IDC ANALYZE THE FUTURE

IDC VENDOR SPOTLIGHT

A segurança cibernética nos ecossistemas Cloud e os desafios ao redor de mobilidade

Maio, 2018

Carlo Dávila

Patrocinado por: Kaspersky Lab.

As tendências na adoção de Cloud na América Latina criaram entornos de tecnologia da informação (TI) onde dados e cargas de trabalho, sejam elas on-premises ou em Cloud pública, privada ou híbrida, são acessados desde diversos equipamentos e dispositivos dentro e fora da organização, de forma que a segurança cibernética deve ser replanejada desde a nuvem e para a nuvem, e de acordo com o perfil de risco da empresa.

Neste documento descreveremos como a evolução de Cloud e seus diferentes ecossistemas (EPC, PCS, DHPC, ODHPC - ver parágrafo II, Definições) aumentaram a complexidade e a superfície de ataque nas áreas de TI das companhias da América Latina. De igual forma, analisaremos a adoção de mobilidade nas organizações da região e o estado atual de investimento para estes ambientes. Adicionalmente, revisaremos a oferta de soluções da Kaspersky Lab para enfrentar ameaças cada vez mais sofisticadas e automatizadas, sua relação com a evolução de Cloud e mobilidade e, finalmente, como se deve alterar o enfoque de investimento das organizações em relação à segurança cibernética.

I. INTRODUÇÃO

De acordo com o estudo *IDC FutureScape: Worldwide IT Industry 2018 Predictions, LA Implications*, em 2021 é esperado que o investimento em Cloud incluindo serviços, hardware e software alcance a cifra de 11 bilhões de dólares, impulsionando ambientes heterogéneos – 80% deles em ambientes multi-cloud, inclusive em diferentes provedores.

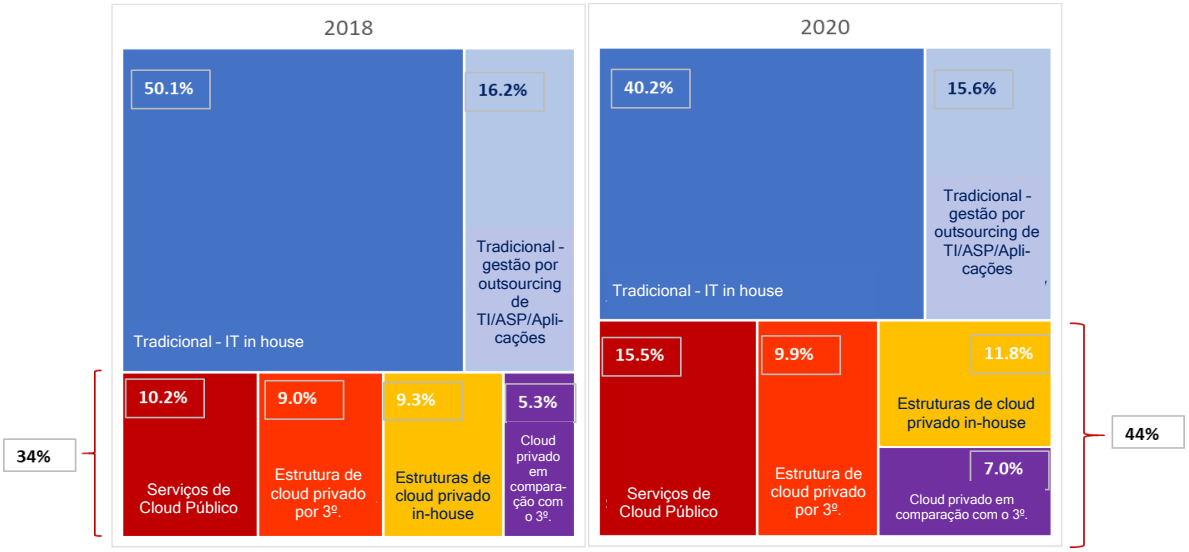
Como pode ser visto na Figura 1, o relatório da IDC *IT Investment Trends 2017Q4* indica que, em 2020, 44% da infraestrutura de TI nas empresas será gerenciada em Cloud.

