Executive REPORT
NEGÓCIOS & TIC – TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

SEUS DADOS ESTÃO SEGUROS NA NUVEM?

McAfee™
Together is power.
NetSafe
CORP
Human-machine
teaming.
Together is power.
© 2018 McAfee, LLC

04 CENÁRIO

Mesmo diante de um cenário desafiador e com tantos casos envolvendo vazamento de dados, quase 100% das empresas devem estar na Nuvem nos próximos anos. Por quê?

06 DESAFIO

Profissionais de Segurança enfrentam inúmeros obstáculos que podem expor informações sigilosas de usuários e levar empresas à uma crise reputacional irreversível

10 SOLUÇÃO

Apesar dos desafios, é possível estar preparado e desenvolver uma estratégia de Segurança a fim de controlar os riscos e mitigar os incidentes

EXECUTIVE REPORT - EXPEDIENTE

DIREÇÃO E EDIÇÃO EXECUTIVA
Graça Sermoud
gsermoud@conteudoeditorial.com.br

DIREÇÃO DE MARKETING
Sérgio Sermoud
ssermoud@conteúdoeditorial.com.br

DESIGN
Rafael Lisboa
rlisboa@conteudoeditorial.com.br

Leovitor dos Santos
lsantos@conteudoeditorial.com.br

EDITOR
Alexandre Finelli
afinelli@conteudoeditorial.com.br

REDAÇÃO / REVISÃO
Jackson Hoepers
jhoepers@conteudoeditorial.com.br

O Executive Report “CLOUD SECURITY” tem Patrocínio

McAfee Together is power.

NetSafe CORP

CLOUD SECURITY: SEUS DADOS ESTÃO SEGUROS NA NUVEM?

MESMO DIANTE DE UM CENÁRIO TÃO DESAFIADOR E COM TANTOS CASOS ENVOLVENDO VAZAMENTO DE DADOS, QUASE 100% DAS EMPRESAS DEVEM ESTAR NA NUVEM NOS PRÓXIMOS ANOS. POR QUÊ? QUAIS OS BENEFÍCIOS PARA OS NEGÓCIOS, OS PRINCIPAIS DESAFIOS DE SEGURANÇA E COMO TER A VISIBILIDADE NECESSÁRIA DO AMBIENTE PARA DEFINIR UMA ESTRATÉGIA DE PROTEÇÃO DE DADOS EFETIVA?

NUVEM DE
OPORTUNIDADES

Em 2010, o Cloud Computing ocupava o topo da lista de prioridades dos CIOs no Brasil, segundo um estudo global do Gartner. O levantamento, feito com mais de 1.500 decisores de TI em mais de 40 países, apontava que a Nuvem não seria apenas mais uma entre tantas outras tendências no mercado de TI, mas que viria para ficar. Segundo a mesma consultoria, espera-se que, até 2020, empresas que não utilizem computação em nuvem sejam tão raras quanto as que hoje não possuem internet.

Para se ter uma ideia, a contratação de infraestrutura, plataforma e Software como Serviço em Nuvem Pública atingirá US$ 1,7 bilhão no Brasil e praticamente o dobro até 2020, segundo previsões da IDC. A demanda está prevista também para o aumento da terceirização, que consumia 25% em 2013 e passou para 37%, em 2015. Esse número pode chegar a 44% em 2018.

As razões pela preferência da adoção em nuvem em vez do investimento num Data Center próprio são inúmeras. Há oito anos, por exemplo, o Brasil enfrentava um cenário econômico aquecido, exigindo do CIO uma postura que acompanhasse o crescimento esperado das empresas. Como a Nuvem surgiu para trazer mais flexibilidade e responder mais rapidamente às demandas de negócio, era compreensível imaginar porque ela se tornou a principal alternativa dos executivos de TI para proporcionar a transformação exigida pelo mercado.

Mesmo hoje em um cenário bastante diferente de oito anos atrás, considerando os atuais desafios político-econômicos, a Nuvem é facilmente associada ao seu custo-benefício, ou seja, baixo valor de investimento comparado aos inúmeros benefícios proporcionados por ela. Graças a esse fator é possível evoluir em escala, armazenando uma quantidade maior de dados sem a necessidade de investir em servidores locais.

A Nuvem também proporciona a acessibilidade e a agilidade que as organizações precisam nos dias de hoje. Em um mundo cada vez mais digital e conectado, é imprescindível que empresas ofereçam opções mais rápidas de acesso de dados aos usuários, independente de onde estejam e através de qual dispositivo, afinal, quanto mais rápido acessar os dados, mais rápida é a tomada de decisão.

