Brasil: Aumento no número de crimes digitais chama a atenção para a necessidade de segurança digital proativa

O Brasil é um dos lugares do mundo em que o crime digital está mais difundido. O país teve um crescimento de 274% no número de ataques, mesmo com leis e esforços oficiais para deter atividades on-line mal-intencionadas.[1] Uma onda recente de ataques de ransomware no Brasil, que afetou autoridades locais de pequeno porte e até mesmo um hospital, gerou a conscientização de que qualquer empresa ou usuário é alvo em potencial de crimes digitais.

No entanto, muitas empresas brasileiras só fortalecem suas defesas contra ameaças após uma violação de segurança substancial. E, agora, com a instabilidade política e a incerteza econômica, um grande número de empresas não está disposto a comprometer-se com novos investimentos. Diante desses desafios, elas devem:

- Ajudar a diretoria a entender por que a segurança digital deve ser uma grande prioridade.
- Considerar a adoção de estratégias, como a terceirização de serviços de segurança e o uso de defesas contra ameaças à segurança na nuvem, para superar restrições orçamentárias e fortalecer rapidamente a defesa contra ameaças.
- Investir de forma proativa em uma arquitetura de segurança que ajude a detectar e combater ameaças avançadas. Uma violação de segurança substancial não deve ser o impulso para melhorias.

Principais constatações

Neste artigo, os especialistas da Cisco analisam os recursos de segurança de TI das empresas no Brasil com dados do Estudo comparativo de recursos de segurança da Cisco de 2015.[2] Por exemplo, aprendemos que:

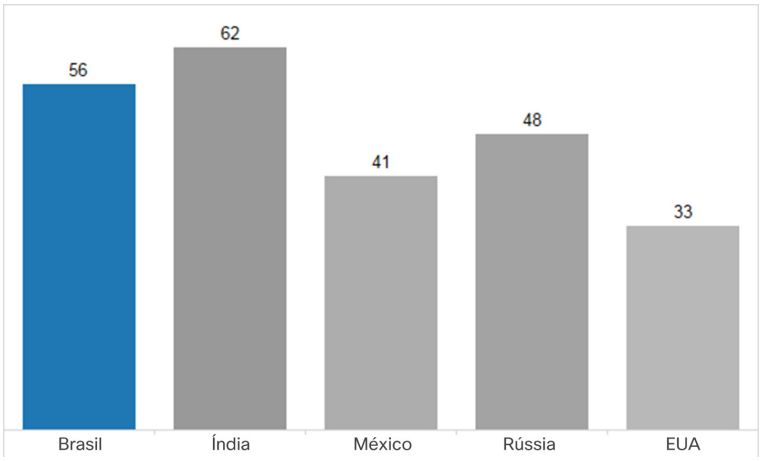
- A maioria das empresas brasileiras que já sofreu uma violação pública (63%) afirmou que a experiência levou a aprimoramentos significativos em seus procedimentos de segurança. As empresas brasileiras também tendem a enfrentar mais críticas da opinião pública após uma violação do que empresas em outros países, como os Estados Unidos.
- As empresas que sofreram violações públicas estão mais inclinadas a adotar defesas contra ameaças baseadas em nuvem do que aquelas que não passaram por uma situação semelhante. É provável que a pressão para melhorar a segurança digital após uma violação pública seja uma das razões para essa tendência. As soluções em nuvem podem ser implementadas rapidamente.
- Quase todas as empresas no Brasil (91%) terceirizam, até certo ponto, a segurança. Das que terceirizam, 69% relataram que o fazem por ser mais econômico.
- Para as empresas no Brasil, a falta de apoio da diretoria está entre as principais barreiras à adoção de processos e tecnologias de segurança avançada. De fato, este obstáculo parece ser mais significativo para o Brasil do que para todos os outros países estudados, inclusive os Estados Unidos.

As empresas brasileiras tendem a melhorar a segurança após uma violação

Embora o crime digital seja abundante no Brasil e esteja aparentemente se agravando, muitas empresas não se consideram possíveis alvos de ataques digitais. Como resultado, elas não tendem a ser proativas quanto ao desenvolvimento de uma estratégia abrangente de segurança digital. Obviamente, a realidade é que qualquer empresa de qualquer tamanho é um alvo em potencial para os criminosos. É provável que muitas empresas brasileiras já estejam comprometidas e não saibam.

Embora muitas empresas no país pareçam identificar o crime digital como um problema para outras empresas, e não para elas mesmas, mais da metade (56%) relatou ter sofrido uma violação pública em 2015 (veja a Figura 1).

