Criptografia Pervasiva

Um Novo Paradigma para Proteção

Introdução

> *"Eu fui um hacker profissional por mais de 15 anos. Eu encontro problemas de ciberssegurança em tecnologia, para que essa tecnologia se torne mais segura. Mas depois de fazer isso por anos, estou um pouco frustrado. Vejo os mesmos problemas repetidamente. Não estamos melhorando. E ao mesmo tempo em que dependemos cada vez mais da tecnologia, ela está se tornando cada vez mais insegura."*
>
> Cesar Cerrudo, hacker profissional, Diretor Técnico dos IOActive Labs,

O aspecto de transformação da informática é um efeito de propagação da forma como as organizações e pessoas estão aumentando suas conexões via internet.

Toda organização impulsiona a tecnologia, até mesmo uma estação de serviços onde cartões de crédito são passados. A necessidade de incorporar dados seguros e processos não é mais uma exigência somente de grandes corporações, mas transformou-se num componente tecnológico essencial para organizações de todos os tamanhos. Essa segurança no mundo de hoje, virtualizado, conectado através da internet e voltado para nuvens está crescendo e complexificando os desafios dos *negócios*, não somente da informação.

O ciberespaço é extremamente difícil de manter seguro. A expansão absoluta e no mundo todo da localização criminal é o menor dos desafios. A integração crescente entre o ciberespaço e o mundo físico tem expandido exponencialmente oportunidades de roubo, danos e corrupção. Alvos emergentes para o crime estão se multiplicando assim como a conexão entre o mundo cibernético e o físico desenvolve novas associações. Reduzir vulnerabilidades e minimizar consequências em redes cibernéticas complexas são as metas, mas elas são cada vez mais difíceis de serem alcançadas.

A tendência está acelerando e os desafios tornando-se impressionantes. A abordagem básica está provando-se ser inadequada para as demandas da agressiva natureza do meio. Em breve, uma mudança de paradigma será necessária.

A Solitaire Interglobal Ltd. (SIL) tem monitorado aspectos do negócio e de segurança por mais de 21 anos. O conjunto de informações via Global Security Watch (GSW) fornece regularmente tendências e informações de risco a milhares de organizações. Para construir efetivamente um quadro global e extensivo dos riscos e oportunidades que são oferecidas, a SIL vê a segurança de forma holística. Isso inclui uma ampla perspectiva de segurança, focada em quatro principais áreas. Elas podem ser generosamente classificadas em:

- Dados – acesso (leitura, cópia) ou manipulação[1]
- Segurança do processamento – habilidade para executar, ocultar, sequestrar
- Arquitetural – propriedade intelectual, tal como modelo de negócios, estrutura de processo, metadados
- Físico – acesso à planta física e às estruturas[2]

Para formar a base deste mais recente estudo, a SIL realizou análises em dados de pesquisa de organizações do mundo real suplementadas por ameaça detalhada e informações de segurança da Global Security Watch (GSW). Não é surpresa que mudanças significativas nos tipos de ameaça, escopo e taxas ao longo dos últimos anos continuam acelerando em níveis sem precedentes.

A empresa GWS é um serviço membro que tem acompanhado a evolução detalhada de ameaças de segurança e efeito associados aos negócios numa escala mundial por 21 anos e atualmente coleta informações relatadas de mais de 8,9 milhões de organizações. Os dados da GSW fornecem uma fonte profunda de ameaça de inteligência a partir de uma perspectiva de negócios que traz contribuições ao estudo com base em informações produzidas no mundo real. Apesar de marcas de ameaça e de outros mecanismos detalhados serem coletados na GSW, o foco principal relaciona-se ao impacto na operação de negócios, nos ativos organizacionais e na prevenção da remediação de custos.

Resumo das Constatações

Um resultado significativo dos dados da GSW e suplementados por mais de 62k análises alvo de segurança e rodadas pela SIL, nos últimos dois anos, é que apesar de algumas organizações não estarem cientes das incursões de segurança, muitas conhecem ou conhecem parcialmente estes eventos. Além disso, mais de 91,3% das organizações no escopo da análise desconheciam a totalidade das ramificações dos crimes cibernéticos aí perpetrados. Todas as auditorias e análises requisitadas por estas organizações mostraram que o escopo das vulnerabilidades foi ignorado ou apenas parcialmente reconhecido pela parcela de negócios da organização. A descoberta mais surpreendente foi que a grande maioria dessas organizações *desconhecia o número total real de incursões*[3] em seus sistemas.

Aumentando o perigo, muitas dessas incursões não foram uma única ocorrência mas, pelo contrário, abriram a janela de danos por um período significativo de tempo. Um exemplo pode ser visto ao olhar-se um resumo publicado das violações do HIPAA até dezembro de 2015.

> *"Mais de 10% das 1.135 principais brechas HITECH de 17 de outubro de 2014, estavam acontecendo e não foram atribuídas a eventos singulares, variando de mais de um dia até 2.891 dias. Analisando isso melhor, foi descoberto que:*
> *-- 4 Brechas duraram mais de 2.000 dias*
> *-- 7 brechas duraram entre 1.000 e 1.500 dias*
> *-- 10 brechas duraram entre 500 e 1.000 dias*
> *-- 35 brechas duraram entre 100 e 500 dias."*

[1] *A segurança de dados inclui algumas formas de acesso às informações de uma organização. Isso pode ser para ler ou fazer uma cópia de conteúdo específico. A manipulação dos dados de uma organização significa que a informação é modificada ou deletada para mudar o conteúdo ou a relação dos atributos e entidades.*

[2] *Segurança física não é tratada neste documento.*

[3] *Incursões são ataques bem sucedidos a um cenário organizacional de TI e incluem uma intrusão inicial ou uma brecha e cada roubo sucessivo, destruição ou bloqueio (i.e. dados, pesquisa ou captura de processo, negativa de serviço, etc.).*

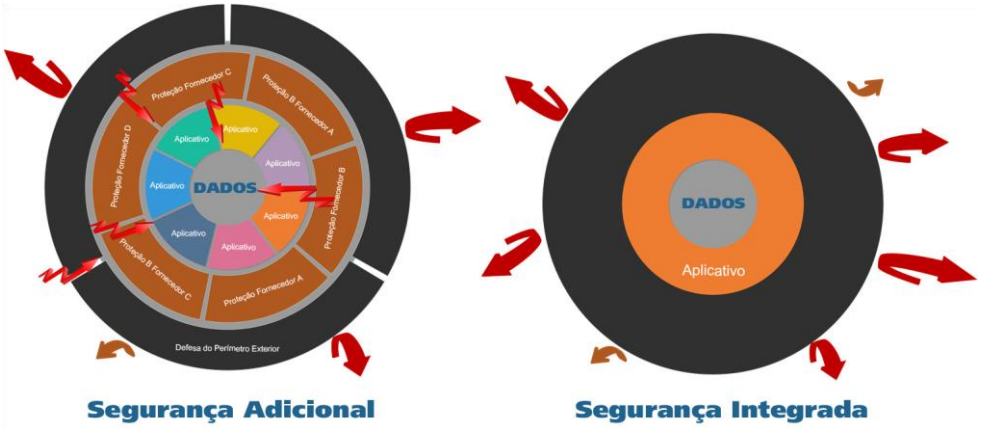
Fonte: Melamedia, LLC análise do Escritório dos Dados de Direitos Humanos, 2015

Períodos ampliados da presença de incursão ativa podem ter efeito negativo substancial na viabilidade organizacional. Empresas sofrem uma redução média de 16,2% a 63,7% de receita bruta e valorização se uma incursão durar mais do que três meses.

Com a aceleração do desenvolvimento da implementação de nuvens, o aumento de saídas, fazendo face a aplicações, expõe a infraestrutura organizacional para uma base maior e menos controlada de usuários. Mudar demandas de mercado impulsiona a organização para um projeto mais rápido e ciclos de implantação. Cada um desses novos grupos de usuários, cada nova aplicação produz um aumento na possibilidade de uma incursão de segurança bem sucedida.

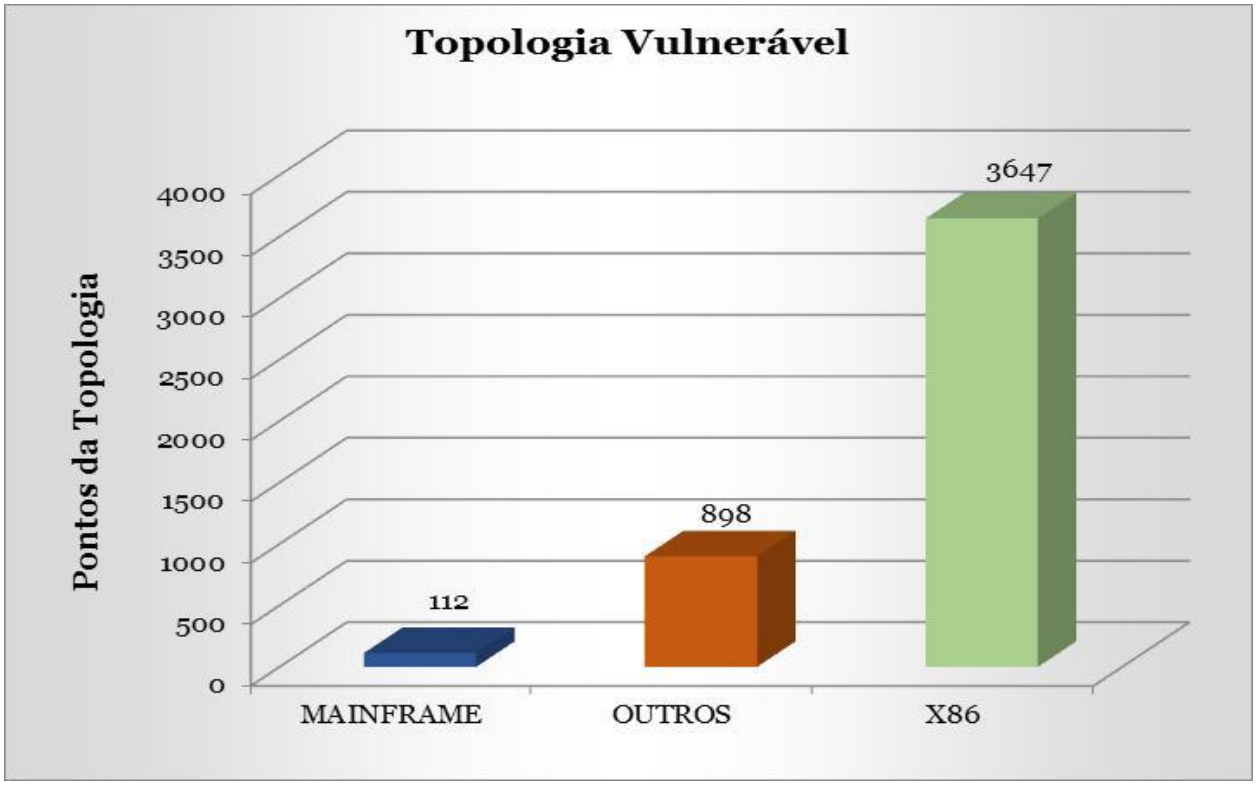
Quando a capacidade de resposta tática inclui a adição de camadas de segurança e proteção, a arquitetura resultante começa a assemelhar-se a uma cebola, algo como camadas sobre camadas, com o objetivo de fornecer segurança adicional. No entanto, na realidade, as próprias camadas podem criar pontos adicionais de topologia vulnerável.

Cada local onde uma solução parcial é “acoplada” continua sendo um outro alvo para um hacker experiente. Com o aumento da complexidade das camadas, maior será a topologia vulnerável. Essa vulnerabilidade é parte do perfil de risco de segurança que é cada vez mais usado por companhias de seguro para determinar a exposição de uma organização a um dano cibernético significativo.



Estresse extra em segurança é criado pelo uso ampliado do software de virtualização. Cada uma dessas máquinas virtuais (VMs) cria novos pontos de vulnerabilidade e aumenta a complexidade do desafio de segurança. Conforme mais organizações aderem e desenvolvem soluções híbridas de nuvens, a demanda ampliada por práticas de segurança resilientes e responsivas deve, da mesma forma, crescer e evoluir.