Por essas razões, fica claro porque parte das soluções tecnológicas já é centrada em cloud. Prova disso é que até 2019 mais de 30% dos novos investimentos em Software feitos pelos principais fornecedores será em um modelo Cloud-only. A tendência é que cada vez mais os programas sejam customizados para as variações de Nuvens, seja ela Pública ou Privada.

Com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) entrando em vigor em maio de 2018, espera-se que as empresas invistam mais para estar em conformidade. Aqueles que confiam na capacidade de seus provedores de nuvem têm mais chances de intensificarem ainda mais os investimentos para o próximo ano, mas mesmo assim, os menos confiantes deverão manter os aportes no nível atual.

Tanto IaaS (Infrastructure as a Service) quanto PaaS (Platform as a Service) disponibilizadas em um modelo cloud-based oferecerão mais poder computacional que as tecnologias comercializadas separadamente em data centers corporativos, mostrando que o futuro da tecnologia está nas nuvens.

NUVEM DE AMEAÇAS

APESAR DOS BENEFÍCIOS, A NUVEM OFERECE INÚMEROS DESAFIOS DE SEGURANÇA QUE, SE NÃO CONTROLADOS, PODEM EXPOR INFORMAÇÕES SIGILOSAS DE USUÁRIOS E LEVAR EMPRESAS À UMA CRISE REPUTACIONAL IRREVERSÍVEL

Se por um lado a Nuvem oferece muitas vantagens, por outro ela permite que a segurança seja um fator preocupante. Segundo uma pesquisa recente da McAfee, intitulada "Navigating a Cloudy Sky", uma em cada quatro organizações que usam a cloud pública teve dados roubados. Considerando que 83% delas armazenam informações confidenciais nesse ambiente, é compreensível entender porque esse canal se tornou motivo de preocupação entre o board executivo e gestores de Tecnologia.

Primeiramente, é preciso esclarecer que existem dois pontos cruciais quando se fala em Segurança e Cloud. A Segurança da Nuvem e a Segurança na Nuvem, temas distintos que devem ser trabalhados de maneiras diferentes. A primeira diz respeito à confiança que você terá no seu provedor, nos controles e garantias de proteção oferecidas. A outra refere-se à estratégia da companhia para se proteger no ambiente de nuvem, independente da infraestrutura disponibilizada pelos fornecedores.

INIMIGO OCULTO

Um dos maiores desafios se tratando de Cloud Computing é a falta de visibilidade no ambiente. O fenômeno do uso indiscriminado de ferramentas e aplicações sem o consentimento da área de TI (a chamada Shadow IT) é apontado como uma das principais causas de vazamento de dados hoje nas organizações.

Estima-se que 97% dos profissionais de TI utilizam algum serviço na nuvem dentro das organizações, com o consentimento ou não. Entre eles estão os serviços de Armazenamento de Dados (Cloud Storage), Mídias sociais, Compartilhamento de Dados, Conversores PDF, etc. Dados confidenciais são trafegados e armazenados nestes serviços de nuvem, onde entre muitos deles é possível dizer que são uma porta aberta e convidativa para vazamento de dados.

A combinação entre os ambientes públicos e privados já correspondem a 59% do uso, sendo mais comum em empresas que têm mais de 5 mil funcionários. O problema é que a maioria das organizações armazena dados sigilosos na nuvem pública e a Shadow IT representa um risco real para as organizações.

Segundo o estudo da McAfee, 58% dos entrevistados disseram que a Shadow IT realmente prejudica a capacidade da empresa de manter os serviços na nuvem protegidos. Um terço deles enfrentou problemas com contas sendo criadas fora da visibilidade de TI, enquanto 35% deles assumiram que entre 20% e 40% do número total de serviços de nuvem pública da empresa é contratado sem o envolvimento direto do departamento de TI. Cerca de 56% dos profissionais entrevistados afirmaram que rastrearam uma infecção por malware vinda de um aplicativo em nuvem.

O crescimento do tráfego nas redes somado à enorme quantidade de dados disponibilizados na Nuvem congestiona as ferramentas de segurança e seu monitoramento, consequentemente. Um estudo do Instituto Vanson Bourne revelou que 72% dos entrevistados não têm uma infraestrutura escalável para fazer frente a essa demanda. Quase 50% deles relatam nem saber o que está criptografado na rede.

Honeywell

REDUZINDO RISCOS POR MEIO DE CONSCIENTIZAÇÃO DE USUÁRIOS

HONEYWELL

Empresa de manufatura com sede em Morris Plains (NJ), e faturamento anual em torno de US$ 39 bilhões.

