Grupos de Segurança Expectativas

NIC BR Security Office
nbso@nic.br
http://www.nic.br/nbso.html

Cristine Hoepers
cristine@nic.br
Klaus Steding-Jessen
jessen@nic.br

ASBR – Trilha Segurança
Pre-GTER 14
São Paulo, SP – 7 de abril de 2002

Notas:

Notas:

Grupos de Segurança – Expectativas

- Possuir um grupo/pessoa dedicada
- Atualização dos dados de contato
- Repassar todas as reclamações
- Orientar seus clientes
- Cooperação entre grupos

Notas:

Atualização dos Dados de Contato

- RFC 2142 (`security@`, `abuse@`, `noc@`)
- junto ao registro.br
- SOA / `postmaster@` / `root@`
- Dados do cliente ao designar um bloco de IPs

Notas:

Repassando as Reclamações

- Repassar para o cliente contendo:
  - subject inalterado
  - cabeçalho com data / todos os *recipients*
  - todo o conteúdo do email
- Cópia para todos os envolvidos

Notas:

Repassando as Respostas

- Repassar para todos os envolvidos:
  - cópia da mensagem com a resposta do cliente
  - descrição das ações tomadas
- Texto em inglês (dependendo do caso)

Notas:

O que NUNCA fazer

- Apenas resposta automática
- Remover conteúdo do *subject* ou da mensagem
- Responder somente para o último que repassou
- Texto "jurídico"

Notas:

Orientando seus Clientes

- DNS reverso
- Resposta a uma Notificação de Incidente:
  - Enviar email para:
    - Todos a quem a reclamação foi enviada originalmente
    - GS de sua rede / empresa / instituição
    - cópia para NBSO
  - Informar as ações tomadas

Notas:

Orientando seus Clientes (cont)

- Notificação de um Incidente
  - enviar email para:
    - RFC 2142 / contatos do domínio / SOA
    - GS de todas as redes envolvidas
    - cópia para NBSO
  - logs
    - completos e em formato texto
    - com horário (sincronizado)
    - com timezone

Notas:

Leitura Recomendada

- Incident Response – Kenneth R. van Wyk, Richard Forno, ISBN 0-596-00130-4, http://www.oreilly.com/catalog/incidentres/

Notas:

Leitura Recomendada (cont)

- Secrets & Lies – Digital Security in a Networked World, Bruce Schneier, ISBN 0-471-25311-1, http://www.counterpane.com/sandl.html

Notas:

Sites de Interesse

- CSIRT FAQ http://www.cert.org/csirts/csirt_faq.html
- Forming an Incident Response Team http://www.auscert.org.au/Information/Auscert_info/Papers/Forming_an_Incident_Response_Team.html
- Security Knowledge in Practice http://www.cert.org/security-improvement/skip.html
- Documentos, RFCs e sites relacionados http://www.nic.br/links.html

Notas: