nic.br cgi.br | cert.br

Workshop Internacional Segurança Cibernética
ANEEL, Brasília, DF
20 de outubro de 2016

Segurança, Estabilidade e Resiliência da Internet no Brasil

Dra. Cristine Hoepers
Gerente Geral
cristine@cert.br

cert.br nic.br cgi.br

Comitê Gestor da Internet no Brasil – CGI.br

Entidade multissetorial, criada em 1995, responsável por coordenar e integrar as iniciativas e serviços da Internet no País. Dentre as atribuições definidas no Decreto Presidencial nº 4.829, de 03/09/2003, 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/

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica

Núcleo de Informação e Coordenação do Ponto BR – NIC.br

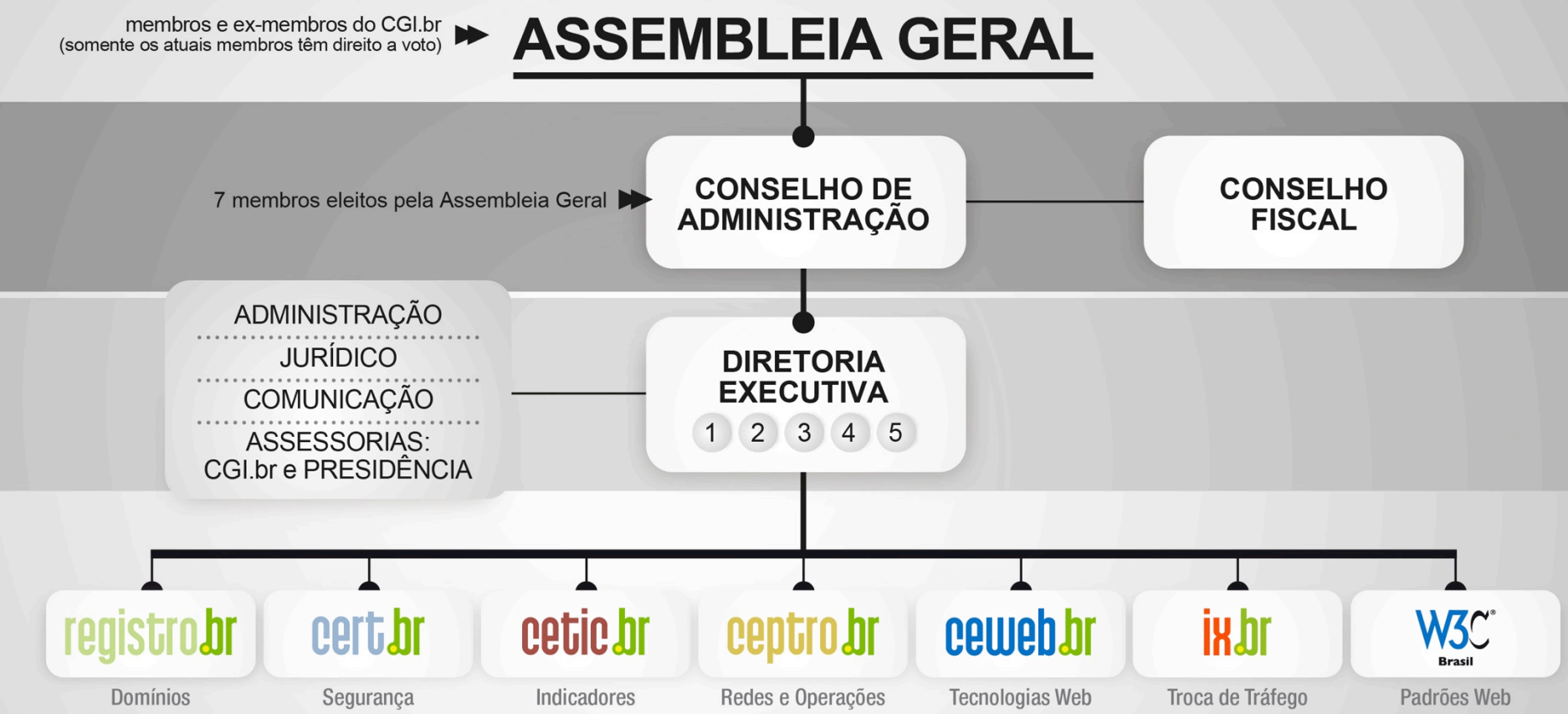
Entidade civil, sem fins lucrativos, criada para implementar as decisões e os projetos do Comitê Gestor da Internet no Brasil - CGI.br.

