INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

Informe Global de Seguridad del Hardware y del Sistema Operativo de Servidores de ITIC de 2021

Junio de 2021

Índice

Resumen ejecutivo

Por tercer año consecutivo, las empresas corporativas clasificaron los servidores de misión crítica de IBM, Lenovo, Huawei y Hewlett-Packard Enterprise (en ese orden) como las plataformas más seguras y las que experimentaron menos vulnerabilidades de datos, siendo las más difíciles de decodificar por los hackers.

Esos fueron los resultados de la última encuesta de seguridad global de hardware para servidores de ITIC, la cual comparó las funcionalidades y características de seguridad de 15 diferentes plataformas. La encuesta independiente basada en la web de ITIC recibió respuestas de más de 1100 negocios en 28 industrias de mercado vertical alrededor del mundo, entre enero hasta mediados de junio de 2021.

IBM, Lenovo, Huawei, HPE y Cisco mantuvieron su posición como las plataformas de servidor más confiables y seguras, a pesar de un estrepitoso 42 % de incremento en brechas de seguridad y ataques durante la pandemia global de COVID-19 en los últimos 18 meses.

Los principales servidores de IBM Z; IBM POWER; el ThinkSystem de Lenovo y KunLun, de Huawei fueron, en ese orden, calificados como los mejores en rendimiento de seguridad, confiabilidad y operación continua durante la era del COVID-19, alcanzando notablemente los mejores resultados de seguridad entre 15 diferentes plataformas de servidores en todas las categorías de seguridad, según la última encuesta de ITIC, la cual incluyó:

- La menor cantidad de brechas/ataques de seguridad exitosos.
- La menor cantidad de tiempo de inactividad no planificado para servidores por *cualquier* razón o por razones de seguridad.
- El tiempo promedio más rápido de detección (MTTD), desde el inicio del ataque hasta su aislamiento y neutralización.
- El tiempo promedio de reparación más rápido (MTTR) para restaurar servidores, aplicaciones y redes a su operación total.
- La menor cantidad de datos robados, perdidos, destruidos, dañados o cambiados, como consecuencia directa de una brecha de seguridad de datos (p. ej. ramsomware, phishing o fraude al CEO).
- La menor cantidad de pérdidas monetarias debido a ataques exitosos.
- La máxima confianza en seguridad integrada del hardware del servidor para ofrecer alertas/avisos y para repeler ataques y brechas de seguridad en datos.

Los sistemas críticos de Hewlett-Packard Enterprise (HPE) y Cisco también proporcionaron un alto nivel de seguridad y entraron a la lista de los cinco servidores más seguros. Por otro lado, los servidores sin marca fueron los más vulnerables, registrando el número más alto de brechas de seguridad concluidos con éxito.

La encuesta de seguridad global más reciente de ITIC también reveló que los servidores de misión crítica de IBM, Lenovo, Huawei y HPE fueron los que tuvieron los tiempos de inactividad más bajos causados por ataques de seguridad y vulnerabilidades de datos (**Ver Anexo 1).**

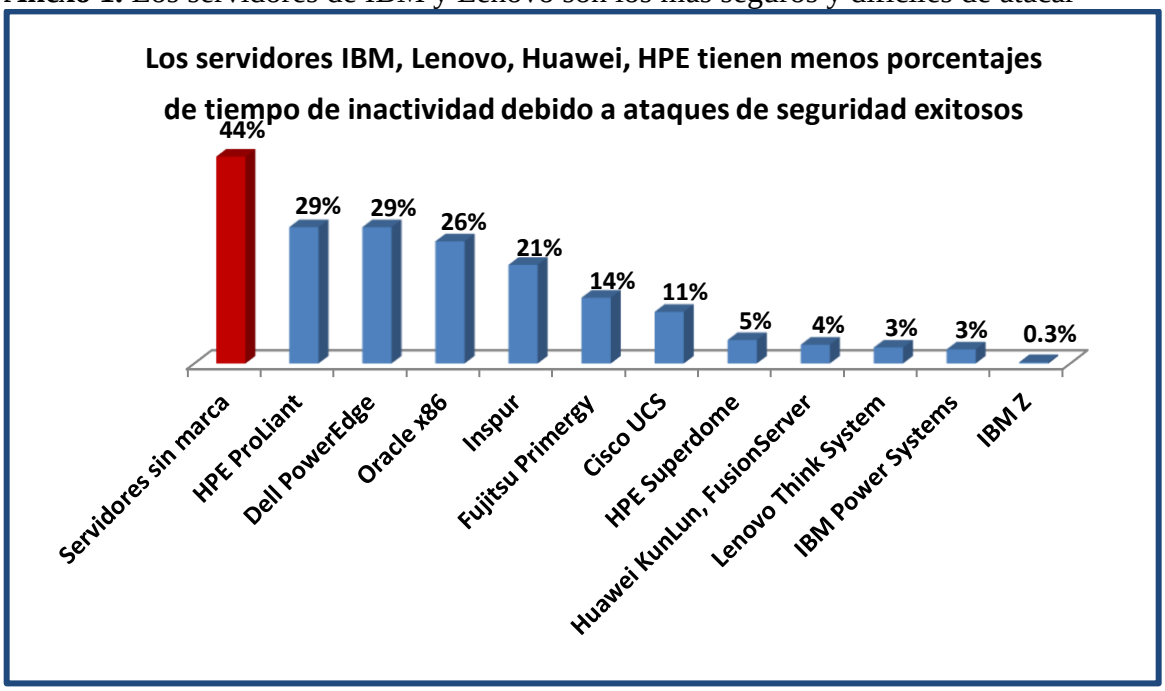
El mainframe de IBM Z superó todas las demás distribuciones de servidores y se convirtió en el único en su clase que alcanzó los niveles de seguridad y confiabilidad más altos en el último estudio de ITIC.

Apenas un minúsculo 0.3 % de los servidores IBM Z de más alta gama sufrieron un ataque de seguridad exitoso. En otras plataformas comerciales de hardware, solo el 3 % de los usuarios de IBM Power Systems y Lenovo ThinkSystem reportaron ataques a sus sistemas, lo mismo en el 4 % de los usuarios de Huawei KunLun y 5 % de HPE Integrity Superdome, entre enero y mediados de junio de 2021.

Uno poco más de uno entre diez (o un 11 %) de los usuarios de Cisco USC fueron hackeados de forma exitosa. El hardware de Cisco tuvo un excelente rendimiento, particularmente si se considera que muchos de los servidores UCS se despliegan de forma remota y en el borde de la

red, siendo así la primera línea de defensa para los ataques virtuales más agresivos. Los servidores sin marca fueron los que más vulnerabilidades sufrieron; el 44 % de los encuestados por ITIC reportaron que sufrieron ataques a sus sistemas.

Anexo 1. Los servidores de IBM y Lenovo son los más seguros y difíciles de atacar



Fuente: Encuesta de seguridad del hardware y del sistema operativo de servidores de ITIC de 2021

En general, los resultados de la encuesta de ITIC indican que existe una clara y creciente brecha en la seguridad y confiabilidad del hardware entre las plataformas que fueron más y menos exitosas. La pandemia impulsó la aparición de ataques de datos relacionados a la COVID-19, así como ransomware, phishing, BEC (Business Email Compromise), fraude al CEO y otros ataques que hasta la fecha continúan.

Los resultados de la encuesta más reciente de ITIC indican que la confiabilidad y la seguridad están intrínsecamente relacionadas, e incluso son simbióticas. Las violaciones tanto a la seguridad como a los datos afectan la integridad, la aplicación, el tiempo de ejecución de la red y la disponibilidad. Los ataques de seguridad y las violaciones de datos son caros y peligrosos. Comprometen la propiedad intelectual (IP) de las empresas, así como la de los asociados de negocios, clientes y proveedores. Un ataque de seguridad exitoso también puede exponer los datos personales de los empleados.

No es casualidad que las cinco principales plataformas de servidores más fiables: el IBM Z, el IBM Power Systems, el Lenovo ThinkSystem, los servidores Huawei KunLun y Fusion, el HPE Superdome Integrity y el Cisco UCS (en ese orden) también ostenten contar con la mayor seguridad disponible.

Introducción

La pandemia global ha causado una ola de violaciones, ramsonware, phishing, Business Email Compromise (BEC), fraudes al CEO y ataques relacionados con la COVID-19, que continúan siendo una amenaza entre todos los sectores verticales, y tienen como objetivo millones de dispositivos y software corporativos y de consumo.

Nadie ni nada es inmune. Esto hace que sea imprescindible una infraestructura de seguridad inherente y robusta.

La última encuesta de ITIC reveló que, en general, el 73 % de los encuestados temen que sus organizaciones sean víctimas de un ataque por hackers profesionales en los próximos 12 a 18 meses. Este tiempo coincide con la tendencia generalizada de escuelas primarias, secundarias y universidades, donde estudiantes y profesores han participado en clases remotas y ahora están preparándose para regresar a las aulas. Así mismo, muchas empresas y agencias gubernamentales están transicionando a un modelo de teletrabajo híbrido como una medida de seguridad.