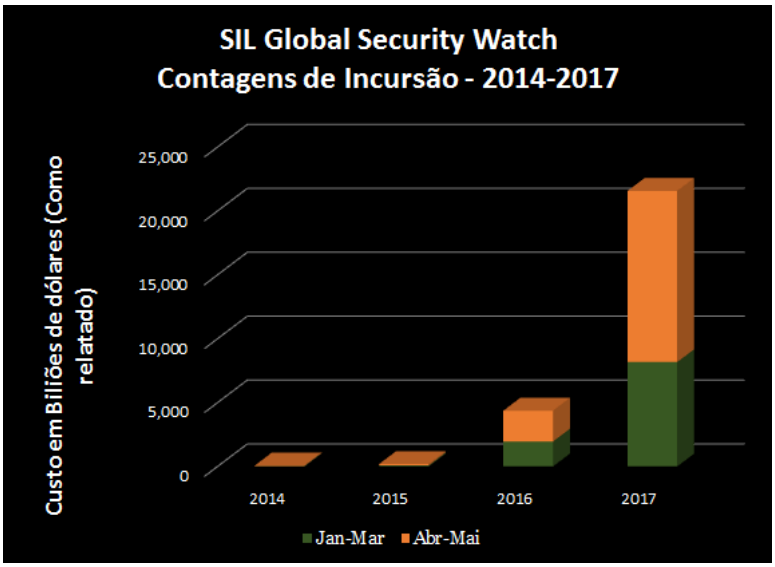
A topologia vulnerável varia significativamente entre arquiteturas fundacionais. Uma análise geral de um grupo de mais de 115K organizações ilustrou essa diferença, conforme vemos aqui.

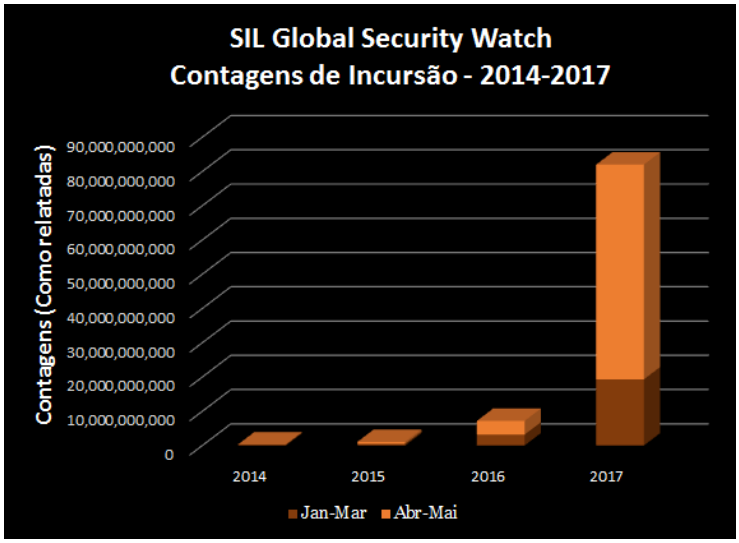


Essa diferença significativa origina-se de uma estrutura base e da estrutura realizada por de trás da arquitetura de plataforma, projeto de ficha, sistema operacional e método de integração em pilha.

Uma análise sobre os detalhes relatados de incursão nos últimos quatro anos mostra um aumento exponencial tanto no número de incursões como nos custos de danos associados.

Observação: A SIL coleta dados no mundo real, implantações de produção. Isso fornece um ponto de vista real, ao invés de teórico, de práticas operacionais, comportamentais e métricas que são inatingíveis por pedidos de vendedores ou benchmarks artificiais.





Não é apenas o número de ataques que mudou. O aspecto das próprias incursões mudou significativamente nos últimos 20 anos. Onde há duas décadas, a segurança lidava principalmente com o controle de acesso, nos dias de hoje, a topologia de ameaças é muito mais complexa.

Um dos vetores de mais rápido crescimento é o ataque de ransomware. Nesse tipo de ataque, a incursão bloqueia os arquivos, diretórios e outros componentes do sistema. Pede-se ao proprietário que pague por um código de desbloqueamento, que pode ou não funcionar.

> *"Nós fomos atingidos por 5 grandes ondas de problemas de segurança esse ano. Alguns deles foram maliciosos, enquanto outros são pura extorsão. Acabamos pagando mais de USD1M para termos de volta nossos principais servidores de web e ainda não temos certeza sobre como os hackers conseguiram acessá-los. Isso nos custou muitos clientes, tempo e dinheiro. Não foi de jeito nenhum um bom sentimento."*

Diretor Financeiro – Produtor de Médio Porte

Comparação de Plataforma de Segurança

A avaliação da Segurança é reflexivo, conforme é avaliado pela ausência de dor ou de problemas. Falhas na segurança são altamente visíveis, enquanto o seu sucesso é invisível. Para construir um entendimento sobre as métricas reflexivas associadas à segurança, a IBM engajou a SIL para conduzir pesquisas, reunir dados e realizar análises para fornecer um entendimento claro acerca dos benefícios e custos relativos que podem ser vistos quando organizações implementam a plataforma do mainframe do IBM Z como parte da sua arquitetura de TI como comparado com outras arquiteturas de plataforma. Esta análise foi primeiramente direcionada ao valor de segurança a partir de uma perspectiva de negócios, para que aqueles cujo papel é atuar como liderança empresarial possam entender o benefício das ofertas de segurança do IBM Z ao avaliar as soluções de segurança.

Durante este estudo, as principais características comportamentais do software e hardware foram examinadas de perto num grande número de sistemas de clientes reais (9.602.000+). Todos esses clientes implantaram a segurança como parte de seus ambientes de produção, mas variaram numa mistura de métodos de segurança e mecanismos. Eles incluem organizações para as quais exige-se o apoio regulado de padrões industriais de segurança da informação, tais como HIPAA, PCI, SOX, etc. A informação do relatório do cliente e a massa correspondente de detalhes do mundo real é inestimável uma vez que fornece um entendimento realístico, e não teórico, de como o uso de diferentes tipos de segurança pode afetar o cliente.

Mais de 81 milhões de pontos de dados de atividades e de impacto de incursões detalhadas do GSW proveem a fundação dos custos e exposições esperados, o que é essencial para compreender a segurança e a proteção de ativos do mercado nos dias de hoje.

Na coleta e análise dos dados do estudo, um número de características foi derivado. Essas características afetam a capacidade explícita, a eficiência e a confiabilidade do ambiente seguro. Também foi analisada a sinergia da segurança e das operações de negócios. O comportamento representado foi projetado e modelado em possíveis opções para implantação. Para construir esse entendimento, mais do que um desempenho absoluto do servidor é exigido, uma vez que a segurança precisa proteger, e não ocultar, o processo empresarial e de operações. Embora a demanda de capacidade e os efeitos de produção de sistemas de segurança sejam importantes, sua tradução em termos de negócios é mais relevante para o mercado de hoje. A perspectiva de negócios engloba uma miríade de fatores, incluindo confiabilidade, graus de segurança, níveis de recrutamento, custo total de segurança (inclusive de recuperação) e outros efeitos. Isso se liga diretamente às decisões que os gerentes de TI, diretores técnicos e lideranças de negócios têm que fazer diariamente.

Perspectivas e Visões

Há dois grupos de perspectivas de visões que emergiram da própria análise. A primeira perspectiva é relacionada às categorias inerentes de atividade relativa e desempenho que incluem:

- Eficiência operacional
- Eficiência de segurança
- Risco TI
- Resiliência e agilidade

Cada uma dessas áreas abre portas para uma outra camada de perspectiva. Nessa camada, a importância e o foco se diferenciam com base na parte da organização que está considerando os desafios e ramificações de segurança. Há dois campos principais nessa responsabilidade e estrutura de consciência, negócios e técnica. Enquanto o lado técnico é uma visão típica do estabelecimento e gerenciamento de segurança, o escopo ampliado do desafio e dos vetores de mudança de crimes cibernéticos moveram a responsabilidade primária de segurança para os negócios.

Em última instância, a TI é projetada para apoiar as funções dos negócios. Uma das fontes primárias dos dados do estudo é a visão de segurança pela gestão de negócios da organização, tanto executiva como a linha de negócios. Os padrões de operação das organizações de estudo são agrupados e alinhados ao longo de quatro áreas de comparação para identificar sua influência na métrica do negócio. Cada uma dessas métricas de negócio tem diferenciação mensurável e significativa quando a solução de segurança do IBM Z é percebida e deveria ser considerada dentro de um pensamento crítico da organização.

Os aspectos técnicos de segurança também são representados no estudo. O fato que essas são as responsabilidades mais tradicionais para a TI não diminui sua importância na evolução do mundo de ciberssegurança.

Muitas das categorias têm descobertas que abordam tanto os pontos de vista empresarial como o técnico. A complexidade do ponto de vista, autoridade, necessidade de negócios e responsabilidade são típicos do desafio bastante complexo que as organizações enfrentam hoje. Este estudo fornece uma articulação baseada em dados de alguns daqueles componentes desafiadores.

A métrica granular resumida no estudo pelo tipo de plataforma mostra como o critério de sucesso específico é diferente na população geral dos implementadores. Essas métricas são amplas em cobertura e tocam áreas de consideração financeira

assim como qualidade organizacional. São apresentadas com definições curtas e com o efeito líquido focado de cada implantação de plataforma. Para ser relevante em uma variedade de indústrias, todas elas foram normalizadas com base na unidade de trabalho[4] e categorizadas por níveis de tamanho da organização (pequeno, médio, grande e muito grande). A medida base foi definida pela média da companhia média, então todas as outras métricas são baseadas numa variância a partir daquele ponto padrão de definição. As implementações incluídas neste estudo foram restritas àquelas da produção.

EFICIÊNCIA OPERACIONAL

A eficiência operacional é a capacidade de uma empresa entregar produtos ou serviços para seus clientes ou parceiros com a melhor forma custo efetivo possível, garantindo ainda padrões de alta qualidade. A eficiência operacional pode ser vista como a razão entre os insumos para o funcionamento do negócio e a produção ganha pela empresa. Quando se melhora a eficiência operacional, a razão entre produção e insumo torna-se mais favorável. Insumos são tipicamente baseados em dinheiro (custo), pessoas (efetivo ou Equivalente a Tempo Completo - FTE) ou tempo e esforço.

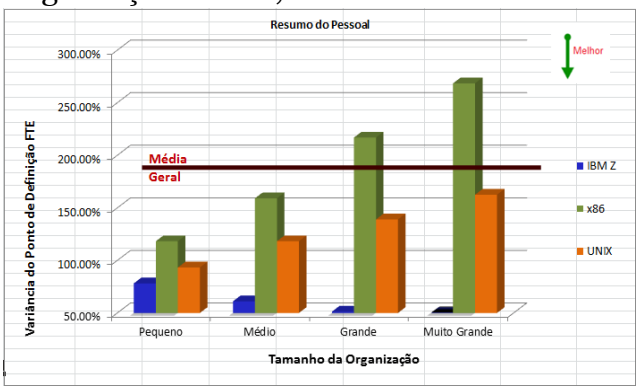
Quando a segurança é vista a partir de uma perspectiva de eficiência operacional, as contribuições têm como fonte essas áreas específicas. A dificuldade em medir a eficiência operacional da segurança origina-se da sua forma incorporada. A análise SIL examinou várias áreas diferentes de importância inclusive:

- Carga do pessoal
- Despesas alvo através da agregação TCO
- Carga de trabalho

Dentro dessas áreas, tanto os negócios como as necessidades de informações técnicas são abordadas. No entanto, as métricas derivadas de dados formam padrões diferentes de negócios versus avaliação técnica. As mensurações permitem a diferentes grupos criar estratégias e aspectos de controle de segurança que se alinham com objetivos apropriados a sua responsabilidade organizacional.

PESSOAL

Um fator subjacente que se mostra em muitas outras áreas é a eficiência da interface entre o administrador da segurança e a infraestrutura. Isso inclui software, hardware e componentes do sistema operacional e o efeito subsequente no pessoal. Conforme o pessoal aumenta, o nível de produtividade melhora. O nível de esforço necessário para alcançar-se a mesma tarefa na arena da segurança diminui, então cada membro da equipe de segurança torna-se mais produtivo.



