Solitaire Interglobal

A sua plataforma é segura? É mesmo?

Uma análise quantitativa dos diferenciais da tecnologia de segurança oferecidos aos negócios pela IBM e por outros fornecedores

1. Introdução

"As empresas precisam estar atentas à sofisticação dos crimes cibernéticos atuais. Práticas e ferramentas de ataque sofisticadas, antes controladas pelos governos, agora são utilizadas e aprimoradas em todo o mundo por quadrilhas especializadas em crimes cibernéticos, que são financiadas pelos serviços contratados e por seus frutos. Além disso, os perfis de ataque estão concentrando-se no nível do kernel do sistema operacional e no hipervisor de virtualização. Assim, os ataques muitas vezes passam despercebido para dispositivos e software de segurança comerciais."

Robert Bigman — CEO da 2BSecure e ex-CISO da CIA

A segurança tornou-se mais complexa no atual mundo virtualizado, conectado e baseado em nuvem dos negócios. Todas as organizações que aproveitam a tecnologia enfrentam vulnerabilidades muito maiores, e os desafios para a segurança passaram da exposição limitada, concentrada na segurança física, para a urgência da exposição eletrônica. A introdução da arquitetura em nuvem e da virtualização que a acompanha criou novas oportunidades de ataque. Com isso, o desafio de proteger os recursos e processos organizacionais, evitando efeitos colaterais nos níveis de serviço, é cada vez maior. Embora muitas organizações vejam a segurança como o mero acesso aos recursos, a Solitaire Interglobal Ltd. (SIL) tem uma visão muito mais ampla do que é segurança, com enfoque em:

- Dados — acesso (leitura e cópia) ou manipulação[1]
- Segurança do processo — possibilidade de executar, atrapalhar e sequestrar
- Arquitetura — propriedade intelectual (por exemplo, modelo comercial, estrutura do processo etc.)
- Físico — acesso à planta ou às instalações físicas

A segurança física e o controle de acesso são aspectos importantes, mas as análises de segurança da SIL concentram-se nas três primeiras áreas. Como resultado desses esforços, a SIL coletou grandes quantidades de dados sobre problemas e desafios de segurança enfrentados por seus clientes em todo o mundo. Esses dados servem de catalisadores para a definição proativa e a análise de tendências de novos problemas, identificando possíveis ameaças em seus primeiros estágios. Por essa razão, os dados compilados mostram mudanças importantes no tipo e no escopo das ameaças, e essa é a base dos dados utilizados no estudo da SIL. O mais surpreendente foi descobrir que a grande maioria dessas organizações *não tinha ideia do total de invasões*[2] em seus sistemas.

De modo geral, o aumento na quantidade de aplicativos para uso externo expõe a infraestrutura organizacional a uma base de usuários maior e sobre a qual há menos controle. Devido ao aumento na virtualização e na computação em nuvem, novas ameaças à segurança estão surgindo. Uma das ameaças que mais cresce é o ataque indireto dos hackers, que interceptam a conexão entre as VMs, como uma quadrilha que cava um túnel para chegar ao cofre de um banco. A segurança é uma área dinâmica e desafiadora, e as empresas têm dificuldades para entender o impacto dela sobre os processos de fornecimento de informações, a equipe de apoio e os diferentes elementos críticos para as decisões que devem ser levados em consideração. A medição da segurança é uma grandeza ponderada, pois ela é avaliada com base na ausência de problemas.

---

[1] *A segurança dos dados inclui qualquer tipo de acesso às informações da organização, como a leitura ou cópia de conteúdos específicos. Por manipulação dos dados de uma determinada organização, entendemos que as informações foram modificadas ou excluídas para alterar o conteúdo ou alterar a relação de atributos e entidades.*

[2] *O estudo combina todos os tipos de ataques, com origem em falhas de segurança hostis ou neutras, invasões ou violações, ou eventos iterativos ou em cascata resultantes do evento inicial. Para esse estudo, todos os eventos iniciais e correlacionados foram tratados da mesma forma e listados na classificação geral de invasões.*

As falhas na segurança são altamente visíveis, ao contrário do seu êxito. Para esclarecer as métricas ponderadas usadas, a IBM contratou a SIL para realizar pesquisas, coletar dados e fazer análises, com a finalidade de esclarecer os benefícios e custos relativos da implementação da plataforma IBM Power. Essa análise concentrou-se principalmente no valor da segurança para os negócios, para que a liderança das empresas pudesse entender os benefícios das opções de segurança oferecidas pela IBM Power ao avaliar as soluções disponíveis.

