RESTAURACIÓN DE SERVIDORES COMPLETA CON HEWLETT PACKARD ENTERPRISE

HPE OFRECE CAPACIDADES DE RECUPERACIÓN Y SEGURIDAD LÍDERES DEL SECTOR A TRAVÉS DE SU CARTERA DE PRODUCTOS PROLIANT GEN10

RESUMEN

La proliferación de ataques cibernéticos causa alarma en empresas y gobiernos mundiales por igual. Estados nación lanzan ataques a infraestructuras de TI gubernamentales para deshabilitar sistemas y paralizar los esfuerzos de seguridad nacional. Piratas informáticos sofisticados atacan entidades corporativas para robar propiedad intelectual, robar datos de clientes o retener información para exigir el pago de rescates.

Los ataques distribuidos de denegación de servicios (DDoS) y otros vectores de ataque tradicionales están dando paso con rapidez a otros medios más insidiosos. Más del 91 % de los ataques de ransomware llegan a través de archivos adjuntos a correos electrónicos.[1] Las organizaciones, con independencia de su tamaño, parecen reconocer este hecho, pues se destinarán más de 10 000 millones de dólares estadounidenses a formación en seguridad para sus empleados.[2] Sin embargo, a pesar de todos estos esfuerzos, los ataques de ransomware se han multiplicado por 15 en tan solo dos años y, el año próximo, se prevé que se producirá un ataque de ransomware empresarial cada 14 segundos.[3] En términos más generales, el coste total de la ciberseguridad para la economía mundial se disparará hasta los 6 billones de dólares estadounidenses en 2021 y hasta los 8 billones de dólares estadounidenses en 2022.[4]

La pregunta no es «si» tu centro de datos va a ser objeto de un ataque, sino «cuándo». Aunque una penetración en la infraestructura de TI puede ser inevitable, sufrir los efectos nefastos de un acceso no autorizado sí se puede evitar por completo. La pregunta que las empresas de todos los tamaños se están planteando es: «¿con qué rapidez puede mi organización de TI detectar, aislar y eliminar malware, restaurar la infraestructura a un estado correcto conocido y reinstalar los sistemas operativos, las aplicaciones y los datos?» Según un estudio llevado a cabo por Accenture, el tiempo de recuperación de un ataque por ransomware medio es de 23 días. ¿El coste medio? 2,4 millones de dólares estadounidenses. Cuando una gran agencia de transportes fue víctima recientemente del ataque cibernético NotPetya, tuvo que restaurar más de 4000 servidores y 45 000 PC en 10 días.[5] Esta operación incluyó limpiar cada servidor y PC. El paso siguiente fue reinstalar los sistemas operativos y más de 2500 aplicaciones, con todos los datos asociados.[5] Aunque la empresa no ofreció un dato público del coste de toda la operación de recuperación, el cálculo aproximado de los daños causados ascendió a unos 300 millones de dólares estadounidenses.[6]

1-4: https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
5: https://www.bleepingcomputer.com/news/security/maersk-reinstalled-45-000-pcs-and-4-000-servers-to-recover-from-notpetya-attack/
6: https://www.cnbc.com/2017/08/16/maersk-says-notpetya-cyberattack-could-cost-300-million.html

La seguridad cibernética es un reto multidimensional que exige una respuesta multidimensional. Moor Insights & Strategy cree que las organizaciones de TI se beneficiarían si consideraran la seguridad integral como un requisito mínimo a la hora de invertir en la infraestructura de servidor. La seguridad con raíz de silicio, complementada con herramientas que permitan una recuperación rápida, debería ser un elemento imprescindible para cualquier servidor instalado y conectado a cualquier centro de datos. Debería contemplarse el uso de herramientas como Server System Restore de Hewlett Packard Enterprise para acelerar la recuperación. De hecho, MI&S no ha visto ninguna otra herramienta para la recuperación de servidores tan completa como esta en el mercado.