DESAFIOS:

- Falta de visibilidade no uso e riscos da cloud causaram dificuldade na capacitação de modelo proativo de segurança;
- Empresa queria aprimorar a percepção da equipe de TI e se tornar "moderna e interessante";
- Serviços redundantes geraram custos desnecessários.

SOLUÇÕES:

- Só é possível proteger aquilo que se tem visibilidade. Aplicação da solução Skyhigh para Shadow IT, traz visibilidade para todos os serviços de cloud, avaliação de risco, detecção de ameaças e aplicação de políticas de segurança.

BENEFÍCIOS:

- Visibilidade aprimorada para habilitar proativamente serviços em nuvem de alto valor agregado;
- Redução de riscos para a organização através da conscientização dos usuários sobre serviços de alto risco;
- Serviços redundantes foram consolidados para reduzir custos entre departamentos;
- Criação de unidade de suporte para múltiplos negócios, para implementar tecnologia aos usuários, tornando-a "interessante" e um verdadeiro catalisador de negócios.
- A solução Skyhigh tem ajudado na transformação digital de muitas empresas, fazendo com que a transição para a nuvem tenha segurança igual ou superior a um perímetro interno controlado pelo cliente.
- A Skyhigh tem ajudado as empresas a cumprir as normas de GDPR.

DIRECTV

IMPLANTANDO CLOUD COM VELOCIDADE E SEGURANÇA

DIRECTV

Companhia de mídia e entretenimento com mais de 32 mil funcionários, sediada em El Segundo (CA) e faturamento anual de US$ 27,4 bilhões.

DESAFIOS:

- Processos ineficientes para compreender os riscos associados a cada serviço em cloud;
- Baixo desempenho e com processos manuais de correlação do uso de nuvem com os riscos;
- Falta de visibilidade no uso de serviços em cloud;
- Requerimentos de privacidade, segurança e compliance.

SOLUÇÕES:

- Skyhigh para Shadow IT;
- Skyhigh para Box.

BENEFÍCIOS:

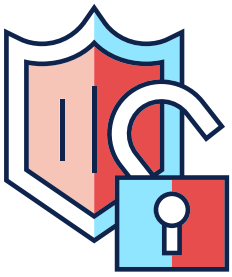
- Adoção acelerada de cloud com segurança de dados desde a implantação;
- Rápido entendimento da proteção e riscos de milhares de aplicações em nuvem;
- Melhor posicionamento da companhia para atender aos requerimentos de criptografia e prevenção à perda de dados;
- Reaproveitamento de horas perdidas semanalmente com análise manual de registros.

"SE NÃO HOUVER GOVERNANÇA DOS DADOS, **O CUSTO DE IR PARA A NUVEM** PODE SER ATÉ MAIS DISPENDIOSO"

VINICIUS FIEL, CISO DO GPA

Essa característica demonstra a dificuldade das corporações em obter a transparência necessária na rede para criar uma política de segurança realmente efetiva, afinal se a informação está na nuvem, é preciso acompanhá-la. Além de dificultar a elaboração de medidas e políticas preventivas, a ausência de visibilidade corrobora para o desafio da governança dos dados, ou seja, como essas informações estão sendo utilizadas, protegidas, classificadas, acessadas e rastreadas durante todo o seu ciclo de vida.

Segundo pesquisa da McAfee, a maior parte dos entrevistados guarda documentações internas, dados sobre cartões de pagamento, de colaboradores ou de identificação do governo. Cerca de 30% mantêm propriedade intelectual, registros de assistência médica, inteligência competitiva e cartões de acesso à rede na nuvem. Em 61% das companhias, por exemplo, tais informações são de cunho pessoal dos clientes.



FALHA NAS APLICAÇÕES

A não visibilidade do que se leva para a Nuvem acarreta em um outro desafio para a área de TI: as vulnerabilidades que muitas aplicações apresentam. Segundo a consultoria WhiteHat, mais de 50% dos aplicativos web utilizados hoje nas organizações têm falhas já descobertas há mais de um ano, mas devido ao desconhecimento dos gestores, não tiveram os patches aplicados.

Diversos estudos apontam que mais de 90% das aplicações web contêm algum tipo de vulnerabilidade de segurança e que cerca de 85% dos ciberataques bem-sucedidos exploram brechas conhecidas, mas não tratadas. O ransomware WannaCry, que fez 200 mil vítimas ao redor do mundo ano passado, é um claro exemplo, já que o malware explorou uma falha que já tinha correção.

