando el rescate, pero ciertamente debido a los desafíos operacionales, una pérdida en el negocio, y un golpe para su reputación. Ante estos retos, he aquí un consejo útil: Considere la posibilidad de contratar a un experto externo, como un proveedor de servicios gestionados (MSP) o un profesional de la seguridad, para que le ayude con el trabajo pesado de la protección contra el ransomware, la educación, la implementación y la configuración.

Educar al personal sobre la importancia de los programas antivirus actualizados y las amenazas de phishing

Las organizaciones que quieran protegerse del ransomware deben educar a los miembros del personal sobre esta amenaza y sus puntos de entrada en la organización. Esto significa educar en el manejo adecuado del correo electrónico y asegurarse de que el software antivirus de los empleados está actualizado. Esto puede parecer obvio, pero suele ser algo que las PYMES no comprueban hasta que es demasiado tarde.

Detectar un posible ataque con antelación es ideal para evitarlo. Su departamento de TI debe comprobar la red con frecuencia para ver qué tipos de archivos se envían y trabajar para entender qué tipos de ordenadores se conectan a su red.

Si algo parece dudoso, suele serlo. Los delincuentes son cada vez más sofisticados a la hora de hacer que sus ataques parezcan legítimos. Y durante esta época, en la que la gente está en busca de información y respuestas, los filtros falsos del público están en su punto más bajo.

Avast Business

Tome estas medidas si su organización se ve comprometida por el ransomware

La ciberseguridad es importante, pero no es infalible. Es muy probable que en algún momento sea víctima de un ransomware. Tal vez ya haya experimentado algo así.

Estos son algunos consejos útiles que su organización puede utilizar para responder a un ataque de ransomware:

1 Capturar el mensaje del ransomware

Cuando su empresa sufre un ataque, su primer impulso puede ser tomar medidas. Pero no se olvide de hacer una captura de pantalla o una fotografía del mensaje de ransomware. Esta imagen capturada le servirá como prueba para su propio uso y en caso de que denuncie el evento de ransomware a las fuerzas del orden.

2 No pagar automáticamente el rescate

Como escribió la profesora de la Universidad de Tufts Josephine Wolff en este artículo para The New York Times, pagar a los atacantes de ransomware sólo sirve para recalcar a la comunidad de hackers que el ransomware es un "modelo de negocio" que da beneficios. Si hay otra manera de salir de la situación, sin arriesgar la vida y la integridad física, considere tomarla. No premie a los malos.

3 Realizar un análisis coste-beneficio

Esto le ayudará a decidir el mejor camino a seguir. El profesor del MIT Larry Susskind señaló que, si el ransomware congela las operaciones empresariales críticas, una organización puede no ser capaz de recaudar ingresos, proporcionar servicios vitales como el agua o la electricidad, o concluir los procedimientos de los pacientes. El ransomware ciertamente crea un riesgo financiero, pero también puede ser una propuesta de vida o muerte. Dicho esto, tiene sentido mirar antes de saltar.

4 Comprender si el problema es un ransomware de cifrado o de bloqueo de pantalla

Si se trata de un ransomware que bloquea la pantalla, la situación puede ser más fácil de remediar. Intente cerrar la aplicación afectada mediante el monitor de actividad de Mac o el administrador de tareas de Windows, reinicie el dispositivo en modo seguro y emplee tecnología de eliminación de malware. Si tiene suerte, esto puede ayudarle a superar la variedad de ransomware de bloqueo de pantalla.

Avast Business

5 Actuar rápidamente para limitar la amenaza

El ransomware puede propagarse como un incendio, por lo que querrá contenerlo lo antes posible. Una forma de hacerlo es desconectando físicamente los dispositivos afectados. Desactive las conexiones Bluetooth y wifi de esos dispositivos y póngalos en modo avión. Desenchufe los cables Ethernet y las conexiones a dispositivos externos como cámaras, discos duros y teléfonos. Las organizaciones también pueden contener el ransomware mediante la microsegmentación. Este enfoque se basa en la supervisión de la red para detectar anomalías y aprovecha la automatización para aislar los dispositivos que presentan comportamientos que indican que pueden haber sido infectados.

Limite los daños causados por el ransomware y siga funcionando con Avast Business Cloud Backup

El riesgo que el ransomware representa para su negocio disminuye significativamente si emplea una solución integral de copia de seguridad y recuperación de terminales basada en la nube, como Avast Business Cloud Backup, que resulta inestimable en caso de un ataque de ransomware. Nuestra solución realiza copias de seguridad de datos críticos, como archivos de contabilidad, archivos de datos de Exchange y bases de datos SQL. La solución de copia de seguridad directa a la nube de Avast Business protege una amplia gama de dispositivos y terminales, independientemente de su ubicación, lo cual es importante en nuestro mundo cada vez más remoto.

Como todos sabemos, enfrentarse a una crisis nunca es divertido. Pero enfrentarse al ransomware en esta época tan complicada puede ser mucho menos doloroso, y puede superarlo más rápidamente y con mucho menos trastorno si ya tiene una buena copia de seguridad y recuperación de desastres. Las empresas que tienen preparadas estrategias y soluciones de copia de seguridad y recuperación de desastres pueden restaurar sus datos y reanudar sus operaciones normales mucho más rápidamente después de un ciberataque.

Acerca de Avast Business

Avast Business ofrece soluciones de seguridad de red y terminales integradas y de calidad empresarial para PYMES y proveedores de servicios de TI. Respaldada por la mayor red de detección de amenazas a nivel mundial, la cartera de seguridad de Avast Business hace que sea fácil y asequible proteger, gestionar y supervisar redes complejas. El resultado es una protección superior con la que las empresas pueden contar. Para más información sobre nuestros servicios gestionados y soluciones de ciberseguridad, visite **www.avast.com/business**.