El día después

Recuperación, resistencia y resiliencia después de un ciberataque industrial

En la alarmante realidad actual, los programas adecuados de respuesta y recuperación ante la amenaza del ransomware deben ser considerados como facilitadores cruciales del negocio. Cuando las operaciones esenciales y la OT de una organización se ven envueltas en esta situación, improvisar no es la mejor solución.

Cuando un importante sistema de oleoductos sufrió un ataque de ransomware, las operaciones se paralizaron durante casi una semana provocando una importante escasez de combustible. El ataque — resultado de una única contraseña comprometida — se enfocó en los sistemas informáticos del oleoducto, pero los sistemas de tecnología operativa (OT) que transportan el petróleo no eran el principal objetivo. Los atacantes robaron datos e infectaron la red informática con un ransomware y, para evitar que se propagara a la OT, se decidió cerrar el oleoducto.

Los ataques de ransomware, que se propagan por la red y cifran los datos, están aumentando en todo el mundo. Hoy en día, resulta casi imposible recuperar la información empresarial debido a que estos ataques son cada vez más sofisticados y, por lo general, los atacantes exigen el pago de un rescate en bitcoins para liberar una clave que permita desencriptar los datos. La organización atacada debe pagar para recuperar el acceso a sus datos o esperar a recuperarlos de otra forma, por ejemplo, mediante aplicaciones de copias de seguridad.

A medida que se disparan los ataques de ransomware, los rescates podrían costar a las empresas un total de 265.000 millones de dólares de aquí a 2031, según Cybersecurity Ventures, que predice que los costos aumentarán un 30% anual en los próximos 10 años.[1]

Gestionar de forma eficaz un ataque de este tipo es fundamental para hacer frente al impacto inicial en las operaciones y los costos, y para ayudar a minimizar una recuperación que puede implicar días o semanas de capacidades limitadas y servicios interrumpidos. Las empresas deben prepararse no sólo para responder a un ataque, sino también para recuperarse rápidamente, y esto es muy importante en el ámbito de las operaciones remotas, en el que suelen intervenir procesos físicos. Aunque muchas empresas se esfuerzan por mejorar sus programas de prevención y respuesta, también necesitan capacidades de recuperación adecuadas.

Las medidas de recuperación para restablecer las operaciones con rapidez requieren una evaluación precisa para determinar que se ha eliminado la amenaza subyacente inicial. No es una tarea fácil en medio de la necesidad de adoptar medidas de respuesta inmediatas que incluyan el bloqueo de los sistemas internos y los elementos clave de la red empresarial, junto con cambios precipitados de las políticas.

También es crucial que el complicado camino de vuelta a la normalidad incluya cambios clave en la seguridad. El proceso de respuesta y recuperación en estas condiciones típicas puede crear desafíos muy complejos.

¿Qué es la tecnología operativa?

La tecnología operativa (OT) implica el uso de hardware y software para controlar equipos industriales. Hoy en día, la seguridad de la OT se está volviendo vital a medida que la OT se integra con la IT para crear una convergencia IT/OT. Como las redes de TI y OT ya no pueden separarse, los ataques a la TI afectan a la OT y viceversa.

Esto ofrece a los atacantes una mayor superficie de ataque y hace que un enfoque de seguridad integral sea fundamental. Sin embargo, en la actualidad las empresas no le están dando la prioridad que deberían y la OT está siendo cada vez más el blanco de ataques perjudiciales.

[1] David Braue, “Global ransomware damage costs predicted to exceed $265 billion by 2031,” Cybersecurity Ventures, 2 de junio, 2022.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

La seguridad de las OT modernas es ahora el precio de hacer negocios

En la actualidad, invertir en la protección adecuada es el precio de hacer negocios. Es importante comprender cómo se comunican las máquinas y aplicaciones de IT y OT conectadas, el estado de su segmentación de red y los riesgos actuales a medida que se disparan los ataques de ransomware.