Dentre suas atribuições estão:

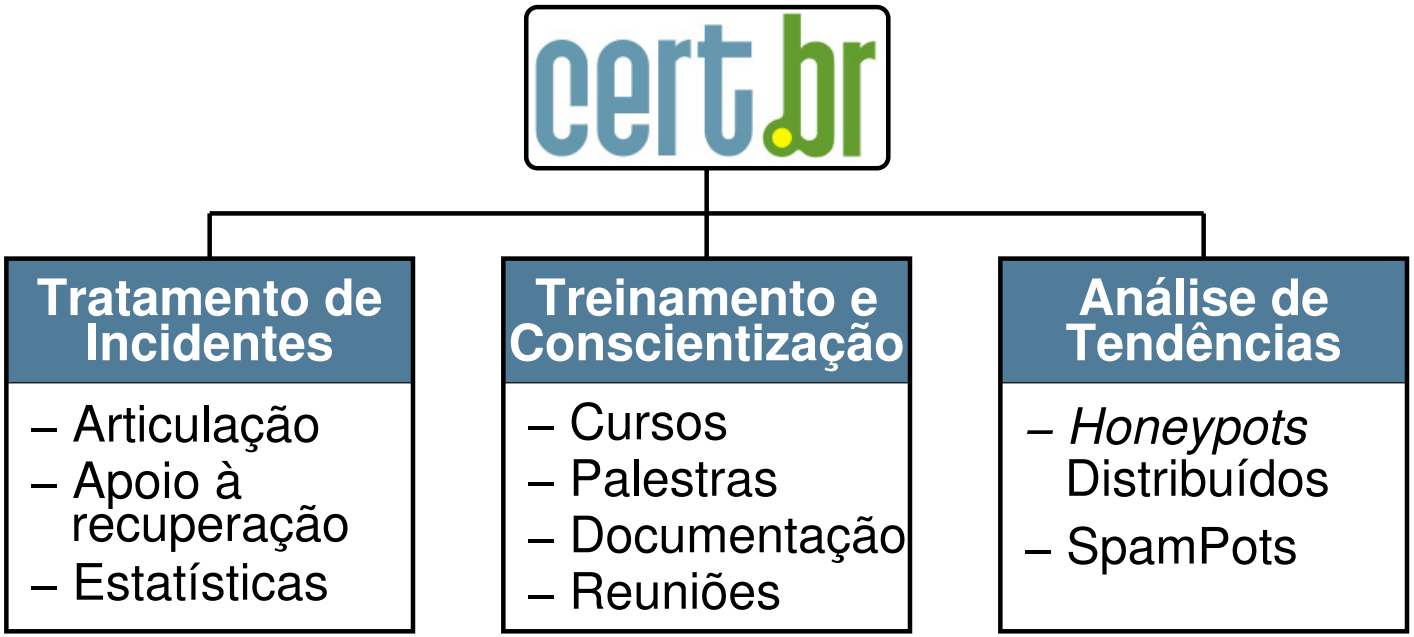
- o registro e manutenção dos nomes de domínios que usam o <.br> , e a distribuição de números de Sistema Autônomo (ASN) e endereços IPv4 e IPv6 no País, por meio do Registro.br;
- **tratamento e resposta a incidentes de segurança em computadores envolvendo redes conectadas à Internet no Brasil, atividades do CERT.br;**
- projetos que apoiem ou aperfeiçoem a infraestrutura de redes no País, como a interconexão direta entre redes (IX.br) e a distribuição da Hora Legal brasileira (NTP.br). Esses projetos estão a cargo do Ceptro.br.
- **promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais, para a segurança das redes e serviços de Internet, bem assim para a sua crescente e adequada utilização pela sociedade.**

http://www.nic.br/sobre/

Estrutura do NIC.br



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997, com base no levantamento sobre o melhor modelo de organização para atuar como facilitador para o tratamento de incidentes de segurança no Brasil

Principais atividades:

- **Tratamento de Incidentes**
  - Ponto de contato nacional para notificação de incidentes
  - Atua facilitando o processo de resposta a incidentes das várias organizações
  - Trabalha em colaboração com outras entidades
- **Formação de profissionais para atuar em Tratamento de Incidentes**
- **Produção de boas práticas e material para conscientização sobre a necessidade de segurança na Internet para diversas audiências**

