Grupo de Resposta a Incidentes de Segurança – Bahia/Brasil
Ponto de Presença da RNP na Bahia
Universidade Federal da Bahia

CERT.Bahia <certbahia@pop-ba.rnp.br>

3º Fórum Brasileiro de CSIRTs
15 de Setembro de 2014

Sobre o CERT.Bahia

- Missão

  Auxiliar as instituições conectadas ao POP-BA/RNP e RedeCOMEP (ReMeSSA) na prevenção, detecção e tratamento dos incidentes de segurança, além de criar e disseminar boas práticas para uso e administração seguros das Tecnologias de Informação e Comunicação (TIC).

- Constituency
  - Instituições qualificadas na política de uso da RNP na Bahia
  - Instituições parceiras da ReMeSSA
- Site:
  - http://certbahia.pop-ba.rnp.br/

Serviços

- Educação e Treinamento
  - Palestras / Treinamento / Documentação
  - Campanhas de Segurança nas instituições
  - Eventos (EnSI, Netcafé, etc)
- Tratamento de Incidentes
  - Desenv. de Ferramentas (TRAIRA, L2M)
  - Acompanhamento e apoio
- Alertas de segurança
  - Sensores de monitoramento e alerta de incidentes de segurança

Contexto

- CSIRT de Coordenação/Backbone
- Rede Acadêmica
- Rede COMEP
- Geograficamente distribuídos
  - Clientes conectados por outros PoPs (DF e PE)
- Interior do estado
  - Infraestrutura
  - Recursos humanos

Como trabalhamos

- Regime dedicação parcial
- Colaboração entre PoP-BA e UFBA
- Parceria com outros grupos de segurança
  - CAIS
  - Honeynet.BR/CERT.BR
  - Dragon Research Group

Panorama atual dos clientes

- Equipes técnicas reduzidas
- Deficiência de conhecimento em segurança
- Nível de maturidade da infraestrutura é baixa
  - Sem políticas definidas
  - Sem ferramentas básicas
  - Sem plano de contingência
  - Sem processo de gestão de incidente de segurança
- **A segurança da informação não é vista de forma estratégica pela alta gestão**

Estratégias

- Reuniões virtuais
- Capacitação e treinamento
- Documentação de boas práticas de segurança
- Desenvolvimento de ferramentas
- Modelos de documentos de segurança

Reuniões virtuais

- Utilização do Webconf
- Alto custo de deslocamento
- Divulgação dirigida sobre questões de segurança da informação
- Interação com clientes (Chat ativo)
- Reuniões gravadas
- Em horário próximo do almoço (13:00)

Capacitação e treinamento

- Identificação das necessidades do cliente
- Modelagem do treinamento
- Treinamento sempre práticos
- Roteiro de laboratório prático se transformam em documentação (Guia)

Documentação de boas práticas de segurança

- Falta de referência de documentação
- Simplificar tecnologias complexas ou não acessíveis
- Evitar congestionamento de informação
- Estabelecer um processo de comunicação mais efetivo

Desenvolvimento de ferramentas

- Entender necessidade dos clientes antes do desenvolvimento
- Uso interno, mas focado na implantação em clientes
- Automatizar tarefas rotineiras
- Reuso de software livre

Modelos de documentos de segurança

- Documentação é a base do trabalho com segurança
- Falta de inspiração para iniciar documentação
- Uso interno, mas focado na implantação em clientes
- Traduzir/adaptar modelos em inglês para português (Ex: SANS)
- Evitar retrabalho

Exemplos

- NetCafé
- Conficker
- Segurança em IPV6
- DNSSEC
- Heartbleed
- Política de senhas

NetCafé

- Webconf
- Temas já abordados
  - Política de segurança
  - Gestão de Riscos de TI sob a ótica da NBR 27005
  - Hardening Linux
  - Segurança em aplicações web
  - Segurança em aplicações mobile
  - Segurança no BGP

Conficker

- Webconf
- Estratégia utilizada
  - Divulgação do problema
  - Analise de vulnerabilidade nos clientes
  - Criação de documentação de detecção e correção
  - Acompanhamento da solução dos clientes

Segurança em IPV6

- Webconf
- Estratégia utilizada
  - Divulgação dos vetores de problema
  - Suporte para dúvidas

DNSSEC

- Webconf
- Mini curso sobre “Boas práticas de implementação de DNS”
- Estratégia utilizada
  - Divulgação dos vetores de problema
  - Capacitação
  - Criação de documentação
  - Acompanhamento de implantação

Heartbleed

- Webconf
- Estratégia utilizada
  - Divulgação do problema
  - Analise de vulnerabilidade nos clientes
  - Criação de documentação de detecção e correção
  - Criação de modelo de justificativa para troca de certificado
  - Acompanhamento da solução dos clientes

Política de senha

- Webconf
- Estratégia utilizada
  - Divulgação do problema
  - Criação de template de documentação
  - Suporte para dúvidas

Estatísticas

- SSL Heartbleed
  - 8 clientes notificados
  - 8 clientes tratados
- DNSSEC
  - 3 instituições implementadas
- Treinamento
  - 130 técnicos treinados
  - 80% das instituições clientes já receberam treinamento

Próximos passos

- Bate papo periódico
- BCP38 (IP spoofing)
- Implementação de segurança de aplicações web
- Implementação de política de segurança
- Implementação da política de senha

Obrigado!!!
:-)

Perguntas?