IDC EXECUTIVE BRIEF

Visibilidade de Rede: Um Componente Essencial na Estratégia de Segurança de TI para Empresas na América Latina

Novembro de 2017

Carlo Dávila, Marcelo Leiva

Patrocinado por: Arbor Networks, The Security Division of NETSCOUT

Um dos principais objetivos a serem estabelecidos por organizações da América Latina é reverter os efeitos deixados pela crise nos preços de commodities durante o ano de 2015, a partir do qual os orçamentos para inovação foram reduzidos. Isso aumentou a distância em relação ao gasto médio despendido por empresas globais em Tecnologia da Informação (TI) enquanto aceleradora de negócios.

Enfrentando uma nova realidade na qual o mundo dos negócios, os concorrentes e as demandas dos consumidores/cidadãos mudaram, essas empresas buscam vantagens competitivas que correspondem a um processo de transformação digital. No entanto, adotar estas tecnologias aceleradoras de inovação traz novos riscos, pois não se trata apenas de adotar uma tecnologia, mas também de reavaliar a segurança para suportar o crescimento e o desenvolvimento de novas ameaças, como os ataques DDoS (Distributed Denial of Service).

Neste documento, analisamos como estes desafios reforçam a necessidade de as empresas protegerem suas informações e sistemas por meio de soluções que visam fortalecer sua estratégia de segurança, como visualizadores de rede. Esses visualizadores permitem que as empresas tenham uma consciência mais detalhada do seu tráfego e determinem quais são os pontos de risco abertos pelos aceleradores de inovação, como a Internet das Coisas (IoT). Essa tarefa não pode ser adiada para amanhã, pois hoje os riscos são latentes.

I. OPINIÃO DA IDC

Em termos globais, a América Latina é uma região que enfrenta um forte desafio na adoção de tecnologia da informação (TI), uma vez que os gastos médios representam metade dos gastos que empresas do mundo inteiro alocam para esta questão. Como visto na Figura 1, que compara a adoção de TI como porcentagem do produto interno bruto (PIB), em 2016 as organizações no mundo inteiro (WW) investiram 1,72% do seu PIB em TI. Na América Latina, esta porcentagem foi de 0,84%, um índice afetado pela crise internacional impulsionada pelos preços mais baixos de *commodities* em 2015.

TABELA 1

Porcentagem de Adoção de TI em Relação ao PIB das Empresas na América Latina e no Mundo

Porcentagem de Adoção de TI em Relação ao PIB	2014	2015	2016	2017	2018	2019	2020
América Latina	0,95%	0,85%	0,84%	0,89%	0,93%	0,98%	1,02%
Mundo	1,80%	1,71%	1,72%	1,75%	1,79%	1,84%	1,87%

