Certificação Básica de Segurança da Informação

Proposta, Conceitos e Planejamento

Raphael Machado - Inmetro

Objetivo da Certificação

- Proporcionar uma avaliação simplificada de segurança, sem o formalismo de certificações internacionais como o Common Criteria e o FIPS 140-2, mas que permita atestar que “providências mínimas” foram tomadas com relação à segurança

Vantagens esperadas

Custo reduzido

Tempo reduzido de ensaios

Competência e metodologias já existentes nos laboratórios atuais

Alinhamento imediato a regulamentações técnicas existentes no Brasil

Cenário atual - mundo

CC, FIPS

CSPN, Austrália, China, Russia,...

Cenário atual - Brasil

- Diversos programas (não-harmonizados) de avaliação de segurança
  - Registrador Eletrônico de Ponto (Inmetro/MTB)
  - Equipamentos de Certifcação Digital ICP-Brasil (Inmetro/ITI)
  - Medidores Inteligentes (Inmetro-Dimel)
  - Defesa e APF (em elaboração)
- Vários reguladores e interessados em avaliação de segurança
- Existência de laboratórios com competência para avaliar segurança

Proposta

- Criar um programa “genérico” de avaliação de segurança
- Programa atenderia às necessidades da Defesa e da APF
- Outros programas em andamento convergiriam para a CBSI
  - Mesma rede de laboratórios (RBSeg)
  - Mesmo arcabouço normativo
  - Mesmas metodologias
- Possível referência para América Latina

Referências para a construção do programa

- Programas já em andamento
- CSPN (ANSSI)
- REMEQ-I

Nicho ocupado pela certificação CBSI

Formalismo “intermediário”: posicionado entre os métodos formais de certificações internacionais e procedimentos *ad hoc* de vários modelos de avaliação existentes.

Organização do programa

- Arcabouço normativo publicado pelo Inmetro
  - Organização do programa
  - Requisitos para laboratórios
- Estabelecimento de uma Rede Brasileira de Avaliações de Segurança da Informação - RBSeg
  - Harmonização
  - Treinamento
  - Ensaios de Proficiência
- Inmetro (Dmtic) atua como um “certificador” de conformidade
- Reguladores demandam produtos "certificados"

Organização do programa - Participantes

- Gestor do Programa (Inmetro)
  - Define as regras e funcionamento do programa
  - Coordena a rede de laboratórios
  - Valida avaliações por laboratórios e emite Relatório Final de Avaliação
- Patrocinador da Certificação (geralmente Fabricante)
  - Solicita avaliação do produto
  - Apoia avaliação do produto fornecendo informações complementares
- Laboratório de Avaliação
  - Realiza ensaios
  - Emite Relatório Técnico de Avaliação
- Demandante de Certificação (geralmente Regulador)
  - Define obrigatoriedade de certificação
  - Identifica riscos e Determina requisitos específicos e soluções aceitáveis

Abordagem/Filosofia do Programa

- Caracterizar o objeto avaliado e a abordagem seguida para alcançar a segurança
  - Fabricante mostra como tratou as questões de segurança
    - Riscos e modelos de ataque foram definidos
    - Requisitos e arquiteturas de segurança foram especificados
    - Soluções especificadas foram implementadas e testadas
  - Avaliar consistência (ex. MitM->autenticação->MAC->algoritmo->implementação)
- Possibilitar uma percepção prática a respeito da explorabilidade de eventuais vulnerabilidades de segurança
  - Laboratório (com competência demonstrada!) relata efeitos de tentativas de ataque
    - Garantir que os laboratórios possuam métodos, ferramentas e pessoal treinado/qualificado

Níveis de Avaliação

- Nível conceitual: sponsor apresenta documentação do objeto de avaliação em nível conceitual – e eventuais problemas/falhas/vulnerabilidades serão avaliados nesse nível.
  - Ensaios: análise de documentação
- Nível operacional: objeto é avaliado em operação, sujeito a testes funcionais e a testes de segurança tais como testes de penetração.
  - Ensaios: testes funcionais, testes caixa-preta, testes de penetração.
- Nível formal: objeto tem seus artefatos de projeto e implementação analisados – incluindo código fonte.
  - Ensaios: análise de software (apoiada por documentos de engenharia)

Desafios / atividades operacionais

- Articular laboratórios e reguladores
- Realizar treinamentos
- Realizar rodadas de ensaio de proficiência

Treinamento

- Treinamento básico sobre o programa
- Treinamento sobre sistema de qualidade
- Treinamentos técnicos

Documentos / Arcabouço Normativo

- Portaria Inmetro
  - Organização e funcionamento do Programa, criação da RBSeg
- Documentos da RBSeg
  - Guias de avaliação
  - Metodologias de ensaio
  - Rodadas de EB
- Portarias Reguladores
  - Obrigatoriedade certificação
  - Riscos, requisitos, soluções aceitáveis ...

Ensaio de proficiência

- Criar aplicação de software com “não-conformidades” e enviar a laboratórios
- Exemplos de não-conformidades
  - Problemas conceituais. Ex.: método de verificação de integridade falho
  - Inconsistência documentação-implementação. Ex.: funcionalidade não-declarada
  - Falha de implementação. Ex.: injeção de código.
- Avaliar resultados dos ensaios, evidências e formato de relatório