Geralmente, as vulnerabilidades mais graves são as que mais demoram para serem corrigidas, já que demandam mais esforço para serem solucionadas. No entanto, quanto pior a visibilidade do ambiente, mais tempo os gestores levarão para implementar a proteção necessária às aplicações.

A falha em software é normalmente gerada por erros de projeto, implementação ou configuração. O problema é que quando um atacante descobre esse erro, acontece a violação da segurança. Normalmente, esses problemas ocorrem devido à necessidade das empresas em adotarem serviços e aplicações, mesmo sem as devidas revisões, para agilizarem seus processos de negócios e também pela falta de segurança no desenvolvimento da aplicação.

SECURITY (NOT) BY DESIGN

A agilidade proporcionada pelo ambiente em nuvem faz com que as áreas de negócios das companhias queiram lançar novos produtos e serviços de maneira cada vez mais rápida. Apesar desse comportamento ser um elemento saudável fundamental no processo de inovação de uma organização, a consumerização popularizou a tecnologia e permitiu que as áreas de TI e SI não sejam envolvidas no início dos projetos de desenvolvimento, somente posteriormente.

Hoje ninguém precisa ser especialista para contratar serviços em nuvem. O que era para ser um fator positivo se transformou em obstáculo, já que essa facilidade dificulta o trabalho das equipes de TI em visualizar todas as aplicações usadas no ambiente corporativo e controlar os riscos trazidos por elas. Essa atitude mostra o quanto o tema ainda desafia os profissionais de SI em se tornarem parceiros do board para serem vistos como habilitadores de negócios, e não criadores de obstáculos.

RESPONSABILIZAÇÃO DE INCIDENTES

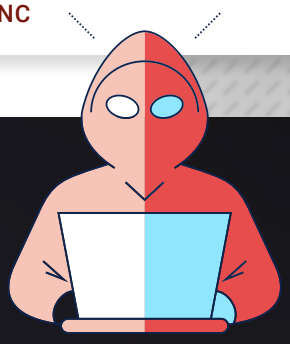
Muitas empresas deixam de investir numa estratégia na Nuvem, pois acreditam que a responsabilidade em caso de incidente é do provedor contratado, gerando uma falsa sensação de Segurança. Mas independente do contrato fixado, a responsabilidade recai sempre sobre a organização que permitiu a ida das informações para esse ambiente.

É claro que os provedores estão cada vez mais preparados para o atual cenário de ameaças. Os grandes players já provêm ambientes mais protegidos, contando com vários recursos de segurança. No entanto, é importante frisar que os provedores protegem o entorno e cabe às empresas investir numa estratégia de segurança complementar para evitar brechas e demais vulnerabilidades.

A estratégia de Segurança da Informação na Nuvem também deve ser gerida por um profissional qualificado e que tenha skills para atuar nesse ambiente tão complexo. Infelizmente, a escassez de alguns requisitos básicos também contribui para um canal mais vulnerável. Cerca de 40% das empresas diminuíram a adoção da nuvem devido a alguma falta de habilidade, em comparação com 49% no ano passado. As taxas de adesão na Nuvem são mais altas nas empresas que relatam mais escassez de qualificações.

HOJE NAS EMPRESAS VOCÊ ENCONTRA **A NUVEM OFICIAL** (TODA REGULADA), A NÃO OFICIAL (**QUE VOCÊ TOLERA**) E AQUELA QUE VOCÊ DESCONHECE (MAS SABE QUE EXISTE)

VITOR SENA, CISO DA EMS, GRUPO NC



CENÁRIO DE AMEAÇAS

- **83% DAS COMPANHIAS** armazenam dados sensíveis em nuvem pública
- **69% CONFIAM** na cloud pública para manter seus dados seguros
- **UM EM CADA QUATRO** já teve dados roubados em nuvem pública (encontrados tanto em SaaS quanto IaaS)
- **UMA A CADA CINCO** empresas sofreu ataques avançados contra a infraestrutura de nuvem pública
- **40% DOS LÍDERES DE TI** estão atrasando a adoção de cloud devido à falta de profissionais qualificados

FONTE: MCAFEE

NUVEM DE SOLUÇÕES

Ao se deparar com tamanhos desafios é compreensível se questionar se as empresas devem mesmo ir para a Nuvem. Mas como dito inicialmente, a migração tende a ser mandatória nos próximos anos devido às inúmeras vantagens proporcionadas por esse ambiente.

Com a transformação digital, o cloud deverá ser uma exigência e será difícil conter esse avanço. Assim sendo, é possível estar preparado e desenvolver uma estratégia de segurança a fim de controlar os riscos e mitigar incidentes, já que existem inúmeras opções de recursos para proteger o ambiente.