Estratégias para Reduzir os Incidentes e seus Impactos

Objetivo primordial é um ecossistema saudável

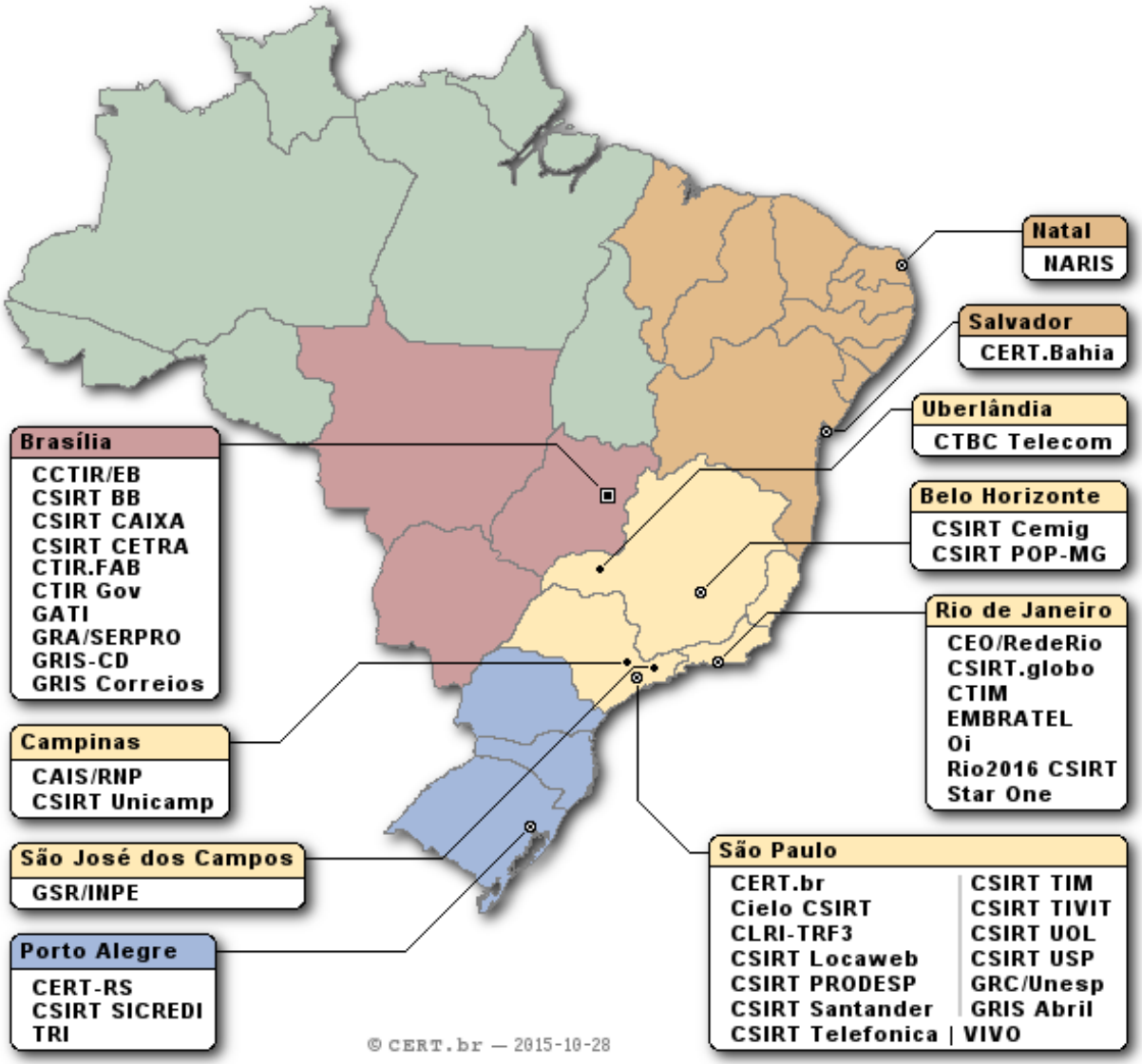
- **Nenhum grupo ou estrutura única conseguirá fazer sozinha a segurança ou a resposta a incidentes - todos tem um papel**
  - **administradores de redes e sistemas**
    - **não emanar "sujeira" de suas redes e adotar boas práticas**
  - **usuários**
    - **entender os riscos e seguir as dicas de segurança**
    - **manter seus dispositivos atualizados e tratar infecções**
  - **desenvolvedores**
    - **precisam pensar em segurança desde as etapas iniciais de desenvolvimento**

Ainda assim incidentes ocorrerão

- **necessário identificar e mitigar mais rapidamente**
  - **redução de impactos é proporcional à agilidade na resposta**
  - **é necessário ter CSIRTs estabelecidos e profissionais preparados**
    - **equipe multidisciplinar é fundamental**
      - conhecimentos técnicos profundos (redes, sistemas, desenvolvimento)
      - habilidades de comunicação e negociação
  - **cooperação é primordial – nacional e internacional**