A eficiência de qualquer um dos componentes específicos que confere tal influência à experiência do usuário é difícil de equacionar em métricas exceto em comparações super detalhadas que perdem sua eficácia em virtude do grau de detalhamento. Uma visão geral dos grupos de esforço da equipe em FTE foi revista para fornecer uma métrica geral para a

[4] *A base da unidade de trabalho foi definida usando-se os padrões publicados do Grupo de Usuário do Ponto de Função Internacional e é baseada na análise do ponto de função (FP).*

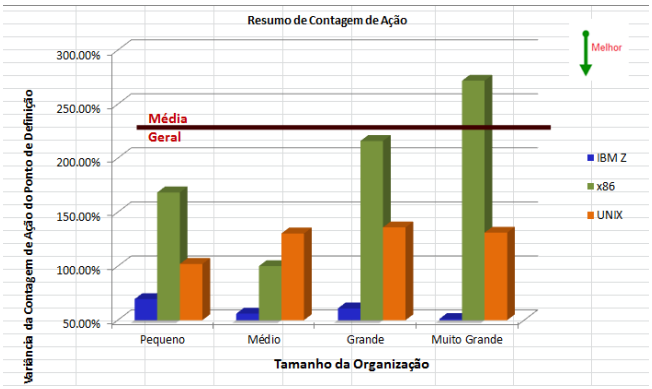
comparação da plataforma. A média geral para o esforço da equipe de segurança foi incluída no gráfico como uma outra medida de comparação. Essa média agrega todos os relatórios independente de seus tamanhos.

Os níveis de esforço comparativo são aqueles necessários para manter um ambiente de "padrão de ouro" para cada grupo do sistema operacional. A carga de trabalho foi normalizada para manter o mesmo campo de comparação de nível conforme definido em comparações anteriores. O ponto de definição da comparação é a mediana do campo geral respondente, uma vez que várias opções estão disponíveis para os componentes de segurança.

> *"Estamos rodando por volta de quatro vezes a quantidade de trabalho na plataforma z (sic) comparando-se com três anos atrás. Perdemos duas pessoas nesse ínterim, mas as pessoas remanescentes estão tocando todo o trabalho.*
>
> *Se você contrastar isso com o aumento em outros grupos da plataforma, teremos que ter quase dez vezes o número de pessoas para tocar o trabalho para aquelas."*
>
> Diretor de Informática - Serviços Financeiros Elevados

Uma vez que diferentes arquiteturas de segurança têm definições variadas de padrões de implementação, é importante manter o rigor desses padrões em mente quando da revisão de pessoal. O perceptível nível mais baixo do pessoal para a implantação e uso do IBM Z é diretamente atribuível à natureza integrada da pilha operacional Z. Isso é uma observação especial conforme a organização aumenta em tamanho ou se caminha para um modelo de serviços em nuvem. O IBM Z requer 88,35% menos tempo do pessoal de segurança em relação a outras alternativas.

Uma parcela importante da eficácia dessa operação é o número de tarefas manuais e a duração necessária para realizá-las. As tarefas que são contabilizadas e cronometradas são aquelas que precisam ser implementadas pelo pessoal da segurança para alcançar o mesmo nível de diligência, atividade proativa e modificação responsiva. Para entender detalhadamente as diferenças da plataforma, a SIL recebeu um detalhado vídeo e informações de captura de ações de mais de 620 clientes. Esses dados foram reunidos numa moção de tempo e num quadro de atividades, analisados para correntes casuais e eficácias, e usados para construir uma comparação de esforço em diferentes plataformas. Os dados de comparação são normalizados para fornecer um patamar de ação conforme discutido em algum ponte deste documento. A comparação de atividade resultante e o quadro de comparação podem ser vistos nas tabelas a seguir.

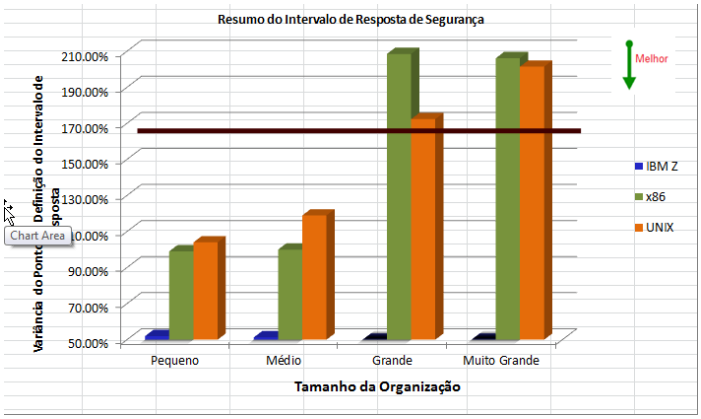


As tarefas de ação de segurança variam significativamente por causa da plataforma subjacente e do tamanho da organização. Em geral, quão maior a organização, mais complexas e variadas devem ser as práticas. O tipo de plataforma acrescenta uma outra dimensão do perfil de trabalho a esse esforço crescente. Comparando a contagem básica de ações que precisam ser realizadas para manter os padrões de segurança, o número de tarefas que devem ser implementadas manualmente pela equipe de segurança do IBM Z é substancialmente inferior àquelas de outros grupos da plataforma. Estudos de tempo e de movimento mostram que as soluções de segurança Z demandam *81,17%* menos tarefas para implementar níveis de proteção padrão. A incorporação de menos tarefas às responsabilidades da

equipe aumenta significativamente sua produtividade. Isso também pode diminuir o nível de FTE que precisa ser mantido na arena de segurança ao exigir um número menor significante de mudanças de contexto que, em retorno, diminui o risco.

> *"Os agentes técnicos de segurança responsáveis por nossas plataformas Z consistentemente têm tempo para completar todas as suas tarefas inclusive as proativas. Isso não é válido para aqueles que apoiam nossos ambientes UNIX e Wintel. Não é por causa de uma diferença em relação à dedicação de tempo. É simplesmente mais fácil proteger Z do que realizar a mesma proteção em outras plataformas."*

Diretor de Segurança - Produtor Médio



Há uma influência correspondente nos intervalos de tempo necessária para implementar os objetivos de segurança. A tabela mostra o impacto nos tempos de resposta à modificação na segurança. Essa métrica mostra a agilidade de segurança associada aos grupos da plataforma. Os quadros de resposta mais baixas aqui documentados indicam uma resposta mais rápida, que, no mundo da segurança, significa minimizar os danos de incursão. Os intervalos de tempo inclusos nesse resumo são aqueles que fazem parte de um design normal, manutenção e comportamento proativo. As atividades e intervalos que fazem parte da investigação da incursão não estão incluídos nesta visualização.

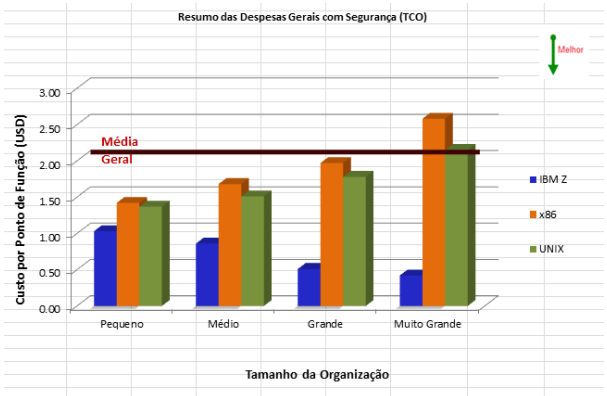
O intervalo de atividades para atividades padrão ouro normais para o pessoal da segurança mostra que há vantagens substanciais neste aspecto do pessoal para implementações Z. As mesmas atividades padrão em Z consomem até *81,66%* menos tempo do que aquelas executadas em outras plataformas.

> *"A nossa segurança no quadro principal é a área de menor problema da nossa organização. Nós frequentemente esquecemos que temos um grupo de segurança no quadro principal porque ele nos causa o menor dos problemas."*

Diretor de TI - Grupo Financeiro Médio

CUSTO TOTAL DE PROPRIEDADE

O custo total de propriedade (TCO) provê uma das principais métricas do negócio para eficácia operacional. A métrica de alto nível agrega todas as despesas dentro da organização que contribuem para qualquer aspecto da implantação de segurança. Nessa parte da análise do estudo, todas as despesas que contribuíram para a proteção dos ativos estão resumidas. Isso inclui segurança física, mas todos os outros aspectos. Mais uma vez, os projetos e seus gastos foram normalizados a partir de uma base padrão. Isso habilita



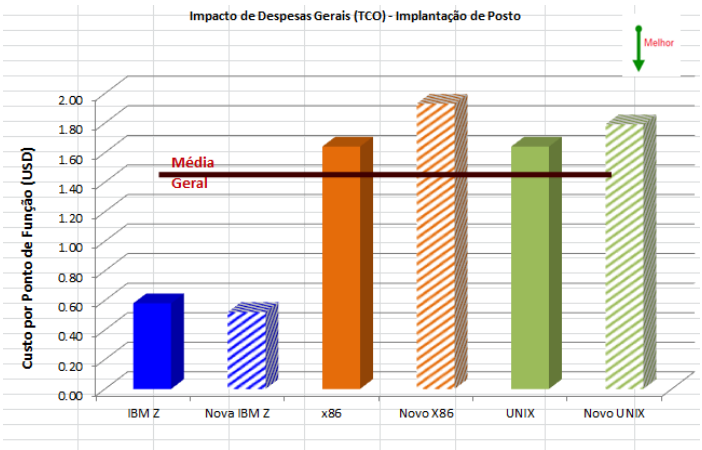
organizações grandes e pequenas, e seus gastos a serem comparados com mais precisão.

Isolar o TCO na prática de segurança é desafiador tendo em vista que a própria segurança está crescentemente incrustada em todos os aspectos das operações de uma organização. Ao normalizar o TCO em uma definição de trabalho padrão, tal como pontos de função, uma comparação precisa pode ser feita e destacada. Os padrões de gastos mostram tendências crescentes de alguns tipos de plataforma conforme a complexidade da implantação aumenta. Há uma tendência contraditória para o IBM Z. Um padrão decrescente da unidade de gastos traduz-se em eficácia da escala, onde o impulso do quadro e a fundação permitem um padrão eficaz de custo do investimento financeiro. Conforme vê-se na tabela ao lado, as despesas para as implementações de segurança Z são menores em 83,72% do que aquelas de outras plataformas. Isso origina-se parcialmente da combinação de base da segurança arquitetural e de uma plataforma altamente escalável. A eficácia dessa sinergia é mostrada conforme a arquitetura é mais pesadamente carregada, uma queda significativa nos custos para a unidade de trabalho é realizada. Essa marca está presente em todas as situações onde a arquitetura é projetada para ambientes escaláveis, mas é normalmente mais vista apenas em hardware. Nesse caso, a convergência do design da escalabilidade está presente tanto no hardware físico como no sistema operacional.

> *"Nosso quadro principal da IBM tem um custo muito mais baixo do que qualquer outra coisa que fazemos como companhia. Os custos, na verdade, têm baixado, nos últimos três anos, apesar de o nosso pessoal financeiro continuar dizendo que temos custos muito altos. Eu continuo dizendo a eles que os nossos custos gerais são menores, uma vez que temos menos problemas, equipe reduzida e uma chance menor de problemas."*

Diretor Financeiro - Grande Distribuidor

A escalabilidade arquitetada é especialmente importante quando os sistemas se tornam mais complexos, tais como quando usuários são escalonados, traga seu próprio dispositivo (BYOD) são proliferados ou aplicativos extensivos em nuvem e acesso múltiplo são implantados. A intensificação da adoção de nuvens e o aumento da implantação de aplicativos em nuvens têm exacerbado a dificuldade em manter uma segurança responsiva. A forma da implantação de nuvens também afeta os desafios de segurança. Seja uma comunidade privada ou pública ou uma nuvem híbrida implantada, as práticas de segurança devem passar por constante evolução.



As vantagens de equilibrar controle e acessibilidade ao uso de nuvens híbridas foram melhor compreendidas e a adoção dessa forma de implantação de nuvens teve como resultado o fato de a nuvem híbrida tornar-se a opção de implementação recente mais popular. Isso apresenta um dos cenários mais complexos da segurança uma vez que arquiteturas de plataformas múltiplas devem todas ser seguras.

