INFORMATION TECHNOLOGY
INTELLIGENCE CONSULTING

ITIC 2021 Global Server Hardware, Server OS Security Report

Junho de 2021

Índice

Resumo executivo

Pelo terceiro ano consecutivo, as corporações classificaram os servidores de missão crítica da IBM, Lenovo, Huawei e Hewlett-Packard Enterprise (respectivamente) como as plataformas mais seguras, que sofreram menos violações de dados e foram consideradas as mais difíceis de serem acessadas por hackers.

Estes são os resultados da pesquisa de opinião ITIC Global Server Hardware Security mais recente, que comparou as características e funções de segurança de 15 plataformas de servidores diferentes. A pesquisa de opinião independente da ITIC, realizada na web, contou com a participação de mais de 1.100 empresas no mundo inteiro de 28 diferentes setores de mercados verticais durante o período de janeiro de 2021 até a metade de junho de 2021.

IBM, Lenovo, Huawei, HPE e Cisco mantiveram suas posições de liderança como as plataformas de servidor mais confiáveis e seguras, apesar de um aumento significativo de 42% nos hacks de segurança e violações de dados durante a pandemia global de COVID-19 nos últimos 18 meses.

Os principais servidores liderados pelo IBM Z, IBM POWER, Lenovo ThinkSystem e Huawei KunLun (nessa ordem), pontuaram seus respectivos melhores desempenhos de segurança e confiabilidade/tempo de atividade durante a pandemia da COVID-19 e alcançaram os melhores resultados de segurança entre todas as 15 plataformas de hardware de servidores convencionais em cada categoria de segurança na pesquisa mais recente da ITIC, incluindo:

- A menor quantidade de invasões de segurança e de violações de dados bem-sucedidas;
- O menor tempo de inatividade geral não planejada do servidor por ***qualquer*** motivo e o menor tempo de inatividade não planejada do servidor como resultado de um incidente de segurança.
- Tempo médio de detecção (MTTD) mais rápido desde o início do ataque até a empresa isolá-lo e interrompê-lo;
- Tempo médio de correção (MTTR) mais rápido para restaurar servidores, aplicações e redes a fim de retornar à operação total;
- A menor quantidade de dados perdidos, roubados, destruídos, danificados ou alterados como consequência direta de uma violação de segurança de dados (por exemplo, Ransomware, fraude de phishing ou fraude de CEO);
- A menor quantidade de perdas monetárias devido a uma invasão de segurança bem-sucedida;
- Maior confiança na segurança integrada do hardware do servidor para fornecer alertas e evitar ataques de segurança e violações de dados.

Os sistemas críticos de negócios da Hewlett-Packard Enterprise (HPE) e da Cisco também forneceram um alto nível de segurança e fizeram parte das 5 principais distribuições de servidores mais seguras. Na outra extremidade do risco, os servidores sem marca novamente provaram ser os mais vulneráveis, registrando os maiores números de invasões de segurança bem-sucedidas.

A pesquisa de segurança global mais recente da ITIC também revelou que os servidores críticos IBM, Lenovo, Huawei e HPE apresentaram as menores porcentagens de tempo de inatividade causados por invasões de segurança e violações de dados bem-sucedidos (**Veja a Figura 1).**

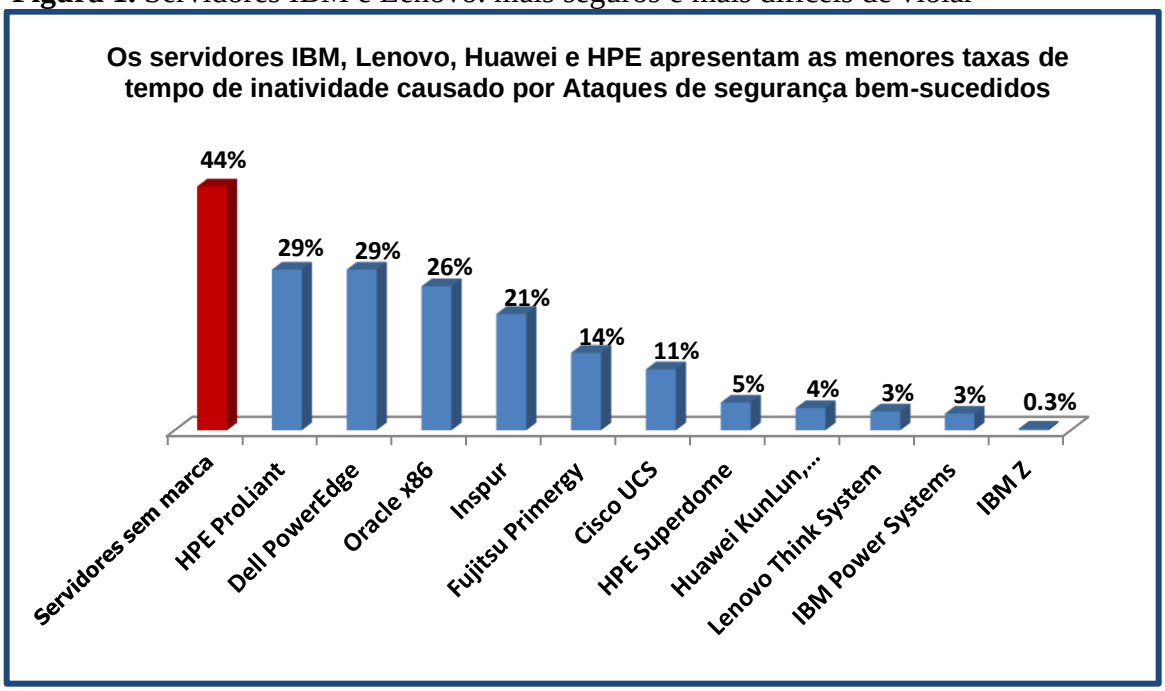
O mainframe IBM Z superou todas as outras distribuições de servidores e possui uma classe própria, pois atingiu as classificações de segurança e confiabilidade mais fortes até o momento de acordo com o estudo mais recente da ITIC.

Apenas 0,3% dos servidores de ponta do IBM Z sofreram uma violação de dados bem-sucedida. Entre outras plataformas de hardware convencionais, apenas 3% dos usuários IBM Power Systems e Lenovo ThinkSystem relataram que seus sistemas foram hackeados com sucesso, enquanto menos de 4% dos clientes de servidor do Huawei KunLun e 5% do HPE Integrity Superdome relataram uma violação de segurança bem-sucedida entre janeiro de 2021 a metade de junho de 2021.

Um pouco mais de 1 a cada 10 servidores Cisco UCS, cerca de 11%, foram hackeados com sucesso. O hardware da Cisco teve um desempenho extremamente bom, especialmente quando se considera que muitos dos servidores UCS são implementados em locais remotos e na borda da rede, que frequentemente são a primeira linha de defesa e sofrem todo o impacto dos ataques de hackers. Os

servidores sem marca eram os mais vulneráveis a violação de segurança. Entre os participantes da pesquisa de opinião da ITIC, 44% relataram que esses sistemas foram hackeados com sucesso.

Figura 1. Servidores IBM e Lenovo: mais seguros e mais difíceis de violar



Fonte: ITIC 2021 Global Server Hardware, Server OS Security Report.

Em geral, os resultados da pesquisa da ITIC indicam que há uma lacuna clara e crescente na segurança e confiabilidade do hardware do servidor entre as plataformas de melhor desempenho e as soluções menos seguras. A pandemia global gerou uma onda de violações de dados relacionadas a COVID-19, ransomware, phishing, comprometimento de e-mail comercial (BEC), fraude de CEO e ataques que continuam inabaláveis.

Os resultados da pesquisa de opinião mais recente da ITIC indicam que a confiabilidade e a segurança estão estritamente interligadas e chegam até a ser simbióticas. Violações de segurança e de dados comprometem imediatamente o servidor, as aplicações e o tempo de atividade e de disponibilidade da rede. As invasões de segurança e as violações de dados geram são caras e perigosas. Elas comprometem a propriedade intelectual (PI) das empresas, bem como a de parceiros de negócios, clientes e fornecedores. Uma invasão de segurança bem-sucedida também pode divulgar os dados pessoais dos funcionários e funcionárias.

Não é por acaso que as 5 plataformas de servidor mais confiáveis como IBM Z, IBM Power Systems, Lenovo ThinkSystem, Huawei KunLun e Fusion Servers, HPE Superdome Integrity e Cisco UCS (respectivamente) também oferecem os melhores níveis de segurança.