Figura 1. Porcentagem de empresas que sofreram violações públicas (por país)



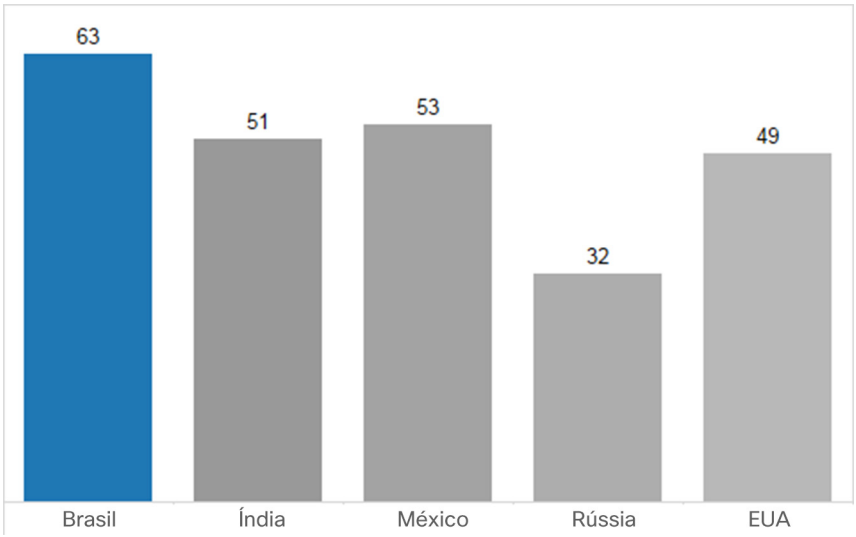
[1] *Crescimento de 274% em número de ataques cibernéticos no Brasil*, Revista Brasil, 22 de fevereiro de 2016: http://radios.ebc.com.br/revista-brasil/edicao/2016-02/pesquisa-revela-crescimento-de-274-em-numero-de-ataques-ciberneticos.

[2] Para obter mais informações sobre o estudo e sobre outros white papers desta série, consulte as páginas finais deste documento.

Além disso, ao que parece, as empresas brasileiras tendem a enfrentar mais críticas da opinião pública após uma violação de segurança do que empresas em outros países. Apenas um terço das empresas norte-americanas relataram ter precisado lidar com críticas da opinião pública após uma violação.

Para muitas empresas no Brasil, uma violação pública funciona como um catalisador para uma mudança positiva. Na verdade, 63% das empresas que já sofreram violações públicas no país declararam que a experiência levou a melhorias significativas em seus procedimentos de segurança. Aproximadamente metade dos entrevistados do México (53%), da Índia (51%) e dos Estados Unidos (49%) e apenas cerca de um terço dos entrevistados da Rússia (32%) afirmaram que uma violação de segurança pública teve um impacto positivo em suas práticas de segurança.

Figura 2. Influência de uma violação pública nos aprimoramentos da segurança (por país)



A adoção de uma solução de gerenciamento de eventos e informações de segurança (SIEM) está entre as melhorias adotadas por muitas empresas brasileiras após violações públicas. 43% das empresas que passaram por violações públicas adotaram o SIEM, em comparação aos 36% relativos às empresas que não sofreram violações públicas. Essa tendência sugere que as empresas que enfrentaram críticas da opinião pública após uma violação estão investindo mais em uma arquitetura de segurança abrangente do que aquelas que não passaram por esse problema.

Embora as restrições orçamentárias e a falta de adesão da diretoria quanto a investimentos em segurança digital sejam obstáculos às melhorias para muitas das empresas brasileiras (para saber mais sobre esses desafios, consulte as próximas duas seções), estas precisam considerar o efeito que uma violação de segurança pode gerar em seus negócios.

As empresas brasileiras que vivenciaram violações públicas também estão mais inclinadas a usar computação forense em endpoints do que aquelas que não tiveram que lidar com as consequências de uma violação. Na verdade, 30% das empresas que sofreram violações públicas no Brasil utilizam essas ferramentas, enquanto apenas 22% das empresas que não enfrentaram problemas com esse tipo de violação o fazem. Esse resultado sugere que uma violação pública pode levar a investimentos em ferramentas que auxiliam as empresas a detectar ameaças avançadas persistentes e investigar ataques digitais.

Além disso, como mostra a Figura 3, as empresas que sofreram violações públicas no Brasil parecem estar mais comprometidas com a melhoria proativa de suas políticas, processos e procedimentos de segurança do que empresas que ainda não lidaram com essa questão. Elas também estão mais inclinadas a usar dados quantitativos pra medir a efetividade dos processos de segurança.