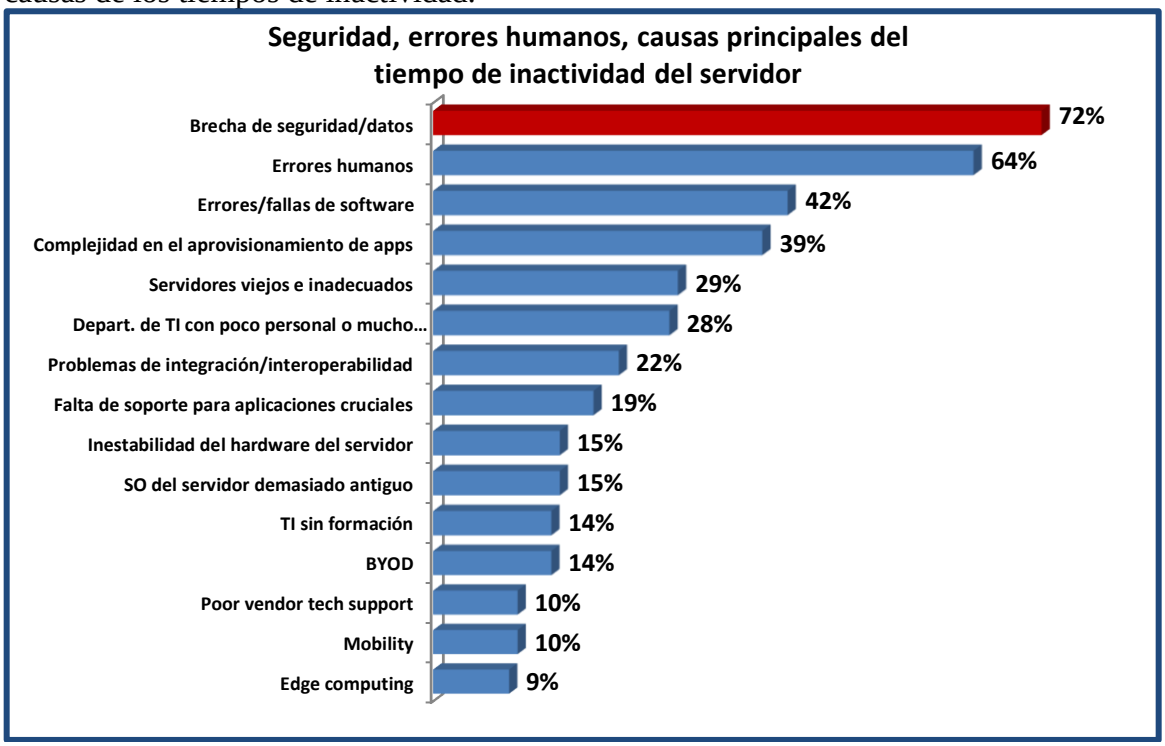
Los resultados de la última encuesta de seguridad se ven fortalecidos por las diferentes agencias del gobierno de los EE.UU., quienes han emitido alertas de ciberseguridad desde inicios del 2020. La Oficina Federal de Investigación (FBI); la Agencia de Seguridad Cibernética e Infraestructura (CISA) del Departamento de Seguridad Nacional y la Oficina de Inspecciones y Exámenes de Cumplimiento (OCIE) de la Comisión de Valores y Bolsa (SEC).

Las amenazas de ciberseguridad relacionadas con COVID-19 incluyen: estafas dirigidas a los beneficios del seguro de desempleo estatal y los cheques de estímulo a nivel federal; salud; bancos; fraudes con criptomonedas y fraudes gubernamentales, según las alertas emitidas por el FBI entre mayo y junio. El FBI señala que también ha visto casos de "...delincuentes que se dedican a la conducta depredadora en línea dirigida a niños que continúan con su educación desde el hogar durante la pandemia."

Los buenos resultados en materia de seguridad obtenidos por IBM, Lenovo, Huawei, HPE y Cisco (en ese orden) son especialmente notables, ya que se produjeron durante el punto álgido de la pandemia mundial de COVID-19. Alrededor del 40 % de los encuestados por ITIC informaron que sus servidores, sistemas operativos y aplicaciones críticas de negocio habían sufrido ataques de seguridad exitosos desde el inicio de la COVID-19 a principios de 2020. Esto supone un incremento de nueve puntos porcentuales en comparación con el 31 % de los últimos seis meses, y un aumento de 21 puntos porcentuales sobre un 19 % de las organizaciones que respondieron que sus servidores habían sido hackeados en la encuesta de ITIC sobre la fiabilidad del hardware y el sistema operativo de los servidores en 2020.

La seguridad es una cuestión comercial y tecnológica que afecta a todas las empresas. Alrededor del 72 % de los encuestados indicaron la seguridad y las brechas de seguridad de datos como las mayores amenazas para los servidores, las aplicaciones, el centro de datos, el borde de la red y la confiabilidad del ecosistema de la nube **(Ver Anexo 2)**. Los ataques son más selectivos, penetrantes y perniciosos. Están diseñados para infligir el máximo daño y pérdidas a sus víctimas, ya sean empresas o consumidores.

Anexo 2. La seguridad, los errores humanos y las fallas de software son las principales causas de los tiempos de inactividad.



Fuente: Encuesta de seguridad del hardware y del sistema operativo de servidores de ITIC de 2021

El panorama de las amenazas: las vulnerabilidades y brechas de seguridad de los datos son la principal y más costosa amenaza contra la confiabilidad

Las violaciones de datos son un gran negocio, y es la principal fuente de ingresos de la creciente comunidad de hackers. Un ataque concluido con éxito es muy costoso, en muchos niveles. En 2020, el costo de una brecha de seguridad de datos promedió los USD 3.86 millones, según el estudio Costo de las Brechas de Seguridad de Datos 2020, realizado conjuntamente por IBM y el Instituto Ponemon[1]. Esto representa un incremento del 10 % desde 2015. Los costos reales variarán en función de la duración y la gravedad de los ataques. Los ataques de ransomware siguen en aumento.

[1] "2020 Cost of a Data Breach Study," IBM y el Instituto Ponemon. URL: https://www.ibm.com/co-es/security/data-breach

Y son muy costosos. El 7 de mayo de 2021, un ataque de ransomware de hackers de DarkSide interrumpió las operaciones de Colonial Pipeline Co. por seis días[2]. El gasoducto de Colonial proporciona el 45 % del gas y el diésel utilizado en la costa Este de los Estados Unidos, desde Nueva Jersey hasta Florida. Interrumpió las entregas y provocó escasez de gas en varios estados, como Florida, Carolina del Norte y Virginia. Llegó a su fin únicamente cuando el CEO de Colonial Pipeline, Joseph Blount, accedió a pagarle a los hackers un rescate de USD 4.4 millones. Blount le mencionó a The Wall Street Journal que había autorizado el pago del rescate por USD 4.4 millones porque los ejecutivos no estaban seguros de que tan grave había sido la intensidad del ciberataque a sus sistemas y, por lo tanto, cuanto tiempo tomaría volver a hacer que el gasoducto funcionara nuevamente.

El ataque de ransomware de Colonial Pipeline es tan solo un ejemplo de muchos casos. Este resaltó las vulnerabilidades, los riesgos y los costos altos asociados con los ataques de ciberseguridad concluidos con éxito. El ataque de ransomware a Colonial Pipeline refuerza una vez más la necesidad de contar con una infraestructura de seguridad robusta y de la más alta tecnología. El hardware de los servidores es el elemento más básico para todas las redes y ecosistemas corporativos.

Un informe de DTEX Systems encontró que "únicamente el 30 % de las organizaciones estaban preparadas para garantizar una migración segura al trabajo remoto". El estudio de DTEX Systems también descubrió que casi el 75 % de las organizaciones están preocupadas por los riesgos de seguridad introducidos por los usuarios que trabajan desde casa, y el 73 % de las empresas admitieron que tienen una visibilidad parcial o nula de la actividad del usuario si su VPN es desactivada por los trabajadores remotos. Otro hallazgo alarmante es que los teletrabajadores utilizan sus laptops de trabajo para uso personal; el 25 % de los encuestados reconoce que esto aumenta el riesgo de descargas peligrosas, y el 15 % afirma que sus empresas son más susceptibles de sufrir ataques de phishing.