Mais ainda, a infraestrutura (IaaS) e as aplicações (SaaS) em Cloud estão dentro das prioridades estratégicas em TI durante 2018 para mais de 23% das organizações da América Latina, com a finalidade de tornar mais eficiente o uso dos recursos e infraestrutura do negócio e agilizar o uso das aplicações. Paralelamente aos serviços em Cloud estão as iniciativas de mobilidade, as mesmas que agregam maior dinamismo à utilização de aplicações que foram já migradas para ambientes de nuvem com a finalidade de aumentar os níveis de eficiência do negócio. Estas iniciativas encontram-se dentro das prioridades para 31% das organizações na região, e representam um dos elementos que aumentaram o risco na segurança com a explosão de dispositivos e computadores como pontos de acesso, dentro e fora da organização.

IDC# LA18013

FIGURA 1

Ambientes multi-cloud na América Latina



Fonte: IDC Latin America IT Investment Trends 2017Q4

Embora a segurança cibernética seja a principal preocupação dos CISOs, visto que 45% das organizações da região a consideram como a principal iniciativa de investimento para 2018, a análise da definição de orçamento de TI para este conceito não está alinhada com o crescimento de Cloud e da mobilidade empresarial. Atualmente, as companhias destinam menos de 10% do orçamento total de TI para soluções de segurança, de acordo com o estudo *IDC Latin America Cybersecurity Report 2017*. O mesmo relatório indica que três em cada cinco organizações consideram que haverá uma redução de 15% do orçamento em segurança cibernética.

A IDC, frente a este panorama de crescimento de Cloud e mobilidade e à restrição em recursos de TI, considera que as estratégias de segurança cibernética devem contemplar a proteção a partir:

- Dos principais pontos de entrada de ataques potenciais - computadores e dispositivos móveis dos usuários
- Das cargas de trabalho em ambientes heterogêneos
- Do data center próprio de um provedor de serviços

Para isso, deve-se conhecer o perfil de risco corporativo e os modelos operacionais e de informação da companhia, apoiando-se em soluções e ferramentas avançadas e automatizadas, agregando também coberturas adicionais de serviços de segurança.

II. DEFINIÇÕES

As definições de ecossistemas de Cloud a seguir são pertinentes para o desenvolvimento deste documento:

- Ecossistemas de serviços de Cloud
  - Public Cloud Services ou PCS - Serviços de Cloud pública. São serviços sob demanda e consumidos em um modelo de assinatura que um provedor distribui através da Internet para uma empresa. Pode ser:

- Infrastructure as a Service, ou IaaS - Infraestrutura como serviço: servidores ou máquinas virtuais e armazenamento de um provedor, a quem se paga pelo uso dos serviços.
- Platform as a Service, ou PaaS - Plataforma como Serviço: um ambiente sob demanda para desenvolvimento, teste, administração e entrega de aplicações. Inclui bancos de dados e ferramentas de integração.
- Software as a Service, ou SaaS - Software como Serviço: oferece aplicações direcionadas tanto ao usuário como às organizações, tais como aplicações de negócios, ferramentas de colaboração e aplicações de segurança, entre outras.

- Cloud privada: São serviços fornecidos pela própria empresa ou um terceiro, seja para a operação central, seja para unidades de operação estendida, com maior restrição de acesso, maior nível de dedicação de recursos e contratos de longo prazo. A Cloud privada pode ser classificada como segue:
  - Enterprise Private Cloud Services (EPC) - Serviços de Cloud privada empresarial com recursos exclusivos para uma mesma companhia. A infraestrutura, os serviços e a administração são de propriedade e responsabilidade da empresa, e residem em suas instalações.
  - Dedicated Hosted Private Cloud Services (DHPC) - Serviços de Cloud privada alocados nas instalações de um prestador de serviços, cujo serviço está definido por meio de um contrato por um período definido de tempo. Este modelo é essencialmente uma versão em nuvem das ofertas tradicionais gerenciadas de Hosting.
  - On-Demand Hosted Private Cloud Services (ODHPC) -Serviços de Cloud privada hospedados nas instalações de um provedor de serviços que provisiona recursos de forma dinâmica para o uso dedicado de uma organização, a partir um grupo de recursos compartilhado.

- Cloud híbrida - Estrutura de TI empresarial que combina recursos de computação heterogêneos, infraestrutura de nuvem pública e privada (IaaS), middleware (PaaS) e recursos de bancos de dados / aplicações (SaaS), bem como ativos de TI não-físicos, em uma configuração automatizada de autosserviço com base no consumo e políticas de uso.

