White Paper

Las cinco tecnologías esenciales para habilitar un marco de ciber-resiliencia

Sponsored by: IBM

Frank Dickson Phil Goodwin

Agosto de 2019

ACTUALIZACIÓN DEL INFORME

Tenga en cuenta que este paper se publicó originalmente en junio de 2018 (n.º de IDC US4401318). Las únicas actualizaciones son la sustitución de uno de los analistas originales y la de la fecha de publicación original.

LA OPINIÓN DE IDC

Según encuestas recientes de IDC sobre el tema de la seguridad, el 50 % de los profesionales en ese área dedican la mayor parte de su tiempo a implementar medidas de seguridad para la nube, y en los últimos 12 a 18 meses muchos han sufrido lo que describieron como una brecha vinculada a la nube, ya fuera un ataque de ransomware (23 %), una brecha de seguridad del IoT (23 %) o un ataque DDoS (23 %). Alrededor del 75 % de esos ataques ocurrieron como consecuencia de algún incidente relacionado con la nube.

Esto no significa que las tecnologías vinculadas a la nube y las nuevas maneras de comunicarse sean la *causa-raíz* de las brechas y fallos en el negocio, sino que a medida que las empresas adoptan nuevas tecnologías sus estrategias de protección deben modificarse para adaptarse a las nuevas circunstancias. Esas estrategias deben incluir mecanismos de seguridad más fuertes y variados, pero también maneras de recuperarse rápidamente en caso de que se produzca una brecha o un incidente.

Las empresas de todo el mundo están avanzando incesantemente hacia la transformación digital, que es el proceso de integrar tecnología en todos los aspectos del negocio con el fin de acelerar las actividades empresariales, sustentar la agilidad y sacar provecho de una visión estratégica y oportunidades dinámicas. Algo imprescindible para la transformación digital es convertirse en una organización impulsada por datos y capaz de monetizar la información. Al mismo tiempo, la transformación digital conlleva inherentemente nuevos riesgos que quizás se hayan pasado por alto anteriormente o que hayan complicado el perfil de riesgo de los procesos de negocio ya establecidos, por lo cual las empresas buscan niveles más altos de integración entre funciones esenciales de soporte de negocio y una mayor disponibilidad de los datos para asegurarse de estar preparadas para hacer frente a cualquier desafío. Esto es lo que se conoce como ciber-resiliencia.

La ciber-resiliencia combina las mejores prácticas vinculadas a la seguridad de TI, la continuidad del negocio y otras disciplinas para crear una estrategia de negocio más alineada con las necesidades y objetivos de la empresa digital actual. En este documento de IDC, se describe de qué manera la transformación digital está quebrantando las protecciones tradicionales entre empresas y participantes dentro de la economía global, mientras las tecnologías esenciales para el negocio se

convierten en puertas de entrada para riesgos, ataques y fallos de sistemas. También se describe cómo las prácticas de ciber-resiliencia pueden ayudar a las empresas a defenderse contra esos riesgos y a recuperarse tras una brecha o fallo de una manera controlada y cuantificable. Por último, se presenta un marco que puede ayudar a las organizaciones a emprender su camino hacia la ciber-resiliencia, además de estrategias para modificar las prácticas de protección y restauración de datos con el objetivo de luchar mejor contra los ataques más dañinos y deliberados que ocurren en la actualidad.

EN ESTE WHITE PAPER

¿Es este el momento en que sus operaciones de negocio se frenan bruscamente? ¿Ha llegado el día en que su empresa debe cerrar sus puertas? Esta es una visión pesimista de la realidad empresarial. En cualquier momento podría ocurrir algún evento que altere el tejido operativo de la empresa, y en la vorágine actual del mundo de los negocios, cada segundo cuenta.