Durante o estudo, as principais características comportamentais de software e hardware foram analisadas atentamente em mais de 63.200 instalações reais. Todos os clientes que participaram do estudo utilizam a segurança em seus ambientes de produção, sendo que alguns utilizam um único padrão de segurança e outros, uma combinação de mecanismos e métodos de segurança. No grupo analisado, temos organizações que precisam seguir padrões regulamentados e do setor (como HIPAA, PCI, SOX, entre outros) para garantir a segurança das informações. As informações desses relatórios sobre os clientes e os detalhes reais apresentados ajudam a compreender como os diferentes tipos de segurança afetam os clientes.

2. Descobertas

A finalidade dessa análise é avaliar o impacto real nas empresas que implantam as plataformas IBM Power em seus sistemas de segurança e compará-lo aos resultados das empresas que usam produtos UNIX ou x86, incluindo componentes agregados. Nessa análise, as diferentes variantes de x86 e UNIX foram divididas em dois grupos e tratadas como duas entidades. As métricas usadas para analisar as diferenças entre as plataformas são objetivas e subjetivas. Como métricas objetivas, temos dados sobre custo, tempo de execução, uso de recursos e outros fatores. Como métricas subjetivas, temos as respostas em diversos níveis, fontes de satisfação do cliente e percepção. No resumo abaixo, destacamos algumas das descobertas.

Resumo

Categoria	Comentário	Dado rápido
Satisfação do cliente	*Os altos níveis de satisfação do cliente são sinal da ausência de problemas — não há uma métrica mais definitiva.*	*Os clientes que utilizam a integração da segurança da arquitetura IBM Power estão 68% mais satisfeitos do que as empresas que utilizam soluções da concorrência.*
Custo total de propriedade (TCO)	*O custo total do IBM Security é consideravelmente mais baixo do que o custo das opções da concorrência, mas a economia real é observada em uma métrica ponderada. O custo das invasões em ambientes que utilizam as soluções IBM é 68% menor, em comparação a ambientes que utilizam soluções de outras marcas.*	*Levando os custos diretos em consideração, o TCO pode ser 52,87% menor com o uso de soluções da IBM. Essa visão simplificada não inclui o alto custo das invasões.*
Equipe	*Em ambientes complexos, a IBM Power requer menos pessoal do que as opções da concorrência.*	*As equipes que utilizam IBM Security são muito mais eficientes; a economia em pessoal para administração da segurança pode chegar a 71%.*
Invasões	*A IBM Power enfrenta menos de 2% das invasões que assolam outras arquiteturas, gerando uma economia de milhões de dólares.*	*Pouquíssimas invasões relatadas ou detectadas em ambientes que usam a pilha de segurança da IBM.*
Exposição da nuvem	*A IBM Power enfrenta menos de 0,3% de todas as invasões relatadas em nuvens públicas e privadas.*	*Nenhum provedor de serviços em nuvem relatou invasões na IBM Power.*

Essas principais descobertas são motivos suficientes para escolher os produtos IBM para a segurança e arquitetura das organizações.

2.1. Perspectiva comercial

Basicamente, a TI e a tecnologia têm a função de viabilizar as funções comerciais. Uma das principais perspectivas do estudo foi a visão da gestão comercial executiva e da linha de negócios (LOB) das organizações. Os padrões operacionais das organizações que participaram do estudo foram agrupados em categorias e comparados para que fosse possível identificar sua influência sobre as métricas comerciais. As métricas são:

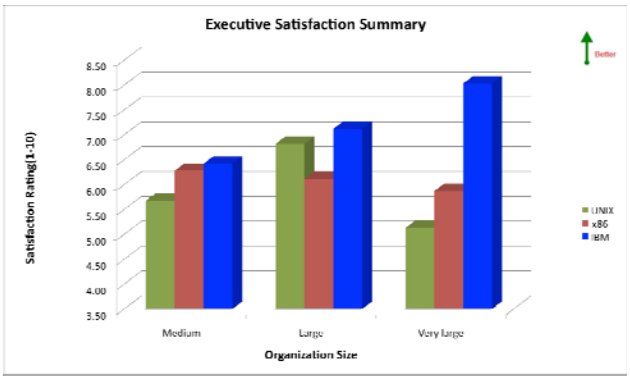
- Satisfação do cliente
- Custo total de propriedade
- Equipe
- Níveis das invasões