FIGURA 2

Taxonomia de Cloud

Fonte: IDC Taxonomy, 2015

- 3ª Plataforma e aceleradores de inovação - existem quatro pilares que formam a 3º Plataforma de tecnologia atual das empresas (mobilidade, Cloud, Social Business e Big data/Analytics) e são a base da transformação digital dos negócios. Os aceleradores de inovação são tecnologias disruptivas como segurança de próxima geração (Next Generation Security), realidade virtual, Internet das Coisas (IoT), sistemas cognitivos, robótica e impressão 3D. Figura 3

- Transformação Digital - inclui processos de transformação em cinco dimensões:
  - Liderança, para desenvolver uma visão para a transformação digital do negócio.
  - Omni-experiência, que permite atrair e aumentar a fidelidade do cliente.
  - Informações, para obter uma vantagem competitiva.
  - Modelo operacional, para tornar as operações comerciais mais eficientes e com resultados.
  - Força de trabalho, transformando a forma como o talento é acessado, conectado ou promovido em uma economia digitalizada.

FIGURA 3

3ª Plataforma, base da Transformação Digital

Mais sobre a 3a.Plataforma: http://www.idc.com/promo/thirdplatform

III. TENDÊNCIAS COM IMPACTO NA SEGURANÇA CIBERNÉTICA DO NEGÓCIO

No caminho para desenhar uma plataforma de segurança cibernética alinhada às estratégias de mobilidade e de implementação de Cloud, deve-se considerar os principais pontos de acesso, desde o escritório dos usuários até os dispositivos móveis, endpoints e smartphones, bem como também o perfil de risco em função da indústria onde a empresa se desenvolve.

A necessidade de proteger os principais pontos de acesso para os criminosos cibernéticos

Atualmente, de acordo com o *IDC Latin America Cybersecurity Report 2017*, Phishing, Malware & Malvertising e os ataques às credenciais são os ataques mais frequentes na América, chegando a ocorrerem de cinco a seis incidentes por ano, sendo de 76% a 84% de origem externa, afetando empresas de qualquer tamanho ou indústria. Soma-se o fato de que as ameaças se tornaram mais sofisticadas e com alguns processos automatizados que requerem menos ação do usuário infectado para propagação dentro de uma empresa. Isto acontece porque, na mesma medida em que as empresas estão sendo digitalizadas, os criminosos cibernéticos recorrem ao mercado negro para fazer

uso de ferramentas automatizadas e compartilhar informação privilegiada que lhes permitam a infiltração em ambientes da organização de forma mais rápida, através dos colaboradores que, de forma inadvertida, possam ter recebido qualquer tipo de mensagem eletrônica em seu computador do escritório ou dispositivo móvel (endpoints) com arquivos maliciosos. Uma ação tão simples como clicar em um arquivo ou link suspeito pode resultar na propagação de um vírus ou no sequestro da infraestrutura tecnológica e dados da empresa. Cabe destacar que 31% das organizações implementaram programas internos de comunicação sobre potenciais eventos de segurança, e 27% das companhias seguem um protocolo de comunicação restrito a níveis gerenciais. Este enfoque impacta negativamente na primeira linha de defesa de uma companhia: os colaboradores, visto que a América Latina não é uma região que se encontra investindo ativamente em serviços de segurança direcionados à conscientização dos riscos e dos ataques ao próprio negócio.

Os desafios da segurança em ambientes móveis

De acordo com o estudo *IDC IT Investment Trends*, publicado recentemente, hoje 43% dos colaboradores de empresas de médio porte na América Latina trabalham fora do escritório e se apoiam em dispositivos móveis para trabalhar. Dentre as empresas de médio e grande porte, 80% permitem que os colaboradores conectem-se a partir de dispositivos móveis (próprios ou financiados pela organização) a plataformas e aplicativos do negócio. Quando falamos de mobilidade, nos referimos a possibilidade de acesso à rede e aos serviços da infraestrutura tecnológica da empresa a partir de um laptop, tablet, smartphone ou celular, sejam eles de uso corporativo ou pessoal. Isso deixa claro o desafio de gerenciar o acesso e a segurança de diversos dispositivos que podem ser usados pelos colaboradores, parceiros de negócios e clientes, que também interagem com dados e informação da empresa. Derivado desta situação, a maioria daqueles que estão a cargo da segurança de TI (Chief Information Security Officer, CISOs) mostram sua preocupação ao manter a mobilidade entre as iniciativas de maior prioridade para as empresas. Adicionalmente, de acordo com o estudo *IDC Latin America Cybersecurity Report 2017*, 85% dos CISOs consideram que os laptops e desktops com sistemas operacionais Windows são os endpoints mais vulneráveis; seguidos dos smartphones (43%) e os tablets (23%) com sistema operacional Android. Embora estejam conscientes dos riscos em segurança da mobilidade, 55% das companhias na região não estão considerando investimentos específicos de segurança para ambientes móveis- Ver Figura 4.