No es necesario que esos eventos sean catastróficos para que tengan un impacto duradero. Las empresas más maduras ya tienen instaurada una gestión del riesgo y alguna medida de continuidad o resiliencia empresarial. Seguramente esas organizaciones comprenden que los eventos de gran magnitud que tienen un impacto devastador son menos probables que los eventos pequeños y discretos que pueden hacer tambalearse a las operaciones. Tomemos como ejemplo lo que sucedió con la gripe aviar a mediados del año 2000, cuando las empresas estaban demasiado pendientes del posible impacto que podría tener un virus que se propaga rápidamente por el aire sobre los empleados y las operaciones de negocio. Si bien es cierto que el concepto en sí es digno de preocupación, la probabilidad de que se materialice la fiebre aviar o cualquier amenaza similar ha sido y sigue siendo muy baja. Esta baja probabilidad no impidió que las organizaciones trataran de crear planes de contingencia operativos basados en la naturaleza del impacto potencial. Lo mismo ocurre en el caso de otros desastres naturales o amenazas físicas. El potencial de que tengan consecuencias de gran impacto es motivo de preocupación, y a veces enfocarse en la posible magnitud de un evento único puede impedir que las organizaciones se focalicen en las amenazas muy reales, tangibles y discretas que pueden causar estragos en el negocio.

La transformación digital está poniendo en tela de juicio los conceptos tradicionales de resiliencia empresarial. La transformación digital es el proceso mediante el cual la tecnología se interrelaciona con todos los ámbitos de la experiencia humana. En la empresa, la transformación digital se traduce en un mayor nivel de conectividad entre aplicaciones y procesos empresariales con el fin de incrementar la agilidad del negocio y conectarse más fácilmente con clientes y socios, para brindar a los usuarios una experiencia sin interrupciones las 24 horas del día, los 7 días de la semana. La transformación digital se puede presentar de muchas maneras. Es posible que una empresa esté buscando integrar mejor su infraestructura existente y sistemas heredados, o puede que se esté encaminando lentamente hacia la nube, o quizás tenga en mente una estrategia del tipo “la nube primero”. De cualquier manera que sea, el concepto de una empresa conectada resulta esencial a la hora de evaluar la resiliencia empresarial. Ya sea que se trate de agrupar procesos de negocio o desarrollar entornos multinube o de nube híbrida, cuanto más hiperconectados estén los sistemas y procesos de negocio mayor es la probabilidad de que un evento discreto pueda desbaratar todo el negocio. Lo que alguna vez fuera un pequeño “tambaleo” ahora podría enviar ondas de choque a toda la organización.

Es por eso que la ciber-resiliencia ha cobrado muchísima importancia tanto para los profesionales de seguridad como para los responsables de la continuidad del negocio y planificación de la gestión del riesgo. La ciber-resiliencia es la fusión de ciberseguridad, gestión del riesgo y prácticas de resiliencia/continuidad del negocio con el fin de crear una disciplina que sirva para mejorar las capacidades de respuesta cibernética, desde la detección de eventos y la recuperación hasta la mejora incesante de los procesos. Los clientes están reconociendo que las estrategias tradicionales de continuidad centradas en los fallos e interrupciones de sistemas tienen que evolucionar y enfocarse en las amenazas cibernéticas dirigidas a sus datos. Los procedimientos tradicionales de recuperación tras una interrupción en los sistemas seguramente no le protegerán de una ciberamenaza que pueda dañar los datos.

El crecimiento de la transformación digital y sus falencias

En el año 2017, las empresas gastaron 1,1 billones de dólares en su afán por transformarse en organizaciones conectadas, inteligentes y con una sólida base tecnológica. En 2018 gastarán 1,3 billones más. Para el año 2021, las empresas de todo el mundo gastarán 2,1 billones de dólares al año en su intento por alcanzar esa transformación, y la cifra seguirá en aumento. Según IDC, para el año 2020 solo alrededor del 60 % de las organizaciones habrán emprendido el camino hacia la transformación digital, y el 70 % de los directores de informática habrán desarrollado una estrategia de la nube primero para aportar la agilidad necesaria de la infraestructura, lo que les brindará una enorme oportunidad para incrementar la transformación digital en los próximos tres años.

¿A qué se debe semejante gasto? Simplemente a que las empresas creen que la transformación digital es el camino a seguir en un mundo hiperconectado. Deben buscar innovación y agilidad si desean sobrevivir, y estar preparadas para salir al mercado rápidamente, a escala, con nuevos productos y servicios, al tiempo que desarrollan los conocimientos esenciales que se necesitan para alcanzar audiencias clave y abrir nuevos mercados. En este sentido, IDC considera que el apogeo de la transformación para la mayoría de las organizaciones ocurrirá cuando empleen una infraestructura con un núcleo inteligente que convierta los conocimientos sobre la actividad del negocio en inteligencia accionable, en un proceso continuo y optimizado. Eso es lo que IDC describe como la plataforma de transformación digital (ver la Figura 1). En el centro esta plataforma utiliza datos diversos, distribuidos y dinámicos para generar oportunidades.

FIGURA 1

Plataforma de transformación digital: un marco para el núcleo inteligente

Fuente: IDC, 2018

Sin datos el modelo no funciona. Los datos ya no se pueden convertir en productos ni monetizarlos. Tampoco se pueden utilizar para agilizar el negocio, por lo cual se vuelven imprescindibles para la supervivencia de la empresa, lo que hace que la integridad y la accesibilidad de los datos sean sagradas. Sin embargo, los atributos y la ubicación de los datos relevantes para una plataforma de transformación digital siguen cambiando. Los datos son cada vez más diversos, y abarcan sistemas estructurados y también no estructurados, como los datos de series temporales, los generados por máquinas y los enviados en stream. Los datos son cada vez más dinámicos, no solo en procesamiento por lote sino también inherentemente en tiempo real, mientras se generan datos de telemetría a partir de una cantidad cada vez mayor de sensores y dispositivos. Los datos cada vez se distribuyen más, y se encuentran no solo en centros de datos con ubicaciones centrales sino también en puntos periféricos, en dispositivos y en servicios en la nube. Al ser tan diversos, dinámicos y distribuidos, los datos exacerban la necesidad de implementar un programa efectivo de ciber-resiliencia.

Esto no significa que los datos sean el único factor a tener en cuenta. Para la mayor parte de las organizaciones, el camino hacia la transformación digital comienza con una serie de sistemas poco conectados que esperan poder establecerse como un sistema interconectado. Pensemos en la transformación digital como si fuera una máquina de Rube Goldberg. Recordemos que Rube Goldberg fue un ingeniero, inventor y caricaturista ganador del premio Pulitzer que se hizo famoso por sus ilustraciones de aparatos muy complejos construidos con enseres domésticos para realizar tareas mundanas. ¿Le resulta familiar? Pues así es. Las empresas están conectando sistemas de RR. HH., gestión de contratos, sistemas ERP, aplicaciones dirigidas al cliente, etc., con la esperanza de que todos funcionen en una misma dirección y orientados al negocio. Es aquí donde la transformación digital comienza a presentar un desafío para quienes están a cargo de reducir el riesgo empresarial.

¿Qué sucede cuando colocamos un palo de escoba entre los radios de una rueda de bicicleta? Si los radios no están conectados con nada, probablemente no suceda nada. Pero los radios de una rueda están conectados. Cuando uno o dos radios quedan bloqueados por un objeto extraño, la rueda completa deja de girar. Ese es el riesgo de los sistemas de negocio interconectados. Un solo sistema que falle puede interrumpir las actividades de toda la empresa.

Si lo relacionamos con la ciber-resiliencia, esto significa que cualquier proceso empresarial podría representar una puerta de entrada a otros procesos de negocio. Es decir, que la superficie de ataque de un proceso tiene el potencial de permitir el acceso lateral a prácticamente cualquier otro proceso.

Los obstáculos en el camino hacia la transformación digital

Si bien el gasto en transformación digital es impresionante, IDC ya vislumbra que habrá cada vez más presiones externas que comenzarán a tener un impacto sustancial en la estrategia de ciberseguridad de las empresas. Como ya mencionamos, la interconexión entre sistemas y el empleo constante de servicios externos tales como la nube y el IoT entrañarán riesgos para los cuales hoy muchas organizaciones no están preparadas.

IDC calcula que, para el año 2020, alrededor del 60 % de las organizaciones habrán emprendido un camino hacia la transformación digital, y el 70 % de los directores de informática habrán desarrollado una estrategia del tipo “la nube primero”. El número de por sí es impactante, pero aún no sabemos a ciencia cierta cuántas de esas organizaciones reconocen que la disponibilidad de esos datos y aplicaciones (información) es imprescindible para el éxito de la transformación digital. Sin esa disponibilidad, los datos no pueden monetizarse. Las empresas que tengan una mayor disponibilidad de la información gozarán de una ventaja competitiva relativa frente a las empresas que no la tengan. Aunque IDC ha observado un gasto cada vez mayor en torno a los productos y servicios anti DDoS, a muchos clientes les cuesta instaurar una estrategia coherente para la defensa de los datos, y disponibilidad de la información que sea rápida e integral, y que abarque todo el proceso de acceso a los datos.

Otro desafío externo para las organizaciones son las crecientes exigencias impuestas por el marco regulatorio. Para el año 2025, más del 70 % de los datos corporativos estarán sujetos al cumplimiento normativo. Estos datos no solo requieren un manejo especial sino que también generan riesgos adicionales para la organización, que podría tener que pagar multas elevadas por no proteger correctamente los datos.

El aumento en el uso de la nube y del IoT

La disponibilidad de los datos y el cumplimiento normativo son fuerzas externas que afectan significativamente al negocio pero que, al mismo tiempo, solo podrían verse afectadas de manera indirecta por el negocio. Esto sucede sobre todo porque cada vez más empresas emplean dispositivos en la nube o IoT para funciones críticas de negocio.

Hoy las empresas están utilizando la nube híbrida, y la mayoría de las aplicaciones futuras estarán basadas en la nube. En una encuesta reciente, las organizaciones indicaron que la mitad de sus cargas de trabajo están desplegadas en un modelo de nube híbrida. Esta misma cohorte prevé ejecutar el 62 % de sus cargas de trabajo en la nube híbrida en los próximos dos años. La seguridad es tanto un impulsor como un inhibidor para la adopción de la nube híbrida, ya que los datos críticos ahora se extienden por numerosas regiones geográficas, centros de datos y la nube, y deben estar protegidos de acuerdo con los requisitos corporativos, independientemente de dónde residan. Las empresas consultadas esperan aumentar un 40 % el gasto en servicios de datos para la nube híbrida en los próximos 12 meses. Las principales prioridades son la copia de seguridad y la restauración, además de las evaluaciones del coste/valor de los datos.

Cada vez más las empresas están recabando datos sensibles no solo provenientes de la nube sino también de dispositivos del IoT. Si bien estos dispositivos suelen tener un poder de procesamiento inferior al de los sistemas completos, los atacantes han demostrado tener la capacidad de emplear dispositivos de IoT como parte de su estrategia de ataque. Esta capacidad, combinada con una carencia general de seguridad en torno a los dispositivos de IoT, implica que las organizaciones deben determinar cómo defender mejor los dispositivos de IoT que pueden ser difíciles de acceder, supervisar y resguardar, además de los dispositivos tradicionales de computación.

Mayor complejidad de los fallos

Si bien IDC observa que las empresas muestran más confianza en su capacidad de brindar seguridad a la nube, y la tasa de adopción de la nube y de soluciones de seguridad basadas en la nube no ha dejado de aumentar, un desafío para el cual las empresas parecen estar menos preparadas que nunca es la creciente complejidad de las interrupciones.

En una encuesta reciente de IDC a sus clientes, el 56 % de los consultados indicaron que habían sufrido un ataque DDoS que duró de 5 a 24 horas, el 8 % afirmaron que habían sufrido un ataque que duró de 1 a 7 días, y lo más alarmante es que el 6 % de los encuestados dijeron haber sufrido un ataque que duró más de 8 días.

La copia de seguridad y la recuperación ante desastres son protecciones insuficientes a la hora de luchar contra las amenazas modernas. La mejor práctica de IDC recomienda un RTO (tiempo de recuperación objetivo) de una hora para las aplicaciones de funcionalidad crítica y de cuatro horas para aplicaciones no críticas. Es posible que ciertas copias de momentos determinados (instantáneas) sean incompletas o ineficientes, lo que las hace vulnerables a los ataques cuando no están diseñadas correctamente. El marco por lo general está diseñado para una restauración al nivel del sistema y no para una restauración del entorno, por ejemplo, daños en la plataforma o configuración. Un mantenimiento inadecuado y la falta de higiene en las pruebas también pueden sabotear sólidos esquemas de protección de las instantáneas.

Las investigaciones de IDC revelan que el coste “promedio” del tiempo de inactividad supera los 200 000 dólares por hora, aunque varía según el tamaño y el sector de la empresa. Por lo general, estos costes se pueden utilizar para ayudar a orientar a las organizaciones a la hora de tomar decisiones

vinculadas a construir planes de recuperación e infraestructura. Las estimaciones de costes incluyen la pérdida de ingresos real y los costes de la recuperación, entre ellos, los gastos propios del cumplimiento regulatorio, que suelen ser elevados. Estas estimaciones no contemplan el coste vinculado a la reputación y el daño a la marca a largo plazo que pueden ocurrir como resultado de una brecha que roce lo vergonzoso, pero sí se pueden utilizar para ayudar a determinar el gasto organizativo adecuado en una estrategia de infraestructura para remediar una brecha. Un ejemplo reciente e ilustrativo de ransomware es el que ha sufrido la ciudad de Atlanta, que acaba de gastar casi 3 millones de dólares en medidas de emergencia durante las tres semanas posteriores a un incidente de ransomware que inhabilitó algunos servicios urbanos. La ciudad ha solicitado otros 9,5 millones de dólares para recuperar y reforzar las defensas. Si bien esta suma adicional de recursos puede parecer extrema, si sirve para evitar otros 3 millones de dólares de gastos ocasionados por ransomware en el futuro inmediato, un desembolso único de 9,5 millones es más que razonable.

Cada vez más ataques avanzados

IDC también sigue notando un aumento en la cantidad de ataques avanzados. Las estadísticas del sector muestran que muchos ataques no se detectan durante más de 200 días. Con tanto tiempo para esconderse en una red, los atacantes pueden instalar malware que se abra paso a través de los sistemas de copia de seguridad. Como resultado, los datos de restauración también se infectan. Los ataques pueden permanecer latentes durante semanas o meses, y esto permite que el malware se propague a todo el sistema. Incluso después de que se detecte un ataque, puede resultar extremadamente difícil eliminar el malware que esté tan diseminado por toda la empresa.

DESCRIPCIÓN DE LA SITUACIÓN

El concepto de ciber-resiliencia

Cada vez existen más recursos de infraestructura disponibles en la nube y en dispositivos del IoT. Sin embargo, las defensas tradicionales para contrarrestar efectivamente las amenazas que van surgiendo no son eficaces, por lo cual las empresas deben adoptar una nueva postura con respecto a la seguridad. El panorama actual de las amenazas requiere una solución integrada que abarque todo el ciclo de vida de los datos. Las empresas deben centrarse en acortar las etapas del ciclo de vida entre defensa y detección y entre respuesta y restauración para lograr una capacidad de ciber-resiliencia.

El marco de ciber-resiliencia

La ciber-resiliencia es un marco de medición diseñado para ayudar a las empresas a hacer frente a los ataques. No se trata de una única capa de protección o de un único producto sino de una forma en que las empresas pueden estructurar sus defensas de manera que ningún evento resulte catastrófico. La ciber-resiliencia es un proceso iterativo que ofrece la forma de recuperarse tras un ataque. En comparación con las defensas tradicionales que ya no sirven una vez ocurrido el incidente, la ciber-resiliencia posibilita una vigilancia constante en toda la organización.

El marco de ciber-resiliencia está compuesto por cinco elementos (ver la Figura 2):

Identificar: correlacionar activos y procesos críticos, evaluar el riesgo y la preparación para afrontarlo, etc.