Introdução

A pandemia global gerou uma onda de violações de dados, ransomware, phishing, comprometimento de e-mail corporativo (BEC), fraude de CEO, entre outros ataques relacionadas à COVID-19, que continuam inabaláveis em todos os mercados verticais, visando invadir diversos dispositivos e softwares corporativos e pessoais.

Nada, nem ninguém, está imune. Isto transforma a infraestrutura de segurança inerente e robusta em um requisito.

A pesquisa mais recente da ITIC descobriu que, no geral, 73% dos entrevistados temem que suas organizações sejam vítimas de um ataque realizado por hackers profissionais nos próximos 12 a 18 meses. Este período coincide com a tendência generalizada de escolas do ensino fundamental ao médio, faculdades, universidades, estudantes e professores que adotaram o ensino à distância durante a pandemia e que agora estão se preparando para voltar para a sala de aula. Do mesmo modo que muitas empresas e agências do governo estão agora executando uma transição para o modelo híbrido de teletrabalho como medida de segurança de saúde.

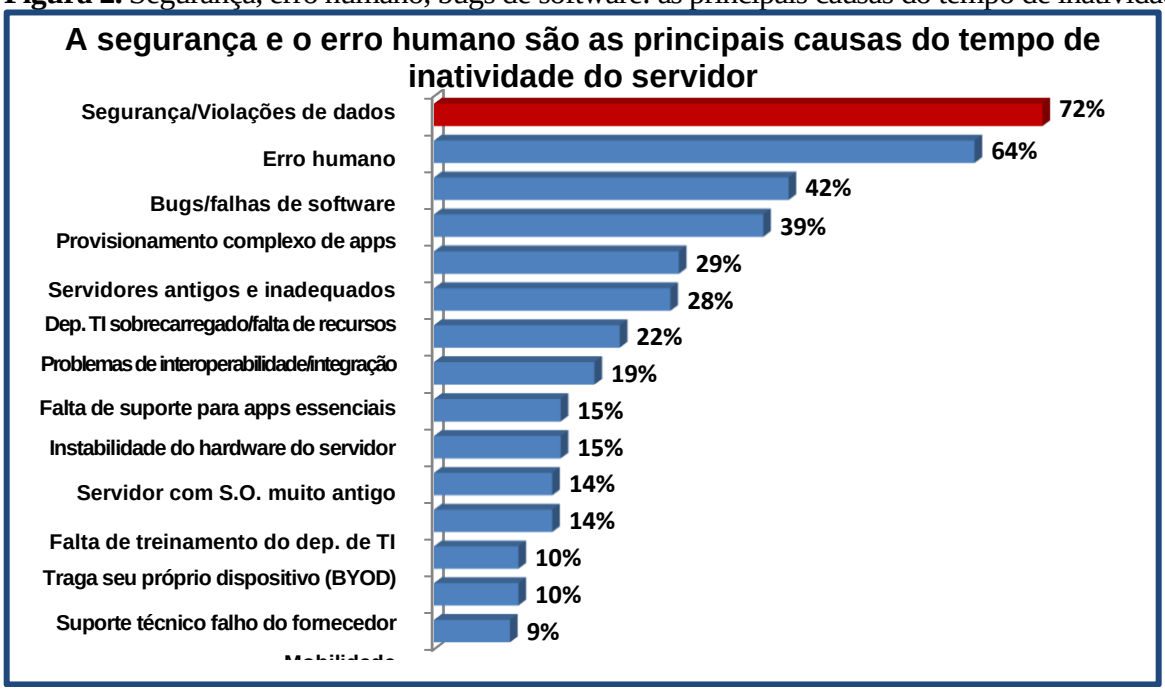
As últimas descobertas da pesquisa de opinião de segurança da ITIC são apoiadas por diversas agências do governo federal dos EUA, que emitiram vários alertas de risco de cibersegurança desde o início de 2020. O Federal Bureau of Investigation (FBI), o Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) e o Office of Compliance Inspections and Examinations (OCIE) da Securities and Exchange Commission (SEC).

As ameaças de cibersegurança relacionadas à COVID-19 incluem: golpes visando benefícios de seguro-desemprego estadual e bolsas de benefícios federais, cuidados de saúde, bancos, idosos, criptomoeda e esquemas de fraude do governo, de acordo com alertas do FBI publicados em maio e junho. O FBI observa que também identificou casos de "(...) criminosos envolvidos em comportamentos predatórios on-line visando crianças que continuam a estudar em casa durante a pandemia".

Os fortes resultados de segurança publicados pela IBM, Lenovo, Huawei, HPE e Cisco (respectivamente) são especialmente notáveis, uma vez que ocorreram durante o auge da pandemia de COVID-19. Cerca de 40% dos entrevistados da pesquisa de opinião da ITIC relataram que seus servidores, sistemas de operação e aplicações críticas de trabalho sofreram hackeamento de segurança bem-sucedido desde o início da COVID-19, no início de 2020. Isso representa um aumento de 9% de 31% apenas nos últimos 6 meses e um aumento de 21% acima dos 19% de organizações que afirmaram que seus servidores foram hackeados com sucesso na pesquisa ITIC 2020 Global Server Hardware, Server OS Reliability survey.

A segurança é uma questão tecnológica e de negócios que impacta todas as empresas. Cerca de 72% dos entrevistados citaram a segurança e as violações de dados como a maior ameaça a servidores, aplicações, data centers, borda de rede e confiabilidade do ecossistema de nuvem **(Veja a Figura 2)**. Os hackeamentos são mais direcionados, pervasivos e perigosos. Eles são desenvolvidos para causar o máximo de dano e perdas às suas vítimas de empresas e consumidores.

Figura 2. Segurança, erro humano, bugs de software: as principais causas do tempo de inatividade.



Fonte: Pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Security.

O panorama das ameaças: as vulnerabilidades de segurança e a violação de dados são as maiores e mais caras ameaças à confiabilidade

As violações de dados são um grande negócio e também o principal negócio para a crescente comunidade de hackers profissionais. Um hackeamento bem-sucedido pode gerar custo altos em vários níveis. Em 2020, o custo de uma violação de dados foi em média de 3,86 milhões de dólares, de acordo com o estudo do custo de uma violação de dados de 2020 realizado pela IBM e pelo Instituto Ponemon[1]. Isto representa um aumento de 10% desde 2015. Custos reais podem variar de acordo com a duração e gravidade dos ataques. Os ataques de ransomware continuam surgindo.

[1] "Estudo do custo da violação de dados de 2020", IBM e o Instituto Ponemon. URL: https://www.ibm.com/security/data-breach

E geram muitos custos. O ataque de ransomware de 7 de maio de 2021 pelos hackers DarkSide fechou a Colonial Pipeline Co. por 6 dias[2]. A Colonial Pipeline fornece 45% do gás e diesel para a costa leste dos EUA, de Nova Jersey à Flórida. O ataque interrompeu a distribuição e causou escassez de combustível em vários estados, incluindo Flórida, Carolina do Norte e Virgínia. O executivo Joseph Blount da Colonial Pipeline conseguiu encerrar os ataques quando concordou em pagar aos hackers um resgate de 4,4 milhões de dólares. Blount disse ao The Wall Street Journal que autorizou o pagamento do resgate de 4,4 milhões de dólares porque os executivos não tinham certeza de quanto o ciberataque havia violado seus sistemas, e, consequentemente, o quanto demoraria para recuperar o funcionamento do gasoduto.

O ataque de ransomware à Colonial Pipeline é apenas um exemplo entre muitos. Destaca as vulnerabilidades, os riscos e o alto custo associados aos ataques de segurança bem-sucedidos. O hackeamento de ransomware ao Colonial Pipeline reforça ainda mais a necessidade de criar uma infraestrutura de segurança robusta e de primeira linha. O hardware do servidor é o elemento fundamental de toda rede corporativa e seu ecossistema.

Um relatório DTEX Systems descobriu que "apenas 30% das organizações estavam preparadas para garantir uma migração completa para o trabalho remoto". O estudo DTEX Systems também revelou que quase 75% das organizações estão preocupadas com os riscos de segurança gerados por usuários que trabalham em casa e 73% das empresas admitiram que têm visibilidade parcial ou nenhuma visibilidade da atividade do usuário se sua VPN for desativada por funcionários remotos. Outra descoberta alarmante é que os teletrabalhadores usam seus notebooks de trabalho para uso pessoal, com 25% dos entrevistados reconhecendo que isso aumenta o risco de downloads direcionados e 15% afirma que suas empresas são mais suscetíveis a ataques de phishing.

