Criptografia Pervasiva - um resumo

Um novo paradigma de proteção

Sou hacker profissional há mais de 15 anos. Procuro problemas de cibersegurança em tecnologia para tornar a própria tecnologia mais segura. Mas, após fazer isso por muitos anos, estou frustrado. Vejo os mesmos problemas se repetirem novamente. Não estamos melhorando. E, embora dependamos cada vez mais da tecnologia, ela está se tornando cada vez mais insegura."

Cesar Cerrudo, hacker profissional e Diretor de Tecnologia do IOActive Labs,

Todo o ciberespaço e sua infraestrutura subjacente estão vulneráveis a uma ampla variedade de riscos e à exposição de ameaças e perigos físicos e virtuais. Cibergrupos e indivíduos sofisticados exploram vulnerabilidades isoladas e congregadas para roubar dinheiro e informações ou mesmo para corromper, colocar em perigo ou danificar operações. A combinação de ampla oportunidade ao crime no ciberespaço e a capacidade de executar de locais geograficamente dispersos gerou uma transformação nas ações criminais tradicionais.

É extremamente difícil a proteção do ciberespaço. A integração crescente entre o ciberespaço e o mundo físico expandiu exponencialmente as oportunidades de roubo, danos e corrupção. Reduzir as vulnerabilidades e minimizar as consequências em ciber-redes complexas são as metas, porém, cada vez mais difíceis de se atingir. A abordagem básica de segurança está se provando inadequada às demandas de natureza agressiva do ambiente. É necessária uma mudança de paradigmas. E rápida.

Os dados de pesquisa foram compilados pela Solitaire Interglobal, Ltd. (SIL). Informações de empresas preocupadas com a eficácia de sua segurança compõem a base de dados do estudo, complementadas por informações de ameaças e segurança do Global Security Watch (GSW), cujo principal foco é o impacto sobre a operação da empresa, ativos organizacionais e prevenção e remediação de custos. Esta análise examinou o impacto real sobre a segurança da empresa com base na arquitetura da plataforma. Para esse fim, foram comparadas métricas das principais arquiteturas, como plataformas IBM Z, UNIX e produtos x86. No breve resumo abaixo, destacamos algumas das descobertas.

A versão atual da plataforma IBM Z tem uma vantagem substancial em termos de TCO, desempenho e risco, em comparação com as outras opções de plataforma do mercado hoje. O nível atual de criptografia seletiva disponível e a resistência da plataforma nativa aos vetores de ameaça comuns dão às organizações uma proteção básica significativa.

A chegada da criptografia pervasiva muda radicalmente não apenas a proteção do que está disponível nas ofertas Z, mas no setor em geral. Esta mudança de paradigma é um desafio para qualquer outra opção que tente atender a empresa hoje.

RESUMO DOS RESULTADOS ENCONTRADOS

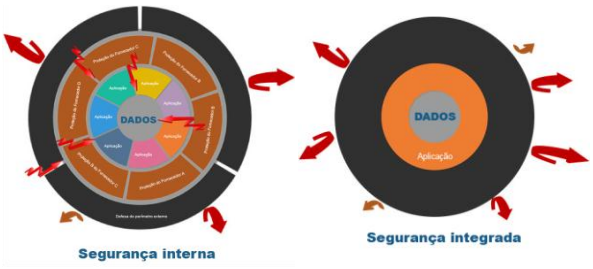
Resumo

Categoria	Comentário	Dado rápido
Velocidade de resposta	As mesmas atividades padrão em Z consomem até *85,80%* menos tempo de clock do que aquelas executadas em outras plataformas.	A resposta de segurança mais rápida é dada por Z.
Risco	O perfil de risco SIL define a classificação de risco da plataforma Z a menos de *1/20* de qualquer das soluções alternativas.	O risco de segurança é significativamente mais baixo durante a implementação em plataformas Z.
Eficácia da segurança	Com base nas instalações iniciais, a solução de segurança Z de base oferece *8,5 vezes* o nível de interceptação das soluções de plataforma alternativa a 93% menos custo na despesa total, e com 81% menos esforço.	As plataformas IBM Z oferecem os ambientes de aplicação mais seguros.
Eficácia da segurança	As plataformas Z oferecem interceptação de incursão base que é *20,74%* melhor do que as soluções de plataforma alternativas com segurança totalmente aumentada.	A segurança de base proporcionada pelas plataformas Z é mais eficaz do que as soluções aumentadas em plataformas alternativas.