Figura 3. Percentual de empresas brasileiras que concordam com diversas afirmações sobre políticas de segurança (por status de violação pública)

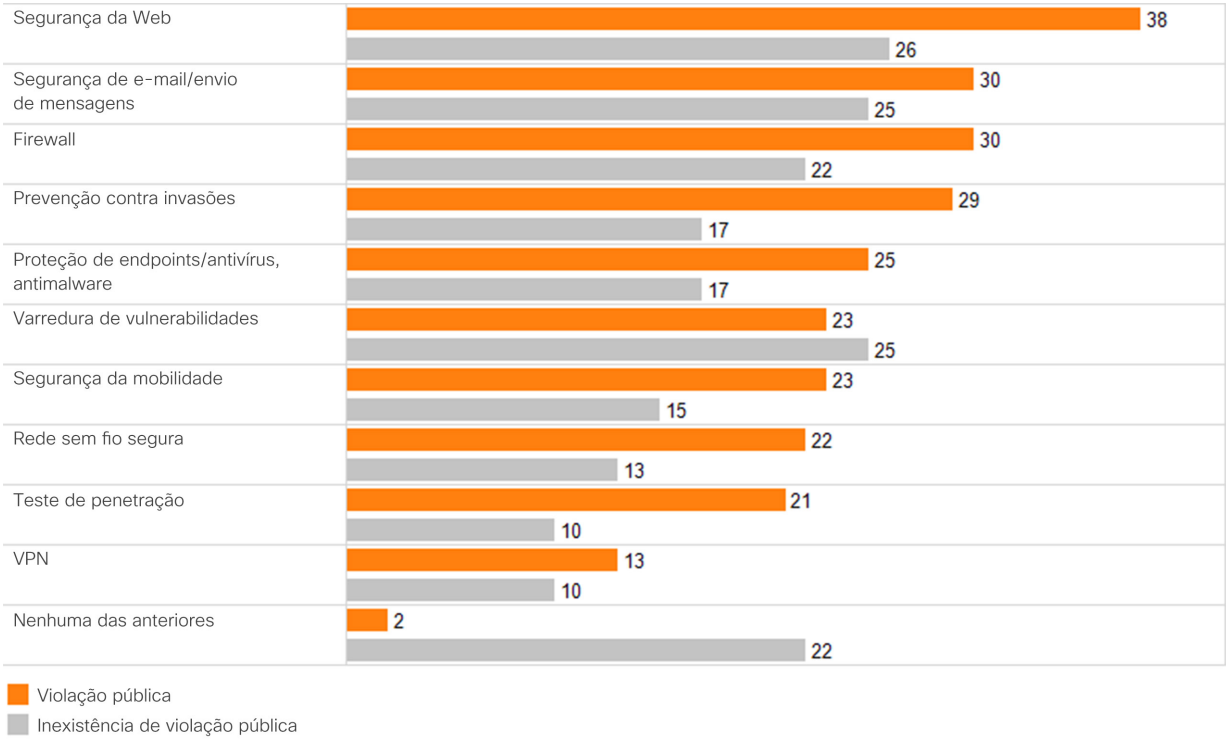
Empresas que passaram por violações públicas no Brasil buscam na terceirização e na nuvem a solução para melhorar a segurança

Como em todos os outros países avaliados, as empresas brasileiras mencionam restrições orçamentárias como o principal impeditivo para a adoção de processos e tecnologia de segurança avançada. Assim, quando as empresas que sofreram violações públicas estiveram sob pressão para fortalecer seus procedimentos de segurança, muitas buscaram estratégias econômicas como a terceirização dos serviços de segurança e o uso de defesas contra ameaças baseadas em nuvem.

Descobrimos, aliás, que a maioria das empresas no Brasil (91%) terceirizam, até certo ponto, a segurança. 69% dos entrevistados mencionou a economia como o principal motivo de sua opção pela terceirização. A capacidade de responder a incidentes com mais rapidez é outro fator importante, de acordo com 57% das empresas brasileiras pesquisadas.

As empresas no Brasil que já lidaram com uma violação pública também tendem a investir mais em segurança da Web e prevenção contra intrusões na nuvem do que as empresas que não passaram por esse problema. (Consulte a Figura 4). Apenas 2% das empresas que já sofreram violações públicas no Brasil relataram não usar algum tipo de defesa contra ameaças à segurança na nuvem.

