Combate ao Cibercrime e Proteção dos Consumidores

Instituto Brasileiro de Defesa do Consumidor - IDEC
cristiana.gonzalez@idec.org.br

- Contexto de abundância e disponibilidade de dados;
- Dados criados toda a vez que estamos online (e também offline), usamos o celular, pagamos com o cartão de crédito;
- Esses dados são armazenados, analisados, estudados e vendidos para governos e empresas com finalidades diversas: vigilância, controle, marketing, obtenção de lucro;
- Internet adquire duplo caráter: confere autonomia e poder ao indivíduo e, ao mesmo tempo, é abusada por instituições das quais os próprios indivíduos dependem.

- vazamentos de fotos íntimas
- crimes de pornografia infantil.
- fraude
- Furto e perda de dados
- Spam
- Malware

FOREIGN AFFAIRS

BRAZIL'S CYBERCRIME PROBLEM
Robert Muggah and Nathan Thompson

SNAPSHOT September 17, 2015 South America Cybersecurity

Brazil's Cybercrime Problem

Time to Get Tough

By Robert Muggah and Nathan Thompson

Brazil is at the epicenter of a global cybercrime wave. The country ranks second worldwide in online banking fraud and financial malware, and the getting worse. According to official sources, the number of untry grew by 197 percent in 2014, and online banking t this past year.

mercado

Pequenas e médias empresas são os maiores alvos de ataques cibernéticos; saiba como se prevenir

REINALDO CHAVES
COLABORAÇÃO PARA A FOLHA

27/04/2015 ⊙ 02h00

Compartilhar 426 OUVIR O TEXTO + Mais opções

Os golpistas eletrônicos estão de olho nas micro, pequenas e médias empresas. É o que mostrou pesquisa feita pela Fiesp (Federação das Indústrias do Estado de São Paulo) em janeiro e fevereiro com 425 indústrias paulistas de todos os portes

- “Cibercrime é como qualquer outro tipo de crime, só que é cometido com táticas diferentes” Bruce Schneir

- Estatísticas
- Leis atuais se aplicam
- Cuidados que o usuário deve ter

Estatísticas?

Microsoft Research

Our research Connections Careers About us

All Downloads Events Groups News People Projects Publications

Sex, Lies and Cyber-crime Surveys

Dragnets
Tracking Censorship and Surveillance

Does Cybercrime Really Cost $1 Trillion?

osses is derived from surveys. We examine some
by survey. First, losses are extremely

CATO AT LIBERTY

APRIL 15, 2012 1:26PM

From Cybercrime Statistics to Cyberspying

By JIM HARPER SHARE

Someone finally decided to examine "cybercrime" statistics, and here's what they found:

> The cybercrime surveys we have examined exhibit [a] pattern of enormous, unverified outliers dominating the data. In some, 90 percent of the estimate appears to come from the answers of one or two individuals. In a 2006 survey of identity theft

Economia do Cibercrime

- Do ponto de vista Econômico: poucos criminosos conseguem alcançar ganhos efetivos; é uma atividade de baixa lucratividade para a maioria

- Spam, roubo de senhas, entre outros. O acesso a recursos comuns é um mau negócio. Não importa o quão grande é a oportunidade inicial, a entrada de mais pessoas no mesmo negócio reduzem o retorno do investimento.

- “dinheiro fácil" se esgota facilmente

- Efeito exagerado das estatísticas de cibercrime é proporcional à forma como os dados são gerados;

- números são superestimados;
  - Ex. cartões de crédito roubados;

- Vendidos a centavos de dólar porque são difíceis de serem monetarizados;

- É difícil encontrar os cibercriminosos milionários porque raramente existe algum

- PL Azeredo (PL nº 84/1999)
- Lei Carolina Dieckmann (PL nº 2793/11)
- Reforma ECA (PL nº 250/08)
- Marco Civil

- Existem outras formas de lidar com esses problemas: CERT

- O primeiro passo para se prevenir dos riscos relacionados ao uso da Internet é estar ciente de que ela não tem nada de "virtual". Tudo o que ocorre ou é realizado por meio da Internet é real: os dados são reais e as empresas e pessoas com quem você interage são as mesmas que estão fora dela. Desta forma, os riscos aos quais você está exposto ao usá-la são os mesmos presentes no seu dia a dia e os golpes que são aplicados por meio dela são similares àqueles que ocorrem na rua ou por telefone

- É preciso, portanto, que você leve para a Internet os mesmos cuidados e as mesmas preocupações que você tem no seu dia a dia, como por exemplo: visitar apenas lojas confiáveis, não deixar públicos dados sensíveis, ficar atento quando "for ao banco" ou "fizer compras", não passar informações a estranhos, não deixar a porta da sua casa aberta, etc

- Para tentar reduzir os riscos e se proteger é importante que você adote uma postura preventiva e que a atenção com a segurança seja um hábito incorporado à sua rotina, independente de questões como local, tecnologia ou meio utilizado:

- Mecanismos de segurança, Contas e senhas e Criptografia.

- responsabilidade dos intermediarios;
- inimputabilidade da rede;
- censura privada.

- Direitos Autorais - reforma da Lei 9610/98
- Exceções e Limitações: usos não comerciais
- Relatório Especial da ONU: acesso à cultura e ao conhecimento reconhecidos como um direito humano

U.S.A X Aaron Swartz

- Processo criminal por fazer download de uma base de dados acadêmica. Jstor
- Download era permitido. Download muito rápido.
- Acesso à rede do MIT era permitido
- Estatuto não regulava os meios de acesso do computador nem o que é possível fazer com a informação uma vez que se tem acesso a ele.
- Perdas “calculadas” - $91 M ($19 x 4.8M de artigos)
- “acesso não autorizado” - 1 ano de prisão

- Falso “trade-off”: privacidade x segurança

- Se por um lado existem algumas medidas de segurança violam a privacidade, existem outras que não colidem com esse direito: fechaduras; cercas; travas de segurança para portas em uma cabine de avião;

- Segurança e privacidade estão alinhados: quem não tem privacidade está mais exposto, vulnerável e desprotegido.