Categoria	Comentário	Dado rápido
Esforço da equipe	Estudos sobre tempo e movimento demonstram que as soluções de segurança Z exigem *81%* menos tarefas para a implementação dos níveis de proteção padrão.	O IBM Z exige menos esforço da equipe para fazer a proteção.
Remediação	Os custos de remediação nas implementações de segurança do Z são em média *98,82%* mais baixos do que nas plataformas alternativas.	Consertos de danos em segurança são mais baratos no Z.
Custo total de propriedade com segurança	O TCO para as implementações de segurança no Z são mais baixos em até 83,72% do que aqueles de outras plataformas.	Seu dinheiro com despesas de segurança rendem mais no Z.
Custo total da informação	As implementações do IBM Z demonstram um TCI 84,83% mais baixo em uma ampla gama de tamanhos de empresas	Trabalhar com suas informações no Z é mais barato.
Criptografia pervasiva	A arquitetura de mainframe da IBM consegue fornecer criptografia até 18,4 vezes mais rápida, por apenas 5% do custo das outras soluções de plataforma.	A criptografia pervasiva muda o jogo.
Recursos para a mitigação de riscos	Uma organização com orçamento de TI de $12 milhões de dólares veria diferença na reserva necessária de $764.400 para x86 em comparação a $160.524 para o IBM Z.	O risco mais baixo no Z se converte em menos reservas financeiras para a cibersegurança.
Exclusividade	Neste momento, o IBM Z é a única arquitetura que consegue oferecer suporte ao modelo de criptografia pervasiva.	Proteja seus recursos de TI agora.

Longos períodos de incursão ativa podem ter um efeito negativo substancial sobre a viabilidade organizacional. A empresa começa a sofrer entre 16,2%-63,7% de redução média na receita bruta e na valorização, se uma incursão durar mais do que três meses.

Quando a resposta tática inclui a adição de camadas de segurança e proteção, a arquitetura resultante começa a se assemelhar a uma cebola, com camadas de segurança adicional. No entanto, as próprias camadas reais podem criar pontos adicionais de topologia que podem ser atacados.



Cada local com uma solução parcial "aplicada" é também outro alvo para um hacker bem preparado. Quanto mais complexas as camadas, mais aumenta a possibilidade de ataque à topologia. Tal vulnerabilidade é parte de um perfil de risco de segurança, que é cada vez mais usado pelas seguradoras para determinar o grau de exposição de uma organização a ciberdanos significativos.

Cria-se uma pressão adicional por segurança com o uso crescente de software de virtualização. Cada uma dessas máquinas virtuais cria novos pontos de vulnerabilidade e contribui para a complexidade do desafio da segurança. Essa diferença significativa deriva da estrutura de base e da estratégia subjacente à arquitetura da plataforma, design do chip, sistema operacional e método de integração de stacks.

Não somente o número de ataques mudou. Mudou muito a própria aparência da incursão.

Um dos vetores de maior crescimento é o de ataque de ransomware. Nesse tipo de ataque, a incursão trava os arquivos, diretórios e outros componentes do sistema. O proprietário tem de pagar por um código de destravamento, que pode ou não de fato funcionar.

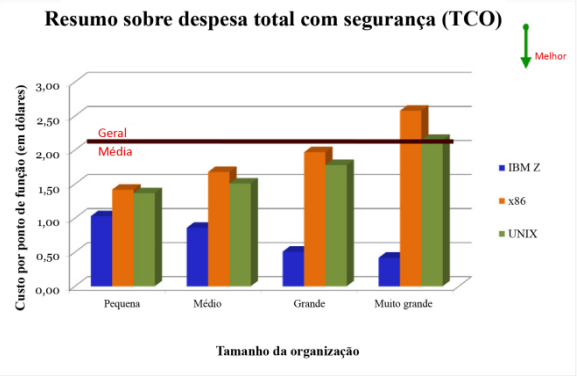
A medição da segurança é uma grandeza ponderada, pois é avaliada com base na ausência de problemas e aborrecimentos. As falhas na segurança são altamente visíveis, ao contrário do seu êxito. O estudo dirigiu-se principalmente para o valor da segurança na perspectiva da empresa, para que a liderança das empresas pudesse entender os benefícios das opções de segurança oferecidas pelo IBM Z com a criptografia pervasiva, ao avaliar as soluções de segurança.