Aunque las IT son la columna vertebral de cualquier organización, las empresas dedicadas a la manufactura, la minería, el petróleo y el gas, los servicios públicos y el transporte dependen en gran medida de la OT para conectar, supervisar, gestionar y proteger sus operaciones industriales. Y aunque la OT suele asociarse a las actividades industriales, otros sectores persiguen la eficiencia a través de la OT, como los gigantes del comercio electrónico que dependen de depósitos automatizados y operaciones conectadas digitalmente.

Es posible que su organización cuente con activos de OT aunque no esté dirigida por esta tecnología. Los dispositivos médicos, la automatización de almacenes, los aparatos de edificios inteligentes y los grandes sistemas de aire acondicionado son OT que podrían verse afectados en un ataque. Cuanto antes identifique y comprenda la importancia de los sistemas OT en su organización, antes podrá mejorar su ciber-resiliencia.

Aumentan las amenazas a las infraestructuras críticas y a la seguridad pública

Mientras que las alteraciones y los compromisos de IT pueden tener impactos generalizados obvios que afectan a los servicios al consumidor, a la seguridad de los datos y a la seguridad pública, los ataques de ransomware que alteran los sistemas OT de infraestructuras críticas también pueden crear trastornos y amenazas para el público.

Por ejemplo, un ataque que inhabilite una importante empresa de suministro eléctrico puede tener graves consecuencias para la seguridad pública en medio de la falta de servicios críticos, por lo que es primordial una rápida recuperación. Consideremos el impacto público de un ataque que interrumpe los servicios públicos de agua durante días o semanas. La naturaleza y las repercusiones de los ciberataques actuales son cada vez más amplias y pueden suponer — más allá de los impactos en las cadenas de suministro de manufactura que entregan productos de consumo esenciales — una amenaza para los ecosistemas públicos que prestan servicio a grandes áreas geográficas y poblaciones.

Un buen ejemplo es el ataque WannaCry de 2017, que infectó equipos en más de 150 países. Fue uno de los ataques de ransomware de mayor envergadura hasta la fecha e interrumpió los servicios sanitarios, las telecomunicaciones y el transporte. El daño a los servicios públicos y a la seguridad no tenía precedentes[2].

Mientras que las empresas pueden depender de un único proveedor de IT principal, esas mismas empresas podrían depender de 10 o 20 proveedores de sistemas de OT interconectados, lo que complica — y requiere conocimientos específicos de recuperación — en un ataque con técnicas sofisticadas.

Cuidado: el pago de un rescate no garantiza nada

El proceso de recuperación para restablecer y volver a poner en funcionamiento la actividad normal suele requerir actualizar — o reconstruir desde cero — las bases de datos, los sistemas empresariales y las operaciones interrumpidas. Existe una alta probabilidad de que, incluso si se paga un rescate, o si una empresa recupera los datos cifrados sin tener que pagar, algunos segmentos de la empresa se enfrentarán a una reconstrucción costosa y lenta que tardará meses en completarse.

Desafortunadamente, las empresas suelen asumir por error que las operaciones se restablecen de forma inmediata si pagan el rescate y obtienen la clave de recuperación para desencriptar los datos.

Un análisis exhaustivo de cómo se produjo la vulneración — y la identificación de las lagunas de seguridad — es crucial para mejorar las medidas de protección de las OT y ayudar a minimizar los riesgos futuros. En la mayoría de los casos, las empresas cuentan con planes adecuados de continuidad de negocio y recuperación ante desastres para cubrir riesgos convencionales como fallos técnicos o catástrofes naturales. Pero es posible que carezcan de un manual completo — y continuamente actualizado — que aborde los graves trastornos que puede provocar un ataque de ransomware.

El éxito a la hora de repeler un ataque hoy no garantiza el éxito de mañana. Las vulnerabilidades de las OT y las superficies de ataque cambian y se multiplican a medida que las empresas "derivan" o evolucionan. Por lo tanto, es fundamental probar los planes de acción y las simulaciones de recuperación.

Para la mayoría de los ejecutivos, un simulacro de ataque de ransomware suele ser un acontecimiento revelador, que pone de manifiesto tanto la falta de medidas de protección de las OT como las lagunas que pueden impedir la recuperación. Los líderes que se reúnen en una sala de simulación podrían estar volando a ciegas al darse cuenta de que no pueden identificar rápidamente el impacto de un ataque o gestionar escenarios extremos.

