

# Os dados de seus usuários estão seguros?

QUARTA-FEIRA, 15 DE JUNHO DE 2016

0  
SHARES

Facebook

Twitter

Google+

LinkedIn

**SEGURANÇA** — Em uma era em que ser um cibercriminoso é encarado praticamente como uma profissão, a segurança dos dados do usuário estão em constante ameaça. É justamente por este motivo que empresas que coletam informações no mundo online precisam estar protegidas, garantindo a confiança de seus clientes e a credibilidade dos negócios.

Um recente estudo da Trend Micro, chamado Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015, revelou que com R\$ 300 é possível realizar um curso para se tornar um criminoso na web. Entre outras descobertas chocantes, já é possível adquirir softwares e credenciais de cartões de crédito para a prática ilegal, tudo isso com suporte integral de um especialista, oferecidos abertamente nas redes sociais.

De acordo com a consultoria PWC, em sua pesquisa The Global State of Information Security Survey 2014, os incidentes podem acontecer tanto com o envolvimento de inimigos externos, como hackers, que representam 32% desse tipo de ataque, quanto com funcionários (31%) e ex-funcionários (27%). O material revela ainda, que as despesas e a falta de compreensão sobre a importância da segurança das informações são, cada uma, os maiores obstáculos para realizar melhorias.

## A fragilidade dos dados na internet

Mesmo com investimentos crescentes na área, é cada vez mais comum se deparar com casos que expõem a fragilidade das empresas que atuam com dados de usuários em todo o mundo.

Nos Estados Unidos, mais de 20 milhões de usuários tiveram dados como histórico escolar, endereços residenciais e antecedentes criminais roubados. As informações administrativas privilegiadas eram exclusivas do Escritório de Administração Pessoal dos Estados Unidos (OPM), que sofreu um ataque que causou a exposição. Os dados estão, agora, nas mãos de hackers que vêm se mostrando cada vez mais mal intencionados.

Outro caso que ficou famoso, dessa vez no Canadá, foi o do site de infidelidade Ashley Madison. Depois de ser atingido por violações de hackers, 33 milhões de contas de usuários foram publicadas na rede mundial. O

vazamento trouxe consequências trágicas para famílias de diversas nacionalidades e ainda causou o afastamento do presidente-executivo da companhia, que agora tem a reputação manchada e enfrenta inúmeros processos judiciais.

Os usuários brasileiros também não estão livres deste inimigo. Neste ano, por aqui, o Ministério Público Federal do Espírito Santo precisou investigar como instituições bancárias e financeiras conseguiram informações sobre trabalhadores com pedido de aposentadoria. O caso veio à tona após as vítimas receberem ligações que ofereciam crédito consignado em nome de alguns bancos antes mesmo de terem as solicitações atendidas pelo governo.

Em maior ou menor escala, a segurança dos dados dos usuários não está sendo tratada com o devido respeito. Muitas empresas ainda não possuem sequer programas para prevenir ameaças, muito menos para identificar vulnerabilidades ou detectar possíveis brechas que facilitam também outros crimes, como falsa identidade, calúnia, injúria e pedofilia.

Proteção para o usuário e confiança para o negócio

Fundamental para os negócios, a garantia de um ambiente seguro para inserir informações pessoais e bancárias precisa ser planejada, principalmente para as pequenas e médias empresas, que enxergam no TI uma forma cara de gastar dinheiro, sem saber que 61% dos ataques miram nelas.

As formas de proteção vão além das ferramentas convencionais, pois precisam acompanhar a evolução e a sofisticação dos novos ataques cibernéticos. Por isso, a segurança da informação deve ser pensada de forma inovadora, e contar com os serviços de uma empresa especializada em soluções para cada negócio.

De forma ampla, recomenda-se, hoje em dia, uma série de cuidados, que vão desde boas práticas de uso da rede até a criptografia dos dados. Conheça algumas soluções que as empresas podem adotar para seus usuários com o auxílio profissional:

Boas práticas

As senhas são a primeira defesa de cada usuário. Exigir um sistema de senha longo e de difícil associação (maiúsculas, minúsculas, números e símbolos) e a troca periódica é uma opção para proteger o usuário. Também o incentive a atualizar os aplicativos móveis, já que cada nova versão costuma contar com proteção contra novas estratégias criminosas.