Ao implementar as medidas e os controles corretos, é possível ter plena visibilidade da rede e estabelecer as políticas necessárias, fazendo com que o negócio extraia todas as oportunidades que a nuvem tem a oferecer. Algumas soluções já nascem na Nuvem com essa proposta, como o Cloud Access Security Broker (CASB), que ajuda a transformar o ambiente em um canal mais transparente.

Por essa razão, a McAfee concluiu, no início deste ano, a aquisição da Skyhigh Networks, pioneira no segmento de CASB, trazendo um complemento estratégico para o portfólio da companhia. Com a compra, a organização terá à disposição um arsenal de ferramentas que prometem oferecer mais disponibilidade das redes, cargas de trabalho e dados, proteção avançada contra ameaças e segurança das informações.

As soluções da McAfee ajudam as organizações das seguintes maneiras:

PROVENDO VISIBILIDADE: por meio de recursos que ajudam as organizações a mapear onde seus principais recursos residem na nuvem, identificando informações confidenciais através de palavras-chave, padrões de dados, impressões digitais, metadados e tipos de arquivos, além de analisar o comportamento em todos os serviços de nuvem, usuários e dispositivos.

PREVENINDO CONTRA AMEAÇAS: quando as medidas de segurança são implementadas à proteção em camadas nas redes, cargas de trabalho e arquivos, de modo que os administradores possam adotar uma ação corretiva imediata e automatizada.

PROTEGENDO OS DADOS: através da identificação e controle de acesso a informações que já estão na nuvem, sendo movidas para ela ou originárias dela. Com isso, os gestores podem constantemente impor permissões de compartilhamento em aplicativos, gerenciar controles de acesso entre vários ambientes, restringir a capacidade de baixar dados confidenciais para dispositivos não gerenciados.

Recentemente, a McAfee anunciou ainda o lançamento da CASB Connect, estrutura de autoatendimento que permite a qualquer provedor de serviços em Nuvem, cliente ou parceiro criar conectores leves de APIs para o McAfee Skyhigh Security Cloud sem precisar escrever uma linha de código. Dessa forma, as empresas podem atribuir o mesmo conjunto de políticas de Segurança em todos os aplicativos na Nuvem.

"Migrar para a Nuvem pode trazer uma falsa sensação de Segurança, no entanto, ter visibilidade é essencial para gerar as melhores estratégias de proteção de dados. O CASB é muito conhecido por seus recursos de autenticação e trazer à tona a questão da Shadow IT, mas é interessante ver como a ferramenta ganha novas atribuições à medida que a Nuvem evolui. Visibilidade é essencial, pois o risco invisível é pior que o risco aceito", finaliza Bruno Zani, head de Cloud Security da McAfee.

"VISIBILIDADE É ESSENCIAL, POIS O RISCO INVISÍVEL É PIOR QUE O RISCO ACEITO", BRUNO ZANI, HEAD DE CLOUD SECURITY DA MCAFEE.

CASB, SEGUNDO O GARTNER

O Gartner relata um crescimento significativo do mercado de CASB, desde 2013. Foi previsto que, até 2020, cerca de 85% das empresas contarão com alguma solução, um grande crescimento comparado ao cerca de 5% que havia em 2015.

GARANTA SUA PRESENÇA NOS CONGRESSOS ORGANIZADOS PELA CONTEÚDO EDITORIAL:

TI Varejo
novas tecnologias, e-commerce, soluções e serviços

26 de junho — **São Paulo**

Com temas focados em Tecnologia aplicada ao Varejo, o evento reúne os principais executivos de comércio eletrônico e loja física para debater a transformação digital do setor.

SECURITY LEADERS

29 e 30 de agosto — **São Paulo**

O evento reúne C-Levels da comunidade de Segurança da Informação para discutir os rumos da proteção de dados, da prevenção e dos impactos dos ataques cibernéticos nas organizações em todo mundo

CLOUD & AI
CONGRESSO

08 de novembro — **São Paulo**

Este congresso vai reunir executivos de TI e Segurança de todas as verticais de negócio para debater como a convergência das tecnologias de cloud computing e inteligência artificial pode levar os negócios para altos níveis de inovação

SEJA UM PATROCINADOR: Sergio Sermoud - ssermoud@conteudoeditorial.com.br
FAÇA SUA INSCRIÇÃO: Renata Ramos - mramos@conteudoeditorial.com.br

McAfee™
Together is power.

NetSafe
CORP

Human-machine teaming. Together is power.