Figura 4. Percentual das empresas no Brasil que usam defesas contra ameaças na nuvem (por status de violação pública)



Em particular para empresas de pequeno e médio porte com limitações de orçamento e recursos, a terceirização e as defesas contra ameaças baseadas em nuvem podem oferecer o caminho melhor e mais curto para aprimorar a segurança e desenvolver uma abordagem mais abrangente da segurança digital no longo prazo. Por exemplo, já que as empresas de pequeno e médio porte normalmente não têm sistemas de TI antigos complexos, elas podem migrar para a nuvem com rapidez. E como talvez elas não disponham de orçamento para contratar profissionais de segurança em tempo integral, a terceirização é uma maneira eficiente de obter acesso a especialistas.

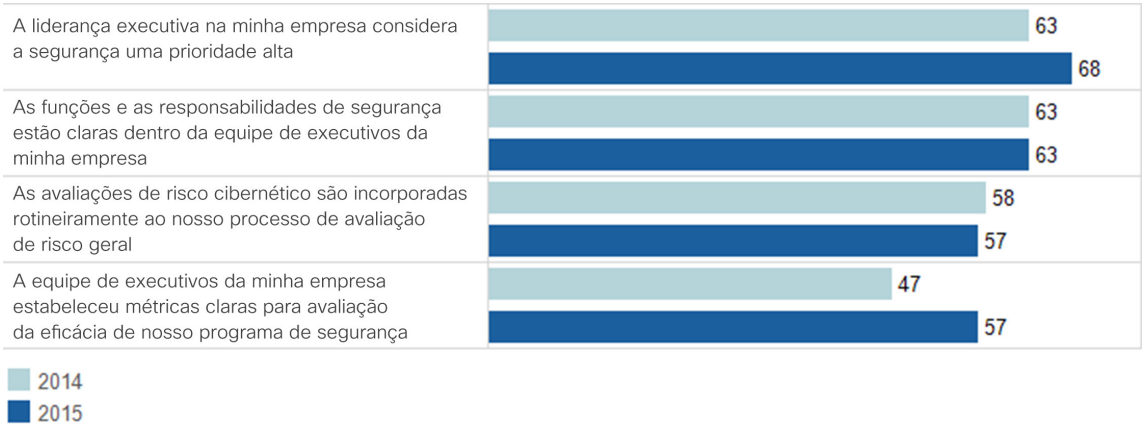
A falta de adesão da diretoria prova ser um obstáculo para o aprimoramento da segurança

A falta de apoio da diretoria é um empecilho maior para as empresas brasileiras que desejem adotar processos e tecnologia de segurança avançada do que para as empresas em outros países. 29% dos entrevistados no Brasil citaram a falta de adesão da diretoria como um desafio, em comparação a 24% dos entrevistados nos Estados Unidos e a 19% em todos os outros países.

Entretanto, as conclusões de 2014 e de 2015 mostram claros sinais de melhoria. Por exemplo, quase todas as empresas examinadas no Brasil (95%) para o estudo de 2015 revelaram que têm um executivo responsável pela segurança, sendo que esse percentual era de 89% em 2014.

Além disso, 68% das empresas no Brasil relataram que a liderança executiva dá prioridade alta à segurança digital. Isso representa um aumento de 5% em relação a 2014. (Veja a Figura 5).

Figura 5. Percentual de empresas no Brasil que concordam com afirmações sobre a liderança executiva (por ano)



Houve também um aumento de dez pontos percentuais nas empresas brasileiras confiantes de que sua equipe executiva estabeleceu métricas claras para avaliar a eficácia do programa de segurança desenvolvido: 57% em 2015 contra 47% em 2014.

É provável que o aumento da cobertura dos meios de comunicação sobre ataques digitais no país, como a recente onda de campanhas de ransomware, esteja ajudando a conscientizar os executivos em relação a essas ameaças. A pressão do legislativo também pode ser um fator a influenciar a mudança na percepção da segurança digital, que passa a ser vista como prioridade empresarial. Como exemplo, destaca-se a promulgação da lei do Marco Civil da Internet,[4] que rege o uso da Internet no Brasil e imputa responsabilidade às empresas pela perda de dados. Essa dinâmica pode motivar muitas empresas no país a investir em processos e tecnologia de segurança avançada e instituir uma abordagem mais abrangente relativa à segurança digital.

[4] Marco Civil da Internet (Lei nº 12.965/14), PublicKnowledge.org, maio de 2014: https://www.publicknowledge.org/assets/uploads/documents/APPROVED-MARCO-CIVIL-MAY-2014.pdf.