O estudo mais recente da ITIC indica que o custo por hora do tempo de inatividade continua a subir. Agora ultrapassa os 300.000 dólares para 89% das PMEs e grandes empresas. No total, 42% dos participantes da pesquisa de empresas de médio e grande porte relataram que, em média, uma única hora de inatividade custa às suas empresas mais de 1 milhão de dólares. Na pior das hipóteses, uma violação de dados que ocorre durante os horários de pico de uso e interrompe as operações comerciais cruciais, pode custar às empresas milhões por minuto. Qualquer empresa que sofra uma indisponibilidade prolongada de horas ou dias como resultado de um ataque de ransomware direcionado provavelmente incorrerá em muitos milhões em danos.

Além das óbvias perdas monetárias devido à queda de produtividade e às operações interrompidas, as empresas devem levar em consideração o número de horas de trabalho e de

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

administradores de TI e segurança envolvidos nos esforços de correção e recuperação total da operação. As empresas também devem determinar se algum dado ou propriedade intelectual (PI) foi perdido, roubado, danificado, destruído ou alterado. As organizações também devem considerar o custo de qualquer processo judicial bem como possíveis multas associadas a incidentes de segurança e à violação de dados. Alguns custos, como danos à reputação de uma organização, são incalculáveis e podem resultar na perda de negócios.

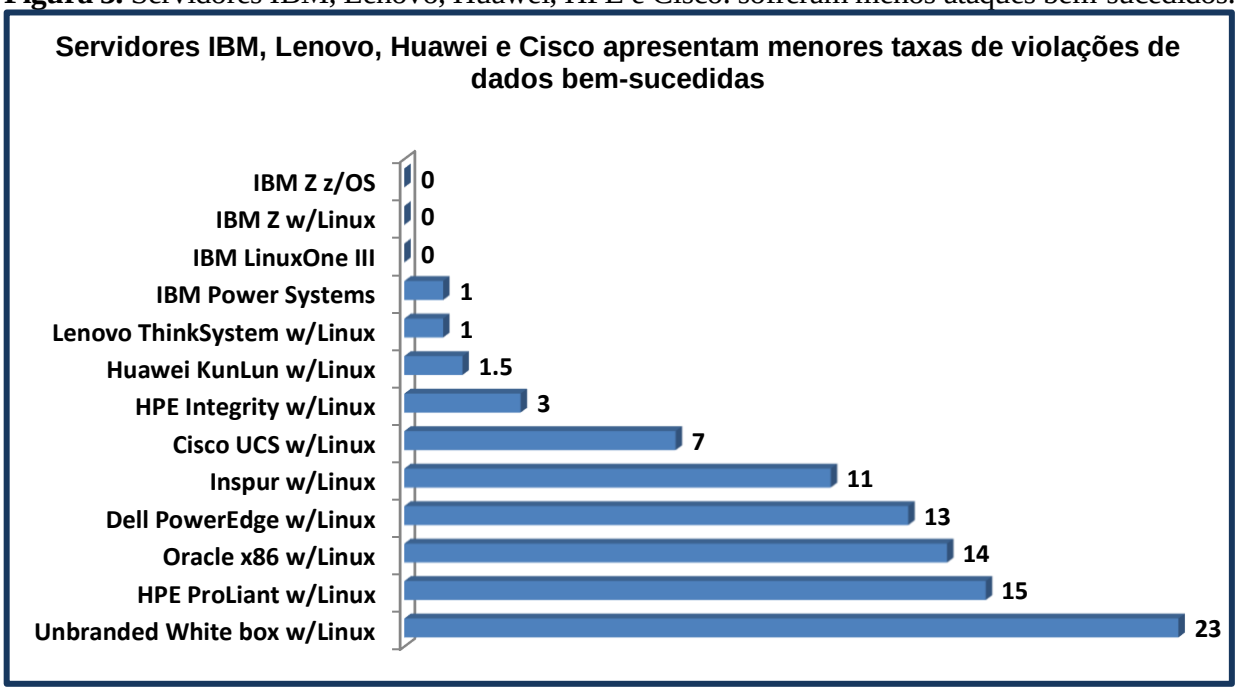
Hackers escolhem seus alvos com grande precisão e são rápidos em aproveitar todas as oportunidades. A pandemia da COVID-19 é o principal exemplo. Os(as) hackers imediatamente voltaram suas atenções para teletrabalhadores e alunos de ensino remoto fazendo aulas on-line e por Zoom. Miraram nos chamados "alvos fáceis". Municípios locais e estaduais, distritos escolares de pequeno e médio porte, hospitais, clínicas de saúde, consultórios médicos e agências bancárias que podem não ter segurança local em tempo integral e administradores de TI e podem não ter implementado medidas de segurança recentemente.

Fornecedores de servidor: a estratégia de segurança da IBM, Lenovo, Huawei e HPE.

Não é nenhuma surpresa que fornecedores como IBM, Lenovo, Huawei, HPE, que sempre alcançam as melhores classificações de confiabilidade de servidor, também estejam entre as plataformas de hardware mais seguras. Esses fornecedores e, mais recentemente, a Cisco, tornaram a segurança do servidor (no caso da Lenovo, a segurança do servidor, PC e de notebooks) uma prioridade e investiram pesado no reforço da segurança em relação aos seus produtos nos últimos anos. Portanto, quando a pandemia da COVD-19 aconteceu, eles já tinham uma segurança forte e integrada, o que ajudou muito.

Como indicado na **Figura 3**, a maioria das plataformas de hardware de servidor seguro sofreram menos violações de segurança bem-sucedidas. Todos os participantes que usam IBM Z em execução no z/OS, Red Hat Enterprise Linux (RHEL) e IBM LinuxONE III afirmaram que essas plataformas não sofreram violações de segurança bem-sucedidas nos últimos 16 meses. Eles foram seguidos pelos servidores IBM Power Systems e Linux ThinkSystem com uma violação cada; Huawei KunLun que sofreram em média 2 violações; o HPE Integrity com 3 violações bem-sucedidas e os servidores Cisco UCS com 7 violações de dados. Os servidores sem marca apresentaram maior vulnerabilidade, com uma média de 20 violações de dados bem-sucedidas nos últimos 16 meses.

Figura 3. Servidores IBM, Lenovo, Huawei, HPE e Cisco: sofreram menos ataques bem-sucedidos.



Fonte: Pesquisa de opinião **ITIC 2021** Global Server Hardware, Server OS Security.

Dados e análise: resultados de segurança do fornecedor

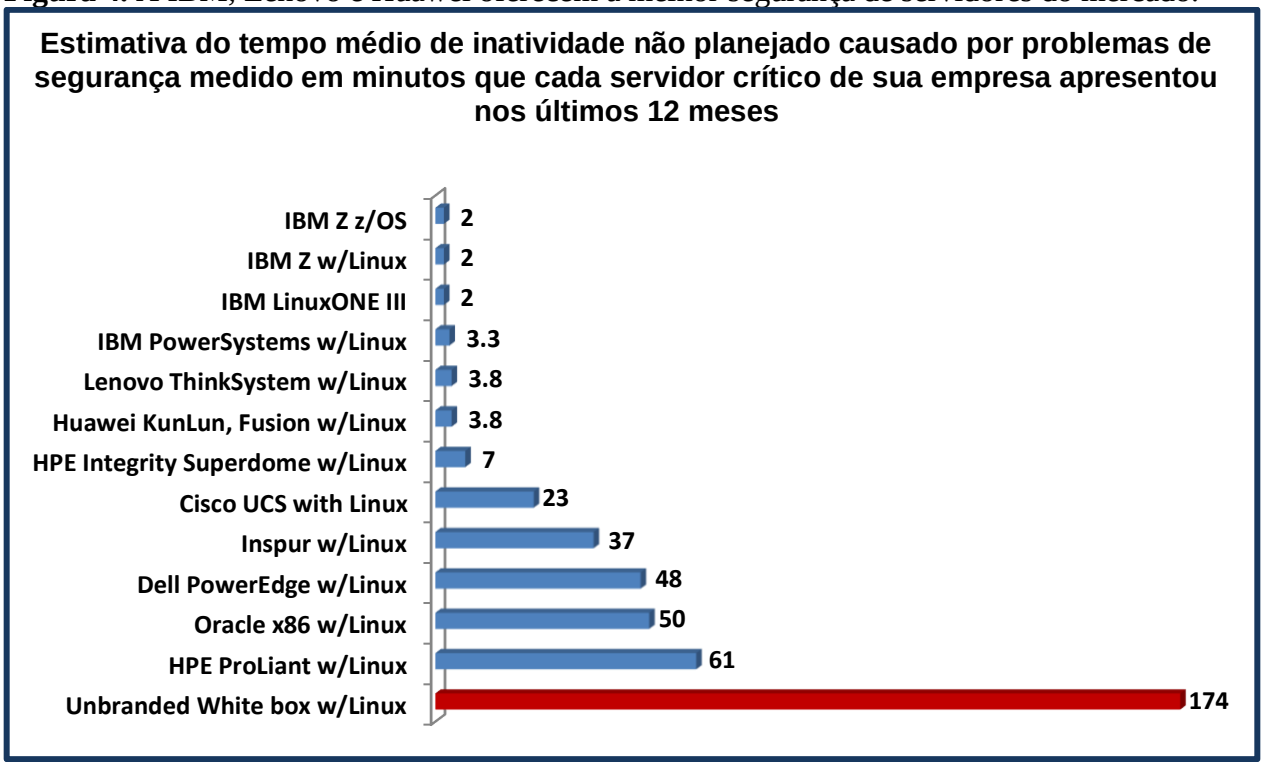
Para reiterar, a pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Security descobriu que os servidores IBM Z, IBM Power Systems, Lenovo ThinkSystem e Huawei KunLun e Fusion (respectivamente) alcançaram os melhores resultados em todas as categorias de segurança, incluindo:

- A menor quantidade de ataques de segurança **bem-sucedidos** e de violações de dados;
- O menor tempo de inatividade geral não planejada do servidor por ***qualquer***motivo e o menor tempo de inatividade não planejada do servidor como resultado de um incidente de segurança;
- O tempo médio de detecção (MTTD) mais rápido desde o início do ataque até a empresa isolá-lo e interrompê-lo;
- O tempo médio de correção (MTTR) mais rápido para restaurar servidores, aplicações e redes para retornar à operação total;
- A menor quantidade de dados perdidos, roubados, destruídos, danificados ou alterados como consequência direta de uma violação de segurança de dados (por exemplo, Ransomware, fraude de phishing ou fraude de CEO);
- A menor quantidade de perdas monetárias devido a um ataque de segurança bem-sucedido;
- A maior confiança na segurança integrada do hardware do servidor para fornecer alertas e evitar ataques de segurança e violações de dados.

Como ilustra a **Figura 4**, os servidores essenciais IBM Z, IBM Power Systems, Lenovo ThinkSystem e Huawei KunLun sofreram menor tempo de inatividade não planejado como resultado direto de incidentes de segurança e violações de dados bem-sucedidos.

O IBM Z e o IBM LinuxONE III apresentaram em média, apenas 2 minutos de tempo de inatividade não planejado por servidor causado por problemas de segurança. Eles foram seguidos pelos servidores POWER8 e POWER9 da IBM, que apresentaram pouco mais de 3 minutos de interrupções não planejadas por servidor como resultado de um problema de segurança. O hardware Lenovo ThinkSystem e os servidores Huawei KunLun e Fusion apresentaram, cada um, em média 3,8 minutos de tempo de inatividade não planejado por servidor associado a incidentes de segurança. Mais uma vez, os servidores sem marca, muitos dos quais executam versões não licenciadas de sistemas operacionais de servidor e aplicações de software, acumularam 174 minutos ou quase 3 horas cada um de tempo de inatividade diretamente atribuídos a problemas de segurança. Isso torna os servidores IBM Z até 87 vezes mais seguros e confiáveis do que o hardware sem marca e menos seguro, enquanto as soluções IBM POWER8 e POWER9 são até 58 vezes mais seguras do que os servidores sem marca.

Figura 4. A IBM, Lenovo e Huawei oferecem a melhor segurança de servidores do mercado.



Fonte: Pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Security.

O tempo médio de detecção é um medidor crítico

Os hacks de segurança e violações de dados são uma realidade para quem tem negócios na era digital. Em algum momento, toda empresa e sua linha crítica principal de servidores de negócios, sistemas de operação de servidor e de aplicações serão vítimas de uma tentativa de violação de dados de algum tipo ou bem-sucedidas.

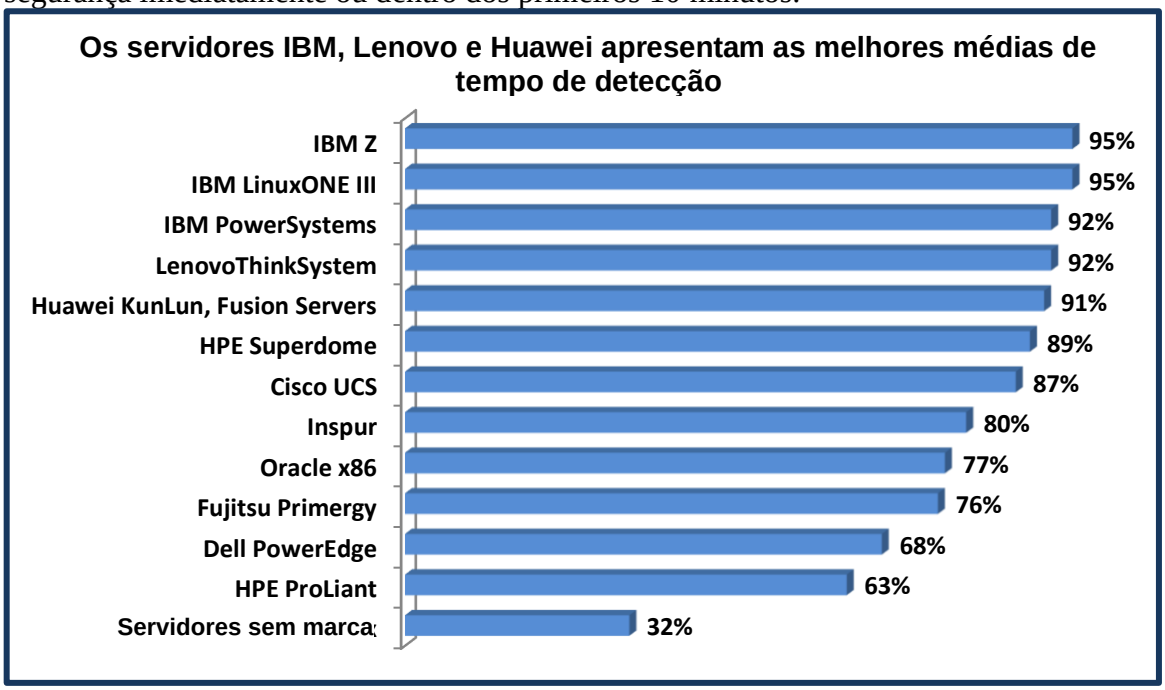
As organizações devem contar com um servidor integrado potente e segurança de infraestrutura que reconhece os riscos, envia alertas e alarmes, além de ter a capacidade de isolar as ameaças. Uma forte preparação por parte da empresa e uma equipe bem treinada de profissionais de segurança e administradores de TI são de extrema importância.

Quanto mais rápido os servidores e softwares da empresa conseguirem detectar um problema de segurança e gerar uma resposta, maiores as chances de isolar e interromper o ataque ***antes*** que ele possa se infiltrar na rede do ecossistema, interromper transações de dados e operações diárias e acessar dados sensíveis e PI.

A **Figura 5** mostra mais uma vez que os servidores IBM Z, IBM Power Systems, Lenovo Think-System, Huawei KunLun e Fusion Servers, HPE Superdome e Cisco UCS (respectivamente) se destacaram contra os ataques. Estes servidores tinham as melhores porcentagens de tempo médio de detecção (MTTD) entre todas as plataformas de servidores.

Uma esmagadora maioria de 95% dos entrevistados da pesquisa que usam IBM Z e IBM LinuxOne III indicaram que seus servidores foram capazes de detectar uma tentativa de violação de segurança “imediatamente ou nos primeiros 10 minutos” após o ataque e interrompê-lo. Eles foram seguidos em ordem pelas distribuições IBM Power Systems, Lenovo ThinkSystem e Huawei KunLun; 92% de cada um desses usuários da plataforma disseram que foram capazes de identificar e impedir uma violação de segurança “imediatamente ou nos primeiros 10 minutos”. Quanto mais rápido os servidores de infraestrutura central crítica, sistemas operacionais e aplicações críticas puderem impedir um ataque, maiores serão as chances da empresa sofrer tempo de inatividade curto ou nulo ou ser vítima de roubo, alteração, danos ou comprometimento de dados e PI.

Figura 5. Mais de 90% dos servidores IBM, Lenovo e Huawei detectaram ataques de segurança imediatamente ou dentro dos primeiros 10 minutos.