ANATOMÍA DE UN ATAQUE

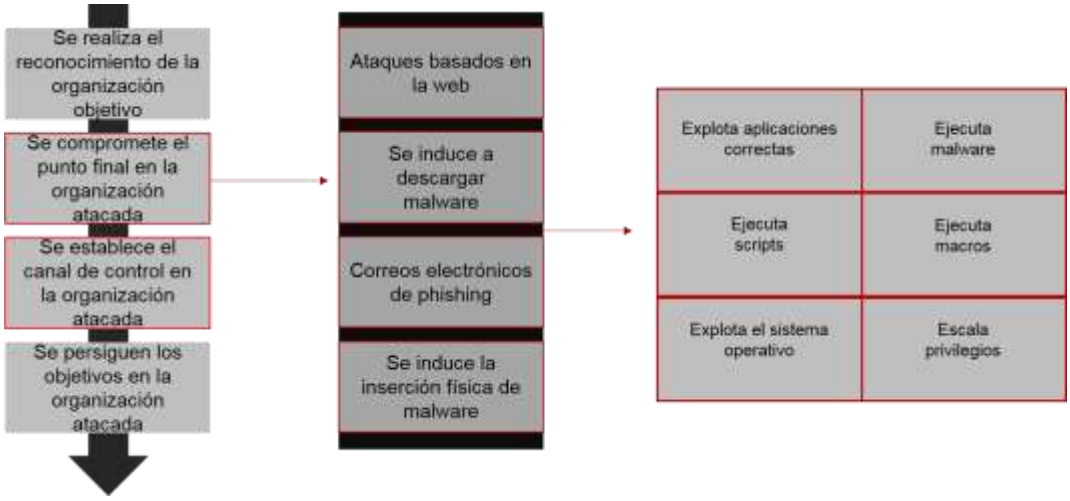
Los ataques cibernéticos contra los centros de datos han evolucionado de manera significativa. Los malos han descubierto que no es necesario acceder al interior del perímetro, mientras exista una persona en el otro extremo de una cadena de correo electrónico. Las violaciones de la seguridad más graves son el resultado de errores humanos. Un dispositivo USB abandonado en el suelo de un aparcamiento en el exterior de un edificio en una base militar de Afganistán fue la causa de la puesta en riesgo más grave sufrida por los equipos informáticos del ejército de EE. UU. en toda su historia y el tiempo recuperación ascendió a 14 meses.[7] Una contraseña manuscrita en un lugar a la vista de todos fue la causa del infame ataque a Target en 2013.[8] Y las contraseñas almacenadas en un lugar visible en GitHub provocó la brecha de seguridad de Uber en 2016.[9]

El proceso de atacar una organización se puede desglosar en cuatro fases diferenciadas:

- *Realizar reconocimiento* – Identificar el objetivo. Buscar puntos débiles evidentes para explotar. Planificar el ataque (DDoS, correo electrónico de phishing, etc.).
- *Acceso no autorizado* – Enviar el correo electrónico de phishing. Insertar el malware por USB u otros medios. Ejecutar ataque DDoS.
- *Conseguir un canal/plano de control* – Inyectar malware en el entorno a través de una serie de medios.
- *Ejecutar plan* – Descargar. Cifrar. Borrar. Distorsionar.

7-9: Declaraciones de James Morrison, técnico informático del FBI, junio de 2017.

FIGURA 1: LAS FASES DE UN CIBERATAQUE



Fuente: Moor Insights & Strategy

Si todo suena muy militar, es porque lo es. Los ataques a entidades gubernamentales y corporativas son cualquier cosa menos aleatorios. Los estados nación son el origen de muchas de las herramientas de piratería informática existentes. Y, de hecho, esos mismos estados nación son los autores materiales. Por otro lado, consideremos la cantidad de dinero en juego. Como he mencionado anteriormente, los ataques cibernéticos costarán a la economía mundial en torno a 6 billones de dólares estadounidenses en 2021, lo que equivale a un tercio del PIB de EE. UU. y supera el valor de todo el mercado mundial de las drogas ilegales.

Los ataques de *bootkit* o *firmware* son quizá los más perniciosos. Estos ataques permiten que los delincuentes accedan a un servidor debajo de la capa del sistema operativo. Este nivel de acceso permite que el malware se mantenga presente, pero que sea prácticamente indetectable incluso para las tecnologías de seguridad más modernas implementadas en el centro de datos. Los ataques de firmware también son los más difíciles de combatir y los que tienen más probabilidades de no ser detectados (con una media de 99 días de plazo hasta su detección).

A pesar de lo difícil que resulta mantener el control sobre el firmware de los servidores de una empresa, las organizaciones de TI están indebidamente preparadas para ello. En un estudio realizado por ISACA (Information Systems Audit and Control Association), tan solo el 8 % de las empresas disponía de medidas adecuadas para controlar y gestionar el firmware de su entorno.