Las primeras 72 horas son clave para la recuperación

Las firmas de KPMG han sido testigo de la falta de una planificación sólida y de capacidades de copia de seguridad de OT, así como del costoso impacto en el tiempo de recuperación. La necesidad de rapidez en la recuperación es fundamental. Pero demasiadas organizaciones asumen por error que la recuperación requerirá varias semanas para volver a la normalidad, en lugar de varios meses o más. El resultado suele ser una respuesta lenta a la hora de identificar un ataque real, los activos y operaciones empresariales afectados y la secuencia de acontecimientos que debe desarrollarse sin demora.

Cuando se produce un ataque, las 72 horas iniciales son críticas, pero nunca fáciles para los líderes, normalmente presas del pánico, que de repente se ven inmersos en un escenario catastrófico que exige negociar con un grupo de delincuencia organizada mientras intentan comprender el alcance del ataque.

[2] Jennifer Gregory, "WannaCry: How the Widespread Ransomware Changed Cybersecurity," Security Intelligence, 30 de octubre, 2020.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

La necesidad de programas de recuperación de OT bien estructurados se ha vuelto indispensable, teniendo en cuenta todo el ecosistema en términos de procesos y activos críticos, capacidades de apoyo y copia de seguridad, y la secuencia necesaria para restaurar las operaciones con rapidez. Las funciones y responsabilidades deben estar definidas con claridad. También es imprescindible un plan de comunicación con todos los stakeholders.

Las empresas deben comprender que la recuperación del OT plantea desafíos únicos que deben abordarse con antelación y en función de las condiciones que varían de un sector a otro. La simple detención de los sistemas o la desconexión de elementos de la red de la empresa no siempre es posible en el caso de las OT, dado que pueden controlar sistemas críticos y procesos físicos sensibles.

Un enfoque demasiado simplista consistente en recurrir al funcionamiento manual durante una crisis puede resultar imposible por muchas razones. Por ejemplo, los almacenes de productos automatizados digitalmente suelen carecer de personal para la entrega manual. En el caso de un distribuidor eléctrico, la organización puede carecer de personal cualificado en operaciones manuales.

La recuperación rápida exige una estrecha colaboración

En el modo de recuperación, los especialistas en ciberseguridad deben colaborar con los especialistas en OT desde el principio para elaborar escenarios específicos y aprovechar los planes existentes. Al mismo tiempo, es probable que los ingenieros y administradores de OT dispongan de protocolos para otros tipos de situaciones de emergencia que puedan respaldar los esfuerzos de respuesta y recuperación.

Inicialmente, considere la posibilidad de clasificar el incidente y revisar los procedimientos y su lista de respuestas, ayudando a garantizar la alineación con las mejores prácticas y las normas de la organización. Esto incluye las tecnologías y herramientas existentes y las que puedan proporcionar otros.

Con esta información recopilada, identifique a los principales afectados y la "cadena de custodia", es decir, las pruebas digitales y físicas relacionadas con el ataque. Para los implicados en la cadena de custodia, el due diligence en la recolección de evidencias digitales es crítico para evitar comprometer las pruebas. El enfoque de recuperación bien establecido de KPMG se estructura en cinco fases.

Fase 1: Respuesta | Pasos para responder a un ciberataque

- No se deje llevar por el pánico y mantenga la mente fría.
- Identifique y analice la amenaza.
- Informe del incidente.

Fase 2: Reparación | Pasos para reparar la causa raíz

- Contener y erradicar la amenaza.
- Hacer un registro detallado del ataque.

Fase 3.1: Recuperación táctica | Pasos para recuperarse de un ataque

- Determinar el impacto del ciberataque.
- Identificar la huella del adversario en la infraestructura, los canales de mando y control, y las herramientas y técnicas.
- Utilizar toda la información disponible para crear el plan de restauración.
- Comenzar a ejecutar la restauración validando y aplicando contramedidas de reparación en coordinación con el equipo de respuesta a incidentes y otro personal de seguridad de la información.
- Documentar cualquier problema que surja, cualquier indicador de compromiso y las dependencias recientemente identificadas.

