Universidade Federal do ABC

Segurança de Redes

Políticas de Segurança da Informação

Prof. João Henrique Kleinschmidt

Santo André-SP

Política de SI

Política de
Segurança da Informação (SI)
é a documentação das
decisões de SI

NIST Security Handbook

Política de SI

Política de SI

ou

Políticas de SI ?

Tipos de políticas

1. Programa de Política (organizacional)
   - Diretrizes da diretoria para criar um "programa" de segurança, estabelecer os seus objetivos e atribuir responsabilidades
2. Políticas temáticas (sobre algum assunto)
   - Questões específicas de interesse da organização
   - Decisões administrativas sobre
     - Política de privacidade de e-mail
     - Política de acesso à Internet, etc
3. Políticas de sistemas
   - Regras de segurança específicas para proteger sistemas (redes, máquinas, software) específicos

Implementação de Políticas

- Padrões
  - Uniformidade de uso de tecnologias, parâmetros ou procedimentos, para beneficiar a organização
    - Ex: Uso de Windows versão xxx
- Diretrizes
  - Em alguns casos, a aplicação de padrões não é possível, conveniente ou acessível (custos)
    - Ex: auxílio no desenvolvimento de procedimentos
- Procedimentos
  - Passos detalhados para serem seguidos pelos funcionários
    - Ex: Cuidados na criação de contas de e-mail

NBR/ISO 27002 Política de Segurança

- Cláusula de controle (área)
  - 5. Política de segurança da informação
  - Sub-cláusula: 5.1. Política de segurança da informação
  - Sub-sub-cláusula: 5.1.1. Documento da Política de SI
  - Sub-sub-cláusula: 5.1.2. Análise crítica e avaliação
- Objetivo de controle (da sub-cláusula 5.1)
  - Prover à direção uma orientação e apoio à SI
- Comentários adicionais (da sub-cláusula 5.1)
  - Convém que a direção estabeleça uma política clara e demonstre apoio e comprometimento com a SI através da emissão e manutenção de uma política de SI para toda a organização

NBR/ISO 27002
Política de Segurança

- Sub-sub-cláusula 5.1.1
- Documento da Política de SI
  - Convém que um documento da política seja aprovado pela direção, publicado e comunicado, de forma adequada para todos os funcionários
  - Convém que este expresse as preocupações da direção e estabeleça as linhas-mestras para a gestão da segurança da informação
  - No mínimo, convém que as seguintes orientações sejam incluídas:

NBR/ISO 27002
Política de Segurança

1. Definição da SI, resumo das metas e escopo e a importância da segurança como um mecanismo que habilita o compartilhamento da informação
2. Declaração do comprometimento da alta direção, apoiando as metas e os princípios da SI
3. Breve explanação das políticas, princípios, padrões e requisitos de conformidade de importância específica para a organização
   - Conformidade com a legislação e cláusulas contratuais
   - Requisitos na educação de segurança
   - Prevenção e detecção de vírus e software maliciosos
   - Consequências das violações na política de SI

NBR/ISO 27002
Política de Segurança

4. Definição das responsabilidades gerais e específicas na gestão da SI, incluindo os registros de incidentes de segurança
5. Referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras que convém que os usuários sigam
6. Convém que esta política seja comunicada através de toda a organização para os usuários na forma que seja relevante, acessível e compreensível para o leitor

NBR/ISO 27002 Política de Segurança

- Sub-sub-cláusula 5.1.2
- Análise crítica e avaliação
  - Convém que a política tenha um gestor que seja responsável por sua manutenção e análise crítica, de acordo com um processo definido
  - Convém que este processo garanta que a análise crítica ocorra como decorrência de qualquer mudança que venha a afetar a avaliação de risco original, como
    - Um incidente de segurança significativo
    - Novas vulnerabilidades
    - Mudanças organizacionais ou na infra-estrutura técnica
  - Convém que sejam agendadas as seguintes análises críticas periódicas:

NBR/ISO 27002
Política de Segurança

1. Efetividade da política, demonstrada pelo tipo, volume e impacto dos incidentes de segurança registrados
2. Custo e impacto dos controles na eficiência do negócio
3. Efeitos das mudanças na tecnologia

Política: componentes

- Objetivo
  - Por que a política?
- Escopo
  - Toda a organização ou parte dela?
- Responsabilidades
  - Quem são as pessoas? Estrutura formal?
- Conformidade
  - Como fiscalizar"?
  - O que acontece para quem não cumprir?
    - Intencional, não-intencional (falta de treinamento?)