Todas essas métricas apresentam diferenciais consideráveis e mensuráveis quando levamos a solução de segurança IBM Power em consideração. As métricas comerciais mais granulares são aquelas que mostram a diferença no dimensionamento específico do êxito das organizações em geral, em comparação ao êxito das organizações que implantaram a IBM Power. Essas métricas têm ampla cobertura e levam as finanças, bem como a qualidade da

organização, em consideração. Para serem significativas em diversos setores, todas as métricas foram padronizadas com base em uma unidade de trabalho[3] e divididas em categorias, de acordo com o tamanho das organizações (pequenas, grandes e muito grandes). A medida básica foi definida pela empresa média comum. Assim, todas as outras métricas baseiam-se em uma variação desse padrão. As implementações tratadas neste estudo estão restritas às implementações na produção.

Satisfação do cliente

A SIL usou três métricas diferentes de satisfação do cliente: feedback dos executivos, feedback dos usuários finais da TI e feedback do pessoal operacional. A primeira forma de verificar o êxito do sistema é o feedback da gestão executiva. A satisfação da gestão executiva geralmente se concentra na aplicação e no custo, não na segurança. Esse nível de satisfação é totalmente ponderado e fica evidente apenas quando não há problemas. Nesse caso, a satisfação está relacionada à segurança transparente e bem-sucedida. Para os executivos, uma das principais formas de percepção de êxito é a quantidade de reclamações que eles recebem sobre o sistema operacional, que é inversamente proporcional ao êxito. Há pouquíssimas reclamações decorrentes do uso dos sistemas IBM Power. Todos os executivos citaram pelo menos uma das opções a seguir como motivo de satisfação e apenas 5% dos entrevistados citou o custo da segurança. Os três principais motivos citados foram:

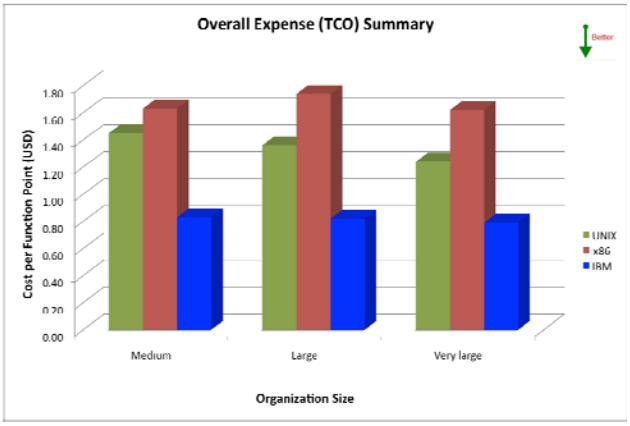


1. Ausência de invasões à segurança
2. Transparência das métricas de segurança para os usuários finais
3. Custo de segurança razoável

Os resultados das métricas de reclamações dos usuários finais da TI e do pessoal operacional encontram-se no documento principal do estudo.

Despesa total (TCO)

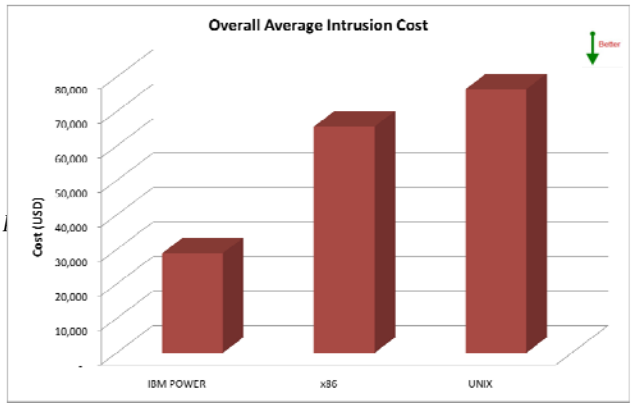
O custo leva em consideração o custo total para a empresa ao longo de um determinado período e é padronizado com base no contingente de funcionários, na receita das vendas e na contagem das entidades jurídicas. A métrica financeira TCO é mais abrangente do que as métricas operacionais diretas. Combinada a outras métricas comerciais, ela ajuda a definir uma perspectiva adequada.