Grupos de Tratamento de Incidentes Brasileiros:
41 times com serviços anunciados ao público

Público Alvo	CSIRTs
Qualquer Rede no País	CERT.br
Governo	CTIR Gov, CCTIR/EB, CLRI-TRF-3, CSIRT PRODESP, GATI, CTIM, GRA/SERPRO, CTIR.FAB, GRIS-CD, CSIRT CETRA, GRIS Correios
Setor Financeiro	Cielo CSIRT, CSIRT BB, CSIRT CAIXA, CSIRT Sicredi, CSIRT Santander
Telecom/ISP	CTBC Telecom, EMBRATEL, CSIRT Telefonica|VIVO, CSIRT Locaweb, CSIRT TIM, CSIRT UOL, StarOne, Oi,
Academia	GSR/INPE, CAIS/RNP, CSIRT Unicamp, CERT-RS, NARIS, CSIRT POP-MG, CEO/RedeRio, CERT.Bahia, CSIRT USP, GRC/UNESP, TRI
Outros	Rio2016 CSIRT, CSIRT TIVIT, GRIS Abril, CSIRT Globo, CSIRT Cemig



http://www.cert.br/csirts/brasil/

Outras Atividades do NIC.br que Aumentam a Segurança, a Estabilidade e a Resiliência da Internet no Brasil

cert.br nic.br cgi.br

Infraestruturas Críticas da Internet

Mesmo sendo uma rede distribuída e descentralizada, diversos elementos são críticos para sua contínua operação:

- Recursos de Numeração
  - Endereços IP e Sistemas Autônomos (ASNs)
- Roteamento
- Sistemas de registro de nomes de domínio (.br, .com, .de, etc)
- Sistemas de Resolução de Nomes (DNS)
- Pontos de Troca de Tráfego
- Infraestrutura física

Registro.br:
Segurança e Resiliência de DNS no Brasil

Implementação das extensões de segurança do DNS (DNSSEC) em todo o <.br>

Manutenção de cópias (*mirrors*) de servidores DNS raiz (*root servers*) em diversos pontos do Território Nacional

- **Estes servidores são os ponteiros iniciais para que se possa percorrer a árvore de resolução de nomes**

***Mirrors* estão presentes em 97 países:**

País	servidores
EUA	86
Brasil	19
Alemanha	15
Canadá	13
França	13
Austrália	12
China	10
Itália	10
Japão	09
Nova Zelândia	09

Fonte: Packet Clearing House – em 26/07/2016
https://prefix.pch.net/applications/ixpdir/summary/root-servers/