Durante a coleta e análise dos dados do estudo, diversas características surgiram. Essas características afetam a capacidade observável, a eficiência e a confiabilidade do ambiente protegido. Também foi examinada a sinergia das operações de segurança e de negócios. A perspectiva da empresa engloba uma miríade de fatores, incluindo confiabilidade, graus de segurança, níveis de contratação de pessoal, custo total de segurança (incluindo recuperação) e outros efeitos. Esses se articulam diretamente às decisões que os gestores de TI, diretores de tecnologia e líderes de empresas têm de tomar diariamente.

CUSTO TOTAL DE PROPRIEDADE

O custo total de propriedade (TCO) oferece uma das principais métricas empresariais para a eficiência operacional. Mais uma vez, os projetos e suas despesas foram normalizados com uma base padrão que permite que as despesas organizacionais grandes e pequenas sejam comparadas de forma mais exata.

Os padrões de despesas demonstram tendências crescentes de alguns tipos de plataformas, à medida que aumenta a complexidade da implantação. Há uma tendência contraditória para o IBM Z. Um padrão em queda nas despesas da unidade se converte em eficiência em escala, na qual o alavancar de estruturas e da base proporciona um padrão econômico de investimento financeiro. Conforme se vê no gráfico a seguir, as despesas para as implementações de segurança em Z são mais baixas em até 83,72% do que aquelas de outras plataformas. Isso deriva parcialmente da combinação da base de segurança da arquitetura e da plataforma altamente escalável.



> *"Nosso mainframe IBM tem um custo muito mais baixo do que qualquer outra coisa que fazemos na empresa. Os custos na verdade diminuíram nos últimos três anos, embora nosso financeiro continue nos dizendo que os custos estão altos demais. E eu continuo dizendo a eles que nosso custo geral é baixo, dado que temos menos problemas, menos gente trabalhando e menos chance de ter problemas."*
>
> Diretor Financeiro - Distribuidor de grande porte

Em situações em que a segurança é tratada com uma série de componentes de proteção adicionais ou quando a principal governança de segurança reside apenas na aplicação implementada, a comparação das despesas gerais dá um salto significativo quando se adicionam novos serviços. O gráfico a seguir mostra este tipo de efeito. Os projetos incluídos nesta parte da análise demonstram o impacto a curto prazo da aquisição de segurança. Em todos os casos, essas 16.027 organizações adicionaram uma única aplicação em nuvem às implementações em nuvem já existentes. As implementações visavam nuvens públicas, privadas e híbridas e eram designadas a mais de 1000 usuários.

Comunicar o custo real e o impacto da segurança é outro desafio. A articulação de um caso de expansão e melhorias na segurança de uma empresa é um assunto frequente de discussão, bem como objeto de reclamação, entre profissionais de segurança em todo o mundo. O impacto do custo da segurança como um aspecto da eficiência operacional não é claramente entendido pela maioria dos executivos de empresas. Em um conjunto de dados coletados entre 2015-6, que incluía mais de 9,5 milhões de executivos de empresas, menos de 11% nunca tinha visto um caso de empresa relacionado a despesas de segurança. Menos de 0,9% dessas pessoas diziam entender como surgiam os custos com segurança, as economias em escala e as despesas projetadas. Infelizmente, menos de 35% dos responsáveis por tomar as decisões estratégicas da empresa acreditavam que sua equipe de segurança sabia como projetar ou mesmo calcular custos. Todos eles contribuem para uma situação em que a redução ou mesmo o aumento da alocação de custos com a carga de trabalho geral da segurança são algo inesperado e não muito bem-vindo. Com este ponto cego, a gerência executiva deixa de entender a eficiência que pode ser dimensionada das implementações de segurança do IBM Z.

