Desafios para Identificação e Tratamento de Incidentes na Internet

Cristine Hoepers
cristine@cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
Núcleo de Informação e Coordenação do Ponto BR
Comitê Gestor da Internet no Brasil

Agenda

- Contextualização: CERT.br e a Governança da Internet no Brasil
- Ataques mais frequentes
- Desafios
  - na identificação
  - no tratamento dos incidentes
- Considerações finais

História e Governança da Internet no Brasil

Evolução da Internet no Brasil

- 1989 – Criação e delegação do código de país (ccTLD) ".br" à FAPESP
- 1991 – Primeira conexão TCP/IP brasileira, realizada entre a FAPESP e a *ESNet*
- 1995 – Portaria Interministerial MC/MCT nº 147, de 31 de maio, cria o CGI.br
  - coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados
- 1995 – Criação do Registro.br
- 1997 – Criação do CERT.br (à época NBSO)
- 2005 – Criação do NIC.br, entidade sem fins lucrativos para executar as diretrizes do CGI.br e prestar serviços para a estabilidade e segurança da Internet no Brasil

http://www.nic.br/imprensa/releases/2010/rl-2010-12.htm

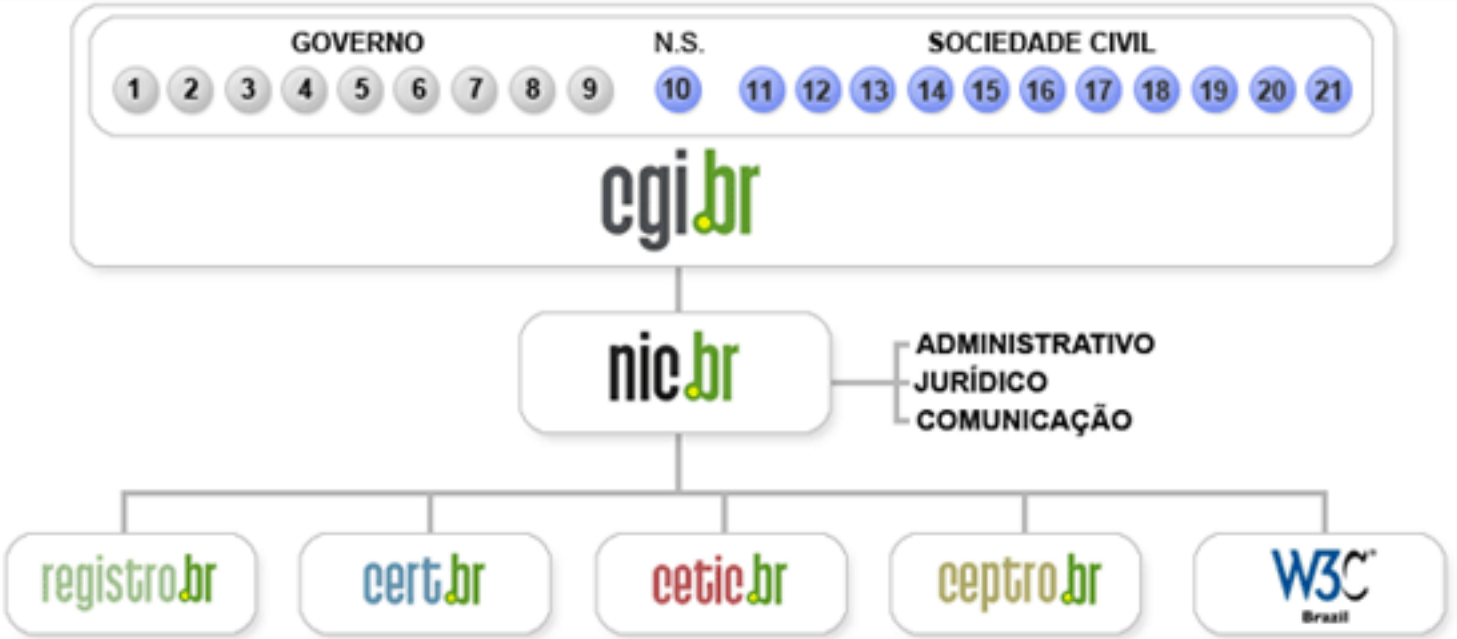
Comitê Gestor da Internet no Brasil – CGI.br

Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03 de setembro de 2003, destacam-se:

- **a proposição de normas e procedimentos relativos à regulamentação das atividades na internet;**
- **a recomendação de padrões e procedimentos técnicos operacionais para a internet no Brasil;**
- **o estabelecimento de diretrizes estratégicas relacionadas ao uso e desenvolvimento da internet no Brasil;**
- **a promoção de estudos e padrões técnicos para a segurança das redes e serviços no país;**
- **a coordenação da atribuição de endereços internet (IPs) e do registro de nomes de domínios usando <.br>;**
- **a coleta, organização e disseminação de informações sobre os serviços internet, incluindo indicadores e estatísticas.**
- **ser representado nos fóruns técnicos nacionais e internacionais relativos à Internet;**

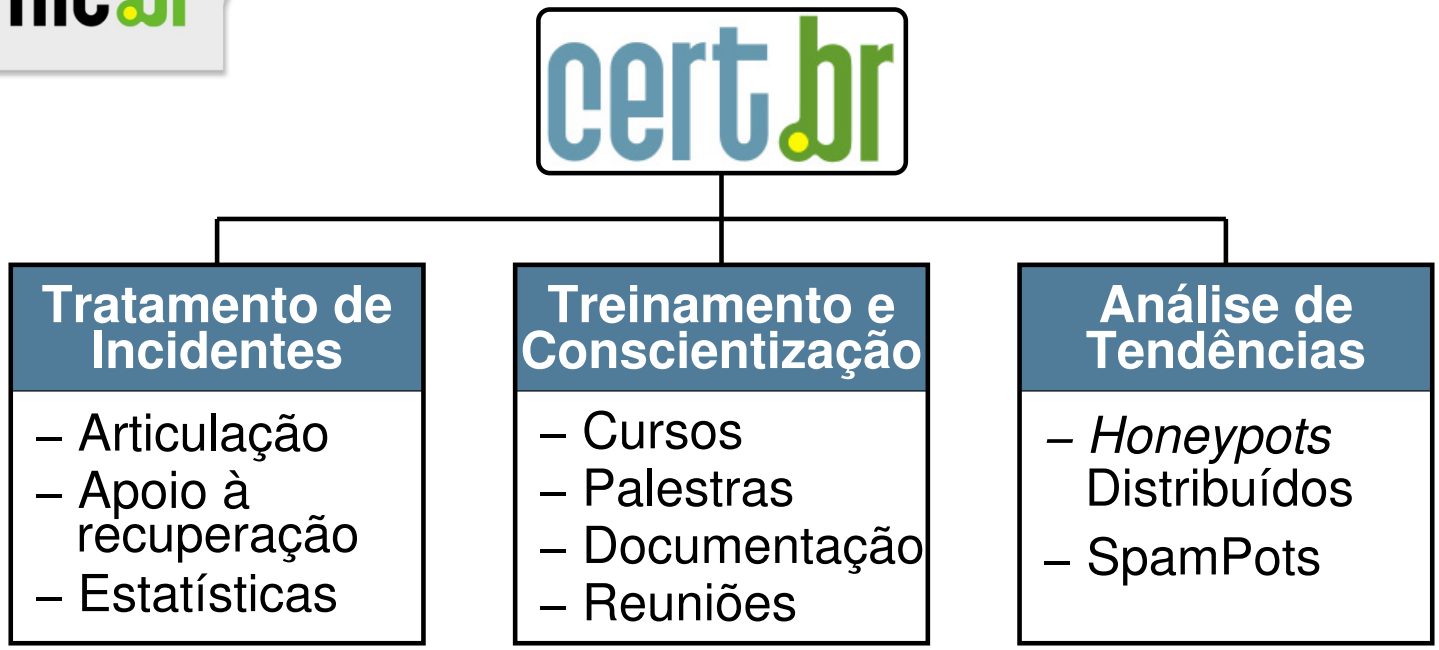
http://www.cgi.br/sobre-cg/

Estrutura do CGI.br e NIC.br



1 – Ministério da Ciência e Tecnologia (Coordenação)
2 – Ministério das Comunicações
3 – Casa Civil da Presidência da República
4 – Ministério da Defesa
5 – Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 – Ministério do Planejamento, Orçamento e Gestão
7 – Agência Nacional de Telecomunicações (Anatel)
8 – Cons. Nacional de Desenvolvimento Científico e Tecnológico
9 – Fórum Nac. de Secretários Estaduais para Assuntos de C&T
10 – Representante de Notório Saber em assuntos de Internet

11 – provedores de acesso e conteúdo
12 – provedores de infra-estrutura de telecomunicações
13 – indústria de bens de informática, telecomunicações e software
14 – segmento das empresas usuárias de Internet
15-18 – representantes do terceiro setor
19-21 – representantes da comunidade científica e tecnológica



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil
http://www.nic.br/grupo/historico-gts.htm | http://www.cert.br/sobre/

Ataques e *Modus Operandis* mais Comuns

Ataques mais Comuns

- **Contra usuários finais**
