Avanços em segurança cibernética e privacidade de dados

Março de 2017

Destaques

Em um mundo cada vez mais digital, os aplicativos estão se tornando a espinha dorsal para suportar operações, produtos e serviços das organizações. A transformação digital, associada à criação de valor e vantagens competitivas, está na agenda dos executivos empresariais. A segurança cibernética e a privacidade da informação devem ser parte integrante da estratégia de negócios digitais das organizações.

As empresas podem aproveitar a simplificação inerente à arquitetura tecnológica na adoção de soluções em nuvem para lançar produtos e serviços seguros e inovadores na nuvem.

A Internet das Coisas (IoT) cresce em todo o mundo e traz uma preocupação adicional em relação à segurança cibernética e à privacidade da informação. Temendo os riscos do uso de dispositivos de IoT, muitas organizações estão revendo suas políticas de governança de dados, reavaliando tecnologias, dispositivos e aplicações de IoTs e introduzindo o tema nos programas de conscientização sobre segurança cibernética para colaboradores. Os fabricantes estão preocupados em tratar dos riscos de segurança desde a concepção do dispositivo de IoT.

A Pesquisa Global de Segurança da Informação da PwC deste ano aborda como as organizações de todo o mundo estão lidando com a dinâmica e a complexidade dos desafios da cibersegurança e da privacidade.

A análise das respostas foi feita entre 4 de abril e 3 de junho de 2016. Participaram mais de 10 mil executivos de segurança de TI e áreas de negócio de 133 países.

A confiança virtual se tornou essencial para as plataformas digitais. O volume de dados criados, compartilhados e analisados de consumidores e empresas cresce exponencialmente. A privacidade de dados e a segurança digital tornaram-se requisitos fundamentais para estabelecer a confiança virtual e apoiar os negócios.

As organizações com visão de futuro estão caminhando para um novo modelo de segurança cibernética, que proporcione agilidade diante dos cenários de transformação digital, evolução com base em informações analíticas e adaptabilidade de acordo com o ambiente de riscos, ameaças e regulação.

No centro dessa nova abordagem, estão soluções como inteligência analítica de ameaças, monitoramento em tempo real, autenticação avançada e software de código aberto.

Embora nem todas essas tecnologias sejam novas, a forma inovadora como elas estão sendo distribuídas e gerenciadas chama a atenção. A tecnologia em nuvem e os serviços gerenciados de segurança são exemplos da inovação na prática.

Para proteger ativos digitais e criar vantagens de negócios, as organizações estão concentrando sua atuação em quatro áreas:

- Adoção de novas medidas de proteção para os modelos de negócios digitais na nuvem.
- Implementação de programas de inteligência analítica sobre ameaças e compartilhamento de informações com outras organizações para obter conhecimento e ser mais eficiente na detecção de ameaças, resposta a incidentes e mitigação de riscos cibernéticos.
- Atualização de políticas de governança e treinamento de pessoal para usar o potencial da Internet das Coisas com segurança.
- Adoção de uma abordagem proativa para gerenciar as ameaças geopolíticas.

pwc

Instantâneo

Dados da Pesquisa Global de Segurança da Informação 2017

59%

registram impacto nos gastos com segurança da digitação do ecossistema empresarial

62%

usam serviços gerenciados para cibersegurança e privacidade

51%

fazem uso de modelos analíticos de *Big Data* para modelar e identificar ameaças

49%

dos que usam software de código aberto apontam que houve melhora do programa de cibersegurança

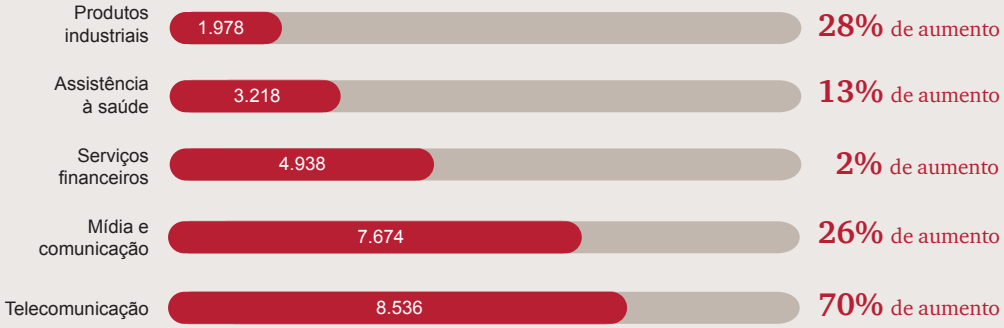
Orçamentos em cibersegurança permaneceram estáveis em 2016...