EFICÁCIA DA SEGURANÇA

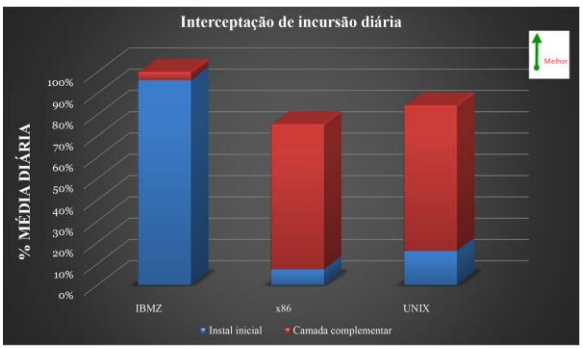
Para examinar a eficácia da segurança, a SIL encontrou comparações mensuráveis em uma combinação de métricas objetivas e subjetivas. As métricas objetivas incluíam a capacidade de as medidas de segurança captarem e impedirem a incursão bem-sucedida, tanto para incursões relatadas quanto para as descobertas em auditorias detalhadas. As informações contidas nesta medição têm aplicabilidade tanto para o lado técnico quanto para o lado empresarial de uma organização, desde que a quantidade de incursões possa ser bem traduzida em termos dos efeitos sobre a base da organização.

Cada uma dessas áreas oferece alguns diferenciais principais para a solução de cibersegurança do IBM Z.

RESISTÊNCIA À INCURSÃO

A principal métrica em termos de sucesso de segurança é o número de incursões que são pegas, neutralizadas ou impedidas de causar qualquer forma de dano. As incursões agregadas nesta métrica não incluem aquelas que foram bloqueadas por quaisquer firewalls ou dispositivos de segurança complementares. Em vez disso, foram contadas somente aquelas bloqueadas pela solução de segurança presente na plataforma.

O nível de bloqueio da incursão dado pela instalação inicial de cada uma das plataformas compõe a base para qualquer segurança adicionada, obrigatória ou instalada. Este gráfico mostra a segurança dada pela instalação inicial e a camada complementar, expressa como uma porcentagem de incursões que foram bloqueadas. Com base nas



instalações iniciais, a base das soluções de segurança do IBM Z oferece *13,21 vezes* mais do que o nível de interceptação das soluções de plataformas alternativas. Além disso, a solução Z oferece uma proteção de base que excede 92,1%, mesmo sem a complementação interna necessária para as arquiteturas alternativas.

As camadas de segurança complementares são aplicações, táticas e técnicas adicionais, etc. Essas diferem de uma organização para outra, mas são variáveis com base na visão geral de segurança, postura e governança de cada local. Níveis mais altos de exigência de segurança complementar indicam níveis mais altos de esforços da parte do pessoal de segurança e do software.

A combinação de capital intelectual e serviços automatizados, aliada ao design da arquitetura das soluções de cibersegurança do IBM Z, resulta na interceptação de uma porcentagem significativamente mais alta de incursões. A plataforma Z entrega interceptação de incursão na base que é *20,74%* melhor do que a segurança combinada de uma base aumentada com esforços amplos, competentes e rigorosos de táticas, técnicas e procedimentos de segurança complementares, dados por outras soluções em plataformas alternativas.

> *"Não tenho ideia do motivo de haver menos problemas de segurança com a plataforma z (sic), eu só sei que não temos. O pessoal de segurança está sempre me dizendo coisas sobre isso e aquilo, em resumo, a coisa simplesmente funciona. A última vez que tivemos problema com segurança nessa plataforma foi quando alguém roubou a senha de outra pessoa. A última em que eu tive problema com segurança em uma plataforma diferente foi há uma hora atrás. Me perguntaram qual eu preferia."*

Diretor de TI - Grande distribuidor

A natureza da segurança embutida do Z é significativamente diferente daquela que é criada com soluções de proteção adicionais. Com um grupo maior de interfaces para salvaguardar, a proteção dos dados e processos da organização é mais vulnerável quando definida no dispositivo. Por isso, as estratégias mais eficientes centralizam mais a definição e o controle das políticas. A stack de segurança altamente integrada e embutida do Z oferece uma vantagem substancial neste aspecto.