Fonte: Pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Security.

Resultados de segurança do fornecedor de servidores

Destaques da pesquisa de opinião da IBM Security

- Os servidores **IBM Z** continuam a alcançar altas pontuações para confiabilidade geral, acessibilidade, desempenho e segurança entre todas as plataformas de servidores. A família IBM Z, o "Z" refere-se a tempo zero de indisponibilidade, sempre supera **todos** os concorrentes em todas as categorias de confiabilidade, além de oferecer o menor custo total de propriedade (TCO) e o mais rápido retorno sobre investimento (ROI). Os servidores de sistemas z13, z14 e z15 obtiveram as melhores classificações de confiabilidade, tempo de atividade, disponibilidade de aplicação e segurança de modo geral em termos de minutos reais de tempo de inatividade não planejado por servidor anualmente. O mainframe IBM z e as distribuições IBM LinuxONE apresentam tolerância real a falhas apresentando apenas 0,60, menos de um minuto de tempo ***não planejado*** por servidor, por ano de inatividade anual devido a falhas de servidor, em comparação com os 0,74 segundos das plataformas Z e LinuxONE que alcançou a média na pesquisa da ITIC 2019 Global Server Reliability. Enquanto a redução de 0,14 segundos anual por tempo de inatividade do servidor parece insignificante, na realidade reduz o tempo de inatividade em quase 19% e diminui o TCO do IBM Z e LinuxONE em USD 230 - de USD 1.232 por servidor por minuto em 2019 para USD 1.002 por servidor por minuto no estudo mais recente da ITIC 2021 Global Server Hardware Security. No total, o IBM Z registra

apenas 4,32 segundos de tempo de indisponibilidade quase imperceptível mensalmente. Igualmente importante, dado o pico contínuo de hackeamentos de segurança e violações de dados, a segurança do servidor IBM Z é extremamente necessária. O Z continua registrando a menor porcentagem, menos de 1%, de violações de dados bem-sucedidas de janeiro a meados de junho de 2021. Além disso, os participantes da pesquisa de opinião do IBM Z e do LinuxONE III também relataram um MTTD (tempo médio de detecção) mais rápido, com 95% do entrevistados corporativos da ITIC afirmando que seus administradores de TI e de segurança foram capazes de detectar e encerrar ataques nessas plataformas. De modo individual e coletivo, estes resultados destacaram o sucesso dos produtos Z e LinuxONE III. As plataformas também foram reforçadas pela aquisição da Red Hat pela IBM em 2019. Isto resultou em um aumento significativo da carga de trabalho do Linux nas plataformas Z e LinuxONE. Executivos(as) da IBM declararam publicamente que a empresa observou um aumento de 55% na arquitetura MIPS do Linux. Também notaram que 92 dos 100 principais clientes do Z da IBM executam cargas de trabalho Linux. No total, a plataforma Z tem uma média anual de 100 a 200 novas implementações, segundo a IBM.

- O **LinuxONE III da IBM** é baseado na plataforma IBM Z. Ele é usado especificamente em ambientes de nuvem híbrida e utiliza a criptografia pervasiva do Z. A plataforma LinuxONE III e a IBM z15 também incorporam o IBM Hyper Protect Data Controller, que oferece proteção e privacidade transparentes de ponta a ponta no nível dos dados. O IBM Hyper Protect Data Controller permite que as empresas criptografem, concedam e revoguem acesso e mantenham o controle dos dados, mesmo quando sai do sistema de registro**.** O resultado: o IBM LinuxONE III obteve a mais alta classificação em segurança e confiabilidade na pesquisa da ITIC de 2021 com 95% das empresas LinuxONE III detectando e eliminando violações de dados "Imediatamente ou dentro de 10 minutos" após o início do ataque.
- **IBM Power Systems** 92% dos clientes do IBM Power Systems relataram que seus administradores de TI e de segurança foram capazes de detectar e impedir ataques "Imediatamente ou dentro de 10 minutos" após o início de uma violação. Os sistemas de escalabilidade horizontal POWER9 da IBM estão disponíveis no mercado há 3 anos e os servidores da nova geração Power10 estão com o lançamento agendado para o outono de 2021. A IBM atualiza continuamente a linha, com ênfase no desempenho, suporte a cargas de trabalho essenciais, suporte a bases de dados de análise avançada, in-memory e com segurança integrada. Todos os modelos do Power Systems estão habilitados para a nuvem. O IBM Power Systems tem segurança integrada em todas as camadas da solução: processador, sistemas, firmware, sistema operacional e hypervisor. Com criptografia acelerada integrada ao chip, os dados são protegidos em movimento e em repouso. A IBM afirma que o PowerVM hypervisor não possui relatos de vulnerabilidades de segurança. Os servidores POWER9 também são preparados para a nuvem e incluem capacidades integradas de virtualização do PowerVM. Os servidores de escalabilidade horizontal POWER9 são desenvolvidos para serem integrados às estratégias de nuvem e IA das organizações. Isso fornece o alto desempenho e os recursos RAS necessários para dar suporte às cargas de trabalho críticas, como bancos de dados IBM Db2 e Oracle, bem como SAP HANA. O Power10 foi desenvolvido para aumentar a eficiência e o desempenho em formatos de 7nm (nanômetros). A IBM estimou que isso resultará em melhorias de até 3x mais eficiência de energia do processador, capacidade de carga de trabalho e densidade de contêiner em comparação ao POWER9. Além disso, os próximos servidores Power10 também incorporarão uma série de capacidades avançadas, incluindo: suporte para

clusters de memória de vários petabytes que ampliarão a capacidade da nuvem de suportar cargas de trabalho que exigem uso intensivo de memória. O Power10 também contará com capacidades de segurança habilitadas por hardware, como criptografia de memória transparente para segurança de ponta a ponta. O processador IBM Power10 foi projetado para oferecer desempenho de criptografia significativamente mais rápido com o número de mecanismos de criptografia AES por núcleo 4 vezes maior em comparação ao IBM POWER9 para atender aos mais altos padrões atuais e padrões de criptografia futuros antecipados, como criptografia segura quântica e criptografia totalmente homomórfica. Além disso, oferece novos aprimoramentos para a segurança de contêiner.

Destaques da pesquisa de opinião da Lenovo

- Os servidores **Lenovo ThinkSystem** alcançaram as melhores taxas de MTTD entre todos os servidores baseados em Intel x86 com 92% dos participantes da pesquisa de opinião afirmando que seus administradores de TI e segurança detectaram e interromperam tentativas de hackeamento e violações de dados imediatamente ou dentro de 10 minutos a partir do início da invasão. Isto não é por acaso. Nos 7 anos desde que a Lenovo adquiriu o negócio de servidores baseados em x86 da IBM e na década desde que adquiriu a linha de PCs e notebooks da IBM, a Lenovo tornou a segurança sua principal prioridade. Consequentemente, os servidores e desktops da Lenovo foram se fortalecendo à medida que a empresa se aprimora continuamente e aprimora o desempenho, a confiabilidade e a segurança dos servidores e de seus desktops e notebooks. O serviço técnico e o suporte da Lenovo também são de primeira linha. Os servidores ThinkSystem da Lenovo mostraram melhorias contínuas de confiabilidade, com seu melhor tempo médio de atividade até o momento: 1,51 minutos de tempo de inatividade por servidor devido a problemas de hardware. Como a IBM, a Lenovo desenvolveu e executou uma estratégia e tática de segurança excelente e eficaz. Em 2018, a Lenovo revelou a tecnologia de segurança de ponta a ponta ThinkShield para seus PCs e notebooks. A tecnologia avançada ThinkShield tem mantido os PCs e servidores da Lenovo em boa posição ao longo dos últimos 3 anos, à medida que os ataques de segurança surgiam. Durante a pandemia global da COVID-19, à medida que muitas organizações migraram para uma equipe remota tanto de trabalhadores como estudantes, os administradores de TI e de segurança têm sido pressionados para acompanhar as violações de dados. A solução de segurança ThinkShield da Lenovo oferece suporte essencial para essas organizações. O ThinkShield, por exemplo, apresenta uma classificação de destaque no ThinkSystem SE350. Este modelo é o primeiro servidor voltado para a borda da Lenovo, destinado à rede de borda para fornecer a largura ideal de banda, reforçar a segurança e reduzir o tempo de inatividade. O ThinkSystem SE350 é um servidor que exige pouco espaço. Mede 1,75 polegadas de altura, 8,1 polegadas de largura e 14,9 polegadas de profundidade e pode ser montado em uma parede, empilhado em uma prateleira ou instalado em um rack. O ThinkSystem SE350 também foi desenvolvido para servidores de alto desempenho. É baseado no processador da Intel Xeon-D, equipado com 256 GB de RAM e 16 TB de armazenamento interno em estado sólido. O ThinkSystem SE350 tem características de segurança física aprimoradas como painel de travamento, detecção de intrusão, detecção de violação e armazenamento criptografado. Possui um software de implementação zero-touch. A estratégia global da Lenovo reúne a inovação e sistemas de data center confiáveis, flexíveis e seguros. Esta é uma estratégia inteligente que também tem ramificações de grande alcance para os servidores da Lenovo, redes e, em última análise, para seus clientes corporativos. O erro humano é de longe a maior causa do tempo de inatividade do servidor. Os usuários finais estão tradicionalmente entre os elos mais fracos da cadeia de