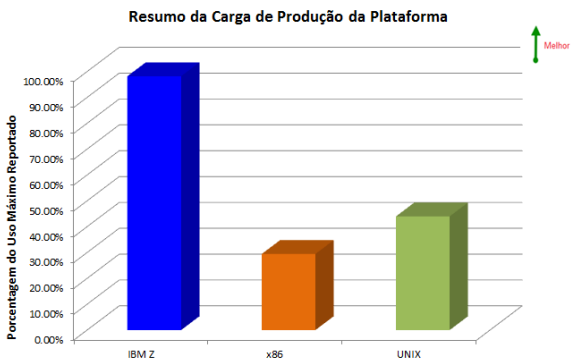
Em situações onde a segurança é realizada com uma série de componentes adicionais de proteção ou onde a governança principal de segurança é tão somente residente no

aplicativo implantado, a comparação geral das despesas aumenta significativamente quando novos serviços são acrescentados. A tabela seguinte mostra esse tipo de efeito. As projeções incluídas nessa parte da análise mostram o impacto no curto prazo da aquisição de segurança. Em todos os casos, essas 16.027 organizações adicionaram um único aplicativo às implantações existentes de nuvem. A implantações almejaram nuvens híbridas, públicas e privadas e foram projetadas para mais de 1K de usuários.

O TCO baseado em pontos da função mostra a diferença de despesas de curto prazo que está presente no momento da aquisição. O impacto na despesa geral da unidade de trabalho ilustra a influência nos negócios que a tecnologia apresenta. A carga de trabalho adicional permitiu a implantação do IBM Z, a fim de dispender um custo de segurança estável num número maior de pontos de função sem acrescentar qualquer despesa significativa. Outro grupo de plataformas exigiu despesas adicionais em relação a licenças, etc. O impacto médio antes da implantação adicional de nuvens diminuiu as implementações de Z numa média de *14,02%,* enquanto que soluções de plataformas alternadas aumentaram em *19,62%*. A tabela resumo ilustra bem a média de cada um dos grupos arquitetural. Os dados subjacentes para os projetos individuais são perceptíveis uma vez que nenhuma das implementações do IBM Z mostrou um crescimento do TCO no ponto da função, apesar de duas delas terem mostrado um impacto nulo. As outras arquiteturas demonstraram resultados individuais que variaram de um aumento de *2,9% para 38,4%*. O padrão do impacto é significativo quando considerado dentro de um quadro de negócios em expansão almejando a nuvem, dispositivos de usuários distribuídos e em ascensão, e que enfrentam ofertas novas e substanciais de serviços.

Comunicar o custo real e o impacto da segurança é um outro desafio. A articulação de casos de negócios para melhorias de segurança e expansão é um assunto de discussão frequente e objeto de reclamações de profissionais de segurança no mundo todo. O custo do impacto de segurança como um aspecto da eficácia operacional não é claramente compreendido pela maioria dos executivos empresariais. Num agrupamento de dados coletados em 2015-6 que incluíram mais de 9,5 milhões de executivos organizacionais, menos de 11% deles já tinham visto um caso de negócios sobre gastos com segurança. Menos de 0,9% dessas pessoas alegaram compreender como os custos de segurança, economias de escala e despesas projetadas foram derivadas. Infelizmente, menos de 35% das pessoas responsáveis pela tomada de decisões organizacionais acreditaram que o seu pessoal de segurança tenha entendido como projetar e calcular custos. Tudo isso contribui para uma situação onde a redução, ou o aumento das alocações gerais dos custos de carga de trabalho são inesperados e não contemplados. Com esse ponto cego em especial, a gerência executiva falha ao entender a dimensão da eficácia das implantações de segurança do IBM Z.

CARGA DE TRABALHO



A mensuração do TCO é primeiramente uma métrica empresarial. Ela incorpora características chave da escalabilidade da arquitetura a ser expandida e impulsiona melhor os gastos. No entanto, a métrica relaciona-se com escalabilidade e resiliência na sua forma mais bruta. Gerir eficientemente os recursos de segurança repousa em controlar o tempo do pessoal assim como os custos intrínsecos da infraestrutura e do software para manter as práticas de segurança. A arquitetura de plataforma escalável e resiliente compõe a fundação para gastos eficazes de recursos de tempo e

dinheiro. Uma plataforma mais escalável significa que menos projetos de implementação precisam ser realizados e que a habilidade dos recursos de TI para apoiar os negócios aumentaram consideravelmente. Consequentemente, uma plataforma altamente escalável que requer menos atividades para implantar uma carga de trabalho adicional aumenta a eficácia operacional do grupo de serviços de TI.

Uma dimensão para a implantação de escalabilidade e resiliência é o nível no qual a arquitetura da fundação pode ser lançada antes de uma performance errática e incerta. A habilidade para usar uma maior porcentagem da capacidade teórica máxima de uma máquina traduz-se em gastos e riscos menores. A carga de produção máxima relatada do grupo de estudo foi usada para articular a confiança dos profissionais responsáveis por implementar suavemente as operações na habilidade de a plataforma manter uma carga de trabalho. As cargas de trabalho que aumentaram para um nível mais alto, mas tiveram uma duração de menos de 10 minutos, foram omitidas dessa análise.

> *"Quando você nos perguntou quão alto os nossos sistemas normalmente funcionam, nós não apenas mandamos para você os dados, mas, na verdade, nós os examinamos. Eu não percebi que a nossa carga média nas nossas plataformas Wintel estavam abaixo de 14% enquanto o nosso quadro principal funciona consistentemente a 98%+. Acho que nunca percebi como aquela plataforma era muito mais eficaz. De alguma forma, presumi mentalmente que todas aquelas caixas poderiam ser impulsionadas para o mesmo nível. Isso definitivamente nos fará examinar mais de perto qual aplicativo hospedamos e onde o fazemos."*
>
> Diretor de Operações - Grande Organização de Saúde

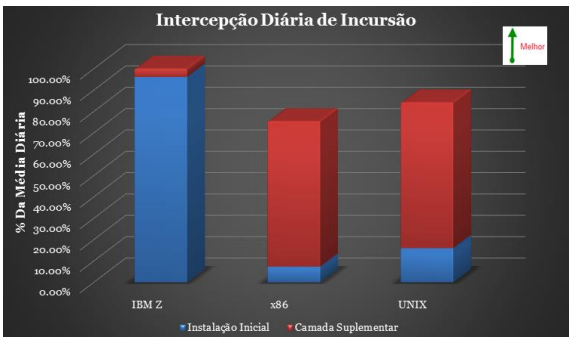
EFICIÊNCIA DE SEGURANÇA

Para examinar a área de eficácia da segurança, a SIL estabeleceu comparações mensuráveis numa combinação de métricas objetivas e subjetivas. As métricas objetivas incluíram a habilidade de medidas de segurança em capturar e prevenir incursões bem-sucedidas, ambas nas incursões relatadas e naquelas descobertas por auditorias detalhadas. As informações incluídas nessa mensuração têm aplicabilidade tanto para o lado técnico como empresarial de uma organização desde que a quantidade de incursões possa ser amplamente traduzida em incidência no resultado da organização.

Cada uma dessas áreas fornece diferenciações chave para a solução de segurança cibernética do IBM Z.

RESISTÊNCIA DA INCURSÃO

A primeira métrica do sucesso da segurança é o número de incursões apreendidas, neutralizadas e que preveniram a causa de qualquer forma de danos. As incursões agregadas nessa métrica não incluem aquelas que foram bloqueadas por extensões de firewalls e dispositivos de segurança. Ao invés disso, foram contabilizadas apenas aquelas bloqueadas por uma solução de segurança presente na plataforma. Esses números foram normalizados pela conta residente real da máquina virtual (VM) na plataforma, desde que cada VM represente uma entidade lógica separável. Isso é uma métrica indicativa uma vez que nenhum ajuste foi feito para o número de usuários dentro de cada VM.



O nível de bloqueios de incursões fornecido pela instalação inicial para cada uma das plataformas forma a fundação para qualquer extensão de segurança requerida e instalada. Esse gráfico mostra a segurança fornecida pela instalação inicial e pela camada suplementar, expressas como porcentagem de incursões que foram bloqueadas. Baseada em instalações iniciais, a fundação de soluções de segurança do IBM Z fornece*13,21 vezes* o nível de intercepção de soluções de plataformas alternadas.

Além disso, a solução Z fornece uma base, proteção fundacional que excede 92,1%, mesmo sem a suplementação extra necessária para arquiteturas alternadas.

Camadas suplementares de segurança são aplicativos de extensão, táticos e técnicos, etc. Estes variam de organização para organização, mas são variáveis baseadas na supervisão individual de segurança, postura e governança. Níveis mais altos de exigências suplementares de segurança indicam níveis elevados de esforço por parte do software de segurança e do pessoal.

A combinação de capital intelectual e serviços automatizados, acoplados ao design arquitetural das soluções de segurança cibernética do IBM Z resulta na intercepção de uma porcentagem significativamente mais alta de incursões. A plataforma Z entrega interceptações de incursões base que são*20,74%*melhores do que a segurança combinada de fundação potencializada com esforços extensivos, competentes e rigorosos para táticas de segurança suplementares fornecidas por outras soluções de plataformas alternadas.

Uma visão mais profunda da eficácia da solução de segurança requer um olhar mais profundo. Serviços de segurança começam com a fundação da arquitetura, incluindo hardware, software e componentes de mildware. Atuando como uma camada acima disso estão as políticas organizacionais, procedimentos, postura e governança. Enquanto isso pode ser medido em relação às melhores práticas atuais e considerado como uma diferenciação chave, este estudo está focado no exame das soluções de vendedor que combinam hardware, software e mildware da plataforma, inclusive sistemas operacionais.

> *"Eu não tenho a menor ideia porque há menos problemas de segurança com a plataforma z (sic), eu simplesmente sei que não existe nenhum. O pessoal da segurança está constantemente me contando coisas sobre isso e aquilo, mas pode-se resumir que ele simplesmente funciona. A última vez que tivemos problemas com a segurança nessa plataforma constatou-se que alguém tinha roubado a senha de outra pessoa. A última vez que eu tive problemas numa plataforma diferente foi há mais ou menos uma hora. Me pergunte qual eu preferiria!"*
>
> Diretor de TI - Grande Distribuidor

A natureza da segurança Z incrustada é significativamente diferente do que aquela que foi criada com soluções extra de proteção. Com um grupo mais amplo de interfaces para manter a segurança, a proteção dos dados e processos da organização é a mais vulnerável quando definida no nível do dispositivo. Uma estratégia mais eficaz direciona o controle e a definição de política para um ponto mais centralizado. A pilha altamente integrada e incrustada de segurança Z fornece uma vantagem significativa nessa área.

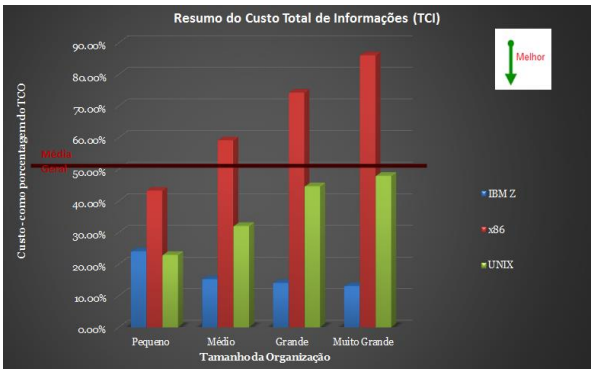
Um outro fator de complexidade que é pertinente à eficácia do exame de segurança comparativa é a emergência da informática móvel. Com conexões públicas de rede e hotspots aumentando exponencialmente, uma contribuição crescente para o risco de segurança origina-se em políticas, governança e na eficácia desses pontos de acesso desconhecidos. Se a solução de segurança for projetada para ser distribuída, ao invés de administrada centralmente, o perfil de risco para o aplicativo e para os seus dados

aumenta significativamente. Neste tipo cada vez mais comum de topologia, a solução Z tem vantagens arquiteturais. Para aquelas implantações flexíveis, o perfil de risco SIL define a taxa de risco da plataforma Z em menos de 1/20 de qualquer das soluções alternadas.

CUSTOS E DESPESAS

Os custos associados à segurança incluem tanto a métrica tradicional do TCO e a métrica mais recente do custo total de informação (TCI) que fornece uma visão ampliada das contribuições de custo dentro de uma organização.

O TCO é composto pelas despesas necessárias para gerar uma operação contínua. As categorias de custo nessa métrica incluem equipe operacional de TI; apoio à interrupção e reparação de aplicativos; serviços externos para suplementar a equipe operacional ou a solução de problemas; despesas de eletricidade e refrigeração; licenciamento e manutenção de software e hardware; e espaço de piso.