  - **fraudes, *phishing*, *bots*, *spyware*, etc**
  - **motivação financeira**
  - **abuso de *proxies*, na maioria instalados por *bots***
- **De força bruta (adivinhação de conta/senha) contra serviços de rede**
  - **SSH, FTP, Telnet, VNC, etc**
  - **acesso a servidores, roteadores, modems banda larga, celulares, etc**
- **Não tão frequentes, mas com grande impacto por serem contra a infraestrutura crítica da Internet**
  - **ataques contra servidores DNS**
  - **contra protocolos de roteamento como o BGP**
- **Com rápido crescimento nos últimos anos**
  - **ataques a aplicações Web vulneráveis**

Ataques a Usuários Finais

- Fruto da mudança no enfoque dos atacantes
  - é mais fácil e "rentável" atacar um usuário
- Fraudes financeiras
  - páginas falsas estão voltando a ter números significativos
  - *drive-by downloads* sendo usados intensamente no Brasil
    - casos publicados na mídia incluem:
      sites principais da Vivo, da Oi e da Ambev
- Outras motivações
  - espionagem, sabotagem
  - nesses casos chamados de APTs ("*Advanced Persistent Threats*")
- Casos conhecidos cujos vetores iniciais foram usuários redes de alto valor
  - Comprometimento da DigiNotar – PKI da Holanda
  - Caso Aurora (comprometimento do Google, Microsoft, etc por meses)
  - New York Times

Se Consegue Quase Tudo no Mercado Negro

Overall Rank		Item	Percentage		2010 Price Ranges
2010	2009		2010	2009	
1	1	Credit card information	22%	19%	$0.07–$100
2	2	Bank account credentials	16%	19%	$10–$900
3	3	Email accounts	10%	7%	$1–$18
4	13	Attack tools	7%	2%	$5–$650
5	4	Email addresses	5%	7%	$1/MB–$20/MB
6	7	Credit card dumps	5%	5%	$0.50–$120
7	6	Full identities	5%	5%	$0.50–$20
8	14	Scam hosting	4%	2%	$10–$150
9	5	Shell scripts	4%	6%	$2–$7
10	9	Cash-out services	3%	4%	$200–$500 or 50%–70% of total value

Fonte: Underground Economy Servers—Goods and Services Available for Sale
http://www.symantec.com/es/es/threatreport/topic.jsp?id=fraud_activity_trends&aid=underground_economy_servers