segurança global, particularmente durante a pandemia global da COVID-19, que viu uma porcentagem significativa de usuários finais adotando o teletrabalho e estudantes envolvidos no aprendizado remoto. Faz sentido para a Lenovo proteger os desktops e os servidores. A Lenovo aplica rigorosas normas, políticas e procedimentos de segurança em suas instalações de manufatura e cadeia de suprimento global. A equipe de engenharia de qualidade da Lenovo mantêm o direito de auditar os fornecedores de confiança da empresa a qualquer momento, dando à empresa ainda mais controle e visão sobre a segurança dos componentes de seus dispositivos. O ThinkShield também oferece segurança desde o seu projeto. Isso inclui BIOS e firmware seguros, bem como telas de privacidade e bloqueadores de câmera de notebooks em seus dispositivos para minimizar "hackeamento visual" quando os usuários móveis estão em locais públicos. O ThinkShield foi projetado para proteger as identidades e credenciais dos usuários, oferecendo autenticadores certificados pela FIDO e integração com o Intel Authenticate (oferecendo até 7 fatores de autenticação). O ThinkShield também apresenta a proteção USB inteligente baseada em BIOS, que funciona configurando portas USB para responder apenas a teclados e dispositivos apontadores. A Lenovo também enfatiza que suas plataformas abertas de servidor, armazenamento, rede e gerenciamento de sistemas se integram perfeitamente aos ambientes existentes e legados. Em entrevistas pessoais com analistas da ITIC, os clientes da Lenovo citaram a facilidade de implementação e de integração e a compatibilidade com versões anteriores, componentes que contribuíram para a confiabilidade e estabilidade subjacentes da plataforma ThinkSystem. Os usuários da Lenovo também elogiaram o serviço pós-venda e de suporte do fornecedor. O projeto de sistema da Lenovo suporta bancos de dados críticos, aplicações empresariais, grandes ambientes de dados e análise, e ambientes de nuvem e virtualizados. Ambos os sistemas incorporam vários recursos de tolerância a falhas e alta disponibilidade em um pacote lid-less otimizado para rack de alta densidade que minimiza o espaço necessário para suportar "operações de computação em rede de alta capacidade" e simplifica a manutenção, já que o sistema nunca precisará ser removido do rack. Em agosto de 2020, a Lenovo estreou vários novos modelos de seus servidores ThinkSystem de um soquete baseados nos processadores Advanced Micro Devices AMD EPYC série 702. Os novos produtos do portfólio de servidores da Lenovo são projetados especificamente para lidar com cargas de trabalho crescentes e com uso intensivo de dados, como segurança de vídeo, armazenamento definido por software e inteligência de rede. Também oferece suporte a ambientes virtualizados e borda de rede, onde a segurança é essencial. O resultado é uma solução que proporciona alta capacidade e eficiência para clientes que priorizam o balanceamento de rendimento e segurança com fácil escalabilidade. A Lenovo afirma que os dois novos servidores ThinkSystem "fornecem o desempenho de um servidor de soquete duplo ao custo de um servidor de soquete único", além de ter o potencial de reduzir os custos de licenciamento de software dos clientes em até 73% e reduzir o TCO em até 46% .

Destaques da pesquisa de opinião de segurança da Cisco UCS

- **O sistema de computação unificado (UCS) da Cisco** continua a ter uma boa pontuação e manteve os 2,3 minutos de de tempo de inatividade por servidor que foi alcançado pela primeira vez na atualização semestral da pesquisa de opinião ITIC 2020 Global Server Hardware, Server OS. De janeiro a meados de junho de 2021, os servidores da Cisco mantiveram-se estáveis em 2,3 minutos de tempo de inatividade por servidor. Isto não é fácil, considerando que muitos servidores Cisco UCS estão posicionados na borda da rede, que é a linha de frente dos ataques de segurança. Apesar disso, 87% dos entrevistados da pesquisa de opinião da Cisco UCS disseram ser capazes de detectar, isolar e interromper as violações de segurança imediatamente ou dentro de 10 minutos após a invasão. Participantes da pesquisa de

opinião da Cisco UCS também relataram que os servidores passaram por 7 violações de segurança bem-sucedidas nos últimos 18 meses. Em resposta ao aumento das violações de dados, a Cisco iniciou a publicação do Cisco UCS Hardening Guide. O documento está disponível para baixar gratuitamente. Este documento contém informações detalhadas para ajudar os usuários a proteger os dispositivos da plataforma Cisco UCS a fim de melhorar a segurança de rede. Estruturado em torno dos 3 planos pelos quais as funções de um dispositivo de rede são categorizadas, este documento fornece uma visão geral de cada recurso do Cisco UCS Software e faz referências à documentação relacionada. Além disso, a Cisco forneceu diversas atualizações de gerenciamento e desempenho com o objetivo de melhorar o TCO e acelerar a instalação e implementação. A Cisco afirma que seu UCS viabilizará uma redução de 86% no cabeamento e no provisionamento em questão de minutos (em vez de dias ou semanas), enquanto reduz as despesas de capital em mais de 40%. Os fabricantes garantem aos usuários 100% de compatibilidade entre os componentes. E o balanceamento de carga não será um problema.

Destaques da pesquisa de opinião de segurança da HPE

- A linha de servidores **Superdome da HPE** (incluindo os modelos Integrity e Flex) também apresentam alta confiabilidade de 99,999% a 99,9999% para uma maioria de 92% de seus clientes. E 89% dos entrevistados da pesquisa de opinião da HPE disseram que suas empresas identificaram e interromperam as violações de segurança "imediatamente ou nos primeiros 10 minutos". Os dados da pesquisa de opinião da ITIC mostram que os servidores Superdome da HPE passaram por 3 invasões de segurança bem-sucedidas nos últimos 18 meses. Isto coloca as plataformas de hardware HPE no topo, entre os 5 sistemas mais seguros. O portfólio do Superdome também se beneficia da estabilidade inerentemente forte do hardware HPE. A HPE tem feito da segurança, da inovação da funcionalidade e do desempenho, do suporte e de serviços técnicos pós-venda, sua prioridade. Tudo isso é crítico na era digital cada vez mais insegura, complexa e interconectada. A HPE está bem estabelecida entre empresas, desde pequenas e médias até as empresas maiores multinacionais. O HPE Superdome Flex Server possui capacidades de segurança RAS e proteção de ponta a ponta para as cargas de trabalho vitais. O HPE Superdome Flex Server, por exemplo, oferece escalabilidade de até 32 soquetes. Isto é 2,3 vezes maior que a capacidade de escalabilidade das informações das gerações anteriores de servidores. Ele também possui um design in-memory e capacidade de memória de 768 GB a 48 TB em uma única plataforma. O HPE Superdome Flex Server tem um design modular que varia de 4 a 32 soquetes e complementos de 4 soquetes. A HPE também diz que o servidor Superdome Flex tem um ponto de entrada mais econômico para cargas de trabalho críticas com 4 soquetes, ele oferece custo de aquisição até 45% menor em comparação com os modelos anteriores. A HPE também enfatiza a confiabilidade afirmando que as capacidades integradas do RAS do Superdome Flex Server oferecem de 99,999% a 99,999% de disponibilidade de um único sistema. A HPE também afirma que o servidor Superdome Flex reduz o erro humano por meio de seu mecanismo de análise de erro de manipulação de falha preditiva. Segurança e erro humano são dois problemas intimamente relacionados e prejudicam a segurança e a confiabilidade. Este mecanismo prevê falhas de hardware e inicia a auto-reparação, sem necessidade de intervenção humana ou "assistência por operador". Ele contém erros no nível de firmware, incluindo erros de memória, antes que qualquer interrupção possa ocorrer na camada do sistema operacional com a abordagem "Firmware First" do HPE. A HPE também oferece continuidade para cargas de trabalho Linux com sua solução de cluster de recuperação de desastre e de alta disponibilidade HPE Serviceguard for Linux (SGLX). Isso

permite às empresas proteger seus servidores executando o Linux em diversas falhas de infraestrutura e aplicações ao longo de ambientes físicos ou virtuais e de qualquer distância.