El estudio más reciente del ITIC indica que el costo por hora de los tiempos de inactividad sigue en aumento. Ahora supera los USD 300,000 dólares para el 89 % de las PYME y las grandes empresas. En general, el 42 % de las empresas medianas y grandes encuestadas informaron que, en promedio, una sola hora de tiempo de inactividad cuesta a sus empresas más de USD 1

[2] "Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom", The Wall Street Journal, 19 de mayo de 2021. URL: https://www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636

millón. En el peor de los casos, una brecha de seguridad de datos que se produzca durante las horas de mayor uso e interrumpa las operaciones cruciales del negocio puede costar a las empresas varios millones por minuto. Cualquier organización que sufra un tiempo de inactividad prolongado de horas o días como resultado de un ataque de ransomware dirigido incurrirá, casi con toda seguridad, en muchos millones en daños.

Además de las obvias pérdidas monetarias debidas a la productividad y a la interrupción de las operaciones, las empresas deben tener en cuenta la cantidad de horas de trabajo y el número de administradores de TI y de seguridad implicados en los esfuerzos de resolución y de retorno total a la operación. Las empresas también deben determinar si se han perdido, robado, dañado, destruido o modificado datos o cualquier tipo de propiedad intelectual. Las organizaciones también deberán considerar los costos de cualquier litigio, así como las posibles multas/penalidades civiles o penales asociadas a los incidentes de seguridad y las violaciones de datos. Algunos costos, como el daño a la reputación de una organización, son incalculables y pueden suponer una pérdida del negocio.

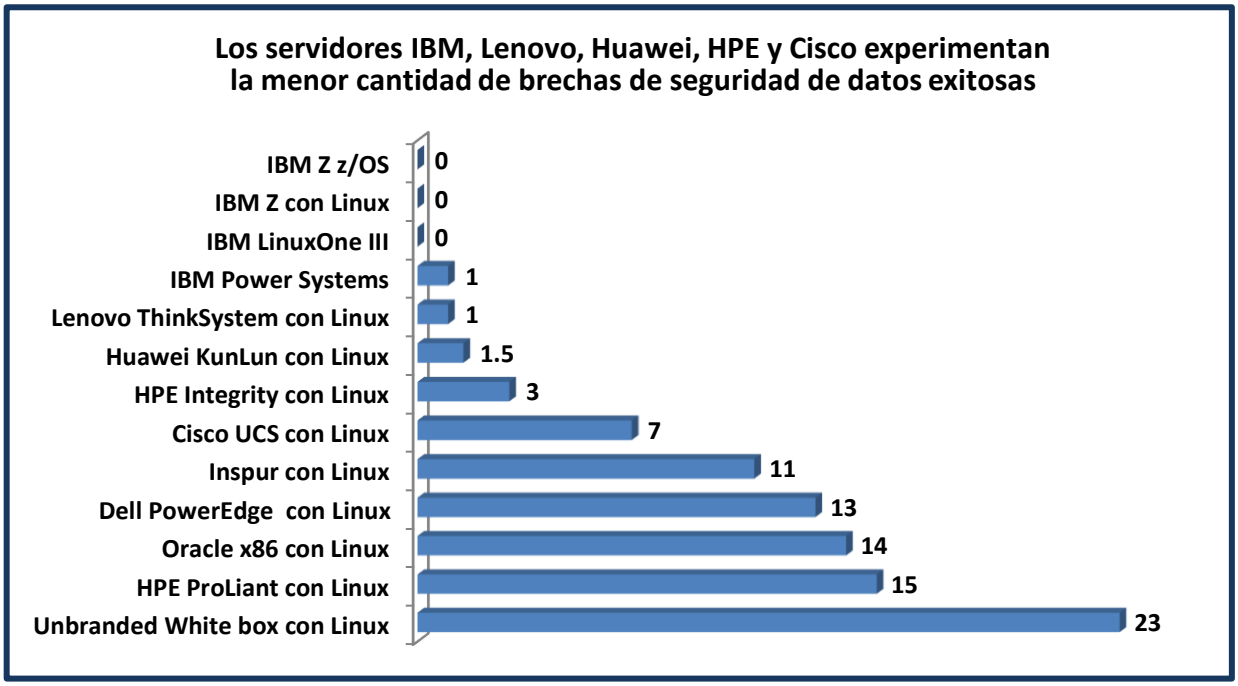
Los hackers eligen sus objetivos con gran precisión y son muy eficaces para aprovechar cualquier oportunidad que se les presente. La pandemia de COVID-19 es un buen ejemplo. Los piratas informáticos inmediatamente pusieron sus ojos en los teletrabajadores y en los estudiantes que aprenden a distancia tomando clases en línea y por Zoom. Se centraron en los llamados "objetivos blandos". Los gobiernos locales y estatales, los distritos escolares, hospitales, clínicas, consultorios médicos y sucursales bancarias de pequeño o gran tamaño podrían no contar con un sistema de seguridad integral, y los administradores de los sistemas de TI de estas organizaciones podrían no haber actualizado su seguridad.

Proveedores de servidores: IBM, Lenovo, Huawei y HPE y su estrategia de seguridad

No es de extrañar que proveedores como IBM, Lenovo, Huawei o HPE, cuyos servidores siempre obtienen las principales puntuaciones de confiabilidad, se encuentren también entre las plataformas de hardware más seguras. Estos proveedores, y más recientemente Cisco, han hecho de la seguridad de los servidores -y en el caso del servidor Lenovo, la seguridad de las computadoras de escritorio y portátiles- la prioridad máxima y han invertido mucho en reforzar la seguridad de sus productos en los últimos años. Por lo tanto, cuando surgió la pandemia de la COVID-19, dichos sistemas ya contaban con una seguridad muy sólida, lo que les ayudó a sobrellevar las vulnerabilidades que se presentaron.

Como indica el **Anexo 3** , las plataformas de hardware con servidores más seguros fueron las que sufrieron menos vulnerabilidades de seguridad. Los encuestados que utilizaban IBM Z y que ejecutaban z/OS y Red Hat Enterprise Linux (RHEL) e IBM LinuxONE III dijeron que dichas plataformas no habían sufrido ataques de seguridad exitosos en los últimos 16 meses. Les siguieron los servidores IBM Power Systems y Linux ThinkSystem, con uno cada uno; Huawei KunLun, que tuvo una media de dos ataques; el HPE Integrity, con tres vulneraciones exitosas, y los servidores UCS de Cisco, con siete violaciones de datos. Los servidores sin marca fueron los más permeables, con un promedio de 20 violaciones de datos exitosas en los últimos 16 meses.

Anexo 3. Los servidores de IBM, Lenovo, Huawei, HPE y Cisco son los que menos ataques exitosos han sufrido



Fuente: Informe global de seguridad del hardware y del sistema operativo de servidores de ITIC de 2021

Datos y análisis: resultados de seguridad de los proveedores

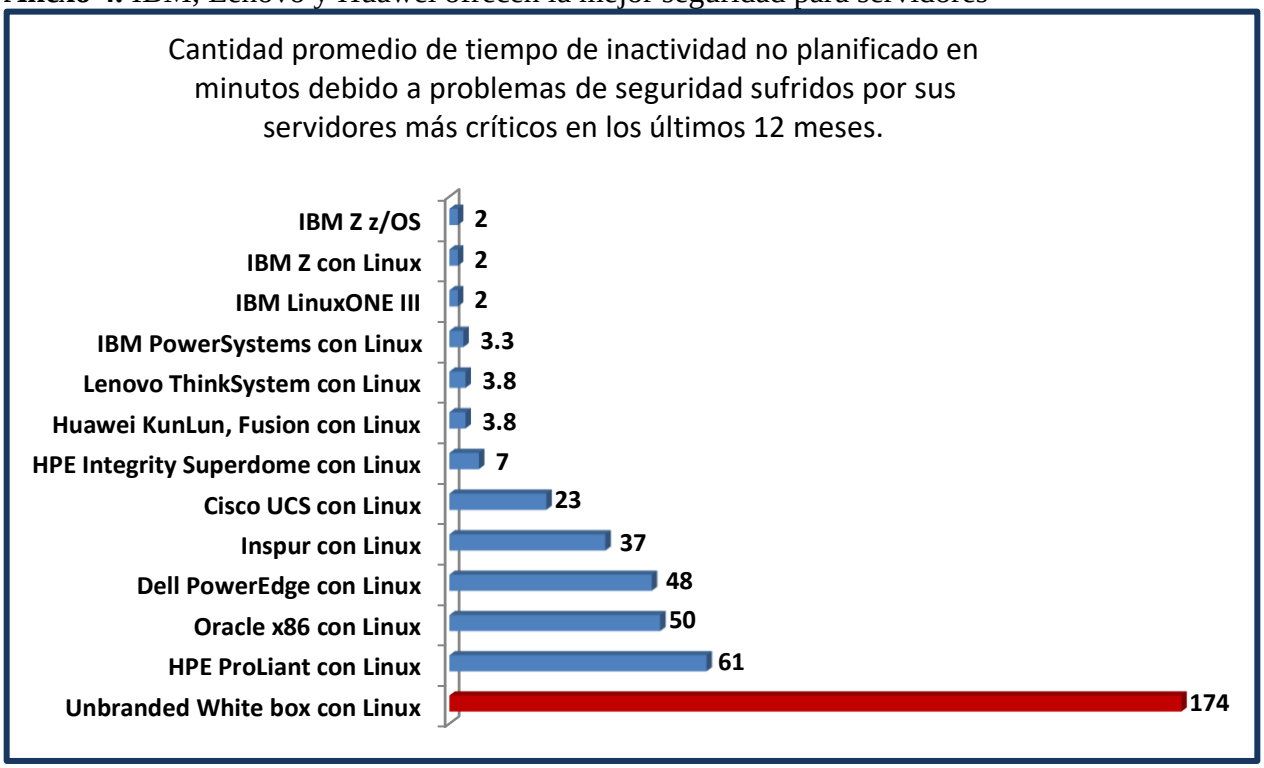
Para reiterar, la encuesta de Seguridad Global de Servidores 2021 de ITIC encontró que los servidores IBM Z, IBM Power Systems, Lenovo ThinkSystem y Huawei KunLun y Fusion (en ese orden) lograron los mejores resultados en cada categoría de seguridad, incluyendo:

- La menor cantidad de brechas/ataques de seguridad **exitosos**.
- La menor cantidad de tiempo de inactividad no planificado para servidores por ***cualquier*** razón o por razones de seguridad.
- El tiempo promedio más rápido de detección (MTTD), desde el inicio del ataque hasta su aislamiento y neutralización.
- El tiempo promedio de reparación más rápido (MTTR) para restaurar servidores, aplicaciones y redes a su operación total.
- La menor cantidad de datos robados, perdidos, destruidos, dañados o cambiados, como consecuencia directa de una brecha de seguridad de datos (p. ej. ramsomware, phishing o fraude al CEO).
- La menor cantidad de pérdidas monetarias debido a ataques exitosos.
- La máxima confianza en seguridad integrada del hardware del servidor para ofrecer alertas/avisos y para repeler ataques y brechas de seguridad en datos.

Tal como lo ilustra el **Anexo 4** , los servidores de misión crítica de IBM Z, IBM Power Systems, Lenovo ThinkSystem y Huawei KunLun fueron los que experimentaron la menor cantidad de tiempo de inactividad no planificado como resultado directo de incidentes de seguridad y violaciones de datos.

Tanto IBM Z como IBM LinuxONE III promediaron en general solo 2 minutos cada uno de tiempo de inactividad no planificado por servidor a causa de un problema de seguridad. Les siguieron de cerca los servidores POWER8 y POWER9 de IBM, que experimentaron algo más de 3 minutos de interrupciones no planificadas por servidor como resultado de un problema de seguridad; el hardware Lenovo ThinkSystem y los servidores Huawei KunLun y Fusion experimentaron cada uno, en promedio, 3.8 minutos de tiempo de inactividad no planificado por servidor asociado a incidentes de seguridad. Una vez más, los servidores sin marca, muchos de los cuales ejecutan versiones sin licencia de sistemas operativos de servidores y aplicaciones de software, acumularon 174 minutos o cerca de tres horas cada uno de tiempo de inactividad directamente atribuible a problemas relacionados con la seguridad. Esto hace que los servidores IBM Z de alta gama sean hasta 87 veces más seguros y confiables que el hardware de los servidores sin marca menos seguros, mientras que las ofertas de IBM POWER8 y POWER9 son hasta 58 veces más seguras que los sistemas sin marca.

Anexo 4. IBM, Lenovo y Huawei ofrecen la mejor seguridad para servidores



Fuente: Informe global de seguridad del hardware y del sistema operativo de servidores de ITIC de 2021

El tiempo promedio de detección es un barómetro crítico

Tanto los ataques de seguridad como las vulnerabilidades de datos forman parte de cualquier operación comercial en la era digital. En algún punto, tanto las organizaciones como los servidores de su principal línea de negocios, sistemas operativos y aplicaciones serán víctimas de una violación de seguridad de datos de cierto tipo.

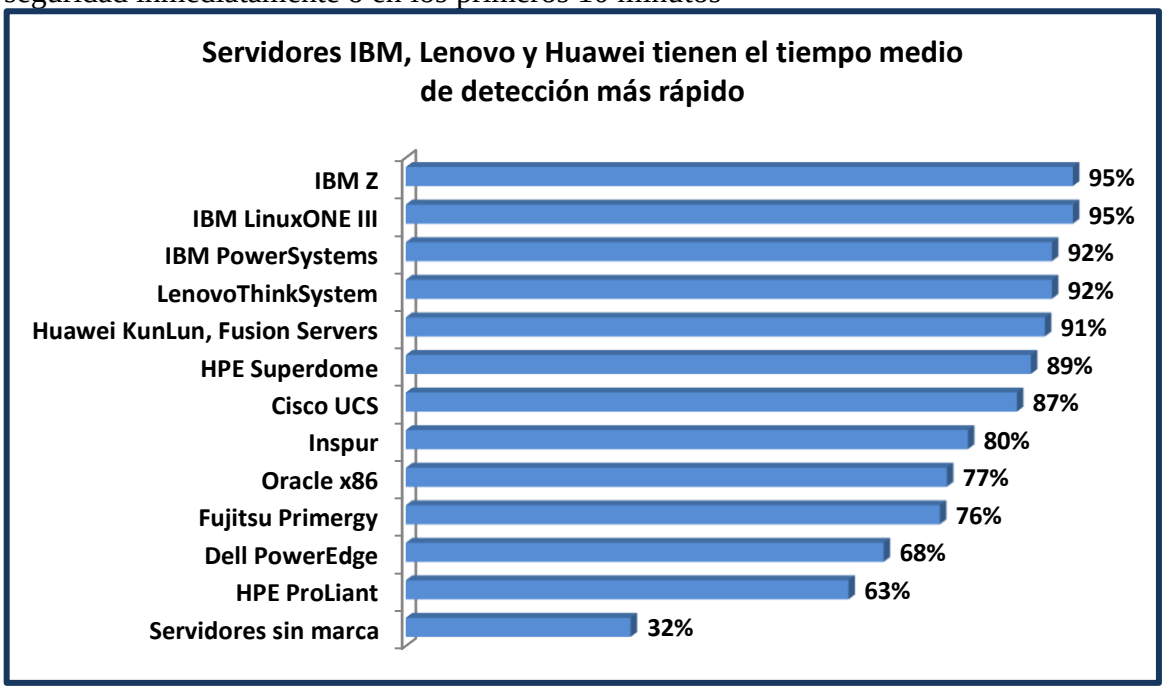
Las organizaciones deben contar con un servidor fuerte y una infraestructura de seguridad que reconozca el peligro, envíe alertas y alarmas, y que posea la capacidad de aislar las amenazas. La preparación de las corporaciones y contar con profesionales de seguridad capacitados correctamente y administradores de TI son de vital importancia.

En cuanto más rápidos sean los servidores y el software de la empresa para detectar un problema de seguridad y responder a él, mayores serán las posibilidades de aislar y frustrar el ataque ***antes de que*** pueda infiltrarse en el ecosistema, interrumpir las transacciones de datos y las operaciones diarias y acceder a datos confidenciales e IP.

El Anexo 5 muestra que, una vez más, los servidores IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun y Fusion, HPE Superdome y Cisco UCS (en ese orden) sobresalieron a la hora de frustrar los ataques. Estos servidores tuvieron los mejores porcentajes de tiempo medio de detección (MTTD) entre todas las plataformas.

Un abrumador 95 % de los encuestados de IBM Z e IBM LinuxOne III indicaron que sus servidores eran capaces de detectar un intento de vulnerabilidad de seguridad "Inmediatamente o en los primeros 10 minutos" del ataque, para después eliminarlo. Les siguieron, en orden, IBM Power Systems, Lenovo ThinkSystem y Huawei KunLun; el 92 % de los usuarios de cada una de esas plataformas dijeron que eran capaces de reconocer y repeler una brecha de seguridad "Inmediatamente o en los primeros 10 minutos". Cuanto más rápido los servidores sean capaces de repeler un ataque a la infraestructura principal, los sistemas operativos y las aplicaciones de misión crítica, mayores serán las posibilidades de que el negocio experimente poco o ningún tiempo de inactividad o sea víctima de robo, cambio, daño o compromiso de datos y de PI.