FIGURA 4

Qual é o estado de investimento em segurança para ambientes móveis?

Fonte: IDC Latin America Cybersecurity Report 2017.

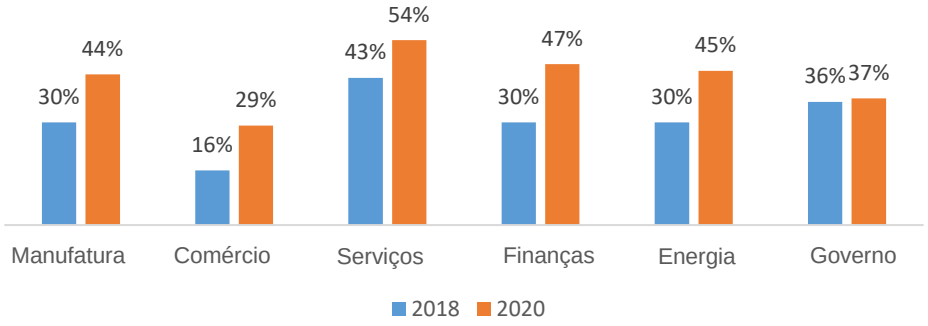
A adoção de Cloud e segurança cibernética nas indústrias da América Latina

Embora 2018 seja um ano de eleições ou mudanças na administração federal, persiste um ambiente de otimismo em investimento de TI na América Latina. Mais de 36% dos países da região consideram que o investimento será maior em 2020. Em particular, como se pode ver na Figura 5, as indústrias que mais investem atualmente em Cloud são Serviços e Governo. No entanto, com vistas para o futuro, os setores Financeiro, de Manufatura e de Energia são os que terão maior variação no investimento em Cloud em 2020, de até 17 pontos percentuais. As cifras apresentadas incluem ambientes multi-cloud:

- Serviços de Cloud pública
- Estruturas de Cloud privada administrada in-house
- Estruturas de Cloud privada gerenciada por um terceiro
- Serviços de Cloud privada compartilhados com terceiros

FIGURA 5

Orçamento de Cloud do Total Anual de TI por Indústria

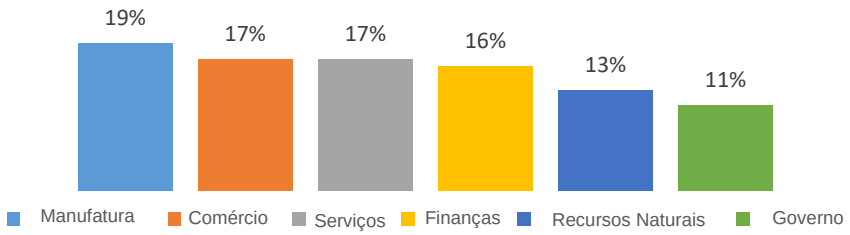


Fonte: IDC IT Investment Trends 2017Q4

Na perspectiva de segurança, novamente nos referimos ao estudo *IDC Latin America Cybersecurity Report 2017*: as empresas que atribuem um maior percentual do orçamento total de TI para a segurança cibernética são Manufatura (19%), Comércio (17%), Serviços (17%) e Finanças (16%) - Figura 6.

FIGURA 6

Qual o percentual do orçamento de TI é atribuído a soluções de segurança cibernética?



Fonte: IDC Latin America Cybersecurity Report 2017.

É importante destacar que o setor financeiro é o que mais investe em segurança de endpoints e em analítica de segurança (mais que o dobro que qualquer outro), sendo uma das indústrias com maiores requerimentos e regulações em termos de segurança. O contraste em investimento é o setor de Governo, com 11% de gastos em segurança sobre o total do orçamento de TI. Os ataques que mais preocupam este setor, assim como o Financeiro, são Phishing e Malware.