PROTECCIÓN CONTRA LOS ATAQUES

Aunque no existe una solución milagrosa que permita proteger el centro de datos, MI&S ha descubierto algunas plataformas de servidor que emplean mecanismos seguros que ofrecen un elevado nivel de protección. Una de ellas es la cartera de servidores ProLiant Gen10 de Hewlett Packard Enterprise.

La raíz de confianza de silicio de HPE proporciona protección en cuanto se enciende el servidor y entra en funcionamiento el firmware Integrated Lights Out (iLO). Al iniciarse el servidor, su firmware se compara con una huella digital inmutable almacenada en ILO 5 para comprobar que todo el código de firmware es válido y no se ha visto comprometido.

Si se ha insertado malware o código comprometido en la ROM del sistema de la interfaz extensible del firmware unificada (UEFI) del firmware iLO 5, el silicio lo detectará porque cualquier código de firmware infectado estará alterado y, por tanto, no coincidirá con el hash grabado en el silicio. A continuación, la UEFI valida la conexión con el sistema operativo a través de un arranque seguro, con lo que se completa una raíz entera o cadena, que está anclada en el silicio. También se valida otro firmware esencial de servidor, para incluir CPLD, M.E., I.E. y la ROM opcional, completándose así la comprobación de casi 4 millones de líneas de código de firmware.

FIGURA 2: RAÍZ DE CONFIANZA DE SILICIO DE HEWLETT PACKARD ENTERPRISE

Fuente: Moor Insights & Strategy

En pocas palabras, la raíz de confianza de silicio de HPE crea una huella digital inmutable que se utiliza para validar el firmware. Los cambios en el firmware se identifican con rapidez, para permitir a las organizaciones de TI responder con mayor rapidez a los ataques de firmware.

RECUPERACIÓN DE UN ATAQUE

El objetivo de tiempo de recuperación (RTO), el tiempo de trabajo en recuperación (WRT), y el tiempo de inactividad máximo tolerable (MTD) son términos con los que muchos profesionales de la TI están familiarizados. Estos términos ayudan a definir la tolerancia de una organización a los tiempos de inactividad en situaciones de recuperación ante

desastres. La mayoría de los planes de recuperación ante desastres (DR) se crearon antes de que la amenaza de los ataques cibernéticos fuera una realidad y, en consecuencia, son incompletos. Tradicionalmente, las recuperaciones de los ataques cibernéticos han estado rodeadas de mucha confusión. En esencia, los servidores deben reconstruirse a partir del firmware y ascender hasta el sistema operativo, las aplicaciones y los datos. En un entorno empresarial, esta tarea puede parecer imposible, aún con las herramientas de gestión de la configuración disponibles de la mayoría de los proveedores de servidores. Estas herramientas suelen carecer de la integración y de los enlaces seguros necesarios para garantizar una recuperación completa y oportuna que no vuelva a introducir el malware en un entorno del cual se acaba de retirar.

Moor Insights & Strategy cree que hay tres cosas que las organizaciones de TI deberían exigir a las herramientas de recuperación empleadas.

- ***Seguridad -*** Limpiar el malware de 5000 servidores simplemente para volver a introducir el malware al instalar de nuevo un sistema operativo es un problema real al que se enfrentan las organizaciones de TI empresariales. Un «enlace» seguro desde la recuperación del firmware al repositorio donde se almacenan las imágenes ISO, las aplicaciones y los datos es algo imprescindible.
- ***Escalabilidad -*** Debemos buscar herramientas de recuperación que puedan restaurar el centro de datos a escala. La empresa de transportes tardó 10 días en restaurar 4000 servidores, un dato impresionante pero que supuso un tiempo de inactividad con un coste aproximado de 200 millones de dólares estadounidenses. La capacidad para restaurar esos 4000 servidores en paralelo hubiera reducido considerablemente el impacto financiero.
- ***Sencillez –*** A medida que la línea que divide las funciones de la TI y la empresa sigue difuminándose, las herramientas empleadas en la restauración de servidores deben ofrecer una capacidad de restauración cercada al clic único. Una herramienta completa sin facilidad de uso es una herramienta completa que carecerá de uso.