Russian Underground – Serviços Disponíveis

- **Pay-per-Install (global mix or specific country): $12–$550**
- **Bulletproof-hosting with DDoS protection: $2000 per month**
- **Styx Sploit Pack rental (affects Java and Adobe Acrobat and Flash Player) $3000/month**
- **Programming: web server hacking $250; browser-in-the-middle $850; trojans $1300**
- **Windows rootkit (for installing malicious drivers): $292**
- **Linux rootkit: $500**
- **Hacking Facebook or Twitter account: $130**
- **Hacking Gmail account: $162**
- **Hacking corporate mailbox: $500**

"Proxy service: HTTP, HTTPS, SOCKS4, SOCKS5; prices: 5 days = US$4; 10 days = US$8; 30 days = US$20; 90 days = US$55"

Offering	Price
Bots (i.e., consistently online 40% of the time)	US$200 for 2,000 bots
DDoS botnet	US$700
DDoS botnet update	US$100 per up

Offering	Price
1-day DDoS service	US$30-70
1-hour DDoS service	US$10
1-week DDoS service	US$150
1-month DDoS service	US$1,200

"Setup of ZeuS: US$100, support for botnet: US$200/month, consulting: US$30."

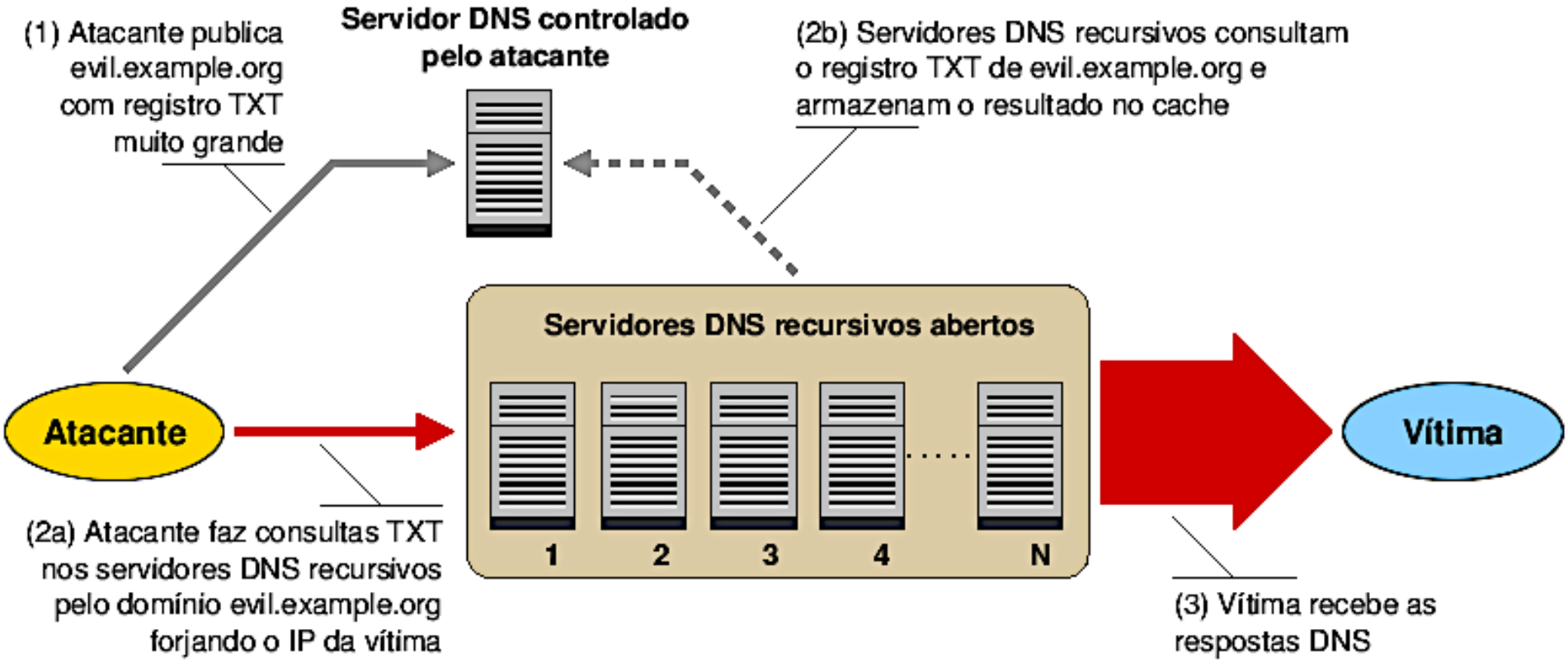
Fonte:Read Russian Underground 101 - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Ataque ao Spamhaus