O TCI é a métrica que enquadra as despesas organizacionais no que diz respeito à sustentação e proteção dos ativos organizacionais de TI e propriedade intelectual (PI). Isso inclui dados, processo empresarial, pesquisa, estrutura de aplicativo e outras propriedades intelectuais. Essas despesas incorporadas às métricas incluem a infraestrutura que sustenta e emprega ativos, pessoal, energia, refrigeração, medidas de segurança, etc. que mantêm o ativo seguro e funcionando. Essa métrica leva em consideração os impactos negativos das perdas e danos de PI; e oportunidades perdidas, e.g., negativa de serviço e períodos de inatividade. A métrica que melhor reflete o impacto e influência da segurança de TI dentro da organização é o TCI uma vez que ele constroi um entendimento da métrica reflexiva de segurança.

Quando observarmos o TCI por diferentes arquiteturas, há várias formas de resumir as questões a ele relativas. Havendo uma ampla variação no tamanho da implantação da infraestrutura, resumir tendo como base o valor total do ativo de TI e PI é estatisticamente vago. Uma base de comparação normalizada expressa o TCI como uma porcentagem do TCO. Os resultados dessa análise podem ser vistos na tabela.

As implementações do IBM Z mostram *84,83%* de TCI menores em uma vasta gama de tamanhos de organizações. Uma vez que essa métrica é o condutor chave para novos custos de implementação, o fator mais inferior reforça o dimensionamento eficiente presente nas implantações Z. A comparação do TCI incorpora o custo de disponibilidade, o efeito de incursão e as métricas do período de inatividade para que visões extras não precisem ser consideradas. O diferencial entre as soluções é amplamente baseado em três contribuições, nas áreas de:

- Custos de pessoal
- Custos ligados aos efeitos de incursão
- Extensões de arquitetura de infraestrutura

Os custos tanto com pessoal como com infraestrutura são auditáveis, enquanto o custo para efeitos de incursões é uma combinação tanto de montantes projetados subjetivos e objetivos. Em todos os casos, os custos vêm diretamente dos relatórios do cliente e não foram alterados, mas, ao invés disso, foram simplesmente agregados e ponderados sobre a base do estudo.

Os custos associados com as configurações de segurança do IBM Z são menores do que x86 e as opções de segurança UNIX tanto na base de despesas tradicionais como em custos reflexivos decorrentes de incursões. Isso representa uma diferença entre

uma pilha de segurança altamente integrada versus uma adicional com outras arquiteturas, criando suscetibilidade e vulnerabilidade ampliada.

FATORES DE RISCO DE SEGURANÇA

Risco de segurança pode ser definido como o potencial que dada ameaça explorará com sucesso as vulnerabilidades de um processo ou um ativo ou um grupo de ativos causando danos para a organização ou para os clientes que serve. É medido em termos da combinação da probabilidade da ocorrência de tal evento e suas associadas consequências. O SIL constroi perfis de risco atuariais usados para fornecer uma visão consolidada do risco geral de uma organização. Isso incorpora contribuições de risco individuais de aplicativos, interfaces, estruturas de gestão, aspectos de engenharia social, etc. Para os propósitos da caracterização do risco numa implantação de segurança, as principais dimensões do perfil de risco são:

- Agrupamento experimental de atividades de incursão
- Custos da incursão
- Exposição

A mudança de cenário no mundo de TI tem incumbido uma mudança na perspectiva para esclarecer as opções a partir de uma perspectiva gerencial. Alguns dos efeitos das incursões relatados pelos clientes são:

- Perda de serviço
- Queda do número de clientes devido à falta de confiança
- Mudanças não estratégicas de arquitetura
- Recuperação de dados perdidos ou danificados
- Perda de capital intelectual exclusivo

Esses efeitos têm aspectos de probabilidade e custo e relacionam-se diretamente à prática organizacional de segurança.

> *"Uma variedade de ataques nos deixou vacilantes diante do desaparecimento de clientes, custos de remediação e outras terríveis influências. Toda a experiência resultou numa grande perda de confiança dos clientes. Nós estamos movendo rapidamente para um MSP que roda parte da carga de trabalho num enorme mainframe, visto que esse parece ser o único local seguro para rodar nos dias de hoje!"*
>
> Diretor - Empresa Média de Distribuição

CUSTOS DAS INCURSÕES

A incursão pode ser definida como um ataque bem sucedido ao cenário organizacional. Esse ataque pode ter o formato de um roubo, destruição ou bloqueio. As proteções atuais têm que cobrir uma variedade mais ampla de pontos de acesso do que o necessário para segurança em todo um nível de plataforma. Nessa situação, o controle sobre todos os aspectos do processamento precisa ocorrer no local. Muitos governos e instalações seguras requerem proteção para a alocação e manuseio das principais esferas de TI: D/F, acesso a rede, gerenciamento de memória e acesso geral à execução normal.

Em alguns casos de incursões de segurança, os custos para uma organização podem levar um longo período para serem calculados. Um exemplo dessa realização tardia

do impacto é quando a pesquisa da propriedade é roubada. A perda do IP exclusivo pode ter um impacto significativo no mercado.

A média dos custos associados a uma incursão indica uma exposição relativa para as diferentes tecnologias. Infelizmente, um clima de "perdas aceitáveis" foi construído no mercado, graças aos custos ponderados através da multiplicidade de incursões menores. Isso definiu um precedente de lassidão na definição de segurança e controle que ignora a exposição real dos impactos mais amplos e mais severos de incursões. Quando uma organização é condicionada a tolerar repetidas perdas "gerenciáveis", ela deixa as suas informações e operações num estado vulnerável e torna-se propícia a danos maiores.

O custo médio de uma incursão está crescendo e essa taxa está acelerando. Parte disso tem como origem a ampliação do escopo de aplicativos, onde mais pessoas e dados podem ser afetados por incursões durante cada período de tempo. O outro fator a se considerar é o fato de aqueles responsáveis pelas incursões estarem ficando melhor e mais agressivos em seus ataques. Isso indica um nível crescente de ameaças que deveriam ser consideradas quando da seleção de componentes de TI.

O custo médio de uma incursão é afetado por uma multiplicidade de características. A velocidade da eficácia da detecção, a habilidade de isolar a incursão para não causar mais danos, o rigor da remediação, etc., tudo influencia o impacto financeiro geral.

O custo substancialmente mais baixo por incursão para a plataforma Z demonstra a sinergia de todos esses fatores. Em geral, a remediação de implantações de segurança Z é em média *98,82%* menor do que as plataformas alternadas. Colocado a partir de uma perspectiva ligeiramente diferente, as organizações gastarão em média *84,65 vezes* mais dinheiro resolvendo danos por incursões se sua plataforma de implantações não for o IBM Z.

O custo para alcançar diferentes níveis de segurança é substancial. Para entender esses fatores, as diferentes formas de segurança podem ser divididas em níveis de controle:

- Corporação normal
- Processamento de cartão de crédito envolvido
- Bancos
- Saúde
- Pesquisa
- Defesa

Baseadas em funcionalidade e controle críticos, considerados equitativamente, as diferentes plataformas fornecem uma cobertura de segurança resumida na tabela a seguir. Essa configuração examina apenas as características de segurança que são aprisionadas com a instalação implantada originalmente desde que as opções de extensão possam ser aplicadas a qualquer opção de segurança.

Segurança Nativamente Coberta pela Plataforma

Descrição do Nível de Segurança	IBM Z	x86	UNIX
Corporação normal	100,00%	18,16%	30,26%
Processamento de cartão de crédito envolvido	99,00%	11,04%	18,28%
Serviços Bancários	94,00%	5,26%	10,22%
Saúde	100,00%	3,24%	8,51%
Pesquisa	92,50%	2,86%	4,16%
Defesa	85,54%	0,26%	1,86%

Durante atividades de estudo separadas, a SIL conduziu uma série de análises de vulnerabilidade para um grupo aleatório de clientes. Um total de 14.625 clientes foram analisados em detalhes durante os estudos de vulnerabilidade da SIL do total de clientes presentes neste estudo principal. A grande maioria desses clientes não estava ciente das incursões críticas em seus sistemas. Em geral, algumas das organizações estavam cientes das violações de segurança. Entretanto, a descoberta mais surpreendente foi o grande número de organizações que tinham experimentado violações de segurança das quais eles não estavam cientes. Durante esse conjunto aleatório de verificações de vulnerabilidades, 82.061 empresas tiveram processos de extração estranhos que ainda estavam em modo de pirataria ativo, informações roubadas e processos afetando em tempo real.

O número de incursões descobertas é significativamente maior do que o nível conhecido inicialmente. Muitos dos resultados de incursões podem não ter sido conhecidos por uma quantidade considerável de tempo, especialmente quando os efeitos do roubo de IP se tornaram evidentes.

A longevidade das incursões aumentou à medida que os invasores se tornaram mais sofisticados. Na análise das incursões residentes insuspeitas mencionadas anteriormente, a longevidade da atividade criminal subjacente foi estudada. Mais de 31,19% dessas incursões parasíticas foram determinadas como existindo por mais de dois anos. Aproximadamente 43.28% delas existiam entre um e dois anos. Outras 23,16% estavam ativas nos sistemas entre três e 12 meses. O lembrete foi dividido entre incursões de curto prazo e aquelas com data de início não rastreável, precedendo medidas detalhadas de segurança. As implementações Z foram notadas pela ausência dessa lista.

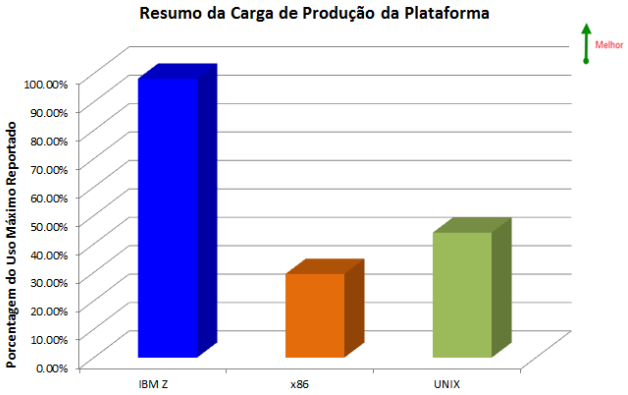
> *"Adquirimos uma empresa como parte dos nossos esforços M&A há cerca de quatro meses. Uma das principais razões para adotarmos a fusão foi tirar proveito de alguns dos seus IPs. Bem, descobrimos logo depois do início da racionalização dos sistemas que eles tinham um monte de programas espiões em seus sistemas. Agora, o nosso departamento jurídico está lutando para nos tirar do acordo, uma vez que o valor do IP está seriamente ameaçado. Que confusão!"*
>
> Diretor de Informática - Empresa de Biologia Muito Grande

Esse tipo de vulnerabilidade estendida e atividade criminal secreta carregam consigo a exposição mais alta para uma organização. Entender o efeito na organização é difícil até o ponto da descoberta final, uma vez que a janela de exposição prolongada

deixa a organização aberta à perda significativa de confiança do cliente, ações legais extensas e remediação prolongada.

RESILIÊNCIA E AGILIDADE

Os principais fatores em uma prática de segurança bem-sucedida são a resiliência da implementação de segurança para lidar com níveis e formas inesperadas de incursões, bem como com a velocidade na qual as respostas aos ataques e ameaças que surgem são implementadas. A resiliência da implementação pode ser vista como a capacidade de lidar com uma demanda de recursos inesperada, sem falha da plataforma como um todo. Casos extremos podem ser vistos nas falhas de implementação com a recusa concentrada de ataques ao serviço. As implementações mais resilientes dependem da capacidade e da elasticidade do sistema operacional e do hardware. A resiliência é uma métrica típica ao avaliar o hardware para compra e os sistemas operacionais para implantação. A taxa de resiliência combinada dos grupos de plataformas é vista no gráfico. A taxa de resiliência em si é o resultado dos pontos de ruptura registrados e relatados do escalonamento desde as implementações do produto que são parte deste estudo. A taxa é expressa como uma porcentagem da carga de trabalho e representa a quantidade de estresses e construção de fila que os algoritmos de despacho, mecanismo de buffering e outros componentes podem tolerar, sem impactar negativamente as operações como um todo.