Destaques da pesquisa de opinião de segurança da Huawei

- Nos últimos 5 anos, a Huawei, com sede em Shenzhen, China, surgiu como um dos cinco principais fornecedores de hardware de servidor em todo o mundo com seu servidor KunLun crítico de ponta e seus servidores baseados em FusionServer x86 de uso geral. Com base na pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS e a pesquisa ITIC 2021 Global Server Hardware Security, os servidores Huawei KunLun e Fusion também estão entre as 3 plataformas de hardware mais confiáveis e seguras. Uma maioria de 91% dos entrevistados da pesquisa de opinião da Huawei observou que seus administradores de TI e segurança identificaram e interromperam tentativas de violação "imediatamente ou dentro de 10 minutos" após a tentativa de invasão. Os participantes da pesquisa de opinião da Huawei indicaram que os servidores KunLun e Fusion tiveram 1,5 ataques durante os últimos 18 meses. Desde 2015, a Huawei fortaleceu suas características de avanços, a segurança inerente e o desempenho geral dos seus servidores. Para competir com o sucesso dos concorrentes, incluindo Cisco, Fujitsu, HPE, IBM, Inspur, Lenovo e outros, a família de servidores da Huawei inclui rack de uso geral e servidores blade para hardware crítico a fim de lidar com a computação de alto desempenho (HPC). A Huawei também inseriu em seus servidores capacidades avançadas para suportar novas aplicações de computação intensiva, como IA, Big Data Analytics, Deep Learning e aprendizado de máquina. A Huawei está priorizando a segurança por meio de documentos de melhores práticas sobre "Como criar um sistema de defesa proativo"? por meio da sua solução HiSec que possibilita uma detecção mais inteligente de ameaça, resposta a ameaças, operações de segurança e manutenção. A Huawei diz que o HiSec melhora as capacidades de prevenção de ameaças de redes corporativas e a infraestrutura de telecomunicações, aumentando assim a eficiência de O&M de segurança e reduzindo os custos de O&M. Além disso, a Huawei oferece novos produtos de segurança para várias soluções de servidor no data center, na nuvem e na rede.

Conclusão

A segurança é a principal preocupação que impacta negativamente a confiança e a disponibilidade do hardware do servidor, dos sistemas operacionais do servidor e das aplicações de negócios mais críticas. Todas as organizações devem considerar a segurança como prioridade e trabalhar em conjunto com seus fornecedores para minimizar os riscos de segurança a um nível aceitável.

Cada segundo e minuto adicional do tempo de inatividade do servidor e de indisponibilidade das aplicações impacta negativamente as operações de negócios, a produtividade da equipe e a receita.

Os resultados da pesquisa de opinião ITIC 2021 Global Server Hardware and Server OS indicam que o mainframe IBM Z, IBM Power Systems, seguido pelos servidores Lenovo ThinkSystem, Huawei KunLun e HPE Integrity Superdome continuam a se fortalecer e a melhorar seu status

como as ofertas de hardware de servidor mais confiáveis. A plataforma IBM Z corporativa é a única a oferecer confiabilidade tolerante a falhas de seis e sete noves (99,9999% e 99,99999%) para mais de 93% de seus usuários de corporativos. Exceto os super computadores e hardware de alta disponibilidade (HA), nenhuma plataforma de servidor chega perto de atingir o nível de confiabilidade, disponibilidade e de tempo de atividade e segurança do Z.

9 entre 10 pesquisas de opinião afirmaram que as soluções IBM Power Systems e Lenovo ThinkSystem registraram ambos cinco e até mesmo os seis noves (99,999% e 99,9999%) de confiabilidade e disponibilidade. As plataformas IBM Power Systems e Lenovo ThinkSystem são até 30 vezes mais confiáveis e oferecem economia de custo até 36 vezes maior que os servidores sem marca e de pior desempenho.

Outra conquista notável é que a IBM e a Lenovo conquistaram o primeiro ou o segundo lugar nas categorias de confiabilidade e disponibilidade ou empataram em primeiro ou segundo lugar nas categorias de tempo de atividade, segurança ou gerenciamento de métricas na pesquisa de opinião.

A confiabilidade é fluida, não estática. Sem servidor, sem parte componente: disco rígido, memória ou CPU, sistema operacional, aplicação, dispositivo ou mecanismo de conectividade é imune a problemas de inércia ou falhas.

Os servidores são a base sobre a qual toda a infraestrutura da rede e o amplo ecossistema da rede se apoia. Quando os servidores falharem, o acesso aos dados será negado. A empresa para. A produção cessa. A receita sofre impactos. Cerca de 88% de todas as empresas agora exigem um mínimo de 99,99% de confiabilidade para o hardware de servidor, sistemas operacionais e aplicações principais de linha de negócios de suas empresas para garantir a produtividade e fornecer acesso ininterrupto aos dados. A alta confiabilidade e disponibilidade também protege as operações diárias da empresa, ativos de dados e a propriedade intelectual (PI), a informação da equipe de funcionários, os processos de negócio e o fluxo de receita.

Em 2021 e além da segurança, o erro humano e os usuários finais constituem as maiores ameaças que podem reduzir a confiabilidade e a disponibilidade de servidores, sistemas de operacionais e aplicações.

Ninguém sabe quanto tempo durará a pandemia global da COVID-19. E mesmo quando a pandemia for oficialmente encerrada, seus efeitos negativos e impactos provavelmente persistirão por anos, especialmente no que diz respeito às ameaças de violação de dados e segurança.

Este é o novo normal: hackers organizados chegaram para ficar. Continuarão a usar esta pandemia para explorar vulnerabilidades. Hackers continuarão a aproveitar todas as oportunidades de exfiltração de dados ativos corporativo e dos funcionários para obter lucro.

A confiabilidade do servidor, os dados ininterruptos e o acesso às aplicações e a segurança são sempre imperativos, mas especialmente durante a pandemia da COVID-19 com o teletrabalho e o aprendizado remoto. Cada segundo e minuto adicional do tempo de inatividade do servidor e

de indisponibilidade das aplicações impacta negativamente as operações de negócios, a produtividade do funcionário e a receita.

Uma parte significativa dos servidores e aplicações da empresa reside agora em ambientes virtualizados de nuvem e na borda da rede. Desde que a pandemia começou há mais de 18 meses, muitas empresas fizeram a transição de seus funcionários para o teletrabalho, escolas e universidades também adotaram o aprendizado remoto. Isto coloca maior pressão sobre as organizações e administradores de TI e de segurança que estão sobrecarregados para garantir tempo de atividade e disponibilidade de todos os ativos de dados.

A segurança é extremamente crucial. Os fornecedores devem continuar a fortalecer a segurança integrada do servidor; fornecer rapidamente correções quando falhas forem encontradas e trabalhar com os clientes para fornecer orientação prescritiva. As empresas também devem assumir a responsabilidade de garantir a confiabilidade e segurança de todo o servidor e da infraestrutura de rede e aplicações de negócios importantes em data centers e na nuvem. É fundamental que as empresas implementem e apliquem políticas e procedimentos de segurança fortes para **todos os funcionários**, especialmente teletrabalhadores e estudantes. Confiabilidade e segurança são elementos fundamentais da infraestrutura da rede. Ambos são necessários para garantir operações diárias ininterruptas, assegurar acesso a dados e proteger o fluxo de receita.

A pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Security enfatiza a necessidade de **todas** as organizações, independentemente do tamanho e do mercado vertical, se esforçarem de forma proativa e contínua para identificar e impedir a crescente variedade de ataques cibernéticos cada vez mais sofisticados e direcionados.

Isso significa implementar todas as medidas de segurança adequadas. A implementação e cumprimento de fortes políticas e procedimentos de segurança computacional é fundamental para **todos os funcionários da empresa**, desde executivos(as) C-suite até profissionais contratados e estagiários(as) da empresa. As empresas devem alocar orçamentos adequados para a compra de produtos de segurança e dedicar o tempo necessário e recursos de terceiros internos e externos apropriados para fornecer aos usuários finais, administradores de TI e profissionais de segurança as ferramentas de segurança e treinamento de segurança.