Valores em milhões de US$

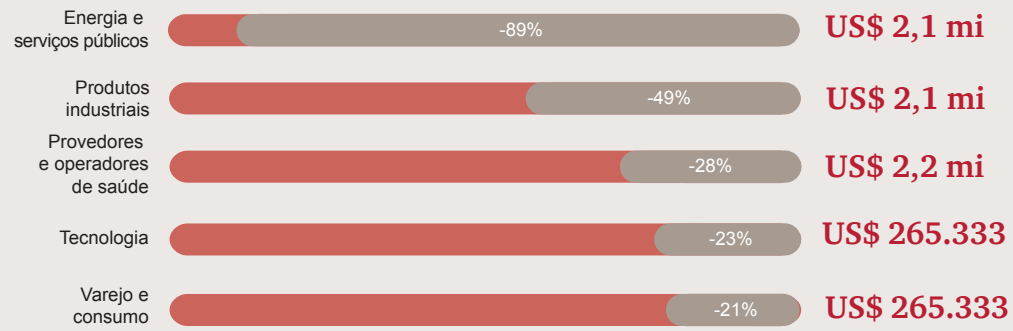
...mas cresceram nos setores de serviços financeiros, farmácia, saúde e automotivo.

11%

No último ano, os entrevistados globais detectaram menos incidentes de segurança. Mas algumas indústrias tiveram aumento de incidentes.



De 12 setores, 9 tiveram menos perdas financeiras causadas por incidentes de segurança. Cinco diminuíram as perdas em mais de 20%.



Diminuição média das perdas financeiras

Investimentos para fortalecer o ecossistema digital

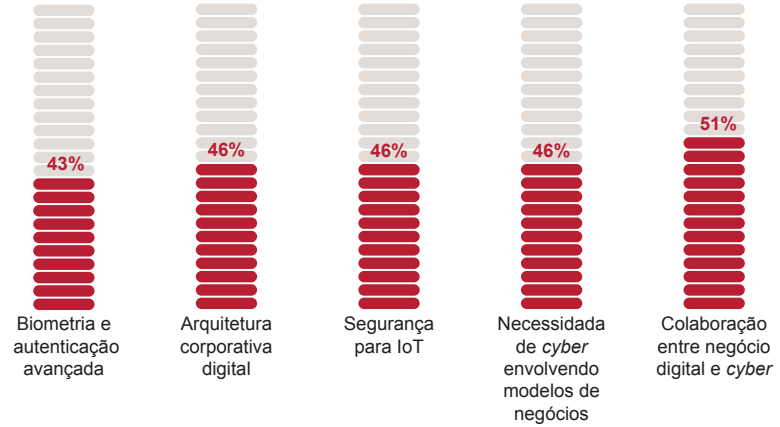
Segurança e confiança cibernéticas são pilares fundamentais na experiência digital. Por isso, as iniciativas digitais das organizações devem considerar, desde o seu início, os requerimentos e investimentos em *cyber* e privacidade. A pesquisa da PwC deste ano revela que as organizações estão priorizando investimentos para fortalecer o seu ecossistema digital. A troca de experiências e a colaboração mútua, o desenvolvimento de novas salvaguardas de segurança para modelos de negócios inovadores e a proteção da Internet das Coisas são exemplos dessa priorização de investimentos.

Com o aumento da confiança nos modelos na nuvem, mais e mais organizações passaram a ter funções críticas de negócios em nuvem. A fusão de tecnologias avançadas com arquiteturas em nuvem permitirá maior rapidez na identificação de ameaças e na resposta a elas, no entendimento dos clientes e do ecossistema de negócios e, em última instância, na redução de custos.

"Cresce o interesse das empresas em ter funções e processos críticos de negócios suportados por tecnologia em nuvem, como contabilidade, finanças, operações e recursos humanos", diz Edgar D'Andrea, sócio da PwC Brasil. "Esse interesse continuará a crescer à medida que os benefícios esperados sejam atingidos e divulgados de forma clara."