Para a Manufatura, os ataques mais frequentes são Phishing, Malware e Malvertising, e sequestro de dados (Ransonware), nesta ordem. Um dos desafios para esta indústria é a adoção de tecnologias disruptivas, como a Internet das Coisas, e, por outro lado, os riscos específicos da indústria como as ameaças aos sistemas SCADA.

Como se pode entender a partir dos parágrafos anteriores, cada indústria terá seu próprio ritmo de adoção de Cloud e mobilidade, bem como desafios diferentes sobre segurança empresarial. Portanto, deve-se implementar uma análise do ecossistema total de TI que permita definir uma estratégia de segurança cibernética de acordo com o perfil de risco da empresa e seus modelos de negócios.

IV. VANTAGENS DE UMA PLATAFORMA DE SEGURANÇA CIBERNÉTICA A PARTIR DA NUVEM E PARA A NUVEM

A tendência na América Latina de ambientes multi-cloud certamente torna imperativo criar uma estratégia que considere a utilização de uma plataforma de segurança cibernética integrada e gerenciada a partir da nuvem e para a nuvem. Nos referimos ao poder de gerenciar a segurança com uma visão 360 graus, apoiando-se na analítica de segurança, inteligência sobre ameaças, automatização de processos, sistemas cognitivos e de visibilidade da rede para proteger cada camada e modelo de Cloud (pública ou privada), o data center próprio e as cargas de trabalho hospedadas em um provedor de serviços, os dispositivos móveis, e os endpoints e smartphones.

Quando uma organização define em sua estratégia de segurança uma mudança nos modelos de investimento, afastando-se de produtos específicos e direcionando-se além do consumo de soluções de plataformas, esta consegue reduzir o impacto de certas preocupações do CISO em relação a:

- Infraestrutura fragmentada
- Orçamentos com perfis de CAPEX
- Necessidade de um importante número de profissionais em segurança cibernética
- Custos associados a capacitação e certificações

Uma companhia que, além de direcionar-se para plataformas de segurança cibernética, busca estabelecer um contrato em um modelo de serviços, pode encontrar vantagens adicionais relacionadas a:

- Orçamentos com perfis de OPEX
- Pagamento por uso
- Eliminação de custos associados a atualizações de plataforma
- Escalamento de capacidades
- Orquestração, consolidação e centralização da gestão de segurança
- Automatização de processos
- Redução de custos associados a instalação On-premises, energia e capacidade de processamento

V. OFERTA E DESAFIOS DA KASPERSKY LAB NA AMÉRICA LATINA

A Kaspersky Lab é uma companhia mundial de segurança cibernética com mais de 20 anos de trajetória no mercado. A Kaspersky Lab utiliza sua experiência em inteligência de ameaças e

segurança para desenvolver soluções de segurança e serviços para proteger empresas, infraestruturas críticas, governos e consumidores em todo o mundo.

O enfoque da Kaspersky Lab é o de detectar e neutralizar qualquer forma de malware, com base no conhecimento sobre ameaças em qualquer parte do mundo e em qualquer idioma, de forma que conta com uma equipe de investigadores em segurança localizados na Europa, Oriente Médio, Ásia, EUA e América Latina chamada GReAT (Global Research and Analysis Team). Recentemente e como parte de sua iniciativa de transparência global, a empresa anunciou para final de 2019 a abertura do seu primeiro centro de transparência, o Transparency Center, na cidade de Zurique – Suíça, para onde se realocará o armazenamento e o processamento de dados de seus clientes - em um a primeira fase, de Europa, América do Norte, Japão, Singapura, Austrália e Coreia do Sul. Adicionalmente, a Kaspersky Lab realocará nas mesmas instalações as ferramentas de programação para desenvolver software com base no seu código fonte, e iniciará a construção de bancos de dados de antivírus com assinatura digital na Suíça antes de sua distribuição para os endpoints dos clientes em nível mundial. A Kaspersky Lab fará com que estas iniciativas sejam supervisionadas por uma organização independente, sem fins lucrativos e com a qualificação necessária para realizar avaliações técnicas e auditorias de software.