Não existe medidas de segurança 100% infalíveis. No entanto, as práticas de segurança multicamadas, reforçadas por testes de vulnerabilidade e treinamento de conscientização de segurança, podem reduzir o número de violações de dados e ataques de ransomware e reduzir o risco a um nível aceitável.

Os sistemas de missão crítica da Cisco, HPE e Huawei também tiveram um desempenho extremamente bom e não tiveram nenhuma queda na confiabilidade nos últimos 18 meses, desde o início da pandemia global da COVID-19. Os servidores Cisco, HPE e Huawei alcançaram quase a paridade de confiabilidade com a IBM e a Lenovo com base na robustez inerente do hardware principal.

Os servidores UCS da Cisco mantiveram o nível de confiabilidade na atualização semestral da pesquisa de opinião ITIC 2021 Global Server Hardware, Server OS Reliability. Desde 2019, as centrais de servidores Cisco UCS relataram que o tempo de inatividade caiu de pouco mais de quatro minutos (4,1) na pesquisa de confiabilidade anterior da ITIC para pouco mais de dois

minutos (2,3) por servidor anualmente devido a falhas de hardware. Isso é crítico. Uma parte significativa dos servidores UCS da Cisco é implementada na borda da rede, há muito considerada um dos pontos mais vulneráveis do ecossistema.

Nenhum fornecedor pode ficar tranquilo por muito tempo. A competição de vendas globais de hardware do servidor no mundo inteiro é intensa. É assim, continuará sendo e quem define as regras do mercado são os compradores. Enquanto muitas empresas, particularmente PMEs, tomam suas decisões de compra com base no preço, uma parte significativa das empresas optam por comprar hardware mais robusto, equipado com segurança integrada, gerenciamento avançado, IA e grande funcionalidade de análise de big data.

Os dados da pesquisa de opinião mostram que as empresas locais valorizam o suporte e os serviços pós-venda. As empresas requerem que os fornecedores atuem rapidamente se e quando problemas surgirem. Os fornecedores devem oferecer aos clientes recomendações realistas e orientação prescritiva para configurações do sistema e ciclos de vida do produto para atingir e manter o desempenho e a disponibilidade ideais.

Como sempre, a ITIC afirma que os fornecedores também têm a responsabilidade de fornecer correções e atualizações em tempo hábil e informar os clientes da melhor maneira possível sobre quaisquer problemas conhecidos de incompatibilidade que possam afetar o desempenho. Os fornecedores também devem ser honestos com os clientes e notificá-los de problemas ou atrasos na entrega de peças de reposição.

Recomendações

Nenhuma plataforma, sistema operacional de servidor ou aplicação de negócios fornecerá uma segurança infalível. No entanto, as empresas IBM, Lenovo, Huawei, HPE e Cisco, que estão entre as plataformas de servidores mais confiáveis, também fornecem os maiores níveis de segurança inerente. Isso permite aos clientes alcançar a maior economia de escala e proteger seus ativos sensíveis de PI e de dados. A segurança é uma responsabilidade de ambas as partes. Embora os fornecedores devam oferecer uma segurança potente, as empresas são responsáveis por manter a confiabilidade de seu servidor e a infraestrutura de rede abrangente. A ITIC recomenda fortemente às empresas:

- **Fazer um inventário.** Saiba os elementos que compõem a sua rede. Isto significa catalogar ***todos*** os servidores, principais aplicações cruciais da linha de negócios, dispositivos de rede (firewalls, roteadores) em todo o ecossistema da rede, incluindo o data center, escritórios remotos, nuvens públicas, privadas e híbridas, dispositivos IoT e a borda da rede.
- **Obter hardware de servidor do tamanho certo**. O hardware do servidor deve ser potente o suficiente para acomodar as cargas de trabalho atuais, bem como o aumento previsto da carga de trabalho e aplicações maiores.

- **Substituir, retroajustar e atualizar regularmente o hardware do servidor.** Isso significa manter-se atualizado com as correções e atualizações indispensáveis de segurança, ***conforme necessário***, para manter o funcionamento do sistema e atingir o pico de desempenho do sistema.
- **Atualizar o software.** Conforme o possível, nunca fique mais de duas versões atrasadas nos sistemas operacionais de servidor e das principais aplicações baseadas em servidor.
- **Implementar políticas e procedimentos de alta segurança.** É importante que empresas de todos os tamanhos e em todos os segmentos de mercados verticais criem políticas e procedimentos abrangentes de segurança corporativa. Divulgue-os através de cópia impressa e por e-mail para todos os funcionários. As políticas de segurança computacional do sistema devem ser parte integrante das diretrizes gerais corporativas e devem conter termos e condições específicas e multas para o primeiro, segundo e terceiro delitos. As empresas também são aconselhadas a fazer com que todos os funcionários participem de um treinamento obrigatório de segurança de computadores, semelhante ao treinamento de assédio sexual.
- **Monitore de perto os acordos de nível de serviço (SLAs).** Preste muita atenção aos contratos de SLA para garantir que os fornecedores de software e hardware da sua empresa e que fornecedores de serviços em nuvem atendam ou excedam os termos dos SLAs para entregar os níveis de confiabilidade acordados.
- **Aplique testes de vulnerabilidade de segurança.** Dado o aumento contínuo em todos os tipos de ataques de segurança e violações de dados, por exemplo, ransomware, ataques de phishing e fraude de CEO, todas as empresas devem realizar testes de vulnerabilidade pelo menos uma vez por ano e de acordo com a necessidade. A ITIC recomenda que as empresas trabalhem com especialistas independentes de empresas terceirizadas.
- **Crie um plano de governança e recuperação.** Tenha um plano de correção e controle em vigor no caso em de sua empresa ser hackeada com sucesso. Atribua uma hierarquia para indicar os responsáveis em caso de violação de dados ou interrupção da rede. O plano de controle e correção também deve designar e atribuir determinadas tarefas para grupos e indivíduos específicos. Certifique-se de que o plano também inclui as informações de contato pertinentes para todos os fornecedores e provedores de serviços terceirizados.
- **Formar e certificar administradores de segurança e TI.** Assegure que os profissionais de segurança e TI recebam treinamento adequado e tenham as certificações de segurança necessárias.
- **Fornecer treinamento aos usuários finais.** Certifique-se de que os usuários finais, bem como trabalhadores contratados e funcionários temporários, recebam treinamento de conscientização de segurança adequado sobre os golpes mais recentes de e-mail, phishing e ameaças de ransomware.

Metodologia

A *pesquisa de opinião ITIC 2021 Global Server Hardware Security Reliability* contou com a participação de executivos(as) C-suite e gerentes de TI de mais de mil empresas no mundo inteiro entre janeiro de 2021 até a metade de junho de 2021. A pesquisa independente baseada na web incluiu questões de múltipla escolha e uma questão dissertativa. Para manter a objetividade, a ITIC não aceitou patrocínio de fornecedores. Nenhum participante da pesquisa de opinião recebeu qualquer remuneração. Analistas da ITIC também conduziram 20 entrevistas diretas com clientes para obter dados valiosos, obter insights mais profundos e conhecimento contextual do impacto e das implicações das vulnerabilidades de segurança e das violações de dados sobre a confiabilidade do servidor corporativo e a infraestrutura de rede. Entrevistados como executivos(as), administradores de TI e segurança e usuários finais. A ITIC implementou mecanismos de autenticação e rastreamento para evitar adulterações e para proibir respostas repetidas pelas mesmas partes.

Dados demográficos da pesquisa de opinião

A ITIC entrevistou 1.100 empresas de todos os tamanhos e de 28 mercados verticais para a pesquisa de opinião. Corporações de todos os tamanhos foram bem representadas. Os entrevistados fazem parte de empresas pequenas e médias (PMEs) com menos de 50 trabalhadores, até empresas multinacionais com mais de 100.000 funcionários.

Todos os setores do mercado estavam igualmente representados: as PMEs com 1 a 100 funcionários representavam 24% dos entrevistados. As pequenas e médias empresas (PME) com 101 a 1.000 funcionários representam 28% dos participantes. Os 43% restantes dos entrevistados fazem parte de grandes empresas que possuem entre 1.001 e mais de 100.000 funcionários. Os participantes da pesquisa de opinião fazem parte de 49 mercados verticais diferentes. Aproximadamente 61% dos entrevistados são da América do Norte, 39% são clientes internacionais que de 22 países da Europa, Ásia, Austrália, Nova Zelândia, América Central/Sul e África.

Anexos

Esta seção fornece links para várias estatísticas e pesquisas da ITIC citadas neste relatório.

Site da ITIC e links para as pesquisas de opinião e posts em blogs:

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/