Seminário Confiança no Ambiente Digital
Brasília, DF
08 de junho de 2017

Desafios da transnacionalidade: Cooperação internacional em matéria de segurança e defesa cibernética

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

CERT.br

- **Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil**
  - criado em 1997 (completando 20 anos)
  - mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil
  - responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil

- **Áreas de Atuação (entre outras)**
  - tentar reduzir os incidentes e seus impactos
    - foco em reduzir o número de vítimas
  - facilitar o processo de resposta a incidentes das várias organizações
  - ajudar a criar um ecossistema mais saudável

Cenário atual (1/2)

- **Quantidade e facilidade dos ataques se deve, em grande parte, à grande vulnerabilidade das redes e dos softwares**

- **Nenhum grupo ou estrutura conseguirá fazer sozinho a segurança ou a resposta a incidentes**
  - todos tem um papel

Cenário atual (2/2)

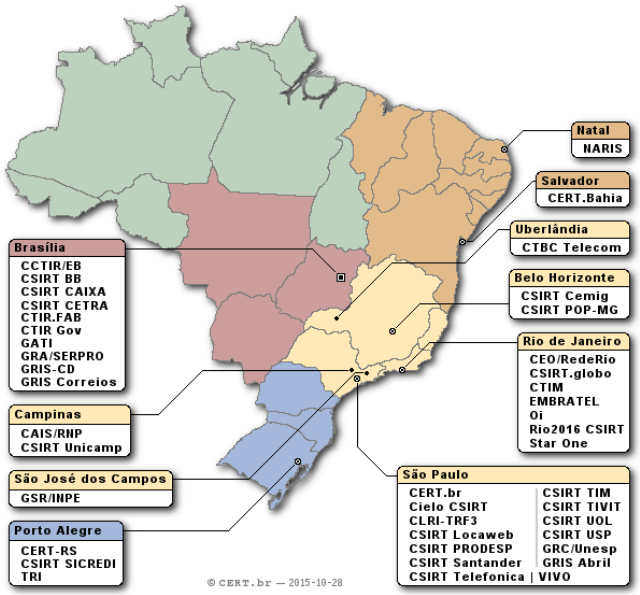
- **Para que a rede fique mais saudável (estável e resiliente) é necessário investir em:**
  - segurança como prioridade na implantação de sistemas
  - educação
    - formação de mais profissionais de redes e desenvolvimento de software
      - com segurança sendo vista como pré-requisito e sendo considerada em todas as fases de projeto e implantação de tecnologias
    - da população em geral
      - principalmente nas escolas - pensando nas próximas gerações

Assumir que incidentes ocorrerão

- **O importante é estar preparado para responder (identificar e mitigar) rapidamente**
- **Redução de impactos é proporcional à agilidade na resposta**
- **Para isso é necessário**
  - ter rede de profissionais preparados para agir quando necessário
    - todos os órgãos de governo, infraestruturas críticas, universidades e empresas de médio e grande porte devem possuir seus próprios grupos (CSIRTs)
  - cooperação
    - redes de cooperação para tratamento de incidentes já existem

Atuação do CERT.br
Âmbito nacional

- auxílio na criação de CSIRTS
- treinamento (cursos e *workshops*)
- fóruns para profissionais de CSIRTS
- eventos (GTS)
- reuniões periódicas com diversos setores
- grandes eventos
  - em conjunto com CDCiber e CTIR, entre outros
- projeto Honeypots Distribuídos
  - termômetro das atividades maliciosas na Internet
  - entender o abuso da infraestrutura da Internet por atacantes, *spammers* e fraudadores
  - 55 sensores em 43 redes (universidades, governo, provedores, operadoras e empresas)



Atuação do CERT.br
Âmbito internacional

- Lacnic (LAC-CSIRTS - região da América Latina e Caribe)
- FIRST (*Forum of Incident Response and Security Teams*)
- licenciado, desde 2004, para ministrar os cursos oferecidos pela Carnegie Mellon para criação de CSIRTs
  - 700+ profissionais treinados em tratamento de incidentes
- projeto Spampots (sensores em 12 países)
  - entender o abuso da infraestrutura da Internet por *spammers*
- cooperação com organizações no combate a *botnets*
  - envio e recebimento de notificações de/para CSIRTs internacionais
    - as recebidas são repassadas internamente
- tradução para o espanhol de materiais de conscientização

Considerações finais

- **Cooperação tem por objetivos:**
  - facilitar acesso a uma rede de contatos (nacional e internacional)
  - conhecer os grupos e pessoas que realmente conseguem ajudar
  - criar uma rede de confiança

- **Confiança:**
  - essencial para a cooperação ocorra de forma efetiva
  - consequência direta de um trabalho longo e contínuo
  - não surge de um dia para outro
  - não pode ser imposta, precisa ser conquistada

Obrigada

www.cert.br

miriam@cert.br

@certbr

08 de junho de 2017

nic.br cgi.br

www.nic.br | www.cgi.br