Os clientes da Kaspersky Lab são diversos, desde usuários caseiros e microempresas até organizações de porte médio e grandes corporações, em praticamente qualquer indústria. Sua base instalada é de 400 milhões de usuários e 270.000 clientes corporativos.

A carteira de segurança da companhia é extensa, incluindo proteção de terminais e outras soluções de segurança, bem como serviços especializados para combater as ameaças digitais mais avançadas e em evolução. Em resposta às necessidades de segurança em endpoints e ambientes híbridos, a Kaspersky Lab disponibiliza seus consoles de gestão de segurança com base na nuvem:

- Proteção aos principais pontos de entrada
  - A Kaspersky Security for Microsoft Office 365 - console de segurança que, assim como o Microsoft Office 365, também reside na nuvem. Baseia-se em tecnologias avançadas como sistemas de detecção automatizada, sandboxing, informação sobre ameaças em tempo real e machine learning para previnir a entrada por e-mails (Exchange Online) de ransomware, arquivos maliciosos, spam, phishing, Business E-mail Compromise (BEC), entre outros, enquanto previne o bloqueio ou a eliminação de mensagens legítimas.

- Segurança para ambientes móveis
  - A Kaspersky Cloud Endpoint Security – proteção para endpoints em Windows, Linux, Mac e dispositivos móveis, sejam eles para uso pessoal ou do negócio, que acessam dados e informação da empresa que residem em aplicativos, folders compartilhados e servidores em plataformas on-premises ou Cloud, em conformidade com o Regulamento Geral de Proteção de Dados (GDPR) da União Europeia. A configuração da segurança acontece de forma centralizada a partir da nuvem por meio de um console de gestão online e de forma remota.

- Segurança para ambientes heterogêneos e multi-cloud
  - A Kaspersky Hybrid Cloud Security – solução de segurança integrada com Amazon Web Services e Microsoft Azure para Data centers definidos por software (Linux ou Windows), protegendo dados, redes, sistemas e cargas de trabalho em ambientes físicos, virtuais ou em Cloud por meio de técnicas de orquestração, higiene operacional e proteção de ataques cibernéticos por meio da análise de comportamento inteligente e algoritmos de aprendizado automático, baseados em machine learning e inteligência artificial.
  - Soluções verticalizadas para as indústrias com requerimentos regulatórios e de cumprimento em segurança cibernética bastante específicos como Finanças, Telecomunicações, Saúde, Governo e Manufatura.

- Segurança corporativa digital
  - Estratégia de continuidade do negócio, gestão de ameaças e defesa com base em tecnologias de segurança e serviços de segurança cibernética de acordo com o perfil de risco da organização, desde a identificação de ataques e investigação de incidentes, até a resposta e remediação a riscos em funcionalidade em cada camada da infraestrutura empresarial.
  - Programas de profissionais de conscientização de segurança corporativa, sandboxing como serviço, suporte padrão e premium, bem como serviços qualificados em segurança, partindo do projeto e implementação, atualizações, avaliação e configuração de soluções pelo perfil de risco, até a monitoria e avaliação da administração dos sistemas de segurança de forma remota ou *in loco*.

A Kaspersky Lab oferece suas soluções por meio de mais de 60 distribuidores certificados em 19 países da América Latina. A capacitação técnica e comercial para os seus parceiros de negócio é gratuita através do Portal de Parceiros, que inclui vídeos interativos, seminários web e exames online, o que lhes permite uma educação e atualização contínua.

Os Desafios na América Latina

A Kaspersky Lab, assim como outros fornecedores de soluções de segurança cibernética, enfrenta desafios na América Latina. Em primeiro lugar estão investimentos e recursos insuficientes das organizações para proteger os pontos de acesso mais visados pelos delinquentes cibernéticos que são os desktops ou dispositivos dos usuários finais da organização, constantemente expostos a ataques cada vez mais inteligentes e automatizados. Faz-se recessária a implementação de programas de conscientização sobre a segurança empresarial junto com a adoção de ferramentas mais automatizadas e inteligentes para a detecção oportuna de ameaças.

Em segundo lugar, as iniciativas de mobilidade criaram a necessidade de gerenciar e proteger localmente e em nuvem os numerosos endpoints a partir dos quais se tem acesso a dados e informação das empresas. Isto também detonou a necessidade de um staff de segurança especializado e constantemente atualizado sobre a evolução das ameaças cibernéticas. A realidade na região é que não é fácil encontrar especialistas em segurança com as certificações adequadas, capazes de administrar produtos múltiplos de segurança e inclusive de diferentes fabricantes.