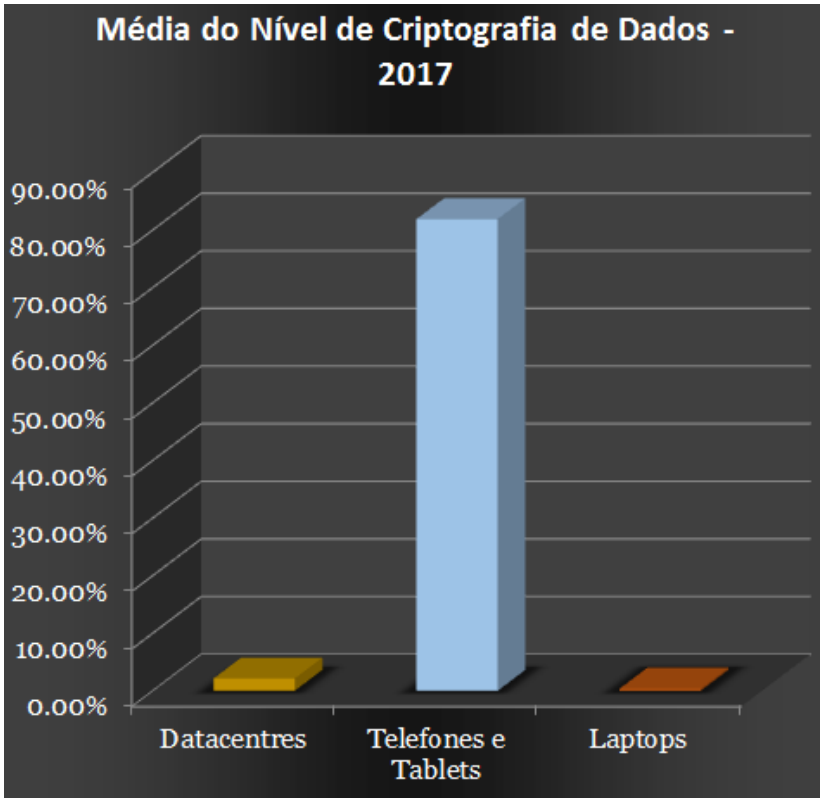


Há uma diferença substancial entre a resiliência das implantações no Z e do restante das soluções. A resiliência média relatada das implementações do IBM Z é igual a *7,41 vezes* a das demais opções. Isso se traduz em menos esforço de engenharia na solução de TI, o que contribui para um TCO e TCI menores relatados anterior neste paper.

Criptografia Pervasiva

Dados corporativos e do cliente de uma organização são um recurso-chave. São literalmente sem preço, uma vez que formam vantagem de mercado e capital intelectual essenciais de qualquer negócio. A criptografia tem sido um modo de proteger esse ativo, uma vez que, desde que encriptado, a sua disponibilidade e vulnerabilidade a hackers é eliminada. Muitos desses ativos estão atualmente desprotegidos.

A perspectiva é diferente em outras áreas das comunicações de dados. O uso de dispositivos móveis foi construído sobre uma visão de privacidade que inclui a criptografia desde a concepção do design inicial. Uma comparação dos diferentes níveis de criptografia é esclarecedora.



Este resumo destaca a diferença básica no enfoque das comunicações móveis e TI convencional. Uma vez que a indústria das comunicações percebeu cedo a importância da criptografia quando se trata de dispositivos móveis, aproximadamente 82% dessas plataformas são encriptadas, sendo que somente 2,13% dos dados empresariais dentro dos datacenters são encriptados. A discordância da falta de criptografia em recursos organizacionais extremamente valiosos localizados nos datacenters e nos laptops é grave.

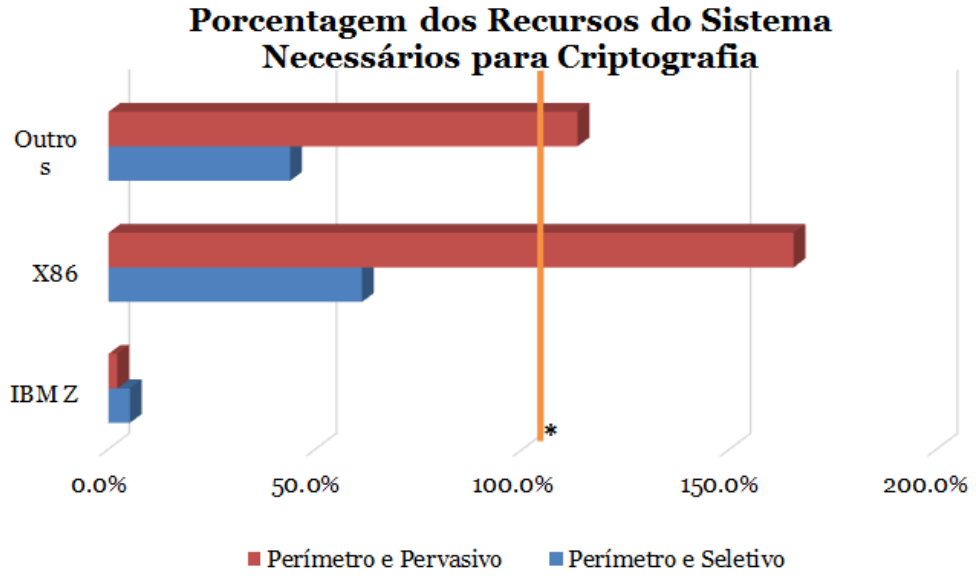
De acordo com as informações da SIL GSW, menos de 3,5% dos 11,2B de registros violados nos últimos três anos estavam encriptados. De modo efetivo, isso significa que logo que uma violação ocorre, as informações estão totalmente vulneráveis aos agressores. A perda de confiança do cliente e do parceiro é compreensível, uma vez que a falta de previsão é uma violação grave da confidencialidade esperada.

Há diversas razões essenciais para níveis baixo de criptografia. O custo em termos de tempo e capacidade do sistema tem encorajado as empresas a se concentrarem nas técnicas de defesa do perímetro e na criptografia seletiva. Com as defesas de segurança do perímetro atualmente consumindo até 61,2% da capacidade total da plataforma, uma mudança de paradigma é necessária.

Um avanço recente em um dos aspectos fundamentais do nosso ambiente computacional atual está pronto para fazer uma diferença significativa no mercado. A mudança é a expansão da criptografia IBM Z atual de um modelo seletivo para um abrangente. Tal modificação significativa na estrutura básica da computação e seu efeito na segurança provocarão um efeito disruptivo importante.

O conceito geral é não introduzir uma camada de decisão que diz o que irá ou não irá ser encriptado. Em vez disso, será possível ter a criptografia como parte do processamento normal. A remoção da decisão para criptografia seletiva é mais economia no custo total e a redução da dificuldade de usar criptografia no mercado atual.

A maior barreira para fazer criptografia em escala total tem sido o custo da criptografia e a carga de desempenho que tal atividade coloca sobre a plataforma de computação. Entretanto, para as organizações relatadas neste estudo, as soluções bolted-on que estão sendo implantadas têm feito com que a capacidade do sistema cresça de modo que haja cargas de até 61% sendo consumidas pelos processos de segurança. Isso se traduz em uma quantidade significativa de custos de infraestrutura, entrave ao desempenho, etc.



**Os recursos do sistema não podem, realisticamente, ultrapassar 100%, indicando que a solução não é viável.*

As exigências de recurso da criptografia atual podem ser claramente vistas no gráfico acima. A chance de uma criptografia pervasiva destaca algumas das diferenças fundamentais na arquitetura. Embora o Z tire proveito de suas habilidades de criptografia em massa para custo reduzido, outras arquiteturas mostram aumento significativo na sobrecarga. Para permitir que as arquiteturas não-Z lidem com a criptografia pervasiva, uma topologia distribuída massiva teria que ser implementada. Levando em conta a carga média para cada plataforma dentro do grupo de estudo, essa implantação resultaria na adição de até ***12,2 vezes*** o número de servidores atuais.

Tal aumento na contagem de plataformas aumentaria substancialmente o custo das operações. O impacto na organização adotando essa solução seria considerável, com um aumento significativo nas despesas com hardware, software e de pessoal. Essa solução atenderia a lacuna de criptografia pervasiva, mas ainda falharia para mitigar a fragilidade da arquitetura bolt-on.

Mesmo sem avanços novos, a arquitetura Z fornece criptografia com gastos de recursos mais eficientes e mais baratos. Ela oferece mais de ***8,5 vezes*** proteção de segurança, com ***93% menos custo*** no gasto total e com ***81% menos esforço***. Entretanto, essa é uma criptografia seletiva que reduz algumas das proteções desesperadamente mais necessárias.

O impacto total de um mecanismo de criptografia mais rápido e capacidade de encriptar informações em massa uma solução totalmente pervasiva ***18,4 vezes mais rápida*** e com somente ***1/20 do custo*** de outras soluções.

Embora a criptografia pervasiva seja viável no mainframe Z, não é atualmente possível implementar em outras arquiteturas. A mais restritiva das arquiteturas, vinculada às soluções x86, exigiria 7,32 *vezes* a capacidade atual para executar a

carga de trabalho necessária para a criptografia pervasiva em um único servidor. As exigências desse tipo de solução exigirão avanços significativos nos designs de chips de plataformas alternativas, base do sistema operacional e outras restrições de capacidade da plataforma interna. Tais avanços são mudanças de longo prazo no design e na fabricação do chip, com tempos de espera típicos de dois a três anos, presumindo-se que a tecnologia básica possa ser criada.

Se isso não for feito, então as demandas da criptografia pervasiva não poderão ser atendidas naquelas plataformas. Os sistemas que são residentes naquelas plataformas continuarão a ser executados com risco e exposição de perfil mais altos, demanda por uma quantidade excessiva de tempo e despesas e consumo desproporcional de recursos organizacionais.

Aplicar a criptografia em uma camada pervasiva reduziria significativamente a porcentagem da plataforma que foi devotada aos próprios processos de segurança. Para as organizações analisadas em um estudo SIL recente, as organizações que implantaram criptografia pervasiva no IBM Z podem reduzir a sobrecarga de processamento geral em até 91,7%.

A exposição ao crime cibernético também é tão grande que as bases do custo da mudança têm que incluir a possibilidade substancial de incursões de hackers que danificam os ativos organizacionais.

A carga de trabalho e a velocidade da resposta são muito importantes quando se trata de segurança. Quanto mais rápido uma organização possa responder a uma ameaça, menor a probabilidade de uma incursão provocar danos. A velocidade da resposta é a métrica-chave não somente para evitar efeitos adversos, mas também para minimizar o impacto. Na comparação da criptografia pervasiva versus seletiva dentro do mesmo estudo, 87,2% das incursões teriam evitado a necessidade de qualquer resposta, uma vez que o modelo abrangente automaticamente mitiga a necessidade.

Para aqueles que exigiam uma resposta, a velocidade da resposta foi muito mais rápida no lado abrangente. A complexidade reduzida da arquitetura de segurança significou a necessidade de menos comandos para lidar com o mesmo problema. Nos testes, a velocidade da resposta exigiu somente 14,2% do tempo exigido para a resposta da criptografia seletiva.

Topologia disponível também foi reduzida. Com menos pontos da camada disponível, as ameaças podem ser tratadas de um modo mais abrangente e menos complexo. Essa menor complexidade também reduziria significativamente o risco de invasões futuras. A topologia disponível medida para o teste contra um grupo de clientes de tamanho médio foi de uma média de 2.423 pontos disponíveis para 196. Isso representa uma redução geral na superfície de ameaça ***próxima de 92%.***

Com um modelo pervasivo, SIL explorou o risco de incursões e exposição usando uma medição e mecanismo de emulação mistos para testar a nova tecnologia. Fornecer o mesmo número de aspectos de proteção aos dados usando criptografia seletiva versus pervasiva mostrou que a combinação de menos tarefas manuais e uma velocidade maior produziu economias de custo de até 81,63%, menos do que o x86, dependendo de uma variedade de fatores.