Prioridade de investimento em segurança cibernética para os próximos 12 meses

Global



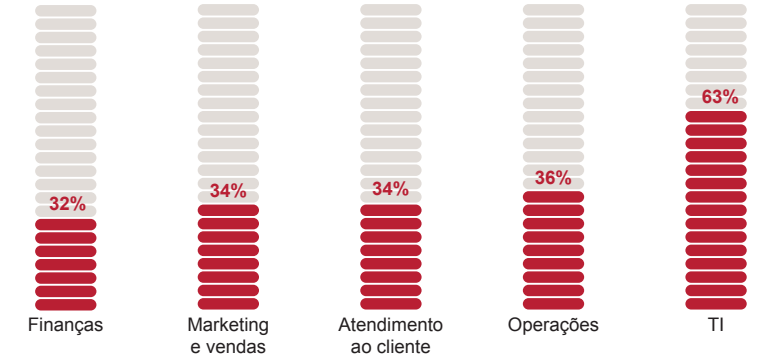
Brasil

60%

indicam investimentos para integração dos negócios *cyber* e digital

Funções de negócio suportadas por tecnologia em nuvem

Global



Brasil

40%

indicam utilização de **funções financeiras** de negócios em nuvem

Como gerenciar a segurança cibernética e a privacidade de dados

Quase dois terços (62%) dos participantes da pesquisa usam fornecedores de serviços de segurança para operar e melhorar seus programas de cibersegurança. Um dos principais motivos para isso é a escassez global de especialistas qualificados em segurança cibernética. Um outro motivo é o custo.

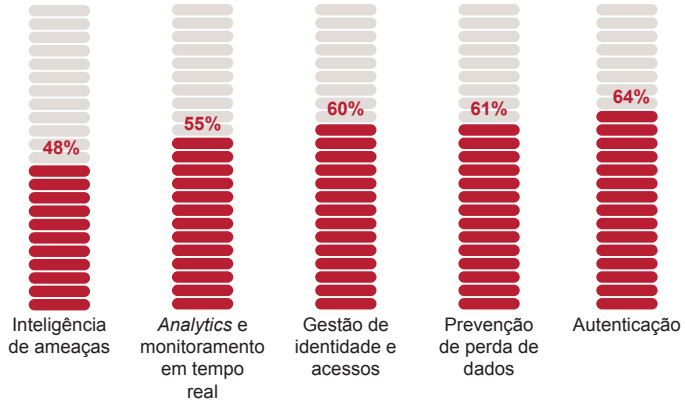
Outra afirmação relevante dos respondentes da pesquisa é que muitos dependem de serviços gerenciados de segurança para atividades operacionais como gestão de acesso e identidades, autenticação de usuários e prevenção de vazamento de dados.

"Os avanços tecnológicos têm sido disruptivos, dificultando que empresas tenham as competências necessárias nas novas tecnologias, como a Internet das Coisas e a computação em nuvem", diz Eduardo Batista, sócio de Cibersegurança e Privacidade da PwC Brasil.

No mundo, tem havido uma explosão no uso da Internet das Coisas (IoT). Os ataques cibernéticos recentes envolvendo IoTs no mundo ampliou o estado de alerta do mercado em relação a riscos, segurança e privacidade desses dispositivos. No Brasil, 57% afirmam que estão investindo no estabelecimento de novas salvaguardas, em adequar padrões e políticas para segurança cibernética de IoTs e em programas de conscientização de segurança e privacidade para executivos.

Serviços gerenciados de segurança utilizados na organização

Global



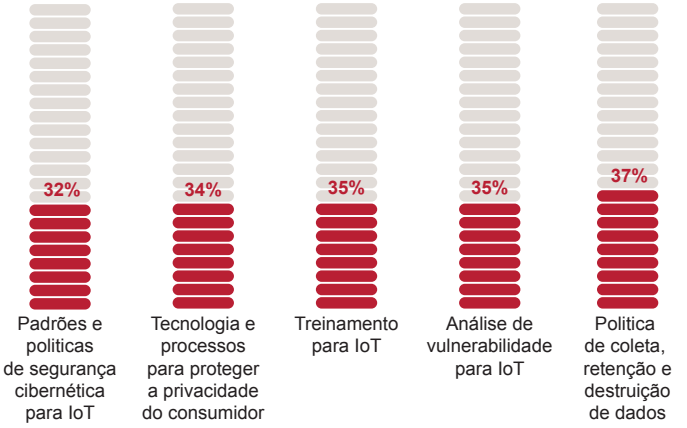
Brasil

78%

utilizam serviços gerenciados de **proteção de dados**

Políticas, processos, tecnologias e competências que a organização planeja implementar nos próximos 12 meses para abordar os riscos associados à Internet das Coisas