Na mídia: "O ataque que quase parou a Internet"…

- **Tentativa de "sequestrar" a rede do Spamhaus via anúncios BGP**
- **100Gbps de tráfego médio de ataque**
  - **picos de 300Gbps**
- **Mover o serviço para um CDN (*Content Delivery Network*) foi o único meio de continuar acessível**
- **Atacantes passaram então a atacar os pontos de troca de tráfego de Londres e Amsterdam**
  - **erro ao deixar endereços IP internos ao PTT públicos permitiu a realização do ataque**
- **Como gerar 300Gbps?**
  - **ataques com uso de amplificação de tráfego ou DRDoS**
  - ***botnets* + servidores DNS recursivos abertos**
    - **mais de 70 mil recursivos abertos notificados no Brasil pelo CERT.br**

Ataques via Servidores DNS Recursivos Abertos



Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

http://www.cert.br/docs/whitepapers/dns-recursivo-aberto/

Preso Suspeito do Ataque ao Spamhaus

Outros ataques em rápido crescimento

- "*Modems*" e roteadores banda larga (CPEs)
  - Botnets usadas para ataques diversos
    - comprometidos via força bruta (telnet)
    - vários modelos permitem reset via WAN – Post na porta TCP/80
  - Comprometimento para alteração do serviço DNS para
    - fraudes financeiras
    - redirecionamento para obter "cliques" de propaganda
    - DDoS
- Dispositivos com sistema Android
  - *Botnets*
  - Fraudes e outros tipos de *malware*
- Sistemas SIP
  - Força bruta para realização de ligações internacionais
  - Fraude

Mas o Foco da Marioria dos Ataques Continuará Sendo

Serviços *Online*

- Grande demanda por *e-services*
- Dados sensíveis estão mais expostos
  - por necessidade, comodidade ou descuido
- Segurança não é prioridade
- Impactos não são compreendidos
- Sistemas críticos são conectados à Internet
  - controle de infrasestruturas críticas
  - caixas automáticos (ATMs)
  - sistemas de imigração e identificação

Clientes/Usuários

- Internet passou a fazer parte do dia-a-dia
- Usuários não são especialistas
- Grande base
  - de dispositivos vulneráveis
  - com banda disponível
- Mais fáceis de atacar
- Possuem dados de valor
  - dados financeiros
  - endereços de e-mail válidos
  - credenciais de acesso
- Dispositivos podem ser usados para outros ataques
  - *botnets*

Desafios para a Identificação

Desafios para a Identificação

- **Os ataques partem de vítimas na maioria absoluta dos casos**
- **Investigação sem contexto pode levar a graves consequências**
  - **e.g. Coréia do Sul x China**
    - **a rede usava como IPs não roteáveis (no NAT) um bloco de IPs alocado para a China – peritos viram o IP de onde veio o *malware* e anunciaram que o ataque vinha da China**
- **A infraestrutura usada nos ataques de alto valor pode ser a mesma do crime organizado**
  - **e.g. DDoS na Estônia e Georgia**
    - **a *botnet* usada era a mesma que há meses enviava *spams* e fazia "*DDoS for hire*"**