En condiciones ideales, las organizaciones de TI deben implementar una plataforma de seguridad cibernética perfectamente integrada. O, al menos, deberían implementar herramientas que compartan el mismo ADN. Es decir, las herramientas empleadas para proteger un entorno residen en la misma cartera tecnológica que aquellas herramientas empleadas para recuperarse de los ataques cibernéticos. De este modo, se garantizan los niveles más altos de integración y la obtención de la solución más completa.

HPE Server System Restore

La restauración de sistemas de servidor es una característica del iLO Amplifier Pack de Hewlett Packard Enterprise. Ofrece una restauración de servidores automática y segura para un máximo de 10 000 servidores en un solo clic.[10] Su extraordinaria potencia reside en su capacidad para gestionar totalmente incidentes cibernéticos en los servidores HPE Gen10 con la Edición de seguridad Premium iLO Advanced instalada. Cuando se detecta

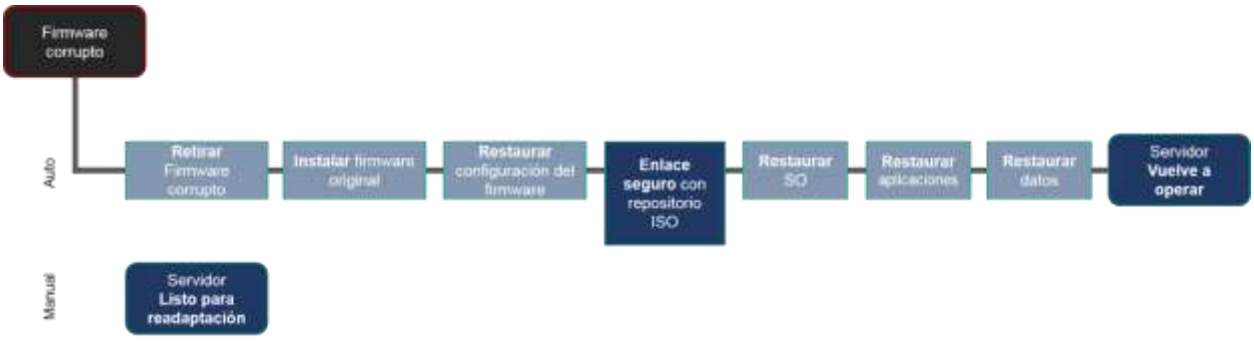
un servidor con firmware dañado, los administradores de TI puede activar una de tres respuestas posibles:

- ***Autorestauración***:
  - El firmware dañado se elimina.
  - Se vuelve a instalar firmware esencial de servidor no comprometido y comprobado.

10: Pruebas internas de HPE. Febrero de 2017.

  - Los ajustes del firmware se recuperan e instalan, ahorrando el tiempo que se tarda en recrear manualmente los ajustes.
  - Se establece un enlace seguro con el repositorio ISO, que evita la instalación de imágenes corruptas.
  - Se completa la facilitación de una restauración del SO desde un sitio ISO.
  - Se completa la restauración facilitada de las aplicaciones.
  - Recuperación de los datos desde un repositorio de copia de seguridad secundario protegido.
  - El servidor vuelve a ponerse en funcionamiento.
- ***Restauración manual:***
  - El firmware dañado se elimina.
  - Se vuelve a instalar firmware de servidor no comprometido y comprobado.
  - El servidor objetivo se mantiene en un estado limpio, a la espera de que el profesional de TI pase a la acción (por ejemplo, readaptación del servidor)

FIGURA 3: OPCIONES DE RESTAURACIÓN DE UN SISTEMA DE SERVIDOR



Fuente: Moor Insights & Strategy

En el momento de redactarse este informe, Hewlett Packard Enterprise parece contar con la oferta de seguridad más completa de un fabricante de servidores de primer nivel gracias a su gama Gen 10. La seguridad basada en la raíz de confianza de silicio puede reducir drásticamente el tiempo que se tarda en detectar los ataques de firmware. Y la restauración de sistemas de servidores ofrece lo que Moor Insights & Strategy considera factores críticos en un proceso de restauración: seguridad, escalabilidad y sencillez. Estas soluciones conforman lo que se podría considerar la cadena de confianza más segura en el sector de los servidores.