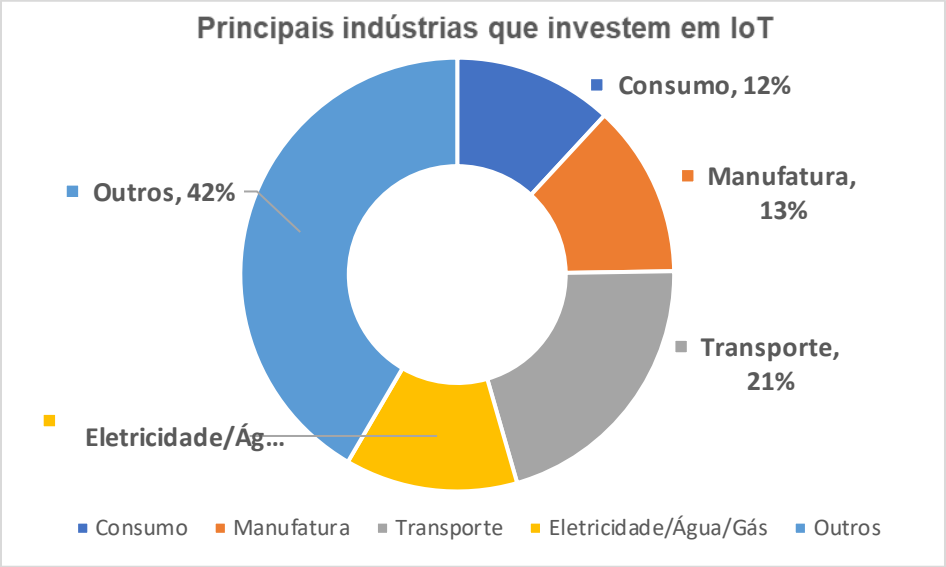
Fonte: IDC

A IDC acredita que, nos próximos cinco anos, as organizações da América Latina irão apressar o ritmo de adoção de aceleradores de inovação para se tornarem mais competitivas no contexto da economia global, com segurança de última geração, IoT e tecnologias cognitivas entre as principais estratégias para uma transformação digital que fomente a diferenciação e a concorrência.

Por exemplo, as indústrias de utilidades (energia elétrica, gás, água), manufatura e transporte concentrarão 47% dos investimentos totais em soluções de IoT na América Latina (Figura 1), com a integração de centenas de sensores para tornar processos operacionais mais eficientes. Este elemento é definido como um fator de impulso para a adoção de soluções de visibilidade de rede.

FIGURA 1

Principais Segmentos da Indústria Investindo em Projetos de IoT na América Latina



Fonte: IDC Worldwide Semiannual IoT Spending Guide, 2016

Para 2018, a IDC prevê que gastos em todo o mercado de IoT na América Latina crescerão cerca de 23%, gastos em módulos e sensores aumentarão em 24%, gastos em segurança de ecossistemas da IoT crescerão em 27% e gastos em software analítico para IoT aumentarão em 27%.

II. DESAFIOS DA INTERNET DAS COISAS

A adoção da IoT está mudando o ecossistema tecnológico, apresentando novas ameaças para dispositivos tanto de consumidores quanto de empresas. Estes dispositivos, em qualquer parte do mundo, representam uma ameaça devido ao seu preço baixo, falta de segurança e implementação rápida por qualquer pessoa, tornando-se um alvo do recrutamento de botnets para lançar ataques no mundo inteiro.

Alguns exemplos incluem projetos de monitoramento em vídeo, com centenas ou milhares de câmeras de IP em projetos Smart City ou sensores em um processo de fabricação. Cada sensor, câmera de IP, impressora, sistema de ar condicionado inteligente, smartphone ou outro dispositivo adicionado à rede significa uma nova plataforma de ataque potencial para cybercriminosos.

A IDC acredita que as organizações devem reduzir suas vulnerabilidades a cyberataques e à evolução destes eventos - que são cada vez mais frequentes, complexos e visados - ao considerar alterações em seu ecossistema de TI. Um exemplo disso é a negação de serviço (DoS), um ataque que evoluiu ao longo de duas décadas de gerações de soluções de segurança e que começou na metade dos anos 90.

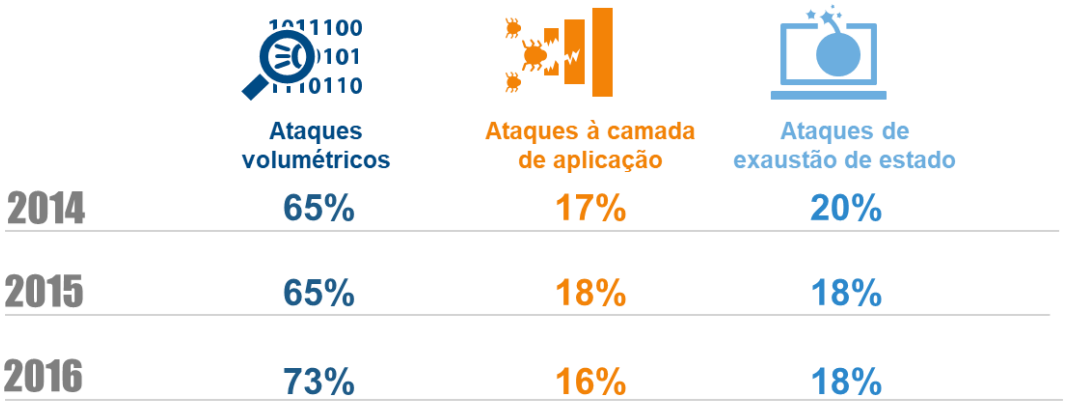
Atualmente, estes ataques são classificados como DDoS e alcançam um espectro mais amplo de pontos de acesso para tráfego maligno, afetando organizações de todos os tipos e tamanhos, e que dependem de uma estratégia de internet além do comércio eletrônico.