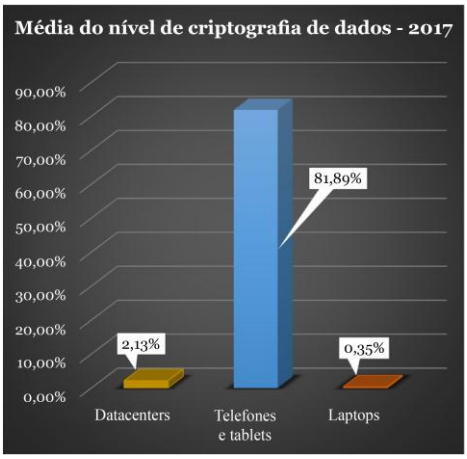
FATORES DE RISCO DE SEGURANÇA

O risco de segurança pode ser definido como o potencial com que uma dada ameaça pode explorar com sucesso as vulnerabilidades de um processo ou um ativo ou grupo de ativos, causando danos à organização ou aos clientes a que ela serve. Isso é medido em termos de uma combinação da probabilidade de ocorrência de tal evento e suas consequências associadas. A SIL cria perfis de risco que são constructos atuariais, usados para oferecer uma visão consolidada do risco global de uma organização. Isso incorpora a contribuição do risco individual de aplicações, interfaces, estruturas de gestão, aspectos de engenharia social etc.

> *"Uma variedade de ataques tem nos deixado enrolados, causando desconfiança de clientes, custos com remediação e outras influências horríveis. A experiência toda resultou em uma grande perda de confiança por parte do cliente. Estamos mudando rapidamente para um provedor de serviços gerenciados (MSP) que execute algumas das cargas de trabalho em um grande mainframe, pois isso parece ser o único local seguro para se executar hoje em dia."*

Diretor - Empresa média de distribuição

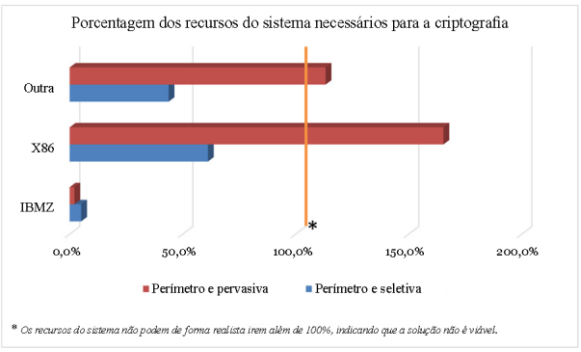
CRIPTOGRAFIA PERVASIVA



Os dados corporativos e os clientes de uma organização são um recurso-chave. Isso é literalmente algo sem preço e compõe a principal vantagem de mercado e do capital intelectual de qualquer empresa. A criptografia tem sido uma forma de proteger esses ativos, dado que, uma vez criptografados, eliminam-se a disponibilidade e a vulnerabilidade a hackers. Muitos desses ativos estão no momento desprotegidos.

A perspectiva é diferente em outras áreas de comunicação de dados. O uso de dispositivos móveis criou uma visão de privacidade que incluiu a criptografia desde o design inicial. Uma comparação entre os diferentes níveis de criptografia é algo esclarecedor.

Este resumo destaca a diferença básica da TI de mainstream e da comunicação móvel. Como o setor de comunicação percebeu logo a importância da criptografia quando se tratava de dispositivos móveis, aproximadamente 82% dos dados nessas plataformas estão criptografados. É grande a discordância sobre a falta de criptografia em recursos organizacionais de grande valor localizados em datacenters e em laptops.



Há diversos motivos-chave para os baixos níveis de criptografia. O custo em termos de tempo e capacidade do sistema estimulou as organizações a se concentrarem em técnicas de defesa perimetrais e na criptografia seletiva. Com a crescente demanda da defesa em segurança perimetral, consumindo até 61,2% da capacidade da plataforma alternativa, é necessária uma mudança de paradigma.

Um avanço recente em um aspecto básico de nosso ambiente computacional atual está pronto para fazer uma diferença significativa no mercado. A mudança é a expansão da criptografia atual do IBM Z de um modelo seletivo para um modelo pervasivo. Tal modificação significativa na estrutura básica da computação e seu efeito sobre a segurança causarão um grande efeito disruptivo.

O conceito global é não introduzir uma camada de decisão que diga o que será ou não criptografado. Em vez disso, será possível ter criptografia como parte do processamento normal. A remoção da decisão da criptografia seletiva é uma economia adicional no custo geral e uma redução na dificuldade de uso da criptografia no mercado atual.