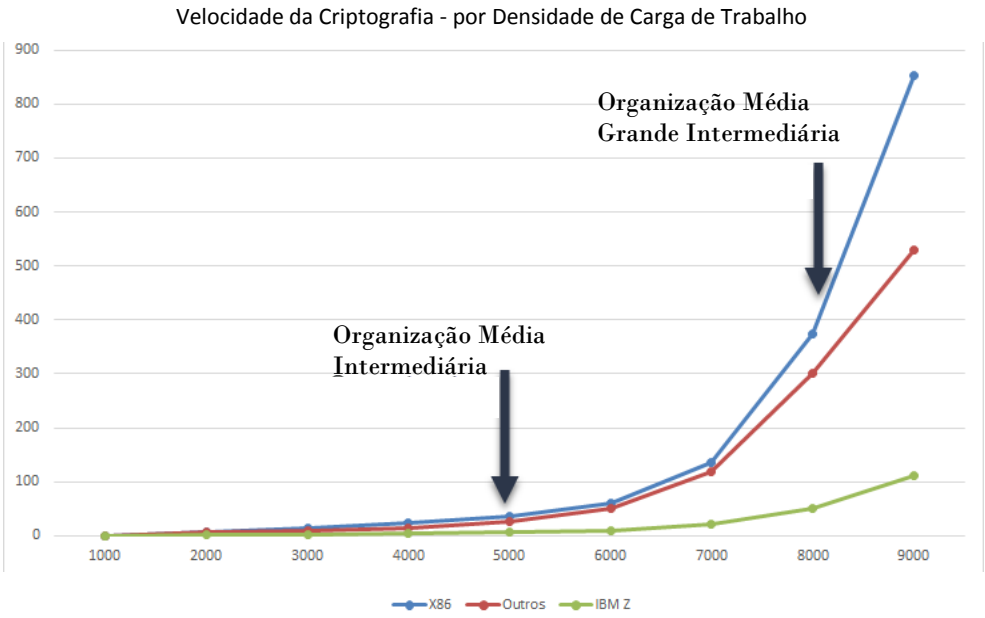
Com a eliminação de proliferação de plataformas que muitas organizações enfrentam hoje, a economia não é apenas nos custos da plataforma. Ele se estende ao pessoal exigido para operar o equipamento, executar os testes de segurança e gerenciar todos os recursos de segurança. A redução de pessoal é ainda mais substancial do que a de equipamentos. Onde hoje a carga do pessoal de segurança para o IBMZ exige aproximadamente 80% menos pessoal, o uso de segurança abrangente permitirá que o número de pessoal permaneça estático, enquanto plataformas alternativas continuarão a crescer substancialmente a cada ano.

Naquele ambiente, um enfoque abrangente para a criptografia é justificado pelo custo. Se o mercado exigir tal mudança de perspectiva, então os esforços dos fornecedores que foram devotados às soluções bolt-on poderiam ser melhor

direcionados para as mudanças de arquitetura e fundamentais necessárias para permitir a criptografia abrangente. Essas mudanças serão mais desafiadoras para algumas arquiteturas do que para outras.

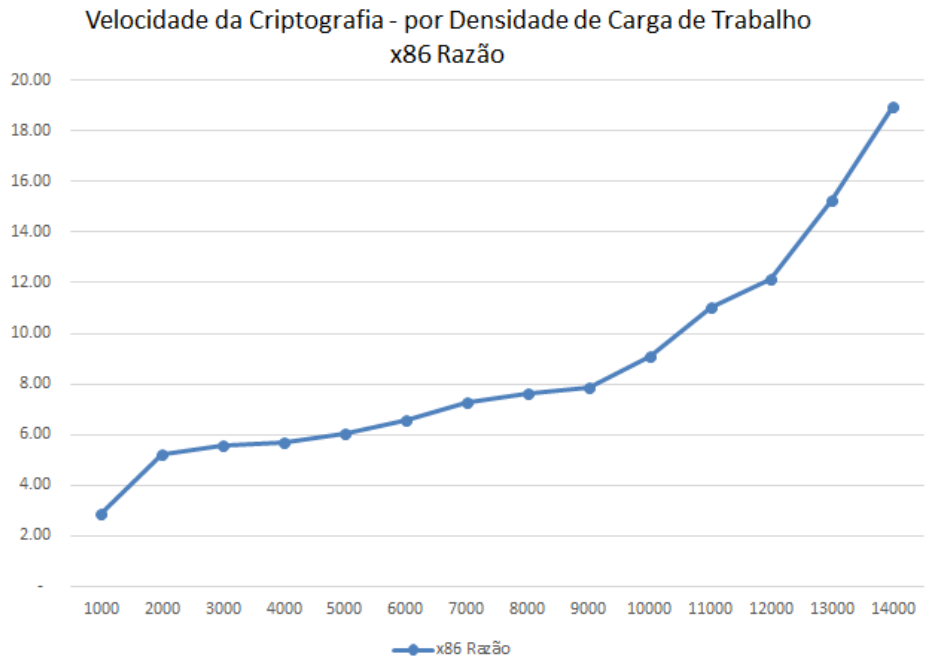
Embora a arquitetura de mainframe da IBM possa fornecer transações individuais 2,87-3,24 vezes mais rápido do que as velocidades do x86, a inclusão da topologia pervasiva e o enfoque aumentam esse multiplicador significativamente. Devido ao fluxo de atividade subjacente permitir que o modelo abrangente lide com lotes de transações como uma unidade em vez que criptografias individuais, as economias na demanda da capacidade são substancial e são refletidas na velocidade.

Esse enfoque para a eficiência da criptografia acrescenta outra ordem de magnitude da velocidade ao mecanismo de criptografia mais rápida, resultando em criptografia 18,4 *vezes* mais rápida do que as plataformas alternativas. A eficiência também afeta os custos. Os custos operacionais resultantes para a criptografia pervasiva são 5,1-8,0% do custo de outras opções, que é uma economia significativa.



Economias adicionais são conseguidas quando a incapacidade de outras plataformas de escalonar para qualquer demanda significativa é fatorada. A queda abrupta do desempenho é severa e torna qualquer solução mensurável insustentável para qualquer outra plataforma, exceto a IBM Z. A densidade das solicitações para a criptografia rapidamente superam a capacidade das demais plataformas de fornecer respostas em tempo hábil e criar tempos de espera significativos para a conclusão. Tal impacto torna rapidamente os contratos em nível de serviço (SLAs) e as expectativas de desempenho inviáveis. Como pode ser visto no parágrafo a seguir, quanto mais alta a densidade das solicitações, maior o aumento da sobrecarga nos demais mecanismos da plataforma. Mais dos recursos disponíveis vão para o despacho e outras atividades do sistema. Quando a demanda por criptografia pervasiva fica alta o suficiente, todo o sistema se torna irresponsivo.

A diferenciação das respostas de arquitetura pode ser vista no gráfico do resumo abaixo.



A rápida queda de desempenho do x86 é indicativo das limitações da arquitetura atual. A adição de processadores ou threading adicionais fornece um alívio limitado para uma pequena quantidade de paralelização. Infelizmente, esse é um enfoque autolimitante, uma vez que a sobrecarga aumenta com cada thread adicional, cancelando rapidamente as melhorias iniciais.

SIL escolheu explorar completamente esse problema complexo analisando detalhadamente a atividade de 117.000 organizações nos últimos 14 meses. Em cada uma das situações, um ambiente emulado foi criado e exercitado diariamente usando informações fornecidas pelo cliente.

O modelo foi primeiro testado para estresse ao assegurar que isso poderia replicar os resultados relatados da carga de trabalho real da produção. Assim que isso foi verificado na precisão, a carga de trabalho e a atividade foram então transferidas para um mainframe simulado usando primeiro a criptografia seletiva e então a criptografia abrangente.

A mesma carga de atividade foi então comparada com todas as três outras situações. Das 1,16 B de incursões que foram capturadas e relatadas pelos clientes remetentes, nenhuma delas teria ocorrido com sucesso se tentadas no IBM Z com a criptografia pervasiva explorada.

O modelo de criptografia seletiva também mostrou uma proteção significativa, com 92,1% de incursões sendo bloqueadas. Entretanto, a criptografia seletiva na realidade foi mais lenta e usou mais capacidade do sistema. A eficiência da criptografia melhorou muito ao mudar para o modelo pervasiva.

Esse tipo de proteção reflete claramente no resultado da organização. As incursões relatadas por esses clientes ao longo de um período de 14 meses representaram mais de US$1,3 bilhão em custos. Os custos incluíram, tempo do sistema, pessoal, despesas com remediação e esforços de mitigação da perda de mercado. Das 1,16B de incursões analisadas ao longo de 14 meses nesse estudo, a criptografia pervasiva teria evitado US$1.3 B em custos associados com essas incursões.

Teria também reduzido significativamente o perfil de risco dos aplicativos ou à segurança da organização. Devido ao maior número de fornecedores de seguro exigindo reservas financeiras com base nos perfis de risco às aplicações e operacionais, qualquer coisa que reduza o risco ajudará a evitar impacto financeiro

significativo na organização. Muitas dessas seguradoras estão pedindo que as empresas tenham reservas financeiras como parte do seu orçamento de TI. Isso começou sete ou oito anos atrás e está ganhando momento hoje. Atualmente, o fator de risco para a arquitetura do mainframe é até 80% inferior do que aquele exigido para sistemas que são baseados em explorações de informática x86 e outras arquiteturas. Essa porcentagem é calculada com base no orçamento geral de TI uma vez que todos os aspectos do ambiente computacional são afetados quando tais incursões ou falhas de segurança ocorrem. Uma organização com um orçamento de TI de USD12M veria uma diferença nas reservas exigidas de USD764.400 para x86 versus USD160.524 para IBM Z.

Uma área de interesse foi o subconjunto de incursões que dependiam do roubo das chaves de criptografia. As informações roubadas eram parte do emparelhamento público e privado usado na indústria para garantir a segurança das atividades intra-plataforma. Essa exposição foi completamente eliminada pelo modelo de criptografia do hardware presente na solução Z. Sem necessidade de emparelhamento handshake, não houve incursões bem-sucedidas relatadas na janela de 14 meses do estudo.

Uma vez que o impacto dos roubos de outras chaves de criptografia totalizou mais de USD6.587.500 no período do estudo, aquela salvaguarda é outra vantagem substancial para a solução de segurança pervasiva.

MSP

Esse tipo de criptografia também tem um efeito significativo naquelas ofertas de serviços na nuvem ou qualquer provedor de serviço gerenciado (MSP). Inerente à arquitetura em nuvem são as dimensões adicionais de perigo com base na própria arquitetura. Qualquer tipo de memória compartilhada ou recursos compartilhados expõe a máquina como um todo ao dano não somente de suas próprias incursões de segurança, mas àqueles de outros. Algumas vezes conhecida como 'sideways hacking,' o isolamento oferecido pelo mainframe acoplado à criptografia abrangente e integrada afeta significativamente os clientes do MSP e o resultado daquela organização. Uma vez que os MSPs frequentemente são travados em contratos de preço, qualquer incursão que seja rastreada até o MSP pode afetar radicalmente seu lucro líquido. A criptografia pervasiva mudaria a sua base e o perfil de risco substancialmente nesses casos.

EVENTOS RECENTES

Durante o período do estudo SIL, houve diversos eventos significativos no mundo da segurança que são pertinentes aos desafios tratados pela criptografia. Um vírus armado que imitava um ataque ransomware foi liberado. Na verdade, ele era uma arma, feita para destruir. O dano desse ataque deliberado foi pervasiva e considerável.

Governos, hospitais, aeroportos e demais negócios foram alvos, atacados e danificados. O custo disso ainda está sendo calculado e provavelmente continuará por muitos anos. O impacto líquido, entretanto, foi que esse tipo de ataque pode e acontecerá novamente. O tipo de criptografia que esse novo avanço representa, vinculado aos componentes da arquitetura Z integrada o teria parado, uma vez que a capacidade de subverter o controle do arquivo é um aspecto protegido da camada de segurança Z e não seria, portanto, vulnerável ao ataque de hackers.

Os trilhões de dólares em efeitos teriam sido economizados e as pessoas fisicamente prejudicadas e os negócios que foram impactados negativamente estariam seguros. Essa mudança fundamental no paradigma da segurança para a indústria é profundo.

Nesse ponto no tempo, nenhuma outra arquitetura de chip pode suportar o modelo de criptografia pervasiva. Isso deve-se às limitações técnicas na banda larga e na sobrecarga. Isso será um desafio para aquelas arquiteturas para desenhar e construir esse recurso, mas é o que a indústria precisa desesperadamente.

EFEITOS PRÁTICOS

O TCO da criptografia exigirá que as empresas analisem seus orçamentos de TI. Uma vez que muito do orçamento de TI é direcionado para o desenvolvimento de aplicativos, alcançando 41,5-68,2% para as organizações dentro do estudo, qualquer mudança que permita que isso seja reduzido tem efeito imediato nos resultados da organização.

Ao mudar a criptografia de um aspecto de segurança fundamental para o centro de um ambiente computacional em vez que fazer mudanças na aplicação para permitir a criptografia, o efeito prático no orçamento de TI seria uma redução de aproximadamente 22,1%.