Conclusão: Agora é a hora de melhorar a segurança digital

Com a atenção internacional se voltando cada vez mais para o Brasil em vista dos grandes eventos no país, o crime, tanto on-line quanto off-line, será inevitavelmente parte desse destaque. Agora é a hora para que as empresas brasileiras mostrem claramente que levam a sério o combate a todo tipo de crime.

Os investidores internacionais querem ter certeza de que as empresas estão fazendo todo o possível para se defender contra o crime digital. Caso o contrário, eles podem, em última instância, desistir de investir no Brasil. Em um momento de instabilidade política e incerteza econômica, é importante reafirmar aos investidores que as empresas brasileiras estão comprometidas com uma estratégia de crescimento de longo prazo.

Para começar, as empresas no Brasil precisam reconhecer a extensão do problema e mudar sua abordagem da segurança. Elas devem:

- Adotar uma perspectiva mais proativa quanto ao fortalecimento das defesas Uma violação de segurança não deve ser a motivação para o aprimoramento. Essas melhorias precisam ocorrer independentemente do status de violação.
- Envolver a diretoria e criar uma cultura mais voltada para a segurança digital. Quando os executivos seniores entendem os desafios de segurança e a importância de resolvê-los, eles se tornam mais propensos a alocar um orçamento adequado para processos e tecnologia de segurança avançada
- Avaliar se a infraestrutura de segurança digital atual da empresa é integrada e está funcionando de forma eficiente. Dada a dinâmica atual no país, as empresas brasileiras talvez não possam fazer os investimentos em segurança pretendidos, mesmo com o apoio da diretoria. No curto prazo, as empresas podem pelo menos garantir que as tecnologias e os processos de que já dispõem estejam atendendo a toda a empresa com eficiência.
- Buscar maneiras alternativas de contornar os obstáculos, como restrições de orçamento e a falta de profissionais qualificados. A terceirização dos serviços de segurança e o uso de defesas contra ameaças na nuvem são exemplos de estratégias econômicas que podem ser implementadas com rapidez por muitas empresas. A terceirização pode ajudá-las a ter acesso aos especialistas de que precisam para tornar a segurança mais sofisticada, além de possibilitá-las atingir outros objetivos. Por exemplo, ela pode liberar mais tempo para que as empresas se concentrem nas atividades empresariais principais ou aprimorem o atendimento ao cliente.

Saiba mais

Para saber mais sobre o amplo portfólio avançado de produtos e soluções da Cisco para proteção contra ameaças avançadas, visite www.cisco.com/go/security.

Sobre o estudo comparativo de recursos de segurança da Cisco de 2015

O estudo comparativo de recursos de segurança da Cisco de 2015 examina os defensores em três dimensões: recursos, habilidades e sofisticação. O estudo inclui empresas de diversos setores, em 12 países. No total, foram entrevistados mais de 2400 profissionais de segurança, inclusive diretores executivos de segurança da informação (CISOs) e gerentes de operações de segurança (SecOps). Entrevistamos profissionais nos seguintes países: Austrália, Brasil, China, França, Alemanha, Índia, Itália, Japão, México, Rússia, Reino Unido e Estados Unidos. Os países que participaram foram selecionados por sua importância econômica e diversidade geográfica.

Para ler as descobertas do amplo Estudo comparativo de recursos de segurança da Cisco, acesse o Relatório de segurança anual da Cisco de 2016 em www.cisco.com/go/asr2016.

Sobre esta série

Uma equipe de especialistas em setores e países na Cisco analisou o Estudo comparativo de recursos de segurança da Cisco de 2015. Eles apresentam uma visão objetiva sobre o panorama da segurança em 10 países e quatro setores (serviços financeiros, serviços de saúde, telecomunicações e transporte). Os white papers desta série destacam o panorama e os desafios de segurança digital enfrentados pelas empresas. Esse processo ajudou a contextualizar as conclusões do estudo e colocou em perspectiva os tópicos relevantes de cada país e setor analisados.

Sobre a Cisco

A Cisco está desenvolvendo soluções de segurança verdadeiramente eficientes, integradas, automatizadas, em aberto e simples de usar. Com base em uma inigualável presença de rede, bem como de um talento e uma tecnologia mais extensos e diversificados do setor, a Cisco oferece melhor visibilidade e agilidade na resposta para detectar mais ameaças e corrigi-las rapidamente. Ao fazer uso da Cisco Security, as empresas estão prontas para usufruir de um novo mundo de oportunidades comerciais digitais com segurança.

Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.