As implementações de segurança IBM Power têm custos menores (até 50,92% menores) em empresas de diferentes tamanhos. Grande parte dos diferenciais das soluções é o custo mais baixo das implantações de segurança eficientes, o que inclui o custo das equipes. Clientes de todos os tamanhos observaram um padrão consistente de diferenciação em três áreas principais:

- Ausência de custo extra para segurança aprimorada
- Custos mais baixos devido aos efeitos das invasões
- Custos com pessoa mais baixos (devido às ferramentas, à flexibilidade etc.)

A combinação da métrica de custo ponderada e do TCO da infraestrutura conferem destaque à pilha integrada de opções da IBM Power e contribui para economias de até 68,2%. Essa é a principal diferença entre uma pilha de segurança altamente integrada pronta para uso, em comparação a arquiteturas agregadas, que aumentam as



[3] *A unidade de trabalho foi definida por meio de padrões publicados em análises de ponto de função (FP).*

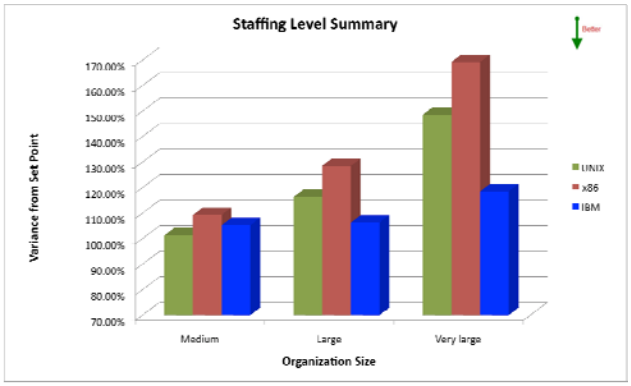
vulnerabilidades. A análise de custo inclui algumas métricas ponderadas, como:

- Perda do serviço
- Declínio do cliente devido à falta de confiança
- Alterações não estratégicas à arquitetura
- Recuperação de dados perdidos ou danificados
- Perda de capital intelectual exclusivo

A média dos custos associados a uma invasão serve de métrica para o impacto financeiro, que é uma indicação da exposição do custo relativo de diferentes tecnologias. Infelizmente, o mercado está satisfeito com o conceito de "perda aceitável", o que abre precedentes para negligências no controle e na definição da segurança, ignorando exposições reais a impactos maiores e mais graves das invasões. Quando uma organização dispõe-se a tolerar perdas "contornáveis" frequentes, suas informações e operações ficam vulneráveis e tornam-se alvos perfeitos para danos maiores.

Equipe

Um fator básico em muitas outras áreas é a eficiência da interface entre o usuário técnico e a infraestrutura. Em vez de comparações altamente detalhadas que perdem seu valor justamente devido ao excesso de detalhes, analisamos uma visão geral de equipes que trabalham em período integral, a fim de fornecer uma métrica geral baseada em um ambiente "padrão ouro".



As equipes de segurança notadamente menores necessárias para a implantação e o uso da plataforma IBM Power são resultados diretos da natureza integrada da pilha operacional IBM Power. Os níveis padrão das equipes necessárias para as implantações da plataforma IBM Power são até 42,8% menores do que os níveis necessárias para as implantações concorrentes.

Níveis das invasões

As invasões podem ser definidas como ataques — roubo, destruição ou bloqueio — bem-sucedidos ao cenário organizacional. Ao analisar as invasões, a SIL levou em consideração:

- a quantidade das invasões
- o tipo das invasões
- o efeito das invasões

As medidas de proteção em vigor devem cobrir ainda mais pontos de acesso do que o necessário para a segurança em toda a plataforma. Nesse caso, é necessário ter controle sobre as principais esferas da TI, E/S, o acesso à rede, o gerenciamento da memória e o acesso geral para execução normal.