IX.br (antigo PTT.br): **Melhora na Disponibilidade e Estabilidade**

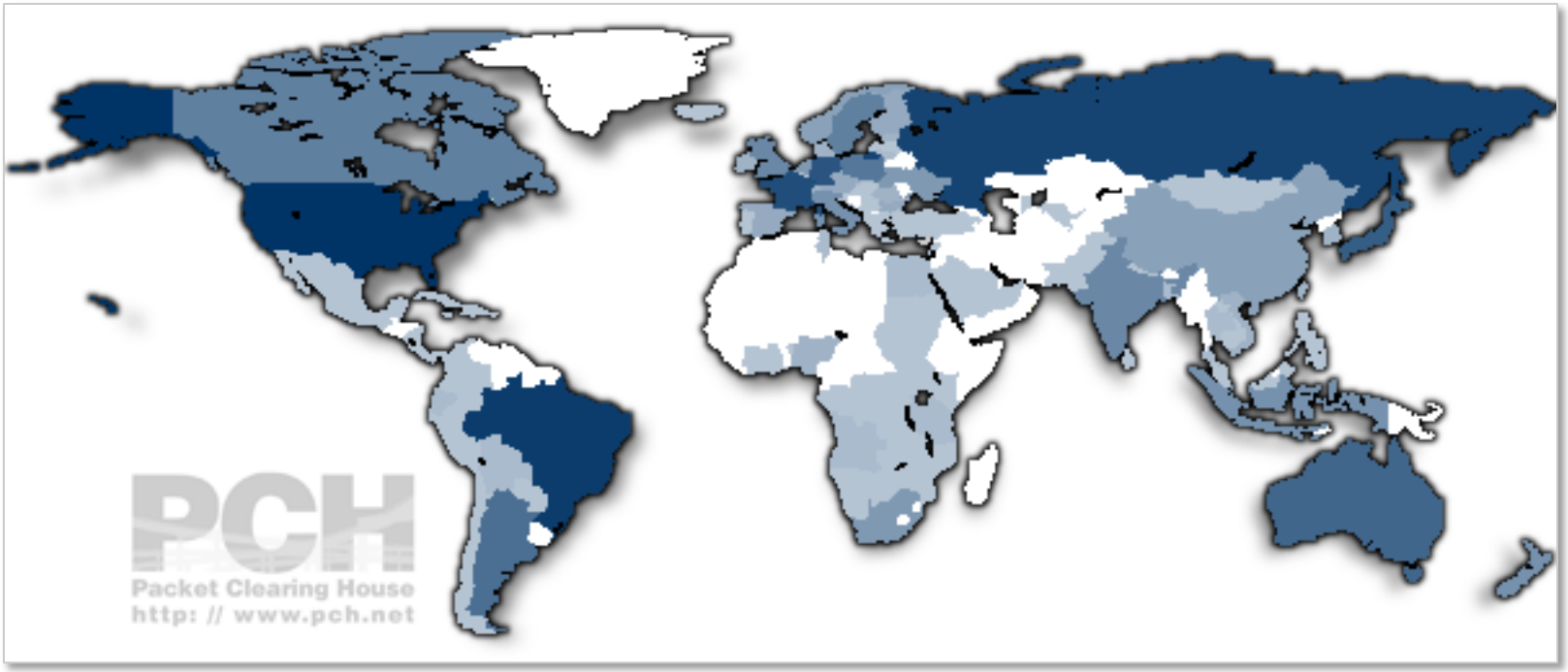
Objetivo primário dos Pontos de Troca de Tráfego: melhor conectividade, qualidade e redução de custo.

26 pontos de troca de tráfego mantidos pelo NIC.br (1.9Tbps):
http://ix.br/localidades/atuais

Efeito para disponibilidade e estabilidade:

- **Estimula as redes a terem Sistema Autônomo (AS) próprio:**
  - seus próprios endereços IP
  - mais de uma saída para Internet e possibilidade de conexão com um Ponto de Troca de Tráfego
  - mais flexibilidade na definição de rotas
    - mais facilidade para lidar com ataques de Negação de Serviço (DDoS) volumétricos

Países com Mais Pontos de Troca de Tráfego



EUA	86	Japão	16
Brasil	27	Austrália	15
Alemanha	21	Argentina	13
Rússia	21	Polônia	10
França	18	Canadá	09

Fonte: Packet Clearing House – em 26/07/2016
https://prefix.pch.net/applications/ixpdir/summary/

Considerações

cert.br nic.br cgi.br

Onde estão as maiores carências

"CERTs are like janitors, cleaning up after the mess made by everyone else. Things are only going to change when we have better software, when security is considered in all phases of project, development and deployment."

- Steve Bellovin, *Keynote FIRST 2014 Conference*

O que impera

- **"Não preciso me preocupar, alguém vai fazer a segurança depois"**
- **"Tenho *firewall* e antivírus, isso me protege"**
- **"Vamos lançar o produto/sistema, depois vemos como fazer a segurança"**

São pelo menos 30 anos investindo em "remendos"

- **Claramente não está funcionando**
- **Número de vulnerabilidades só aumenta**
- **IoT já virou base para o crime organizado (DDoS, mineração de *bitcoins*)**

Quase tudo se resume a 3 vetores de comprometimento

- **Falhas de *software***
- **Falhas de configuração**
- **Engenharia Social**

Alguns Desafios para o Futuro

Qualificação profissional

- redes, administração de sistemas, desenvolvimento de *software* seguro

Ecossistema Internet mais saudável

- Só isso reduzirá os volumes de ataques
- Envolve comprometimento de fabricantes (*software*, smartphones, IoT, etc)

Migrar para o Protocolo IPv6

- os endereços IPv4 na América Latina esgotaram em 10/06/2014
- hoje são atribuídos apenas blocos pequenos para permitir a transição

Adoção de DNSSEC

- Novos protocolos, como DANE, em estudo

Alternativas ou melhorias ao sistema atual de certificados digitais

Segurança na infraestrutura de roteamento

- roteamento funciona por confiança nos anúncios
- em discussão na comunidade o uso de RPKI e S-BGP
  - Em resumo: tabelas de rotas passam a ser assinadas

Obrigada

www.cert.br

cristine@cert.br

@certbr

20 de outubro de 2016

nic.br cgi.br

www.nic.br | www.cgi.br