Anexo 5. Más del 90 % de los servidores de IBM, Lenovo y Huawei detectan los ataques de seguridad inmediatamente o en los primeros 10 minutos



Fuente: Informe global de seguridad del hardware y del sistema operativo de servidores de ITIC de 2021

Resultados de seguridad de los proveedores de servidores

Aspectos importantes sobre la encuesta de seguridad de IBM

- **Los servidores IBM Z** siguen obteniendo las más altas calificaciones en cuanto a confiabilidad general, accesibilidad, rendimiento y seguridad entre todas las plataformas. La familia IBM Z (la "Z" significa tiempo cero de inactividad) supera sistemáticamente a todos los competidores en **todas** las categorías de confiabilidad, y ofrece el menor costo total de propiedad (TCO) y el retorno de inversión (ROI) más acelerado. Los servidores z13, z14 y z15 obtuvieron las mejores puntuaciones de confiabilidad/tiempo de actividad, calificaciones de disponibilidad de la aplicación y seguridad en general, en términos de minutos reales de inactividad no planificada por servidor/tiempo de inactividad, por año. Tanto el mainframe IBM z como las distribuciones IBM LinuxONE muestran una verdadera tolerancia a las fallas, experimentando tan solo 0.60 - menos de un minuto de inactividad no planificada por ***servidor,*** por año, debido a fallas en el servidor, en comparación con los 0.74 segundos que las plataformas Z y LinuxONE promediaron en la encuesta Confiabilidad global de servidores 2019 de ITIC. A pesar de que la reducción de 0.14 segundos de tiempos de inactividad anual por servidor suena poco relevante, en realidad disminuye este tiempo en un 19 %, y reduce el TCO de IBM Z y LinuxOne en USD 230, de USD 1232 por servidor/por minuto en 2019 a USD 1002 por servidor/por minuto en el último informe de seguridad de hardware de servidores de ITIC en 2021. En general, IBM Z registró tan solo 4.32 segundos de tiempo de inactividad imperceptible mensual. De igual forma, y dado al incremento en

ataques de seguridad y brechas de seguridad de datos, el servidor IBM Z es también importante, dada su seguridad superlativa. Z sigue siendo el que menos porcentaje (menos del 1 %) de brechas de seguridad exitosas ha informado entre enero y mediados de junio de 2021. Además, los encuestados de IBM Z y LinuxONE III también informaron un tiempo promedio de detección (MTTD) más rápido, ya que el 95 % de las empresas encuestadas por ITIC declararon que sus administradores de seguridad y TI fueron capaces de detectar y eliminar los ataques en estas plataformas. Tanto a nivel particular como en su conjunto, estos resultados subrayaron el éxito de las ofertas de Z y LinuxONE III. Las plataformas también se han visto reforzadas por la adquisición de IBM de Red Hat en 2019; esto ha dado lugar a un aumento significativo de las cargas de trabajo de Linux en las plataformas Z y LinuxONE. Los ejecutivos de IBM declararon públicamente que la empresa ha visto un incremento del 55 % en los MIPS de Linux. También señalaron que 92 de los 100 principales clientes que usan Z de IBM ejecutan cargas de trabajo de Linux. En general, la plataforma Z tiene una media de 100 a 200 nuevos despliegues anuales, según IBM.

- **LinuxONE III de IBM** está basado en la plataforma IBM Z. Se dirige específicamente a entornos de nube híbrida y utiliza la encriptación integral de Z. La plataforma LinuxONE III y el IBM z15 también incorporan el controlador de datos IBM Hyper Protect, que ofrece protección y privacidad transparentes y de extremo a extremo de los datos. El IBM Hyper Protect Data Controller permite a las empresas encriptar datos, otorgar y revocar el acceso a los mismos, y mantenerlos bajo control - incluso cuando salen del sistema de registro**.** El resultado: IBM LinuxONE III compartió las puntuaciones más altas de seguridad y confiabilidad en la encuesta de ITIC de 2021, con el 95 % de las empresas con LinuxONE III indicando que detectaron y eliminaron las violaciones de datos "inmediatamente o en los primeros 10 minutos después" del ataque.
- **IBM Power Systems** El 92 % de los clientes de IBM Power Systems informaron que sus administradores de TI y de seguridad fueron capaces de detectar y frustrar los ataques "inmediatamente o en los primeros 10 minutos" después de una vulnerabilidad. Los sistemas POWER9 en escala de IBM llevan tres años en el mercado y está previsto que la próxima generación de servidores Power10 esté disponible para fines de 2021. IBM actualiza su línea de productos continuamente, haciendo énfasis particularmente en el desempeño, soporte para cargas de trabajo de misión crítica, analítica avanzada, bases de datos en memorias y seguridad. Todos los modelos de Power Systems están listos para operar en la nube. Los sistemas de IBM Power Systems tienen seguridad integral en todas las capas: procesador, sistemas, firmware, sistema operativo e hipervisor. Con la encriptació acelerada integrada en el chip, sus datos están protegidos tanto en movimiento como en reposo. IBM afirma que su hipervisor PowerVM no ha reportado vulnerabilidades de seguridad. Los servidores POWER9 también están preparados para operar en la nube, e incluyen funcionalidades de virtualización PowerVM integradas. Los servidores de escalabilidad horizontal POWER9 están diseñados para integrarse a las estrategias de nube e inteligencia artificial de las organizaciones. Esto proporciona las funcionalidades RAS de alto rendimiento, que son recursos necesarios para soportar cargas de trabajo de misión crítica. como las bases de datos Db2 y Oracle de IBM, así como SAP HANA. El modelo Power10 está diseñado para operar bajo una mayor eficiencia energética y rendimiento, en un factor 7nm. IBM estima que esto supondrá mejoras de hasta 3 veces más eficiencia energética del procesador, capacidad de carga de trabajo y densidad de contenedores que el POWER9. Además, los nuevos servidores Power10 incorporarán una serie de funciones avanzadas, que incluyen: soporte para clústeres de memoria de varios petabytes, que aumentará la capacidad de la nube para dar sopoerte a cargas de trabajo de memoria intensiva. El Power10 también contará con capacidades de

seguridad para el hardware, como la encriptación transparente de la memoria, ideal para una seguridad end-to-end. El procesador IBM Power 10 está diseñado para obtener un rendimiento de encriptación significativamente más rápido, con cuatro veces más motores de encriptación AES por núcleo comparado con los estándares más exigentes de IBM POWER9, y otros estándares criptográficos futuros anticipados como encriptación cuántica segura y totalmente homomórfica. También ofrece mejoras en la seguridad de los contenedores.

Aspectos importantes de la encuesta de seguridad de Lenovo

- **Los servidores Lenovo ThinkSystem** lograron los mejores índices de MTTD entre todos los servidores que operan en Intel x86, con un 92 % de los encuestados que afirmaron que sus administradores de TI y seguridad detectaron y cerraron los intentos de ataque y las violaciones de datos inmediatamente o en los primeros 10 minutos después del inicio de la vulneración. Esto no es una casualidad. En los siete años transcurridos desde que Lenovo adquirió el negocio de servidores basados en x86 de IBM y la década transcurrida desde que adquirió la línea de PC y notebooks de la misma empresa, Lenovo ha hecho de la seguridad una prioridad máxima. Por ello, los servidores y las computadoras de escritorio Lenovo se destacan en este aspecto, conforme la compañía mejora y fortalece el rendimiento, la confiabilidad y la seguridad de los servidores, sus PCs y laptops. El servicio técnico y el soporte de Lenovo son también de primer nivel. Los servidores ThinkSystem de Lenovo mostraron una mejora continua en la confiabilidad, promediando su mejor tiempo hasta el momento (1.51 minutos de tiempo de inactividad por servidor, por problemas de hardware). Al igual que IBM, Lenovo ha construido y ejecutado un excelente plan de seguridad táctica y estratégica. En 2018, Lenovo presentó la tecnología de seguridad integral ThinkShield para sus PC y laptops. La tecnología avanzada ThinkShield ha mantenido las PC y los servidores Lenovo en buena posición durante los últimos tres años, cuando los ataques a la seguridad aumentaron. Durante la pandemia global de la COVID-19, cuando muchas organizaciones migraron hacia el trabajo remoto para trabajadores y estudiantes por igual, los administradores de TI y de seguridad han sentido la presión por mantenerse al ritmo de las violaciones de datos. La solución de seguridad ThinkShield de Lenovo proporciona un soporte crucial. ThinkShield, por ejemplo, ostenta uno de los mejores lugares en el ThinkSystem SE350. Este modelo es el primer servidor de Lenovo diseñado específicamente para el borde, orientado específicamente para trabajar con la red y ofrecer un ancho de banda óptimo, aumentar la seguridad y reducir los tiempos de inactividad. El ThinkSystem SE350 es un servidor con tamaños reducidos. Mide 1.75 pulgadas de alto, 8.1 de ancho y 14.9 de profundidad, y puede colocarse en un muro, sobre una repisa o en un rack. El ThinkSystem SE350 también está diseñado para servidores de alto rendimiento. Está basado en el procesador Xeon-D de Intel y viene equipado con 256 GB de RAM y 16 TB de almacenamiento interno en estado sólido. ThinkSystem SE350 cuenta con funciones aumentadas de seguridad a nivel físico, como un bisel de bloqueo, detección de intrusiones, detección de manipulaciones y almacenamiento encriptado. Cuenta con un software de implementación de intervención cero. La estrategia global de Lenovo combina la innovación con sistemas de centros de datos seguros, confiables y flexibles. Este es un movimiento inteligente que alcanza a los servidores, redes y, a final de cuentas, a los clientes corporativos de Lenovo. El error humano es, por mucho, la principal causa de tiempo de inactividad del servidor. Por lo general, los usuarios finales son el eslabón más débil en una cadena de seguridad, particularmente durante la pandemia global del COVID-19, donde se vio un aumento significativo de usuarios finales trabajando y estudiando a distancia. Tiene sentido