Fase 3.2: Recuperación estratégica | Pasos para recuperarse de un ataque

- Desarrollar un plan para corregir la causa raíz del ciberataque.
- Implementar cambios para reforzar la postura de seguridad de la organización.
- Una vez completada la recuperación, revise las métricas recopiladas.

Fase 4: Resistencia | Mejorar la postura para resistir un futuro ataque

- Priorizar las capacidades para mejorar la postura cibernética.
- Desarrollar un diseño pragmático y un plan de implantación.
- Implementar las capacidades de forma programática.
- Validar la eficacia con pruebas a nivel reglamentario.

Fase 5: Resiliencia | Mantener la disciplina para permanecer resiliente ante un ataque

- Establecer una solución con herramientas y un equipo para controlar la desviación de la política.
- Agregar y analizar las señales para identificar los problemas.
- Priorizar los problemas e integrarlos en los procesos de corrección existentes.
- Realizar un seguimiento de las medidas correctoras hasta su finalización e informar sobre los cuadros de mando ejecutivos.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Existen diferentes enfoques para ayudar a prepararse contra los ataques. Las actividades potenciales se agrupan en tres categorías, y recomendamos centrarse en las actividades reactivas.

Tras el éxito de un ataque, es importante poner en marcha contramedidas y contener el ataque. Según nuestra experiencia, nunca es posible descubrir y eliminar de antemano todos los puntos débiles. Si se produce un ataque, hay que eliminar el peligro. Por eso nuestro enfoque de recuperación forma parte de las actividades reactivas:

Prevención	Proacción	Reacción
Prevenir los ataques, minimizar la superficie de ataque	**Tomar medidas para que un ataque sea menos severo**	**Ejecutar escenarios de un ataque exitoso**

Faltan capacidades de recuperación mientras se disparan las amenazas

Las empresas avanzan a buen ritmo en el desarrollo de capacidades de respuesta más adecuadas. Pero cuidado: las capacidades de *recuperación* apropiadas siguen mostrando margen de mejora. En nuestra opinión, la planificación típica de la continuidad de la actividad empresarial no sigue el ritmo del cambiante entorno cibernético. Las empresas deben empezar a pensar de forma diferente para comprender el camino fundamental que se necesita para una recuperación eficaz.

Las organizaciones deben empezar a planificar para el peor de los casos, que supone una amenaza potencial para la organización. Además, deben estar preparadas con un equipo de apoyo que pueda intervenir y proporcionar recuperación ante desastres en el momento en que se le avise. Numerosas empresas ofrecen capacidades de respuesta cibernética subcontratadas, pero muy pocas ofrecen capacidades de recuperación cibernética y habilidades alineadas con el entorno de amenazas actual.

Por último, es fundamental probar regularmente las capacidades de recuperación. Disponer de un plan de recuperación ante desastres y de capacidad de recuperación sin realizar pruebas exhaustivas no es una forma recomendable de enfrentarse a las amenazas actuales.

No hay tiempo que perder: la frecuencia y el impacto de los ataques van en aumento

Estos desafíos empresariales son únicos. Buscar soluciones cuando una organización está paralizada y el tiempo no deja de correr ante una amenaza no es el típico dilema de un CEO.

Los líderes empresariales deben ser defensores del cambio y mostrar un sentido de urgencia a la hora de promover estrategias de respuesta de OT, planes de acción inteligentes y mecanismos de recuperación. Con el aumento de los ataques de ransomware, la capacidad de responder y recuperarse ágilmente debería considerarse una ventaja competitiva.

Por desgracia, muchas organizaciones creen que se librarán de un ataque de ransomware y siguen dedicando recursos e inversión inadecuados al problema.

Las empresas con visión de futuro están elevando sus apuestas. Y hay poco tiempo que perder, ya que los ciberdelincuentes siguen haciendo lo mismo con esquemas de ransomware cada vez más lucrativos. Las empresas innovadoras que evalúan las profundas amenazas actuales a la seguridad operativa no piensan si sucederán estos ataques, sino en cuándo ocurrirán.