Desafios do Tratamento de Incidentes

Reais Causas dos Problemas

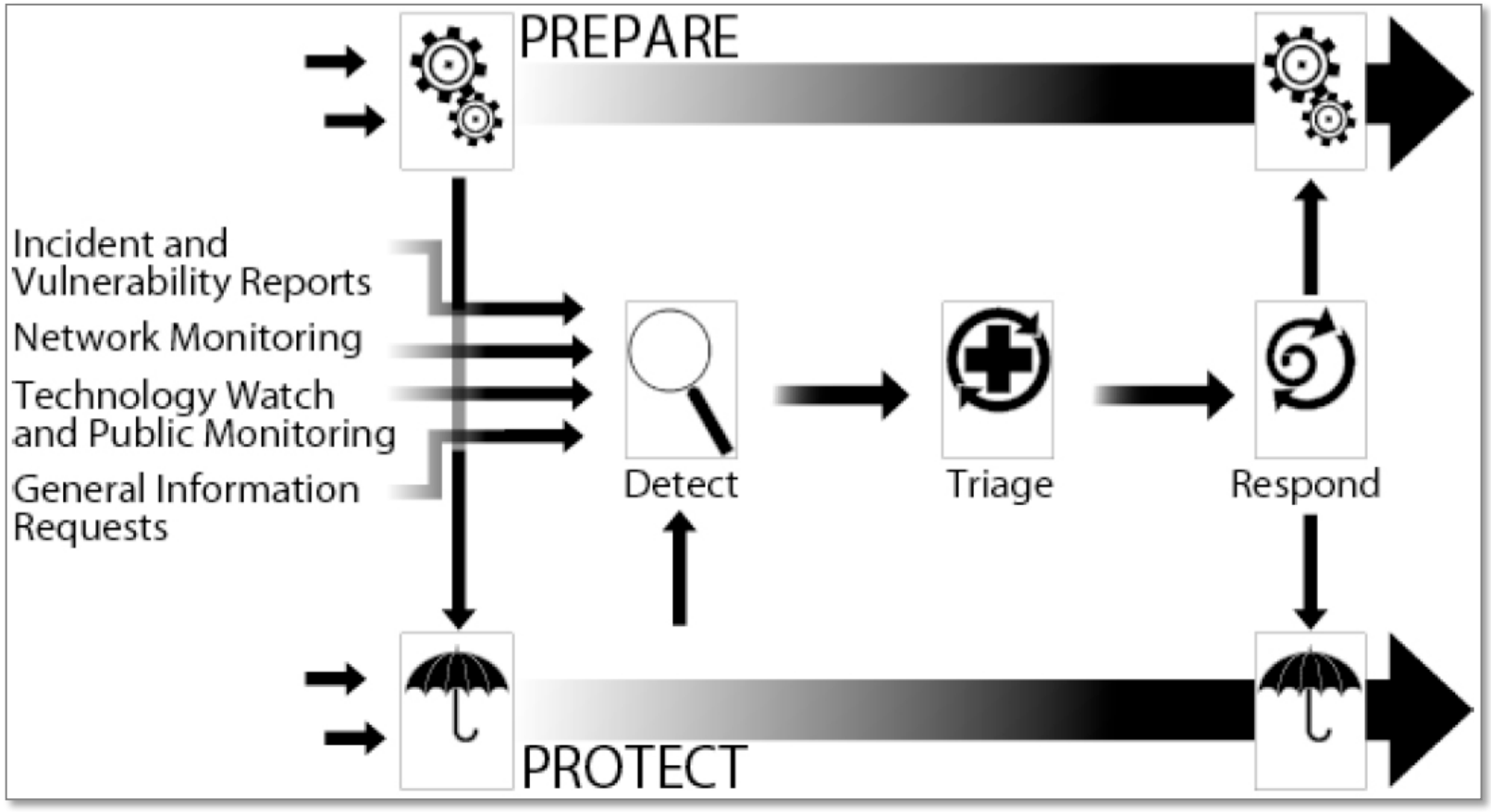
Cenário atual é reflexo direto de

- **Aumento da complexidade dos sistemas**
- **Falta de desenvolvedores capacitados para desenvolver com requisitos de segurança**
- ***Softwares* com muitas vulnerabilidades**
- **Pressão econômica para lançar, mesmo com problemas**
- **É uma questão de "*Economics and Security*" http://www.cl.cam.ac.uk/~rja14/econsec.html**

Os criminosos estão apenas migrando para onde os negócios estão

Tratamento de Incidentes

"Um CSIRT provê serviços de suporte para prevenção, tratamento e resposta a incidentes de segurança em computadores.