Proteger: primera línea tradicional de los mecanismos de seguridad defensivos

Detectar: análisis de la seguridad

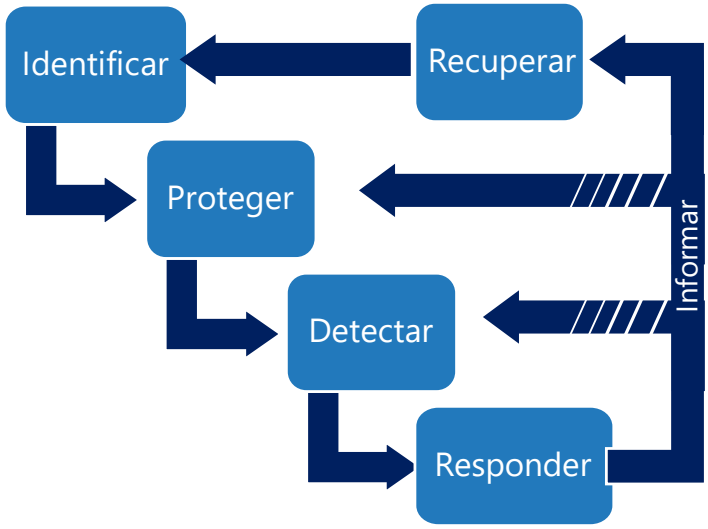
Responder: respuesta ante una brecha de seguridad o fallo

Restaurar: mecanismos coordinados de restauración

La principal ventaja del marco de ciber-resiliencia es que está dirigido al negocio. Tradicionalmente, la seguridad funcionaba como un componente adicional del negocio. La ciber-resiliencia integra la seguridad dentro de la empresa en sí, lo que permite que los cinco componentes estén presentes en todas las áreas del negocio.

FIGURA 2

Marco de ciber-resiliencia



Fuente: IDC, 2018

Evento versus consecuencias

Una y otra vez el sector ha demostrado que los ataques tendrán éxito. La seguridad es compleja, y sencillamente no hay manera de probar que un entorno sea seguro. Los atacantes siguen usando métodos innovadores para irrumpir en las organizaciones, recurriendo a cualquier táctica que sea necesaria para lanzar un ataque con éxito. Lo mejor que puede esperar una organización es contar con una infraestructura reforzada, funciones y procesos auditables, usuarios cualificados, personal de seguridad destacado y procesos de monitorización continua. Estar en esa posición sería fantástico, pero lo primordial para casi todas las organizaciones es crear un enfoque renovado sobre lo que sucede después de un ataque. Si con una lista variada de controles y verificaciones ya sabemos que un ataque tendrá éxito en algún punto, ¿no es razonable estar preparado para las consecuencias? Cuando un ataque tiene éxito, las empresas deben hallar una manera de acortar el ciclo entre detección y respuesta y el ciclo entre respuesta y restauración. Cuanto más cerca se pueda estar de lograr una continuidad de las operaciones, mejor preparados estaremos incluso después de sufrir un ciberataque.

La naturaleza misma del negocio es implacable. No le importa cuán avanzado sea un ataque, ni cómo ha podido infiltrarse el atacante en la organización. El negocio debe seguir funcionando. Al emplear estrategias para minimizar los tiempos operativos en la detección, respuesta y restauración, las organizaciones no solo pueden reducir el coste de un incidente sino también, con el tiempo, crear una ventaja competitiva. Según IDC, las empresas que puedan minimizar las interrupciones tendrán una enorme ventaja con respecto a las que no están bien preparadas para generar confianza entre sus consumidores y socios de negocio.

PERSPECTIVAS FUTURAS

Los cinco componentes clave de la ciber-resiliencia

Aunque el marco de ciber-resiliencia pueda parecer intuitivo, debe implementarse por medio de una cuidadosa selección de tecnologías. No existe un único producto que pueda crear un entorno ciber-resiliente, sino que existen tecnologías clave que una organización puede emplear para afrontar una posible interrupción en las actividades como consecuencia de un ciberataque. Las cinco tecnologías que se describen en las siguientes secciones son fundamentales para que las organizaciones puedan crear un entorno resiliente.