que Lenovo quiera proteger tanto sus computadoras de escritorio como sus servidores. Lenovo aplica rigurosos estándares, políticas y procedimientos de seguridad en sus instalaciones de fabricación y cadena de suministro global. Los ingenieros de calidad de Lenovo tienen el derecho de auditar a los proveedores confiables de la empresa en cualquier momento, dándole un mayor control e insights sobre la seguridad de los componentes de sus dispositivos. ThinkShield también ofrece seguridad a nivel de diseño. Esto incluye seguridad en BIOS y en firmware, así como componentes que apagan la cámara de los portátiles y otorgan privacidad a su pantalla, lo que minimiza el "ataque visual" cuando los usuarios estén en lugares públicos. ThinkShield está diseñado para proteger las identidades y credenciales de los usuarios, ofrece autenticadores certificados por FIDO y se integra con Intel Authenticate (con hasta 7 factores de autenticación). ThinkShield también cuenta con protección USB inteligente basada en BIOS, que funciona configurando los puertos USB para que solo respondan a teclados y dispositivos señaladores. Lenovo también destaca que sus plataformas de servidor abierto, almacenamiento, red de trabajo y gestión de sistemas se integran perfectamente con los entornos existentes y heredados. Durante las entrevistas personales con los analistas de ITIC, los clientes de Lenovo indicaron que, la facilidad de despliegue y de integración, así como la retrocompatibilidad contribuyen a que exista una confiabilidad subyacente y una sólida estabilidad en la plataforma ThinkSystem. Los usuarios de Lenovo también elogiaron el servicio y el soporte postventa. El diseño del sistema de Lenovo también opera con bases de datos de misión crítica, aplicaciones de empresa, analítica de big data y entornos virtualizados y de nube. Ambos sistemas incorporan un gran número de funcionalidades tolerantes a fallas y de gran disponibilidad a un paquete de alta densidad, optimizado para racks y sin tapa que minimiza el espacio necesario para soportar "operaciones masivas de computación en la red" y simplificar el servicio, ya que el sistema nunca precisa ser removido del rack. En agosto de 2020, Lenovo presentó varios modelos nuevos de sus servidores ThinkSystem de socket único basados en los procesadores de la serie EPYC 702 de AMD Advanced Micro Devices. Estos nuevos productos dentro del portafolio de servicios de Lenovo fueron diseñados específicamente para manejar las cargas de trabajo evolutivas y con alta intensidad de datos de los clientes, como la seguridad por video, el almacenamiento definido por software y la inteligencia de redes. También soportan entornos visuaoizados de borde de la red, donde la seguridad es primordial. El resultado es un producto que ofrece poder y eficiencia, para los clientes que buscan un balance entre la operatividad y la seguridad, con fácil escalabilidad. Lenovo afirma que los dos nuevos servidores ThinkSystem "ofrecen el rendimiento de un servidor de doble socket, al costo de uno de socket único" y tienen el potencial de reducir los costos de licenciamiento de software de los clientes hasta en un 73 % y reducir el costo total hasta en un 46 %.

Aspectos importantes de la encuesta de seguridad de Cisco UCS

- **El sistema unificado de cómputo (UCS)** de Cisco continúa con buenas puntuaciones, y ha mantenido su promedio de 2.3 minutos de tiempo de inactividad por servidor alcanzado en la encuesta de mediados de año sobre sistemas operativos y hardware global de servidores de ITIC del 2020. De enero a mediados de junio de 2021, los servidores Cisco presentan 2.3 minutos por tiempo de inactividad por servidor. Cabe considerar que muchos de los servidores Cisco USC se colocan en el borde de la red, siendo así el primer frente de seguridad ante los ataques cibernéticos. A pesar de ello, el 87 % de los encuestados de Cisco UCS indicaron que fueron capaces de detectar, aislar y eliminar ataques de seguridad inmediatamente o dentro de los primeros 10 minutos. Los usuarios de Cisco USC encuestados también indicaron que los servidores experimentaron siete (7)

ataques de seguridad que se concluyeron con éxito en los últimos 18 meses. Gracias a este aumento en brechas de seguridad en los datos, Cisco publicó el Cisco UCS Hardening Guide. El documento está disponible para su descarga de forma gratuita . Contiene información detallada que le ayuda a los usuarios a aumentar la seguridad en la plataforma de los dispositivos Cisco USC, y así mejorar la seguridad en la red. Está estructurado de tal forma que abarca tres planes, en donde se categorizan las funciones de un dispositivo de red, y provee una visión general de cada función del software de Cisco UCS y su documentación de referencia. Además, Cisco ha introducido una serie de actualizaciones de gestión y desempeño, con el fin de mejorar el TCO y acelerar la instalación y la implementación. Cisco afirma que su UCS permitirá una reducción del 86 % en el cableado y permitirá la entrega de servicios en cuestión de minutos (en vez de días o semanas), mientras reduce sus gastos de capital en más del 40 %. Los fabricantes les garantizan a los usuarios un 100 % de compatibilidad entre los componentes. Además, el equilibro de carga no es problema.

Aspectos importantes de la encuesta de seguridad de HPE

- **La línea de servidores Superdome** de HPE (incluidos los modelos Integrity y Flex) también presentan una alta confiabilidad de 99,999 y 99,9999 por ciento para el 92 % de sus clientes. Por otro lado, el 89 % de los encuestados por HPE dijeron que sus empresas descubrieron y cerraron las brechas de seguridad "Inmediatamente o en los primeros 10 minutos". La encuesta de ITIC muestra que los servidores HPE Superdome experimentaron tres (3) ataques de seguridad concluidos con éxito en los últimos 18 meses. Esto coloca a las plataformas de hardware de HPE dentro de los cinco sistemas más seguros. El portafolio de productos Superdome también se ve beneficiado por la estabilidad y fortaleza inherente del hardware de HPE. HPE ha hecho de la seguridad, la innovación de las capacidades/desempeño y el servicio y soporte técnico postventa como sus principales prioridades. Todo esto en una era digital cada vez más insegura, compleja e interconectada. HPE atiende principalmente al segmento corporativo, desde PYMES hasta grandes empresas multinacionales. El servidor HPE Superdome Flex cuenta con funcionalidades RAS y seguridad end-to-end, para proteger las cargas de trabajo vitales. El servidor HPE Superdome Flex, por ejemplo, ofrece una escalabilidad de hasta 32 sockets. Esto supone 2.3 veces la escalabilidad de los servidores de generaciones previas. También cuenta un diseño interior y una capacidad de memoria de 768GB y de 48TB respectivamente, en una única plataforma. El servidor HPE Superdome Flex tiene un diseño modular que escala de forma flexible de 4 a 32 sockets, en incrementos de 4 sockets. HPE indica también que el servidor Superdome Flex tiene un punto de entrada con costos más eficientes para las cargas de trabajo de misión crítica a 4 sockets, lo que da hasta un 45 % menos de costo de adquisición, en comparación con otros modelos anteriores. HPE también hace hincapié en su confiabilidad, pues, según indican, las funcionalidades RAS incluidas en el servidor Superdome Flex dan cinco nueves (99.999%) de disponibilidad en un sistema único. HPE también menciona que los servidores Superdome Flex reducen los errores humanos gracias a la tecnología Analysis Engine, que maneja los errores y las fallas de forma predictiva. La seguridad y el error humano son dos cuestiones que están estrechamente vinculadas y que socavan la seguridad y la confiabilidad. Este motor predice los fallas del hardware e inicia la autoreparación sin necesidad de intervención humana o de "asistencia del operador". Contiene errores a nivel firmware, incluyendo errores de memoria, antes de que ocurra cualquier interrupción en la capa del sistema operativo con el enfoque "Firmware First"

de HPE. HPE también brinda continuidad a las cargas de trabajo de Linux con HPE Serviceguard for Linux (SGLX), su solución de clústeres de alta disponibilidad y de recuperación ante desastres. Esto permite que las empresas protejan sus servidores que ejecutan Linux contra muchísimas fallas de infraestructura o de aplicación en todos los entornos físicos o virtuales, y sobre cualquier distancia.