Com base na funcionalidade e no controle essenciais, diferentes plataformas fornecem diferentes coberturas de segurança. Essas coberturas estão relacionadas aos recursos de segurança que acompanham a instalação básica, ou seja, a configuração pronta para uso, já que é possível complementar todas as configurações de segurança. Se a perspectiva de segurança for dividida nessas diferentes classes, a análise de custo com base nos complementos que devem ser adicionados à plataforma básica para implementar esses níveis mostra que o custo para alcançar a segurança necessária pode ser alto. Um exemplo disso é visto com o uso de um dos perfis de segurança mais comuns, o processamento de cartões de crédito. Neste resumo, o custo para que as arquiteturas alcancem o nível de segurança necessário (100%) é expresso como uma porcentagem do custo total da implementação. Este resumo de custo inclui operações, hardware e middleware, mas não inclui aplicativos.

Segurança no processamento de cartões de crédito, por plataforma

Descrição	***IBM Power***	***x86***	***UNIX***
Configuração básica	*43,15%*	*11,04%*	*18,28%*
Custo adicional para alcançar a segurança necessária	*8,16%*	*46,27%*	*29,53%*

A análise dos requisitos de segurança adicionais encontra-se no documento principal do estudo.

A SIL analisou a vulnerabilidade de um grupo aleatório de clientes. Alguns desses clientes estavam cientes sobre as invasões de segurança, mas todos estavam interessados na eficiência das medidas de segurança em vigor. A descoberta mais assustadora foi o alto índice de organizações que sofreram violações de segurança que passaram despercebidas. Por exemplo, a análise identificou processos de extração estranhos, *sinal de pirataria*, em 105 organizações. Esses processos roubam informações e afetam outros processos em tempo real.

2.2. Perspectiva técnica

Uma das principais perspectivas dessa análise é o ponto de vista do profissional de TI. Como a TI precisa conhecer a arquitetura fundamental e as características importantes de todas as tecnologias, essa perspectiva concentra-se principalmente em entender como a segurança da plataforma IBM Power pode contribuir e o que é necessário. Isso inclui conhecer algumas características básicas de desempenho e desempenhos operacionais.

A perspectiva técnica também é útil para avaliar os negócios, pois está relacionada aos elementos da operação que resultam em fatores de risco, desempenho e eficiência significativos. As métricas levadas em consideração são:

- controle e visibilidade da gestão
- segurança da nuvem
- dispositivos pessoais no local de trabalho (BYOD)

Controle e visibilidade da gestão

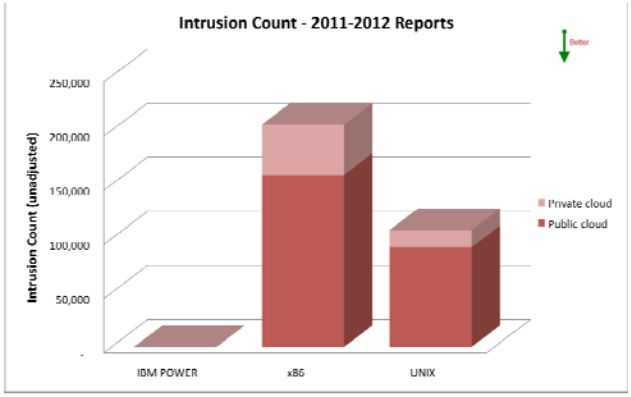
O controle e a gestão do ambiente de segurança são aspectos básicos de todas as implantações de segurança. Para gerenciar a proteção da segurança, alguns pontos de controle e visibilidade comuns podem ser definidos como:

- monitoramento de ameaças e atividade de resposta às ameaças
- dados sobre dados, incluindo a cobertura e a definição dos componentes de segurança
- escopo das invasões

A arquitetura de pilha integrada presente nas plataformas IBM Power fornecem ferramentas de gestão e visibilidade abrangentes, diferentemente das plataformas da concorrência, que proporcionam menos integração. As áreas de integração opcional com sistemas de segurança que não são estreitamente integrados criam outros pontos de vulnerabilidade que os hackers podem aproveitar.