Automatización y orquestación para la recuperación de plataformas y datos de aplicaciones

El término *automatización* siempre ha sido aterrador para los profesionales de seguridad, y ha generado preocupación en torno a la respuesta automática en todo el sector desde que existen las soluciones automatizadas. Pero en el entorno ampliamente automatizado de los ataques actuales, la automatización de la inteligencia es fundamental. En lugar de emplear la automatización como la solución, la orquestación y la automatización deben ser parte de la respuesta.

La orquestación no consiste en sacar a los humanos de la ecuación ni habilitar cambios de políticas a ciegas, sino que se trata de aumentar la cantidad de analistas, brindándoles rápido acceso a la información y la capacidad de responder con mayor rapidez que si lo hicieran manualmente. Además, para que la recuperación de aplicaciones sea efectiva es imprescindible un restablecimiento gradual de los sistemas y datos interconectados. El restablecimiento manual de esos sistemas es propenso al error humano, mientras que la codificación de los procesos de restauración mediante plantillas de software que se validan y evalúan puede mitigar el riesgo en esos procesos.

Protección perimetral en forma de copia a prueba de fallos contra la propagación del malware

La protección del perímetro (“Air gap”) es una medida de seguridad que consiste en separar sistemas o redes de otros sistemas o redes, por medios físicos o virtuales. Las empresas, por ejemplo, pueden optar por aislar completamente las redes o sistemas que contienen datos altamente sensibles de la red operativa que se utiliza todos los días.

Pese a la desaparición del perímetro y a la fluidez en los datos que las empresas desean lograr en toda su organización, la capacidad de crear segmentos aislados de la red es más importante que nunca. Como hemos visto en recientes infecciones de ransomware, un malware automatizado puede estar diseñado para atravesar la red y causar estragos rápidamente. De este modo la organización queda expuesta, tanto internamente como quizás también externamente, según el sistema o los sistemas afectados. En la actualidad, la mejor práctica consiste en crear una copia de protección

perimetral de los datos críticos a fin de mitigar la exposición externa, proteger a la organización de interrupciones en sus operaciones y evitar costes innecesarios.

Tecnología de almacenamiento inmutable o WORM para evitar que los datos se corrompan o se borren

El éxito actual de los ataques de ransomware, como NotPetya, han puesto de manifiesto la necesidad de contar con una protección más fuerte contra la corrupción o el borrado de datos. Todos sabemos que los atacantes procuran borrar logs para cubrir sus ataques, pero el borrado o la corrupción de datos puede destruir un negocio. Después de sufrir los efectos de WannaCry y otros ataques recientes de ransomware, muchas organizaciones se dieron cuenta de que, aunque pagaran el rescate, los atacantes no les devolvían la clave de cifrado. Y, en muchos casos, la clave que les proporcionaba un atacante no funcionaba.

Las organizaciones deben contar con tecnologías que les garanticen datos inalterables. Las tecnologías de almacenamiento inmutables o de "escribir una vez, leer muchas" (WORM, por sus siglas en inglés) pueden responder a esta necesidad, al permitir que las empresas conserven la integridad de sus datos y mantengan una resiliencia empresarial contra lo que han sido algunos de los ataques más paralizantes de los últimos tiempos. Existen muchas formas de tecnología WORM en la capa de software y en la capa de hardware, y ambas sirven para garantizar que los datos no sean manipulados y para proporcionar una cadena de custodia electrónica.

Copias de momentos determinados y verificación de datos eficientes para identificar rápidamente los datos recuperables

Una vez ocurrido el ataque, las organizaciones necesitan una manera de validar y restaurar rápidamente una copia válida de los datos. Como ya hemos mencionado, muchos atacantes viven dentro de las redes durante casi un año, lo que significa que con frecuencia las copias de seguridad también están infectadas. Por este motivo, se necesita una tecnología de instantáneas (de momentos determinados) muy eficiente para conservar múltiples copias de los datos. También es necesario realizar una verificación constante de los datos en esas copias para identificar de manera proactiva posibles infecciones y tomar medidas correctivas. También puede ser de utilidad identificar rápidamente una copia de datos válida para el proceso de restauración. Existen distintos enfoques para respaldar la verificación de datos, con características incorporadas tanto en hardware como en software para garantizar que los datos no han sido infectados.