Por último, temos as diferentes instâncias de Cloud, desde serviços públicos de cloud até estruturas de Cloud privadas administradas pela empresa ou por um provedor de serviços, além de ambientes híbridos; o resultado é um ambiente complexo e bastante heterogêneo. Os CISOs devem seguir administrando a segurança dos ambientes tradicionais de TI e, ao mesmo tempo, criar uma estratégia de segurança nativa de Cloud e de acordo com o perfil de risco da organização.

VI. CONCLUSÕES E RECOMENDAÇÕES

As perdas associadas aos ataques cibernéticos na América Latina chegam aos 90 bilhões de dólares, enquanto o investimento total de TI na região representa somente 45% deste montante, de acordo com um informe do Banco Interamericano de Desenvolvimento e da Organização dos Estados Americanos (2016). Isto nos dá uma dimensão dos desafios na América Latina, região onde o investimento, os recursos com foco em segurança, e as estratégias de prevenção e conscientização de riscos são ainda insuficientes frente ao aumento de projetos em nuvem e mobilidade.

A IDC considera que as empresas devem analisar a utilização de uma plataforma de soluções de segurança cibernética de acordo com o seu ecossistema de TI e perfil de risco, considerando as mudanças no modelo do negócio e sua infraestrutura física, virtual e na nuvem.

- Empreenda programas de conscientização sobre ameaças em segurança ao longo da organização e projete políticas de comunicação sobre incidentes de segurança cibernética.

- Analise as diferentes coberturas da infraestrutura de TI, as cargas de trabalho, redes e serviços, bem como também os diferentes pontos de acesso, tanto locais como em nuvem.
- Adote um modelo de segurança proativo e integral para a interpretação dos riscos, a determinação de ações oportunas e a implementação de um programa de resposta a incidentes, seja interno ou contratado como serviço.
- Apoie-se em ferramentas de segurança de próxima geração que podem ser nativas em Cloud e com base em analítica de segurança e inteligência sobre ameaças, complementadas com sistemas cognitivos e de visibilidade na rede que agilizem o trabalho do staff de TI e habilitem a resposta imediata, automatizada e inteligente frente a novas ameaças.
- Avalie custos de atualizações, certificados e capacitação do seu pessoal em soluções de segurança cibernética com recursos próprios da empresa e compare com os serviços contratados de provedores de soluções de segurança.
- Apoie-se em serviços de profissionais em segurança direcionado para executivos de negócio e para a área de TI, que lhes permitam construir casos de uso e justificação de soluções de segurança de acordo com os requerimentos e regulações da indústria em que a organização se desenvolve.

É também importante considerar que os ataques à segurança são cada vez mais sofisticados e inteligentes, de forma que é importante se apoiar em serviços de consultoria de especialistas em segurança cibernética para o projeto e a avaliação de uma estratégia de segurança adequada, para a constante monitoria e rastreamento de ameaças e de indicadores de risco, bem como para a auditoria da segurança corporativa que garanta a continuidade do negócio.

Sobre a IDC

A International Data Corporation (IDC) é a principal empresa de inteligência de mercado global, serviços de consultoria e eventos para os mercados de Tecnologia da Informação, Telecomunicações e Tecnologia de Consumo.

Com mais de 1.100 analistas em todo o mundo, a IDC fornece conhecimentos globais, regionais e locais sobre tendências e oportunidades em tecnologia e indústria em 110 países.

A análise e o conhecimento da IDC ajudam os profissionais de TI, executivos e a comunidade de investimentos a tomar decisões informadas sobre a tecnologia e atingir os principais objetivos comerciais.

Fundada em 1964, a IDC é uma subsidiária da IDG, a principal empresa de mídia de tecnologia, pesquisa e eventos.

Para saber mais sobre a IDC, visite www.idc.com e www.idclatin.com.

Siga-nos no Twitter: @IDCLatin / @IDC.

IDC Latinoamérica

4090 NW 97th Avenue Suite 350,
Doral, FL, USA 33178
+1-305-351-3020
Twitter: @IDCLatin
www.idclatin.com
www.idc.com