Global



Brasil

57%

estão investindo em padrões e políticas para segurança cibernética em **IoT**

Como preservar a privacidade dos dados

Em todo o mundo, cresce o rigor dos reguladores e das agências de proteção ao consumidor em relação à privacidade de dados. Na União Europeia, por exemplo, a GDPR (General Data Protection Regulation) eleva o nível de atenção e atendimento legal das organizações com relação à privacidade de dados. Nesse contexto, as prioridades relativas à privacidade nos próximos 12 meses passam por estabelecer programas de treinamento e sensibilização, bem como por reavaliar políticas e procedimentos diante das novas exigências.

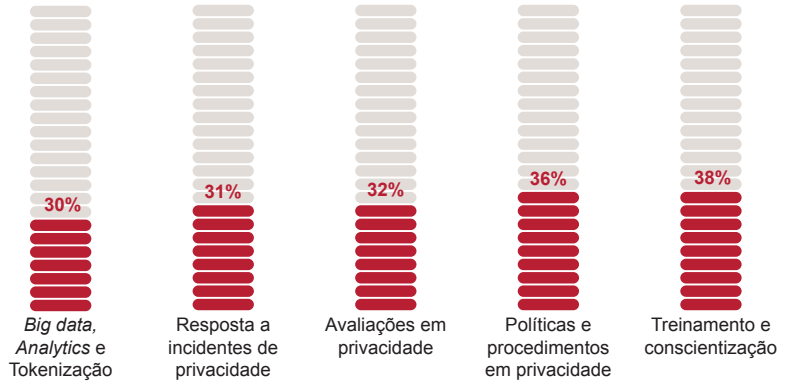
"Os programas de treinamento e sensibilização a respeito de privacidade devem ser orientados pelo tom da liderança a esse respeito, dado o caráter de dependência que o tema impõe ao futuro digital da empresa", diz D'Andrea. "A privacidade da informação deve estar no radar das organizações locais e internacionais."

No Brasil, para salvaguardar a privacidade dos dados, 58% dos participantes disseram contar com treinamentos e programas de sensibilização sobre privacidade como soluções preventivas.

As novas regulamentações de privacidade de dados e regras de uso da Internet criam obstáculos operacionais e, por isso, muitos executivos estão preocupados com essa questão. Os líderes empresariais citaram que o excesso de regulamentação seria a principal ameaça ao crescimento dos negócios este ano.

Prioridade em relação à privacidade de dados

Global



Brasil

58%

indicam elaboração de treinamento e sensibilização para privacidade de dados

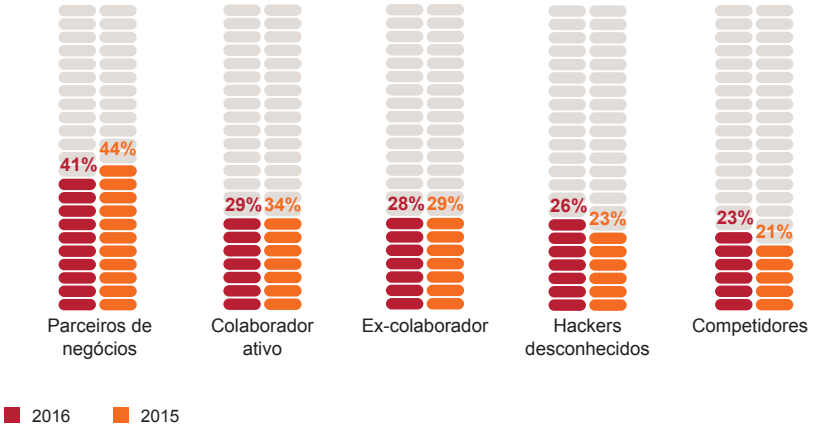
Incidentes: origem e impactos

Os incidentes de segurança atribuídos a pessoas dentro da empresa, isto é, colaboradores ativos, diminuíram, enquanto os atribuídos a pessoas de fora aumentaram. Como na pesquisa anterior, os parceiros de negócios foram apontados como os maiores causadores de incidentes de segurança, com 41% neste ano. No Brasil, 54% relacionaram a origem dos incidentes a parceiros de negócios. No mundo, o comprometimento do e-mail corporativo está entre os impactos mais citados para o negócio. No Brasil, 21% citaram a engenharia social como sendo a principal forma de ataque.