Conforme exposto na Figura 2, ataques DDoS violam a rede de comunicações de diferentes maneiras, portanto, as organizações devem prestar atenção nelas e seguir os procedimentos de prevenção e reação adequados:

- **Volumetria.** Inundam a camada de rede com um volume elevado de solicitações de tráfego falsas que parecem legítimas, aumentando os riscos em uma estratégia tradicional. O resultado é a saturação da rede.
- **Exaustão.** Atacam as conexões disponíveis com os dispositivos de infraestrutura, derrubando sua capacidade de processamento. Em outras palavras, os ataques consomem as conexões de rede da organização.
- **Camada de aplicativos.** Miram algum aspecto de um aplicativo ou serviço na camada 7 da rede. Estes são os ataques mais sofisticados e difíceis de encontrar, já que podem ser tão pequenos quanto um punhado de pacotes de rede.

FIGURA 2

Ataques de DDoS no Mundo Inteiro (Incluindo Sobreposição Multivetorial)



Fonte: Relatório de segurança de Infraestrutura Global da Arbor Networks, The Security Division of NETSCOUT, Relatório de Cybersegurança do Banco de Desenvolvimento Inter-Americano e da Organização dos Estados Americanos, 2016

Hackers usam esses tipos de ataques para obter reconhecimento global e benefícios econômicos. Eles exploram vulnerabilidades potenciais criadas nos processos de transformação digital adicionando uma grande quantidade de dispositivos e um uso mais intenso da infraestrutura. Isso exige a implementação de uma proteção adequada pela organização para reduzir os riscos de ataques.

Os países da América Latina são um campo de interesse para esses criminosos. A redução na adoção de TI – que inclui segurança – entre 2015 e 2016, está permitindo que ocorram cyberataques na região devido à crise econômica internacional. Em contraste, no resto do mundo investimentos em segurança de TI não foram reduzidos.

Ataques de DDoS encontraram vulnerabilidades em países da América Latina, sem uma relação proporcional com o tamanho do país. Em 2016, a Bolívia registrou 65.306 incidentes, enquanto a Colômbia e o Equador registraram 76.124 e 101.677 incidentes cada.

Para a IDC, é essencial que as organizações integrem a modificação dos seus ecossistemas atuais à necessidade de alterar suas políticas de rede quando da análise de cada inovação tecnológica como uma exigência para identificar vulnerabilidades potenciais, áreas de risco e impactos. O resultado deve permitir a integração de vantagens competitivas para o negócio de modo seguro, estabelecendo estratégias de mitigação e de ação contra ataques possíveis, com investimentos mais eficientes em soluções de segurança de acordo com as novas necessidades da organização.

III. CENÁRIO FUTURO

Recentemente, vivenciamos cyberataques globais que comprovaram a confiança excessiva em estratégias de segurança no mundo inteiro. A IDC acredita que estes eventos são mais frequentes e comuns do que se reconhece. Os ataques mantêm um crescimento mais acelerado, em termos de complexidade e quantidade, do que a adoção de segurança de TI.

Será necessário integrar novos elementos que reforcem a segurança da informação para impedir que as organizações sejam afetadas por qualquer ataque de DDoS e, na pior das hipóteses, que tenham suas conexões com a internet exauridas, deixando as organizações off-line e comprometendo cada processo vinculado à internet que elas possam ter. Aqui, as soluções de visibilidade de rede desempenham um papel muito importante ao adicionar elementos de contexto e análise, de modo que soluções de segurança implantadas tornem-se mais eficientes.