A maior barreira em se fazer a criptografia em ampla escala tem sido o custo e a carga de desempenho que tal atividade impõe sobre a plataforma computacional. No entanto, para as organizações envolvidas neste estudo, as soluções internas que estão sendo implantadas fizeram a capacidade do sistema crescer de tal forma que há cargas de até 61% de carga sendo consumida por processos de segurança. Isso se traduz em uma quantidade expressiva em custos de infraestrutura, retardos no desempenho, etc.

As atuais exigências de recursos de criptografia pode ser vista claramente no gráfico acima. Mesmo sem os avanços mais recentes, a arquitetura do Z entrega criptografia com uso mais eficiente e mais econômico de recursos. Ela oferece mais de ***8,5 vezes*** a proteção de segurança, com ***93% a menos em custo***em termos de gastos globais e com ***81% menos esforço***. No entanto, isso é criptografia seletiva, que diminui algumas proteções absurdamente necessárias.

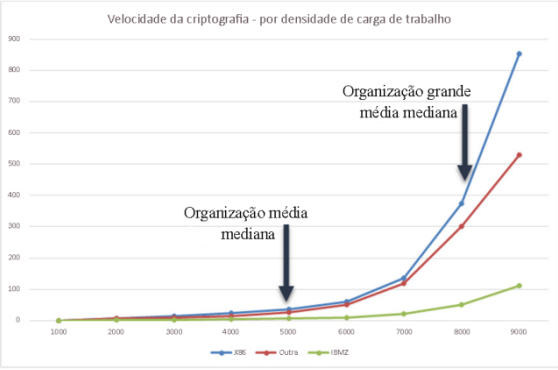
O impacto total do mais rápido mecanismo de criptografia e a capacidade de criptografar informações em massa cria uma solução totalmente pervasiva, que executa ***18,4 vezes mais rápido*** e a apenas ***5% do custo*** das outras soluções.

Embora a criptografia pervasiva seja viável no mainframe Z, no momento não é possível implantar em outras arquiteturas. A mais restritiva das arquiteturas, ligada às soluções x86, exigiria *7,32 vezes* a capacidade atual de execução da carga de trabalho necessária para a criptografia pervasiva em um único servidor. Usando a média por arquitetura dentro do grupo do estudo, isso se converte *12,2 vezes* o número de plataformas instaladas no momento nesses locais. Caso contrário, as exigências desse tipo de solução exigirão avanços significativos no design de chip da plataforma alternativa, na base do sistema operacional e em outras restrições de capacidade interna da plataforma. Tais avanços são mudanças a longo prazo no design e na manufatura do chip, com tempos de inatividade típicos de 2-3 anos, considerando a tecnologia de base em que puderam ser criados.

Se isso não for feito, as demandas por criptografia pervasiva não poderão ser atendidas nessas plataformas. Os sistemas residentes nessas plataformas continuarão a executar com maior risco e mais perfis de exposição, demandarão uma quantidade excessiva de tempo do pessoal e de despesas, bem como consumirão quantidades desproporcionais de recursos da organização.

Aplicar a criptografia em uma camada pervasiva significaria reduzir a porcentagem da plataforma não dedicada aos processos de segurança. Para as organizações analisadas em um recente estudo da SIL, a redução seria em torno de 91,7%.

A carga de trabalho e a velocidade de resposta são muito importantes quando se fala em segurança. Na comparação da criptografia seletiva com a pervasiva, no mesmo estudo, 87,2% mais das incursões foram tratadas automaticamente pelo modelo pervasivo.



Para aqueles que necessitaram de uma resposta, a velocidade desta foi muito mais rápida no processo pervasivo. Nos testes, a velocidade de resposta exigiu apenas 14,2% do tempo necessário para a resposta de criptografia seletiva.

A topologia que pode ser atacada também foi reduzida. Com menos pontos de camadas que podem ser atacados, as ameaças podem ser tratadas de forma mais ampla e de maneira menos complexa. Esta menor complexidade também pode diminuir significativamente os riscos de hacks futuros. A topologia que pode ser atacada caiu de uma média de 2423 pontos atacáveis para apenas 196, ou seja, um redução global de ***quase 92%***.

Com um modelo pervasivo, a SIL explorou o risco de incursões e a exposição, usando uma medição mista e um mecanismo de emulação para testar novas tecnologias. O uso da criptografia seletiva em vez da pervasiva demonstrou que a combinação de menos tarefas manuais e de maior velocidade produziu economias de 81,63% a menos que o x86.