Fonte: ***Defining Incident Management Processes for CSIRTs: A Work in Progress*.** **Figura utilizada com permissão do CERT®/CC e do SEI/CMU.**
http://www.cert.org/archive/pdf/04tr015.pdf

Mito de que só quem sabe invadir sabe proteger

- A realidade:
  - Proteger é muito mais difícil que atacar
    - especialmente contra ataques ainda não conhecidos
  - Raríssimos os atacantes que:
    - sabem como proteger uma rede ou corrigir um problema
    - sabem como funcionam as ferramentas que utilizam
  - Maioria absoluta utiliza ferramentas disponíveis na Internet
  - Um profissional com sólida formação tem mais sucesso em utilizar as ferramentas como auxiliares nos processos de análise de risco e proteção da infraestrutura que um invasor
- Os riscos:
  - Colocar a segurança nas mãos de quem não está preparado
  - Ter informações confidenciais comprometidas
  - Ter *backdoors* e cavalos de tróia instalados em sua infraestrutura

Papel dos CSIRTs na Mitigação e Recuperação

- A redução do impacto é consequência da:
  - agilidade de resposta
  - redução no número de vítimas
- O sucesso depende da confiabilidade
- O papel do CSIRT:
  - auxiliar a proteção da infra-estrutura e das informações
  - prevenir incidentes e conscientizar sobre os problemas
- O CSIRT não é um investigador
- Tratamento de Incidentes não é perícia
- A pessoa que responde um incidente é a primeira a entrar em contato com as evidências de um possível crime
  - seguir as políticas
  - preservar as evidências
  - responder incidentes – retornar o ambiente ao estado de produção

Desafios para a Melhora do Cenário como um Todo

Resiliência da Infraestrutura Crítica de Internet

Contínuo investimento em:

- **Pontos de Troca de Tráfego nas áreas metropolitanas – PTT.br**
- **Sistemas de redundância e mirror de DNS**
- **Adoção de DNSSEC**
  - **Novos protocolos como DANE em estudo**
- **Segurança na infraestrutura de roteamento**
  - **Roteamento dinâmico fuciona por confiança nos anúncios**
  - **Em implantação o uso de RPKI e S-BGP**
  - **Em resumo: tabelas de rotas passam a ser assinadas e publicadas somente pela fonte legítima**

Desafios (1/2)

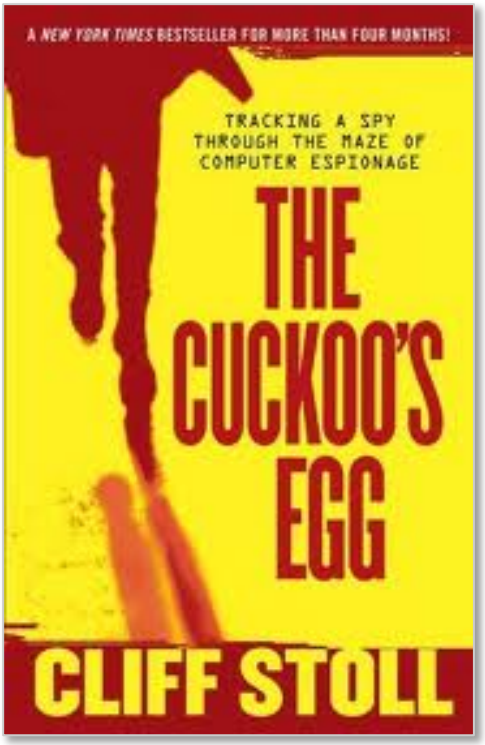
- **Só haverá melhorias quando**
  - **O processo de desenvolvimento de *software* incluir**
    - **Levantamento de requisitos de segurança**
    - **Testes que incluam casos de abuso**