[2] "Executive Order 14028, Improving the Nation's Cybersecurity", NIST. (8 de noviembre, 2021)

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Preparación para la recuperación de OT: estar listo para cualquier cosa

Cuando se produce una emergencia, una incidencia en la producción, un ataque de ransomware o cualquier otro evento, es necesario volver a poner en marcha los procesos de OT y producción lo antes posible. Eso significa estar siempre listo para cualquier cosa. Y dado el cambio constante en los entornos OT de hoy en día, la preparación frente al ransomware no puede ser algo que se aborde trimestral o anualmente. La preparación debe ser un objetivo del día a día.

Siempre hay que tener en cuenta el alcance de las amenazas, en constante crecimiento y evolución. No se trata solo de los sistemas locales, sino también de los sistemas IT y OT y sus componentes OT conectados, como el sistema de control y los controladores lógicos programables (PLC).

Lo que se necesita son capacidades para recuperar sistemas de producción modernos y antiguos, máquinas virtuales (VM), contenedores, controladores lógicos programables (PLC) y aplicaciones desde cualquier lugar en una arquitectura híbrida y moderna de IT/OT. La nube también se ha convertido en parte de los sistemas modernos actuales o de las infraestructuras OT y estas plataformas también deben tenerse en cuenta.

Esta complejidad pone de manifiesto que en estos momentos los enfoques únicos suelen ser inadecuados para los centros de producción y OT.Para estar preparados ante una emergencia, deben alcanzarse los siguientes puntos clave de preparación para la recuperación, con el fin de restablecer las operaciones en un plazo razonable:

En primer lugar, debe conocer todos sus activos vitales para IT y OT y sus dependencias mutuas. Mantenga también actualizados los informes de vulnerabilidad de sus sistemas esenciales y evalúelos con regularidad. Sin este tipo de información, creemos que la recuperación en un plazo aceptable es imposible.

Defina los objetivos de recuperación cuando se restablezca de un incidente. Por ejemplo, la capacidad de recuperación debe dar prioridad a la seguridad humana y medioambiental antes de reiniciar la operación de OT que se vio afectada por el evento de ciberseguridad.

Desarrollar un plan de recuperación ante desastres (DRP) y un plan de continuidad del negocio (BCP), o ambos, para preparar a la organización de IT y OT para responder adecuadamente a un incidente importante de ciberseguridad. Es fundamental que la IT y la OT no se consideren por separado, sino en conjunto (objetivo de convergencia IT/OT).

Establecer sistemas y procesos de copias de seguridad para respaldar el estado de los sistemas OT pertinentes (críticos) (sistemas heredados, Windows/Un ix, PLC, sistemas virtuales, etc.), datos, archivos de configuración y programas para apoyar la recuperación oportuna a un buen estado.

Cree conciencia de las amenazas (no sólo para IT), capacite a sus empleados de OT, simule el peor escenario posible y aprenda de los resultados.

En caso de que aún no haya implementado estos puntos, le recomendamos que lo haga lo antes posible teniendo en cuenta que el entorno de amenazas de OT actual está en constante aumento. Aconsejamos centrarse en los sistemas de OT más importantes en la primera oleada de preparación para la recuperación, seguidos de los medianamente críticos y los menos críticos en las oleadas dos y tres.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Para más información puede contactarse con:

Walter Risi
Partner, KPMG en Argentina
Líder Global de Ciberseguridad IIoT,
KPMG International

E: wrisi@kpmg.com.ar

Marko Vogel
Socio,
KPMG en Alemania

E: mvogel@kpmg.com

Jason Haward-Grau
Director,
KPMG en EE.UU. y Líder Global de Recuperación Cibernética
KPMG International

E: jhawardgrau@kpmg.com

En Chile:

Erick Palencia
Managing Director
Advisory – Consulting
KPMG en Chile

E: erickpalencia@kpmg.com

Algunos o todos los servicios aquí descritos pueden no estar permitidos para los clientes de auditoría de KPMG y sus filiales o entidades relacionadas.

home.kpmg/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2022 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved. KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity.

KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit home.kpmg/governance. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Designed by Evalueserve.
Publication name: The Day After |Publication number: 138514-G |Publication date: December 2022