Aspectos importantes de la encuesta de seguridad de Huawei

- En los últimos cinco años, Huawei, compañía con sede en Shenzhen, China, ha emergido como uno de los cinco principales proveedores de hardware para servidores a nivel mundial, gracias a su servidor de cargas de misión crítica KunLun y sus servidores generales basados en 86, FusionServer. Según la encuesta global de confiabilidad de hardware y sistema operativo de servidores de ITIC en 2021 y la encuesta de seguridad global de hardware en servidores, los servidores Huawei KunLun y Fusion también están dentro de las tres principales plataformas de seguridad en el mercado. El 91 % de los usuarios de Huawei que respondieron a la encuesta notificaron que sus administradores de seguridad y TI identificaron y eliminaron intentos de ataques "inmediatamente o en menos de 10 minutos." Los mismos encuestados indicaron que los servidores KunLun y Fusion sufrieron en promedio 1.5 ataques durante los últimos 18 meses. Desde 2015, Huawei fortificó sus características avanzadas, su seguridad inherente y su desempeño general en sus servidores. Para competir de forma exitosa con sus rivales incluyendo Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo y otros, la familia de servidores Huawei incluye rack de uso general y servidores blade para el hardware de misión crítica, para abordar operaciones de cómputo de alto rendimiento . Huawei también ha incorporado a sus servidores funcionalidades avanzadas para dar soporte a las aplicaciones que necesiten una computación intensiva, tales como la IA, la analítica de Big Data, Deep Learning y Machine Learning. Huawei hace hincapié en la seguridad a través de sus documentos de mejores prácticas llamados "¿Cómo construir un sistema de defensa proactivo?" mediante su solución HiSec que permite una detección más inteligente de amenazas y una respuesta a las mismas, así como operaciones de seguridad y mantenimiento. Huawei afirma que HiSec mejora las funcionalidades de prevención de amenazas , los recursos de las redes de la empresa y la infraestructura de telecomunicaciones, aumentando así la eficiencia de la seguridad O&M y reduciendo sus costos. Además, Huawei ofrece un amplio número de nuevos productos de seguridad para sus diversas soluciones de servidor en el centro de datos, la nube y la red.

Conclusiones

La seguridad es el principal problema que afecta negativamente la confiabilidad y la disponibilidad del hardware y los sistemas operativos de los servidores, así como las aplicaciones críticas de negocio. Todas las organizaciones deberán hacer de la seguridad una prioridad, y deberán trabajar de forma cercana con sus proveedores para mitigar los riesgos y tenerlos en un nivel aceptable.

Cada segundo o minuto adicional de tiempo de inactividad de los servidores y de falta de disponibilidad de aplicaciones afecta negativamente a las operaciones del negocio, a la productividad de los empleados y a las utilidades.

La Encuesta global sobre la confiabilidad del hardware y el sistema operativo de servidores de ITIC 2021 demuestra que IBM Z mainframe, IBM Power Systems, seguido muy de cerca por Lenovo ThinkSystem, Huawei KunLun y HPE Integrity Superdome continúan solidificando y mejorando su estatus como los productos de hardware para servidores más confiables. La plataforma empresarial de IBM Z se destaca por ofrecer una confiabilidad de tolerancia a fallas de 99,9999 y 99,99999 % para el 93 por ciento de sus usuarios empresariales. Excluyendo al hardware para supercomputadoras y alta disponibilidad (HA), ninguna plataforma de servidores están a punto de llegar al punto Z de confiabilidad y disponibilidad, y casi ningún tiempo de operatividad y seguridad.

Nueve de cada 10 encuestados afirmaron que las soluciones IBM Power Systems y Lenovo ThinkSystem registraron 99,999 y hasta 99,9999 % de confiabilidad y disponibilidad. Las plataformas de IBM Power Systems y Lenovo ThinkSystem son hasta 30 veces más confiables y hasta 36 veces más rentables que los servidores sin marca, los cuales obtuvieron las peores puntuaciones.

En otro notable logro, tanto IBM como Lenovo obtuvieron el primero y el segundo lugar en cada categoría de confiabilidad y disponibilidad, o estuvieron empatados en primero y segundo lugar en cada métrica de seguridad y gestión dentro de la encuesta.

La confiabilidad es fluida, no estática. Ningún servidor o componente (disco duro, memoria o CPU), sistema operativo, aplicación, dispositivo o mecanismo de conectividad es inmune a los problemas o fallas inherentes al mismo.

Los servidores son la piedra angular sobre la que descansa toda la infraestructura de red y el ecosistema de red extendida. Cuando los servidores fallan, se niega el acceso a los datos. El negocio se detiene. La productividad cesa. Los ingresos se ven afectados. Alrededor del 88 % de todas las compañías requieren un mínimo de 99,99 % de confiabilidad para sus servidores, sistemas operativos y aplicaciones principales de negocio, para garantizar la productividad y ofrecer acceso continuo a los datos. Una alta confiabilidad y disponibilidad también cuida de las operaciones diarias de la corporación, sus activos de datos y la propiedad intelectual (PI), así como la información personal de los empleados, los procesos de negocios y el flujo de ingresos.

Más allá de la seguridad, en 2021 los errores humanos y los usuarios finales constituyen las mayores amenazas que afectan la confiabilidad y la disponibilidad de los servidores, los sistemas operativos y las aplicaciones.

Nadie sabe cuánto durará la pandemia global de la COVID-19. E incluso cuando la pandemia haya oficialmente terminado, sus efectos negativos e impacto probablemente persistirán por años, especialmente en relación a las amenazas de seguridad y brechas de datos.

Esta es la nueva normalidad: los hackers organizados llegaron para quedarse. Continuarán utilizando esta pandemia para explotar sus vulnerabilidades. Los hackers continuarán aprovechando cada oportunidad que tengan para extraer datos corporativos y de los empleados con fines de lucro.

La confiabilidad de los servidores, los datos ininterrumpidos y el acceso a las aplicaciones y a la seguridad siempre serán imperativos, pero particularmente en la era de la COVID-19, con el teletrabajo y la educación a distancia. Cada segundo o minuto adicional de tiempo de inactividad de los servidores y de falta de disponibilidad de aplicaciones afecta negativamente a las operaciones del negocio, a la productividad de los empleados y a las utilidades.

Una parte significativa de los servidores y las aplicaciones empresariales residen en entornos de nube virtualizados y en el borde de la red. Desde que la pandemia comenzó hace 18 meses, muchos negocios migraron hacia el teletrabajo; las escuelas y las universidades también adoptaron el aprendizaje remoto. Esto supone una mayor presión en las organizaciones y los administradores de TI y de seguridad, para garantizar la operabilidad y la disponibilidad de todos los datos.

La seguridad es extremadamente crucial. Los proveedores deben seguir reforzando la seguridad de los servidores integrados; suministrar rápidamente correcciones y parches cuando se encuentren fallas y trabajar con los clientes para proporcionarles una orientación prescriptiva. Las empresas corporativas también deben asumir la responsabilidad de asegurar la confiabilidad y la seguridad de toda la infraestructura de red y de los servidores, así como de las aplicaciones de negocio y los centros de datos en la nube. Es fundamental que las compañías implementen y refuercen políticas de seguridad y procedimientos sólidos para **todos los empleados,** particularmente para los teletrabajadores y los estudiantes. La confiabilidad y la seguridad son elementos clave para la funcionalidad de la infraestructura de red. Ambas son necesarias para garantizar operaciones diarias ininterrumpidas, el acceso seguro a los datos y para proteger la fuente de ingresos.

La Encuesta global de seguridad en el hardware y en el sistema operativo de los servidores de ITIC en 2021 resalta la necesidad de que **todas las organizaciones**, sin importar su tamaño o la verticalidad de su industria, deben proactiva y continuamente buscar identificar y eliminar los cada vez más crecientes y sofisticados ciberataques.

Eso significa implementar todas las medidas de seguridad apropiadas. Es fundamental instaurar y reforzar políticas y procedimientos de seguridad sólidos para **todos los empleados** de la compañía, desde los altos ejecutivos hasta los contratistas y becarios. Las empresas deberán asignar presupuesto adecuado para adquirir productos de seguridad y dedicar el tiempo necesario y utilizar los recursos internos y externos apropiados para proporcionarle a los usuarios finales, a los administradores de TI y profesionales de seguridad con las herramientas y la capacitación necesarias.

No hay tal cosa como una seguridad 100 % infalible. Sin embargo, las protecciones multicapa, fortalecidas por las pruebas de vulnerabilidad y una capacitación apropiada podrían reducir el número de brechas de seguridad de datos y de ataques de ransomware a niveles aceptables de mitigación.

Los sistemas de misión crítica de Cisco, HPE y Huawei también tuvieron un excelente desempeño y no experimentaron ninguna disminución en su confiabilidad en los últimos 18 meses, desde que apareció la pandemia global de la COVID-19. Los servidores de Cisco, de HPE y de Huawei alcanzaron casi la misma confiabilidad que IBM y Lenovo, según la robustez y el hardware principal inherente de sus sistemas.