LLAMADA A LA ACCIÓN

El mundo está cambiando. Implementar aplicaciones web de triple capa con un DMZ y un cortafuegos ya no es suficiente para proteger el centro de datos. La adquisición y el uso de malware para atacar a las organizaciones es más fácil y frecuente que nunca antes. Y las organizaciones afectadas parecen estar más dispuestas que nunca a pagar el rescate a un delincuente a cambio de la devolución de los datos de sus clientes.

Moor Insights & Strategy considera que las organizaciones de TI de las pequeñas y medianas empresas son los objetivos más preciados para los piratas informáticos. Esto se debe a la combinación de la cantidad de datos que almacenan con las medidas de seguridad menos completas que implementan. No obstante, tanto si gestionas un centro de datos, una sala de servidores o un armario... tus datos están en riesgo.

En un momento en el cual las empresas gastan decenas de millones de dólares en software de seguridad o implementan redes definidas por software para una gestión basada en políticas, los niveles inferiores del hardware quedan desprotegidos ante ataques tipo rootkit que causarán el caos durante meses antes de ser detectados.

Moor Insights & Strategy cree que todas las empresas, sea cual sea su tamaño, deberían buscar la manera de acelerar los proyectos de modernización de las infraestructuras para aprovechar mejor las características de seguridad que pueden ofrecer protección desde el silicio y hasta los niveles superiores. Estas nuevas plataformas de servidor también sientas las bases de unas capacidades de recuperación más completas en respuesta a un ataque cibernético.

Hewlett Packard Enterprise es el único proveedor de servidores de primer nivel que ofrece una raíz de confianza de silicio y recuperación completa a través de la restauración de sistemas de servidor. Por ello, las organizaciones, sea cual sea su tamaño, deberían considerar la implementación del HPE iLO 5 Amplifier Pack y de la Edición de seguridad Premium iLO Advanced.

INFORMACIÓN IMPORTANTE SOBRE ESTE INFORME

COLABORADOR

Matt Kimball, analista ejecutivo de Moor Insights & Strategy

EDITOR

Patrick Moorhead, fundador, presidente y analista principal en Moor Insights & Strategymailto:patrick@moorinsightsstrategy.com

CONSULTAS

Ponte en contacto con nosotros si deseascomentar este informe. Recibirás una respuesta inmediata de Moor Insights & Strategy.mailto:patrick@moorinsightsstrategy.com

CITAS

Este informe puede ser citado por periodistas y analistas acreditados, aunque las citas deberán acompañarse de su contexto y mostrar el nombre del autor, su cargo y «Moor Insights & Strategy». Las personas que no sean periodistas o analistas acreditados deberán solicitar una autorización por escrito de Moor Insights & Strategy para citar cualquier parte de este documento.

LICENCIAS

DIVULGACIONES

Este informe se ha realizado a petición de Hewlett Packard Enterprise (HPE). Moor Insights & Strategy proporciona investigación, análisis, asesoramiento y consultoría para multitud de empresas de alta tecnología mencionadas en este informe. Ningún empleado de la compañía tiene intereses económicos en las empresas citadas en este documento.

DESCARGO DE RESPONSABILIDAD

La información presentada en este documento tiene fines meramente informativos y puede contener imprecisiones técnicas, omisiones y errores tipográficos. Moor Insights & Strategy renuncia a cualquier garantía sobre la precisión, exhaustividad o idoneidad de dicha información y no tendrá responsabilidad alguna por errores, omisiones o imprecisiones de dicha información. Este documento contiene las opiniones de Moor Insights & Strategy, que no se deben tomar como declaraciones de hechos. Las opiniones expresadas en el presente documento están sujetas a cambios sin previo aviso.

Moor Insights & Strategy proporciona estimaciones y declaraciones prospectivas como indicadores orientativos, no como previsiones precisas de eventos futuros. Si bien nuestras estimaciones y declaraciones prospectivas representan nuestra opinión actual sobre lo que depara el futuro, están sujetas a riesgos e incertidumbres que pueden provocar que los resultados reales sean esencialmente diferentes. Queremos advertirle que no debe depositar una confianza indebida en estas estimaciones y declaraciones prospectivas, que reflejan nuestras opiniones exclusivamente en la fecha de publicación de este documento. Recuerde que no estamos obligados a revisar ni publicar los resultados de la revisión de estas estimaciones y declaraciones de futuro en caso de que aparezca nueva información o a la luz de eventos futuros.