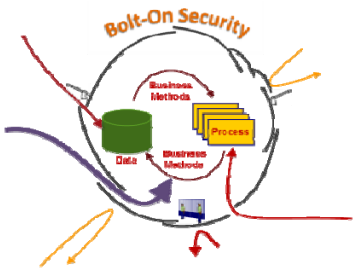
Segurança da nuvem

Hoje, a integração com os serviços em nuvem é uma iniciativa comum no mercado. Levando isso em consideração, parte do estudo observou a implantação na nuvem e a relação com uma estratégia de segurança. Nessa área, diversos pontos foram analisados. Um desses pontos é o uso que os clientes fazem da nuvem, dividido por métodos de segurança. A integração da nuvem no cenário organizacional cresce cada vez mais rápido. Nesse ponto da curva tecnológica, muitas organizações optaram pelas nuvens públicas — em partes devido à falta de informações sobre os custos e riscos das nuvens privadas. Com a ampliação da base de conhecimento, a consideração do aumento da proteção da nuvem privada também cresce, e mais empresas passam a optar pelas nuvens privadas.

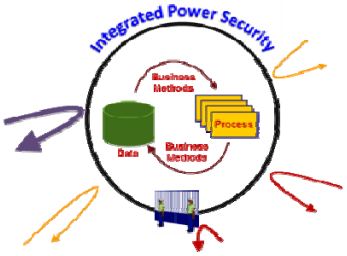


A exposição da segurança da nuvem está aumentando, com o aumento do uso da nuvem. O gráfico mostra as invasões relatadas em organizações que implantaram a arquitetura de nuvem, mostrando os dados das nuvens públicas e privadas. A incidência de violações de segurança e invasões nas nuvens públicas é muito maior do que nas nuvens privadas. Além disso, essa incidência na pilha IBM Power é consideravelmente menor — até 87,58% menos — do que nas demais opções disponíveis. Na verdade, nenhuma nuvem pública relatou violações de segurança nas plataformas IBM Power. Contudo, como poucas nuvens públicas hospedam plataformas Power, as descobertas são sugestivas, mas inconclusivas. Isso é sinal das diferenças inerentes úteis para que os provedores de nuvem escolham suas próprias plataformas.

BYOD



Outro desafio para a segurança dos processos e das informações organizacionais é a crescente tendência da prática BYOD no local de trabalho com a integração de componentes — que atendem e não atendem aos padrões de segurança corporativa — à infraestrutura. No último ano, o uso desses dispositivos no grupo analisado cresceu 642%. Com isso, a segurança dos ativos organizacionais ficou mais complexa e volátil. O aumento nos recursos que permitem recuperar e manipular informações organizacionais por meio desses dispositivos cria outra camada de complexidade na definição de políticas de segurança.



As políticas que definem o acesso aceitável às informações geralmente seguem as tendências nesse ambiente, no qual os controles de segurança distribuídos e segmentados podem criar pontos cegos. A proteção dos processos e dados da organização fica mais vulnerável nos dispositivos. Por isso, as estratégias mais eficientes centralizam mais a definição e o controle das políticas. A natureza abrangente da segurança integrada dos sistemas Power é consideravelmente diferentes da segurança criada com topologias agregadas.

2.3. Conclusão

Conhecer a segurança da TI é um desafio, devido à natureza peculiar das análises de segurança. As métricas usadas são ponderadas, e o sucesso é observado por meio da falta de impacto. A medida da segurança é a mitigação dos riscos, o que indica se a arquitetura de segurança obteve êxito na proteção dos recursos organizacionais, por meio da atenuação das ameaças.

Esse estudo identificou métricas críticas de desempenho e negócios que podem ser usadas para conhecer os pontos positivos, os pontos negativos e as principais estratégias que ajudarão as organizações a escolher o sistema de segurança ideal. O estudo destaca métricas subjetivas e objetivas. Dentre as métricas subjetivas, a satisfação do cliente e a percepção de valor da solução de segurança da pilha IBM Power são muito alas. As métricas objetivas mostram que as opções de segurança da IBM oferecem diversos benefícios no quesito economia. Uma das métricas mais críticas, o custo das invasões relatadas, é a menor para as soluções da IBM.

Para as organizações que desejam implantar a arquitetura em nuvem ou que buscam uma implantação de TI de qualidade, consistente, confiável e eficiente, é essencial escolher uma estratégia de segurança. As organizações que levarem todos os fatores em consideração verão que a pilha de segurança integrada IBM Power é uma opção que merece atenção.

A elaboração deste documento foi financiada pela IBM. Embora este documento utilize informações disponibilizadas ao público por diversos fornecedores, inclusive pela própria IBM, ele não reflete o posicionamento desses fornecedores sobre as questões aqui tratadas.