Manutenção da rede

É essencial que as empresas que atuam virtualmente realizem a manutenção da rede. Este é o momento que a equipe de TI tem para instalar e configurar os

firewalls e soluções de IPS, gerenciar antivírus e remover as pragas digitais do sistema.

#### Vigilância constante

O monitoramento permite prevenir possíveis invasões ou ameaças e ainda conferir o acesso anormal dos usuários, seja interno, como funcionários mal intencionados, ou externos, ao perceber que um cliente alterou o padrão de comportamento no site, por exemplo.

#### Computação na nuvem

Ela pode ser uma facilitadora, mas desperta muita preocupação em termos de segurança da informação. Para que o usuário tenha acesso ao armazenamento via cloud computing, é preciso assegurar a confidencialidade e a autenticidade dos dados fornecidos, além da segurança oferecida pelo dispositivo de acesso.

#### Criptografia de dados

Criptografar os dados garante a privacidade de todos os tipos de informações não só durante o período de uso, mas também quando estiverem inativas.

Registrar o uso da criptografia pode ser uma boa tática para apaziguar a desconfiança do usuário.

A [segurança da informação](#) pode ser adotada desde já; não é preciso esperar uma catástrofe acontecer com o usuário para contratar soluções que não têm o custo elevado em troca de proteção. As oportunidades da Internet não têm fim quando soluções eficazes e profissionais especializados podem combater os cibercriminosos.

---

leia mais

---

## CEOs são os principais alvos dos hackers

---

---

### DÊ SUA OPINIÃO

Comente

Envie-me um e-mail quando meu comentário for aprovado.

[ENVIAR COMENTÁRIO](#)

0 Comments

Sort by [Oldest](#)[Facebook Comments Plugin](#)*Este projeto é mantido pelas empresas:*

Accenture Interactive

[Ad]matic

adyen

AFILIO

All IN

axado

B Seller

BEST OFFSHORENT

buscapé company

Cadastra

cielo

clearsale

Cnova Marketplace

CoreBiz.

DOT

e-Millennium

enext

exceda

Jugme

infracommerce

inteliPost

KPL

Loggi

mercado livre

mercado pago

moip

mundi pagg

neoassist

ORACLE COMMERCE CLOUD

pagar.me

pagseguro

PayPal

PayU

Pier8

pmweb

Rakuten

rede

SAP Hybris

SEOMaster

Serasa Experian

SIEVE

SITE BLINDADO

SUSYSTEMS

stelc

stone

SYNAPCOM

VTEx

Walmart.com

zanox.

*Parceiros Estratégicos:*

ACCORHOTELS

DialHost

direct

LATAM AIRLINES

**e-commercebrasil**  
EXCELÊNCIA EM E-COMMERCEE-COMMERCE  
BRASIL

QUEM SOMOS

IMASTERS

IMASTERS.EXPERT

FÓRUM E-COMMERCE 2014

ARTIGOS

TV E-COMMERCE  
BRASIL

BLOG

ATENDIMENTO

ESTOQUE

FISCAL

GESTÃO

LOGÍSTICA

MARKETING

MERCADO

PAGAMENTO

PLATAFORMAS

SEGURANÇA

SOCIAL MEDIA

VENDAS

CURSOS

CURSOS ONLINE

WEBINARS

WORKSHOPS

CLUBE  
E-COMMERCE  
BRASILFAÇA PARTE DO NOSSO  
CLUBE E TENHA  
VANTAGENS EXCLUSIVAS!

DISCUSSÕES

VENDAS

OPERAÇÃO

GESTÃO DO NEGÓCIO

GRUPOS DE ESTUDO

VÍDEOS

ATENDIMENTO

BACKOFFICE

CASES

GESTÃO DE E-COMMERCE

LOGÍSTICA

MARKETING &amp; VENDAS

PAGAMENTO &  
SEGURANÇA

SEARCH

REVISTA

CONFIRA A ÚLTIMA EDIÇÃO

NEWSLETTER

Fique por dentro de t  
eventos, cursos, con  
muito mais.EVENTOS  
CLUBE E-COMMERCE BRASIL  
REVISTA IMPRESSA  
PRÊMIO E-COMMERCE BRASIL  
CATÁLOGO DE FORNECEDORES  
SOBRE O E-COMMERCE BRASIL**Social  
miner**  
e-commercebrasilA plataforma de people marketing  
do E-Commerce Brasil

Site