Onde hoje a carga para o pessoal de segurança do IBM Z exige aproximadamente 80% menos gente, o uso de segurança pervasiva possibilitará que menos gente fique sem fazer nada enquanto as plataformas alternativas continuam a crescer substancialmente a cada ano.

A economia em termos de custos globais é também substancialmente diferente. O TCO da mesma unidade operacional com criptografia pervasiva comparado com a criptografia seletiva foi de apenas 36,7% do orçamento de TI geral. O impacto sobre a organização com um todo é substancial, abrangendo um grande número de áreas, da linha de trabalho ao desenvolvimento de aplicações.

Enquanto a arquitetura do mainframe IBM consegue entregar transações 2,87-3,24 vezes mais rápido, a inclusão da abordagem e da topologia pervasivas aumenta muito esse multiplicador. O fluxo de atividades subjacentes permite que o modelo pervasivo lide com os lotes de transações como uma unidade, em vez de como criptografias individuais, o que resulta em uma criptografia que é 18,4 *vezes* mais rápida do que as plataformas alternativas. O custo operacional resultante da criptografia pervasiva é de 5,1-8,0% do custo das outras opções.

Uma área de interesse era o subconjunto de incursões que se valiam do roubo de chaves de criptografia. As informações roubadas eram parte do pareamente público e privado usado na indústria para proteger as atividades intraplataforma. Esta exposição foi completamente eliminada pelo modelo de criptografia de hardware presente na solução Z. Sem necessidade de pareamento com handshake, não houve relatos de incursões bem-sucedidas no intervalo de tempo de 14 meses do estudo.

Considerando que o impacto dos roubos de outras chaves de criptografia totalizaram mais de $6.587.500 no período do estudo, esta proteção é outra vantagem substancial da solução de segurança pervasiva.

EVENTOS RECENTES

Durante o tempo do estudo da SIL, houve eventos significativos no mundo da segurança, que são pertinentes aos desafios tratados pela criptografia. Um vírus armado foi liberado e imitava um ataque de ransomware. Na realidade, era uma arma feita para destruir. O dano deste ataque deliberado era amplo e considerável.

Governos, hospitais, aeroportos e empresas eram o alvo a ser atacado e danificado. Os custos disso ainda estão sendo tabulados e provavelmente continuarão por muitos anos. O impacto líquido, no entanto, foi que esse tipo de ataque pode e vai acontecer novamente. O tipo de criptografia que esse novo avanço representa teria paraado se a capacidade de subverter o controle de arquivos foi um aspecto protegido da camada de criptografia e por isso não estaria vulnerável aos ataques de hacks.

Os trilhões de dólares em efeitos que teriam sido economizados e as pessoas fisicamente feridas e empresas impactadas negativamente estariam todos a salvo. Esta mudança fundamental no paradigma de segurança da indústria é algo profundo.

Neste momento, nenhuma outra arquitetura de chip consegue oferecer suporte ao modelo de criptografia pervasiva. Isso se deve às limitações técnicas em largura de banda e overhead. Será um desafio para aquelas arquiteturas se armarem e criarem essa capabilidade, mas é só disso que a indústria necessita.

EFEITOS LÍQUIDOS

O TCO da criptografia exigirá que as empresas olhem seus orçamentos de TI. Como muito do orçamento de TI é ponderado para o desenvolvimento de aplicações, em média 41,5-68,2% para as organizações do estudo, qualquer mudança que permita a redução disso tem um efeito imediato sobre a base de uma organização.

Mudando a criptografia como um aspecto de segurança de base para o centro de um ambiente de computação, o efeito líquido sobre o orçamento de TI seria uma redução de aproximadamente 22,1%.

> *"As implicações disso significam que o ciberataques poderiam ser interpretados como um ato de guerra, de acordo com a organização. Na quarta-feira, o secretário-geral da OTAN, Jens Stoltenberg, disse que um ciberataque pode acionar o Artigo 5º, o principal relacionado à defesa coletiva."*
>
> Luke Graham |@LukeWGraham, sexta-feira, 30 de junho de 2017 | 9:50 AM ET, Tech Transformers, Reportagem especial da CNBC

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.