- Invadir a privacidade, coletar e acessar dados sem autorização não vai necessariamente reduzir a insegurança.

- segurança > vigilância

- uma infra-estrutura de segurança da informação que iniba a vigilância, em vez de uma infra-estrutura insegura que permita acesso fácil a dados pessoais;

- a infra-estrutura deve ser desenhada para a maioria, e não para a minoria.

- se a segurança for prioridade, protegendo-se a privacidade e evitando a vigilância, estaremos protegendo o fluxo global de informação da espionagem e de outros ataques prejudiciais como roubo de identidade.

- Tor é um exemplo: software livre e aberto para navegar anonimamente na Internet;
- Foi primeiro desenvolvido pela US Naval Research Laboratory e pelo Departamento de Estado;
- Usado por dissidentes no mundo inteiro para evadir a vigilância e censura (ex.China)
- Ou o Tor é forte para proteger todos, ou não protege ninguém.

- Em que tipo de mudo queremos viver?
- Queremos reduzir o desequilíbrio de poder, limitando a capacidade do governo de monitorar, censurar e controlar ou permitiremos que empresas e governos tenham cada vez mais poder sobre todos os cidadãos?
- Sistemas deveriam ser desenhados para terem o mínimo de vigilância necessário e coletar o mínimo de informação necessária para determinado objetivo

PL 215/2015

1) penas podem ser dobradas para qualquer crime envolvendo conteúdo publicado pela internet ou outro meio de telecomunicação;

2) para qualquer um desses crimes, não caberá fiança, ou seja, a pessoa acusada vai presa e não pode responder em liberdade;

3) crimes online contra a honra (calúnia, injúria e difamação) se tornam crimes hediondos se derem causa à morte da vítima; difamação ou injúria).

PL 215/2015

4) para crimes online contra a honra, acaba com a necessidade de queixa,ou seja, o Ministério Público pode ajuizar o processo mesmo contra a vontade individual da vítima;

5) para crimes online contra a honra, sem necessidade de ordem judicialprévia, a "autoridade competente" terá garantido pelo provedor deconexão o livre acesso a (em especial a autoridade policial e o MP):

a) registros de conexão à internet de qualquer pessoa (quando e onde se conectou);

b) registros de acesso a aplicações de internet de qualquer usuário(quais sites, apps ou programas ele acessou na rede);

c) dados pessoais de qualquer pessoa;

d) conteúdo das comunicações privadas de qualquer pessoa (emails, mensagens inbox, ligações com voz, ligações com vídeo)

PL 215/2015

6) explicita um direito de remover da internet qualquer conteúdo que associe o nome ou imagem de uma pessoa a:

a) qualquer crime de que essa pessoa tenha sido absolvida em caráter definitivo (ainda que por falta da provas, por exemplo);

b) qualquer fato (com ou sem julgamento) prejudicial à honra (calúnia,difamação ou injúria)

Sem proteção aos dados pessoais a Internet é insegura para todos

APL Dados Pessoais

(+) princípio da necessidade; princípio da não discriminação; princípio da prevenção (privacy by design/ privacy by default); consentimento e autodeterminação; possibilidade de encerrar o tratamento (ou dissociação); direito da portabilidade (informação; anulação; autorização sobre tratamento); transparência na comunicação e interconexão de dados; autoridade competente;

(-) Segurança Pública; Dados Anônimos/Dados anonimizáveis; Dados Sensíveis; consentimento não pode ser restrito quando se trata do poder público; transparência deve se aplicar ao poder público; responsabilidade dos agentes (cláusula geral); regras mais claras sobre vazamento de dados

Relator Especial das Nações Unidas

With respect to encryption and anonymity, States should adopt policies of non-restriction or comprehensive protection, only adopt restrictions on a case-specific basis and that meet the requirements of legality, necessity, proportionality and legitimacy in objective, require court orders for any specific limitation, and promote security and privacy online through public education;

National laws should recognize that individuals are free to protect the privacy of their digital communications by using encryption technology and tools that allow anonymity online;

Companies, like States, should refrain from blocking or limiting the transmission of encrypted communications and permit anonymous communication. Attention should be given to efforts to expand the availability of encrypted data-centre links, support secure technologies for websites and develop widespread default end-to-end encryption. Corporate actors that supply technology to undermine encryption and anonymity should be especially transparent as to their products and customers

The use of encryption and anonymity tools and better digital literacy should be encouraged. The Special Rapporteur, recognizing that the value of encryption and anonymity tools depends on their widespread adoption, encourages States, civil society organizations and corporations to engage in a campaign to bring encryption by design and default to users around the world

ANONIMATO = LIBERDADE DE EXPRESSÃO

Uso dos dados dos Consumidores Online
“Data Brokers” e Publicidade Comportamental

The Switch

These data brokers cost consumers millions by illegally selling off their financial information, says FTC

A 4

By Andrea Peterson August 12 Follow @kansasalps

Most Read Business

1 A stunning stat about pay seems impossible but actually is true

2 Deficits and debt are no longer at the top of the GOP agenda

Transparência

Capacitação

Segurança > Vigilância

Privacidade e Liberdade de Expressão

Anonimização