Los servidores UCS de Cisco mantuvieron sus buenos resultados de confiabilidad en la última encuesta de Confiabilidad de hardware y sistemas operativos de servidores de mediados de año en 2021. Desde 2019, la división de servidores de Cisco UCS indicó que el tiempo reportado de inactividad disminuyó de 4.1 minutos en la encuesta anterior a tan solo 2.3 minutos por servidor/por año, debido a fallas en el hardware. Esto es crítico. Una parte significativa de los servidores USC de Cisco están implementados en el borde de la red, lo que se considera, por mucho, uno de los puntos más vulnerables del sistema.

Ningún proveedor puede dormirse en sus laureles. La competencia en el mercado global de hardware de servidores es intensa. Es y seguirá siendo un mercado de compradores. A pesar de que muchas compañías, particularmente PYMES basan sus decisiones de compra en precios, una gran parte de empresas eligen comprar un hardware más robusto, equipado con seguridad, gestión avanzada, IA y funcionalidades de analítica de big data.

Los datos de la encuesta muestran que las empresas corporativas valoran en niveles extremadamente altos los servicios y el soporte postventa. Las corporaciones requieren que los proveedores actúen rápidamente y cuando los problemas aparezcan. Los proveedores deben ofrecer a los clientes recomendaciones reales y orientación prescriptiva para configurar los sistemas y ciclos de vida del producto, para obtener y mantener desempeño y disponibilidad óptimos.

Como siempre, ITIC indica que los proveedores también tienen la responsabilidad de proporcionar parches, soluciones y actualizaciones puntualmente a los clientes, e informarles, conforme les sea posible, sobre cualquier problema de incompatibilidad que podría impactar el desempeño. Los proveedores también deberán ser honestos con los clientes y notificarles cuando existan problemas o retrasos en las piezas de repuesto.

Recomendaciones

Ninguna plataforma, sistema operativo o aplicación de negocio de servidores le ofrecerá una seguridad infalible. Sin embargo, IBM, Lenovo, Huawei, HPE y Cisco, las cuales están entre las plataformas de servidores más confiables, también le ofrecen el mayor nivel de seguridad inherente a ellas. Esto permite que los clientes alcancen una mayor economía de escala y salvaguarden sus activos de datos y PI más sensibles. La seguridad es una propuesta 50/50. A pesar de que los proveedores ofrecen seguridad de alto nivel, las corporaciones son responsables por mantener la confiabilidad de sus servidores y mejorar la infraestructura de la red. ITIC recomienda firmemente a las empresas a:

- **Hacer un inventario.** Sepa lo que hay en su red. Esto incluye clasificar ***todos*** los servidores, las aplicaciones cruciales a las líneas de negocio, los dispositivos de red (firewalls y routers) en todo el ecosistema de red, incluyendo el centro de datos, las oficinas remotas, las nubes públicas, privadas e híbridas, los dispositivos IoT y el borde de la red.
- **Elegir el tamaño correcto de hardware del servidor**. El hardware del servidor debe ser lo suficientemente robusto para acomodar las cargas de trabajo actuales, así como el aumento anticipado de las cargas de trabajo y aplicaciones mayores.

- **Reemplazar, ajustar y actualizar regularmente el hardware del servidor.** Esto significa mantener al día todos los parches, actualizaciones y soluciones de seguridad ***conforme sea necesario***, para mantener la salud y alcanzar el mayor rendimiento del sistema.
- **Actualizar el software.** Siempre que sea posible, nunca se atrase en más de dos revisiones de seguridad en los sistemas operativos y las aplicaciones basadas en los servidores.
- **Aplicar políticas y procedimientos de seguridad sólidos.** Es fundamental que las compañías de todos los tamaños y en todos los segmentos verticales de mercado instauren políticas y procedimientos de seguridad a nivel corporativo. Compártalos con todos sus empleados a través de copias físicas y e-mails. Las políticas de seguridad informática deben ser una parte integral de todos los lineamientos corporativos, y deben contener disposiciones y penalidades específicas para la primera, segunda y tercera instancia. También se aconseja que los empleados asistan a un curso de seguridad informática, similar a los de acoso sexual en el lugar de trabajo.
- **Supervisar de cerca los acuerdos de nivel de servicio (SLA).** Preste especial atención a los contratos de SLA para garantizar que los proveedores de hardware y software de su empresa, así como sus proveedores de la nube, excedan los términos de los SLA para entregar los niveles esperados de confiabilidad.
- **Realizar pruebas de seguridad ante vulnerabilidades.** Debido al aumento continuo de todo tipo de ataques y brechas de seguridad (como ransomware, ataques de Phishing y fraude al CEO, entre otros), todas las empresas corporativas deben realizar pruebas de vulnerabilidad al menos una vez al año, conforme sea necesario. El ITIC recomienda que las corporaciones colaboren con expertos independientes externos.
- **Elaborar un plan de gobernanza y remediación.** Tenga un plan de medidas correctivas y gobernanza en marcha, en caso de que su empresa sufra un ataque exitoso. Determine la jerarquía para saber quién estará a cargo en caso de que exista una brecha de seguridad o una falla en la red. El plan de gobernanza y remediación deberá asignar y designar tareas específicas a personas y grupos en particular. Asegúrese de que su plan también incluya la información de contacto correspondiente para todos los proveedores internos y externos.
- **Capacitar y certificar a los administradores de seguridad y de TI.** Garantice que los profesionales de seguridad y de TI reciban una capacitación adecuada, y que cuenten con las certificaciones de seguridad correspondientes.
- **Capacitar a los usuarios finales.** Asegúrese de que los usuarios finales y los trabajadores permanentes y temporales reciban una capacitación adecuada de seguridad, particularmente sobre los últimos esquemas via e-mail y phishing, así como las amenazas de ransomware.

Metodología

La *Encuesta global sobre confiabilidad y seguridad en el hardware de servidores 2021* de ITIC encuestó a ejecutivos de alto nivel y a gerentes de TI en más de mil corporaciones en todo el mundo, entre enero y mediados de junio de 2021. Esta encuesta independiente realizada a través de la red incluyó preguntas de opción múltiple y una para desarrollar (tipo ensayo). Para mantener la objetividad, ITIC no aceptó ningún tipo de patrocinio por parte de ningún proveedor. Ningún participante en la encuesta recibió remuneración alguna. Los analistas de ITIC también realizaron veinticuatro entrevistas personales para obtener datos valiosos, obtener insights más profundos y conocimientos contextuales sólidos sobre el impacto y las implicaciones de las vulnerabilidades de datos en la confiabilidad de los servidores corporativos y sus infraestructuras de red. Entre los encuestados se encontraban ejecutivos de la alta dirección, administradores de TI y de seguridad, y usuarios finales. ITIC empleó mecanismos de autenticación y seguimiento para evitar la manipulación y prohibir varias respuestas de las mismas partes.

Datos demográficos de la encuesta

ITIC encuestó a 1100 empresas de todos los tamaños y de 28 mercados verticales. Hubo una buena representación de las empresas de diferentes tamaños. Los encuestados provenían de compañías que variaban entre pequeñas y medianas empresas (PYMES) con menos de 50 empleados, a multinacionales con más de 100 000 colaboradores.

Todos los sectores del mercado estuvieron representados: las PYMES de entre uno y 100 empleados representaron el 24 % de los encuestados. Las pequeñas y medianas empresas (PYMES) de 101 a 11000 empleados representaron el 28 % de los participantes. El 43 % restante de los encuestados provino de empresas grandes, entre 1001 y 100 000 colaboradores. Los encuestados provenían de 49 diferentes mercados verticales. Aproximadamente el 61 % de los encuestados procedían de Norteamérica; el 39 % eran clientes internacionales que procedían de 22 países de Europa, Asia, Australia, Nueva Zelanda, Sudamérica, América Central y África.

Anexos

Esta sección ofrece enlaces a las distintas estadísticas y encuestas del ITIC citadas en este Informe.

Página web de ITIC y enlaces a los datos y publicaciones de posts de las encuestas:

https://itic-corp.com/blog/2019/11/ibm-lenovo-hpe-and-huawei-servers-maintain-top-reliability-rankings-cisco-makes-big-gains-ibm-lenovo-hardware-up-to-24x-more-reliable-28x-more-economical-vs-least-reliable-white-box-servers/

https://itic-corp.com/blog/2019/11/1678/

https://itic-corp.com/blog/2019/08/itic-poll-human-error-and-security-are-top-issues-negatively-impacting-reliability/

https://itic-corp.com/blog/2019/08/itic-2019-server-reliability-mid-year-update-ibm-z-ibm-power-lenovo-system-x-hpe-integrity-superdome-huawei-kunlun-deliver-highest-uptime/

http://itic-corp.com/blog/2017/07/ibm-z14-mainframe-advances-security-reliability-processing-power/

http://itic-corp.com/blog/2017/06/ibm-lenovo-servers-deliver-top-reliability-cisco-ucs-hpe-integrity-gain/