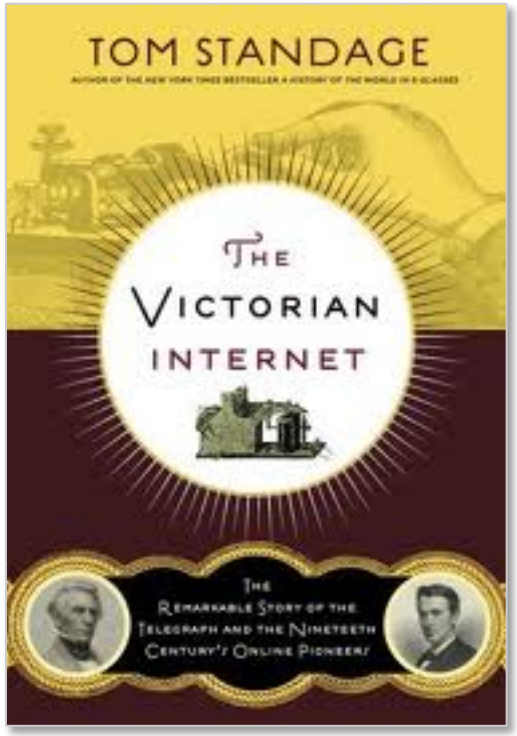
      (e não somente casos de uso)
  - ***Desenvolvimento seguro de software* se tornar parte da formação de projetistas e programadores**
    - **Desde a primeira disciplina de programação e permeado em todas as disciplinas**
  - **Provedores de acesso e serviço, operadoras e administradores de redes em geral forem mais pró-ativos**
  - **Os sistemas para usuários finais forem menos complexos**
    - **Mudança total de paradigma de uso da tecnologia**

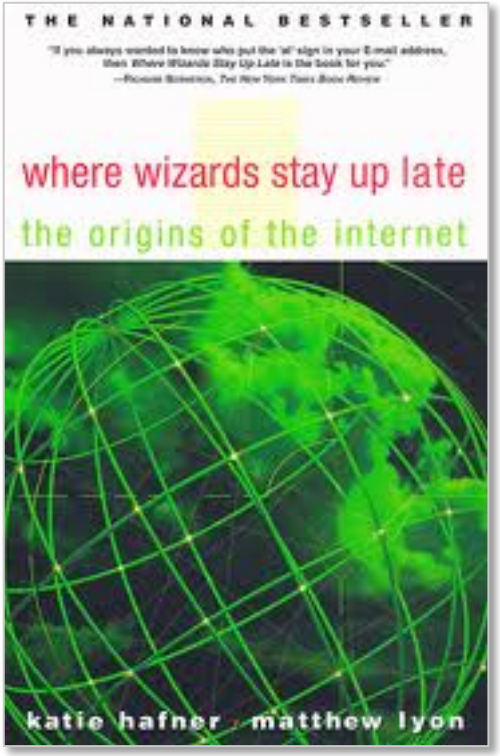
Desafios (2/2)

- **Há falta de pessoal treinado no Brasil para lidar com Redes e com segurança em IPv4**
  - **A falta de pessoal com essas habilidades em IPv6 é ainda mais preocupante**
- **Vencer a cultura de que é melhor investir em tecnologia do que treinamento e implantação de boas políticas**
  - **Quantas instituições realmente implementam tecnologias com base em uma análise de risco?**
- **Ir além do "*compliance*"**

Leituras Recomendadas







Perguntas?

Cristine Hoepers
cristine@cert.br

- **CGI.br – Comitê Gestor da Internet no Brasil**
  http://www.cgi.br/
- **NIC.br – Núcleo de Informação e Coordenação do .br**
  http://www.nic.br/
- **CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**
  http://www.cert.br/

cert.br 15 ANOS