A nova geração de visualizadores inclui dispositivos, soluções e serviços e specializados que oferecerão mais visibilidade e granularidade naquilo que é visto na infraestrutura de tecnologia das organizações. Esses visualizadores oferecem uma compreensão melhor do tráfego de rede e permitem agir de modo mais eficiente contra um ataque, pois facilitam a identificação de padrões de comportamento, movendo um código potencialmente maligno para a quarentena ou para um espaço seguro em uma sandbox para posterior exploração, análise ou autorização.

Estes sistemas são diferentes daqueles incluídos em pacotes de segurança ou nos serviços oferecidos por prestadoras de serviços de telecomunicação, que têm capacidades mais limitadas ao compartilhar seus recursos com outros elementos da solução.

Devemos esclarecer que esses visualizadores não são ferramentas de segurança por si só. Seu maior valor está em fornecer uma análise detalhada de todas as informações que passam pela rede sem afetar seu desempenho. Isso torna as soluções de segurança mais eficientes como parte do ecossistema de TI em uma organização. Esses aplicativos ou serviços são avançados e reagirão aos desafios criados pela inovação tecnológica, com uma adoção mais rápida no mercado da América Latina.

A IDC prevê que os visualizadores de rede crescerão em 12% em 2017 como produtos a serem instalados nas organizações. Também é esperado que cresçam em 13% como serviços em 2017 em comparação com os índices de 2016.

No entanto, a penetração de visualizadores no mercado regional é limitada. Investimentos da América Latina em visualizadores representaram apenas 1,6% do investimento total em soluções anti-DDoS em 2016, de acordo com a pesquisa de mercado da IDC.

ORIENTAÇÕES ESSENCIAIS

Cyberataques são ameaças espalhadas pelo mundo inteiro que, independentemente do tamanho ou do setor das organizações, geraram perdas de ao menos US$ 90 bilhões na América Latina, de acordo com estudos de 2016 do Relatório de Cybersegurança, do Banco de Desenvolvimento Inter-Americano e a Organização dos Estados Americanos em 2016. O índice pode exceder todo o investimento em TI – hardware, software e serviços – na região, que equivale a US$ 49 bilhões, segundo a IDC.

Ao longo dos últimos anos, o investimento baixo em soluções de segurança na América Latina, comparado com os investimentos em outras regiões, deixou as organizações mais vulneráveis a ameaças avançadas. Adicionalmente, os desafios de inovação presentes na região podem aumentar tal vulnerabilidade.

A IDC recomenda que as organizações que adotam aceleradores de inovação avaliem a vulnerabilidade adicional em suas estratégias de segurança com o suporte de serviços de consultoria especializada para verificar se tais estratégias podem responder a ameaças, como ataques de DDoS, em suas redes. Elas também devem integrar soluções de segurança que correspondam ao seu perfil de risco e aos objetivos de negócios que as organizações esperam obter.

Este documento é um ponto de partida sólido que considera as mudanças nos ecossistemas de TI. Por exemplo, ao integrar projetos de IoT, implica-se que há centenas de milhares de pontos de violação vulneráveis que poderiam ser usados em um ataque DDoS. Portanto, a implementação de uma solução de visibilidade de rede é um componente essencial a ser considerado com funcionalidades mais capazes de observar e para proporcionar um contexto que auxilie a estratégia e as ferramentas de segurança a trabalhar adequadamente.

Sobre a IDC

A International Data Corporation (IDC) é a principal empresa de inteligência de mercado, serviços de consultoria e conferências no mundo inteiro para os mercados de Tecnologia da Informação, Telecomunicações e Tecnologia de Consumo. Há mais de 50 anos, a IDC ajudou profissionais de TI, executivos de negócios e a comunidade de investimentos a tomar decisões embasadas relativas à compra de tecnologia e à estratégia de negócios. Mais de 1.100 analistas fornecem conhecimento global, regional e local sobre oportunidades na indústria e tendências de tecnologia em mais de 110 países no mundo. A IDC é uma subsidiária da IDG, empresa líder em tecnologia, investigação e eventos.

IDC Latinoamérica

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