Mais de metade (51%) dos participantes da pesquisa global revelam fazer uso da análise de *Big Data* para modelagem da inteligência analítica sobre ameaças de cibersegurança e prevenção a incidentes. Mas o *Big Data* requer capacidade de processamento e armazenamento, além de cientistas de dados experientes para modelar aplicações analíticas e codificar algoritmos sofisticados. A escassez de profissionais de cibersegurança e as restrições orçamentárias podem acabar reduzindo a capacidade de implementar soluções sofisticadas de *Big Data*. Essa é outra razão pela qual estamos vendo mais e mais organizações adotarem soluções analíticas baseadas em serviços na nuvem.

Provável origem dos incidentes de segurança ocorridos nos últimos 12 meses

Global



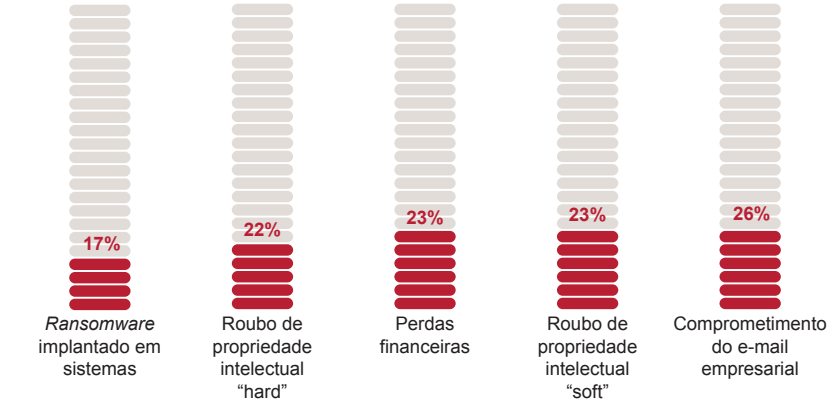
Brasil

54%

dos incidentes são atribuidos a parceiros de negócios

Impactos causados por incidentes de segurança

Global



Brasil

21%

citaram a **engenharia social** como vetor de ataque

Para obter mais informações, entre em contato:

Edgar D'Andrea
Sócio
edgar.dandrea@pwc.com
(11) 3674 3826

Eduardo Batista
Sócio
eduardo.batista@pwc.com
(11) 3674 2583

Rafael Cortes
Gerente
cortes.rafael@pwc.com
(11) 3674 3830

Erik Oliveira
Gerente sênior
erik.oliveira@pwc.com
(11) 3674 3948

Maressa Juricic
Gerente
maressa.juricic@pwc.com
(11) 3674 3930

Lucas Souza
Gerente
lucas.souza@pwc.com
(11) 3674 2822

Magnus Santos
Gerente
magnus.santos@pwc.com
(11) 3674 2921

Phillipe Romão
Gerente
phillipe.romao@pwc.com
(11) 3674 6454

Vinícius Ogawa
Gerente
vinicius.ogawa@pwc.com
(11) 3674 3890

Fernando Mitre
Gerente sênior
fernando.mitre@pwc.com
(11) 3674 3754

Compartilhe conosco o que você acha da série 10Minutos e quais temas gostaria de conhecer melhor. Acesse:
www.pwc.com.br/10minutosopiniao

PwC Brasil @PwCBrasil @PwCBrasil PwC Brasil PwC Brasil PwC Brasil

© 2017 PricewaterhouseCoopers Brasil Ltda. Todos os direitos reservados. Neste documento, "PwC" refere-se à PricewaterhouseCoopers Brasil Ltda., firma membro do network da PricewaterhouseCoopers, ou conforme o contexto sugerir, ao próprio network.Cada firma membro da rede PwC constitui uma pessoa jurídica separada e independente. Para mais detalhes acerca do network PwC, acesse: www.pwc.com/structure

DC0 - Informação Pública