La verificación de datos es fundamental para los procesos de evaluación de desastres y restablecimiento de las operaciones. En primer lugar, todos deseamos garantizar que los datos replicados/de copia de seguridad tengan integridad y que la replicación o copia de seguridad se lleve a cabo correctamente. En segundo lugar, deseamos inspeccionar los datos replicados/de copia de seguridad para garantizar que la misma infección que afectó los datos de producción no se haya propagado a los datos replicados/de copia de seguridad. Según el sistema sobre el que se está realizando la copia de seguridad, los usuarios pueden emplear muchas técnicas de verificación de datos. Por ejemplo, un sistema de base de datos puede contar con herramientas nativas de selección e inspección que sirven para aportar capacidades dentro de una solución más amplia de protección de datos.

Informes reglamentarios y garantías de seguridad

Si bien es cierto que el cumplimiento regulatorio suele tener una mala reputación como un elemento de la lista de verificación que no sirve para mejorar la seguridad global de una organización, la

realidad es que validar que haya controles adecuados de los datos, ya instaurados y funcionando correctamente, puede resultar extremadamente efectivo. Además, al incrementarse el monto de las multas por incumplimiento, contar con un sistema eficaz de informes puede ayudar a las empresas a demostrar que están cumpliendo con las normativas y ahorrarles el tiempo y dinero asociados a costosas auditorías y posibles sanciones.

DESAFÍOS Y OPORTUNIDADES

La ciberseguridad es el principal desafío en el clima actual de los negocios. El ritmo y el volumen de las amenazas a la seguridad son obstáculos que las organizaciones de todos los tamaños deben sortear, por lo cual la planificación y el despliegue de estrategias de ciber-resiliencia ahora cobran mucha más importancia que nunca. Una estrategia efectiva de ciber-resiliencia reúne diferentes componentes, tiene amplio alcance y abarca muchos grupos de interés, que no son solo los profesionales de seguridad, operaciones, ingeniería, asuntos legales y gestión del riesgo, sino también los propietarios de los datos y ejecutivos de líneas de negocio. Para instaurar una estrategia de este tipo se requiere colaboración y planificación en todas las empresas, con diferentes prioridades y profundidad de conocimientos. Esta dinámica al nivel de la organización constituye un desafío que se suele presentar en las empresas más grandes, pero que se puede afrontar con una planificación estratégica de nivel C y estableciendo prioridades.

CONCLUSIÓN

La ciber-resiliencia es esencial para la disponibilidad de los datos y aplicaciones. También es un componente esencial del camino hacia la transformación digital. Sin medidas de ciber-resiliencia adecuadas, las organizaciones serán cada vez más susceptibles a ataques que pueden poner en jaque a una empresa. Además de los ataques maliciosos, al incrementarse los requisitos en materia de cumplimiento normativo que se extienden a muchas regiones geográficas y sectores, las empresas corren el riesgo de tener que pagar cuantiosas multas si no cuentan con una validación continua de los controles.

La postura es más que la simple detección de malware, copia de seguridad o DR: se trata de un enfoque integrado del ciclo de vida para garantizar la disponibilidad de los datos contra todas las amenazas, incluida la plataforma. La ciber-resiliencia debe abarcar repositorios tanto locales como en la nube. Los departamentos de TI deben adoptar una postura integral hacia la ciber-resiliencia y buscar productos que se adapten al abanico completo de ciberamenazas.

Por último, la ciber-resiliencia es un marco que sirve para recuperarse de los ataques. Sin embargo, se necesita una sólida colección de tecnologías clave para poder abordar cada componente del marco. Ya no se puede describir la seguridad en términos de distintos niveles de confidencialidad, integridad y accesibilidad, sino que debe abarcar estos tres pilares todo el tiempo. Las organizaciones que implementen medidas de ciber-resiliencia tendrán una ventaja competitiva en el futuro, cuando los clientes se topen con interrupciones en la disponibilidad de los negocios. Una organización resiliente será aquella que pueda adaptarse y recuperarse de los ataques.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com