Conclusão

> *"As implicações disso é que o ataque cibernético poderia ser interpretado como um ato de guerra de acordo com a organização. Na quarta-feira, o secretário geral da OTAN, Jens Stoltenberg, disse que um ataque cibernético poderia acionar o Artigo 4, o princípio da defesa coletiva."*
>
> Luke Graham |@LukeWGraham, Sexta-feira, 30 de junho de 2017 | 9h50 ET, Tech Transformers, um relato especial da CNBC

A divulgação atual da plataforma IBM Z tem uma vantagem substancial em termos de desempenho de TCO e risco comparado às demais opções de plataforma no mercado hoje. O nível atual de criptografia seletiva disponível e a resistência à plataforma nativa para os vetores de ameaça comuns fornecer às organizações uma salvaguarda fundamental significativa.

Entretanto, o advento da criptografia abrangente muda radicalmente não somente a salvaguarda disponível nas ofertas Z, mas também a indústria em geral. Essa mudança de paradigma é um desafio para qualquer oferta que tente atender o mercado hoje.

As empresas que estão conduzindo ativamente o comércio no espaço cibernético e aquelas que se mudaram para um modelo na nuvem têm uma enorme sensibilidade quando se trata de segurança cibernética. A segurança ao redor dos dados de uma organização e o capital intelectual está se tornando rapidamente o principal foco, à medida que o mundo se torna mais e mais conectado. Esse aumento da integração é acompanhado por desafios maiores, à medida que as empresas se esforçam para proteger sua vantagem no mercado e suas finanças. IBM Z tem uma longa história de proteção dos ativos e implementações altamente seguras e com essa maturidade vêm os recursos que estão ausentes em outras virtualizações, incluindo aqueles que controlam a segurança do acesso e do processo.

Alguns destaques dos achados do estudo podem ser vistos abaixo.

Resumo rápido

Categoria	Comentário	Quick Byte
Velocidade de resposta	As mesmas atividades padrão no Z consomem até *85,80%* menos tempo de relógio do que aquelas executadas em outras plataformas.	Resposta da segurança mais rápida é fornecida pelo Z.
Risco	O perfil de risco SIL define a classificação de risco da plataforma Z em menos de *1/20* de qualquer outra solução alternativa.	O risco à segurança é significativamente menor quando implementando as plataformas Z.
Eficácia da segurança	Com base nas instalações iniciais, a solução de segurança Z da fundação oferece até*8,5 vezes* o nível de interceptação das soluções da plataforma alternativa com 93% menos custo nas despesas gerais e com 81% menos esforço.	IBM Z fornece os mesmos ambientes de aplicação seguros.
Eficácia da segurança	As plataformas Z oferecem interceptação de incursão que é até*20,74%* melhor do que as soluções da plataforma alternativa com segurança totalmente aumentada.	A segurança básica fornecida pela plataforma Z é mais eficiente do que as soluções aumentadas nas plataformas alternativas.
Esforço da equipe	Estudos de tempo e movimento mostram que as soluções de segurança da plataforma Z exigem *81%* menos tarefas para implementar os níveis de proteção padrão.	IBM Z exige menos esforço da equipe para garantir segurança.
Remediação	Os custos de remediação nas implantações de segurança Z são em média *98,82%* menores do que as plataformas alternativas.	Reparar os danos à segurança é mais barato na Z.
Custo total de propriedade da segurança	O TCO para as implementações da segurança Z são menores em até 83,72% do que aqueles de outras plataformas.	As suas despesas em segurança dão mais resultado em uma plataforma Z.
Custo total da informação	As implementações IBM Z mostram TCI até 84,83% mais baixos em uma ampla gama de tamanhos de organizações	Trabalhar com suas informações no Z é mais barato.
Criptografia Pervasiva	A arquitetura do mainframe da IBM pode fornecer criptografia até 18,4 vezes mais rápido, para somente 5% do custo de outras soluções de plataforma.	IBM Z torna a criptografia pervasiva possível.
Financiamento da mitigação de risco	Uma organização com um orçamento de TI de USD12M veria uma diferença nas reservas exigidas de USD764.400 para x86 versus USD160.524 para IBM Z.	Risco menor em uma plataforma Z se traduz em menor reserva financeira para a segurança cibernética.
Singularidade	Nesse ponto no tempo, a IBM Z e a única arquitetura que pode suportar o modelo de criptografia pervasiva.	IBM Z oferece recursos de criptografia incomparáveis.

A natureza de mudança do negócio cibernético está ficando cada vez mais fluida. Mudanças mais rápidas, ataques ativos e um papel de gestão de risco desafiador, tudo isso se combina para apresentar perigos além de oportunidades.

Na análise que a SIL acabou de concluir, o objetivo original foi examinar o impacto no mundo real da segurança dos negócios com base na arquitetura da plataforma. Para esse fim, as principais arquiteturas como, por exemplo, as plataformas Z da IBM e os produtos x86 foram comparadas.

A descoberta inesperada foi uma mudança tremenda na indústria.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) é um provedor de serviços especializado em modelagem de desempenho preditivo. Fundada em 1978, a SIL faz uso extensivo da tecnologia AI e de matemática do caos proprietária para analisar cenários proféticos ou forenses. A SIL analisa mais de 5.900 clientes no mundo todo com desenho de perfil de risco contínuo, análise da causa raiz do desempenho, impacto ambiental, gestão de recursos, tendências de mercado, análise de defeitos, análise da eficiência Fourdham da aplicação, identificação da alavancagem dinâmica organizacional, bem como dissecação de custos e despesas. A SIL também fornece certificação RFP para respostas do fornecedor a organizações governamentais ao redor do mundo e muitas empresas comerciais.

Uma ampla gama de fornecedores de software e de hardware governamentais e comerciais trabalham com a SIL para obter certificação para os recursos de desempenho e limitações de suas ofertas. A SIL também trabalha com esses fornecedores para melhorar os resultados e a escalonabilidade para implementações do cliente e para oferecer perfis de risco e outras estratégicas de mitigação de risco. A SIL está profundamente envolvida no estabelecimento de padrões industriais e certificação de desempenho nas últimas décadas e tem coletado informações ativa para o Operational Characterisation Master Study (OPMS) – concebido para desenvolver um melhor entendimento dos custos organizacionais centralizados em TI e as características comportamentais. O OPMS continuou a construir a base de dados heurística da SIL, atualmente excedendo 475 PB de informação. O aumento da base estatística continuou para melhorar a precisão da SIL e a transformação analítica para níveis incomparáveis na indústria. No geral, a SIL executa mais de 2M de modelos anualmente em apoio aos clientes com assinatura contínua e as solicitações ad hoc.

OBSERVAÇÕES SOBRE A METODOLOGIA

Para entender o impacto das plataformas IBM Z como parte essencial de uma infraestrutura de TI da organização e os efeitos da experiência do cliente, um número significativo de implementações foi examinado. O grau de diferença relativo no comportamento operacional para cada fator, isto é, o número total de interrupções etc. foi então comparado para entender o efeito líquido das respectivas combinações. Os efeitos foram observados no desempenho geral e no consumo da capacidade, bem como em outras métricas do negócio.

O enfoque adotado pela SIL usa uma compilação e a correlação do comportamento da produção operacional, usando sistemas reais e atividades de negócio reais. Para fins dessa investigação, 9.602.042 configurações ambientais foram observadas, registradas e analisadas para substanciar as descobertas. A experiência do cliente foi obtida para coincidir com os dados da implementação. Mais de 6,3M de perfis de feedback de clientes em suas experiências foram analisados, comparados com os ambientes de TI e incluídos no estudo. Usando uma massa grande de clientes e dados experimentais da indústria, um entendimento mais preciso do comportamento do mundo real pode ser alcançado. Os dados desses sistemas foram usados para construir uma perspectiva significativa sobre os desafios operacionais atuais e os benefícios. O comportamento relatado dos sistemas foi analisado para isolar as características da arquitetura do desempenho bruto e de uma perspectiva de efeito no negócio líquido.

Uma vez que uma parte desse estudo examina o impacto da tecnologia emergente no desempenho geral, custo e risco de um número significativo de organizações, emulações operacionais detalhadas foram realizadas com os dados fornecidos pelo cliente. Essa emulação exercitou o ambiente virtual para aquelas organizações por um período de 14 meses de atividade diária, conforme fornecido pelos participantes. Os resultados daquele exercício foram incluídos nas descobertas apresentadas neste paper.

Em uma situação como aquela apresentada por esse estudo, a SIL usa uma metodologia que incorpora a aquisição dos dados operacionais, incluindo as informações da atividade do sistema em um nível muito detalhado. Deve ser observado que os clientes, executando em suas plataformas de produção, forneceram todas as informações. É essencial entender que nenhum dos dados foi coletado de benchmarks artificiais ou de testes construídos, uma vez que o valor nesse estudo vem do entendimento dos processos operacionais reais dentro da organização, em vez da percepção do que está sendo feito. Portanto, esses sites são a representação das situações da vida real, em vez de uma configuração de benchmark artificial. Uma vez que o foco dessa análise foi não definir estritamente as diferenças entre as diferentes variações menores do sistema operacional ou do hardware, as diversas versões foram combinadas para mostrar as diferenças de arquitetura como um todo. Isso fornece uma visão mais geral da estratégia da arquitetura.

A fim de apoiar a natureza abrangente dessa análise, informações de diversas implementações, indústrias, geografias e fornecedores foram obtidas. Em uma coleta desse tipo, há alguma sobreposição como, por exemplo, quando múltiplos fornecedores estão presentes em uma organização. Em tais casos, o total de porcentagens distintas pode exceder 100%. Essas organizações com implementações em múltiplas camadas como, por exemplo, múltiplos locais geográficos ou

classificações industriais têm sido analisadas com derivações distintas de seu feedback para todas as métricas. Filtragem adicional foi realizada para eliminar aquelas implementações que falharam substancialmente em atender as melhores práticas. Devido às taxas de falha, desempenho ruim e custos altos que aparecem em um grande número dessas implementações têm pouco a ver com as escolhas de hardware e software reais, esses projetos foram removidos da base analítica desse estudo.

A representação da indústria cobre manufatura (26,55%), distribuição (19,87%), saúde (4,67%), varejo (12,83%), financeiro (22,16%), setor público (6,54%), comunicações (3,88%) e um grupo diverso (3,50%).

As geografias também foram bem representadas com a América do Norte fornecendo 32,05% das organizações relatando, América do Sul e América Central 10,58%, Europa 33,62%, Costa do Pacífico e Ásia 15,62%, África 4,74%, e aquelas organizações que não se encaixam nessas divisões geográficas relatando 3,38% das informações.

Uma vez que as estratégias e os benefícios tendem a variar pelo tamanho da organização, a SIL ainda agrupa as organizações por categorias de pequena, média, grande e extra grande. Essas categorias combinam o número de funcionários e a receita bruta anual da organização. Essa contagem de funcionários multiplicada pela receita bruta cria uma métrica para uma definição que é usada em toda a análise. Nessa definição, seria possível esperar que uma pequena organização tivesse menos de 100 funcionários e lucro menor do que USD20 milhões, ou um valor de 2.000, por exemplo, 100 (funcionários) X 20 (milhões de dólares de receita bruta). Uma organização com 50 funcionários e receita bruta de US$40 milhões teria a mesma classificação de tamanho e seria agrupada na análise com a primeira empresa. As classificações usadas pela SIL usam limites de 2.000 (pequena), 10.000 (média), 100.000 (grande) e 1.000.000 (extra grande).

As informações nesse estudo foram reunidas como parte de uma coleta de dados contínua e suporte do sistema no qual a SIL está envolvida desde 1978. O pessoal do cliente executou todos os testes nos sites do cliente da SIL. Os resultados dos testes foram publicados para a SIL via pontos de coleta de dados seguros, normais que são usados por aqueles clientes desde que o relacionamento de suporte da SIL foi iniciado. Enquanto as informações eram recebidas nos pontos de dados seguros, o processamento SIL AI padrão preparou os dados em formato padrão, removendo todas as referências detalhadas do cliente. Esses dados purificados foram então inseridos para análise e resultados.

ATRIBUIÇÕES E ISENÇÃO DE RESPONSABILIDADE

Este documento foi desenvolvimento com financiamento da IBM. Embora o documento possa usar material disponível publicamente de diversos fornecedores, incluindo a IBM, não é necessário refletir as posições de tais fornecedores sobre assuntos tratados neste documento.

ZSL03452-BRPT-00