Políticas temáticas

- Abrangem a organização inteira e tratam de assuntos específicos de interesse da organização
- Deve ser "bancada" por alguma gerência sênior
  - Quanto mais controverso o tema, mais importante deve ser a pessoa que "banca" a política
- O aparecimento de novas tecnologias e ameaças requer novas políticas temáticas
- Exemplos
  - Planos de contingência
  - Gerenciamento de riscos
  - Acesso à Internet (só nos horários rígidos de trabalho?)
  - Uso de e-mail (é permitido arquivo anexo?)
  - Uso de programas de mensagens instantâneas
  - Uso de software não oficial

Políticas temáticas: componentes

- Enunciado da política
- Posição oficial da organização sobre a política
- Aplicabilidade
  - Onde, como, quando, quem?
- Papéis e responsabilidades
- Conformidade
- Pontos de contato
- Informações adicionais

Políticas de sistemas

- Programa de política e políticas temáticas tratam questões abrangentes para toda a organização
- Não dizem quais ações devem ser tomadas, como devem ser feitas as configurações, etc.
- Políticas de sistemas tratam de problemas específicos, para segurança de sistemas específicos
- Modelo de políticas de sistemas
  - Objetivos de segurança
  - Regras operacionais de segurança
  - Implementação da política

Políticas de sistemas
Objetivos de segurança

- Requer análise da necessidade de integridade, confidencialidade e disponibilidade
- Deve ser concreto e bem definido
- Série de declarações que descrevem ações significativas sobre recursos específicos
- Devem ser baseados nos requisitos de missão ou função do sistema
- Devem garantir que a política seja aplicável
- Restrições devem ser consideradas
  - Operacionais, técnicas, orçamentárias, etc

Políticas de sistemas
Regras operacionais

- Regras de operação devem ser definidas
  - Quem pode ter acesso físico ao sistema?
  - Quem pode consultar, alterar, remover as informações mantidas pelo sistema?
  - Quem pode ligar/desligar equipamentos?
- Nível de formalidade
  - Políticas formais são mais facilmente seguidas
- Grau de detalhamento
  - Alto: facilita a detecção de violação, mas pode inviabilizar a sua implementação
  - Nem todos os sistemas precisam do mesmo grau de detalhes
  - Exemplos de sistemas com detalhamento alto
    - Controle de acesso, uso aceitável, consequências da violação

Políticas de sistemas Implementação

- A tecnologia desempenha um papel importante nas políticas de sistemas, mas não "único"
- Questões não tecnológicas não devem ser desprezadas
  - Ex: Documentos confidenciais somente podem ser impressos na impressora XYZ
    - Como garantir que pessoas não autorizadas tenham acesso físico à impressora? (ou seja, elas podem não ter acesso aos arquivos, mas também devem ser mantidas longe do papel)
- Exemplos
  - Proibir telefones de ligar para certos números
  - Uso de IDS para auxílio da detecção de intrusões
  - Configurar PCs para não dar boot por unidade externa (pen-drive, CD/DVD, HD externo)
  - Proibir (ou limitar) o uso de modems nas máquinas

Políticas de Sistemas Componentes

- Objetivo
- Escopo
- Política
  - Pontos específicos que devem ser seguidos
- Imposição e conformidade
- Glossário / definições
- Histórico de revisões

Exemplo: SANS Institute Política para roteador

- Objetivo
  - Este documento descreve uma configuração mínima de segurança para todos os roteadores e switches conectados na rede de produção da <organização>
- Escopo
  - Todos os roteadores e switches conectados na rede de produção da <organização> são afetados
  - Roteadores em laboratórios internos/seguros são excluídos
  - Roteadores dentro da DMZ devem seguir política específica

Exemplo: SANS Institute Política para roteador (CISCO)

- Política: padrões de configuração

1. Contas locais não devem ser configuradas nos roteadores. Roteadores devem usar TACACS+ (AAA) para todas as autenticações de usuários
2. A senha de "enable" deve ser criptografada
3. Deve ser desabilitado
   - Broadcast IP direcionado (sub-redes que o host não está)
   - Recepção de pacotes com endereços inválidos (ex: RFC1918)
   - Serviços "pequenos" TCP e UDP (echo, chargen, daytime, discard)
   - Roteamento pela fonte (source routing)
   - Serviços web rodando no roteador
4. Não usar comunidade SNMP public (criar padrões)
5. Regras de acesso devem ser definidas pela necessidade
6. ...

Exemplo: SANS Institute Política para roteador (CISCO)

- Imposição / Conformidade
  - Qualquer funcionário que violar esta política e for descoberto deve ser repreendido, incluindo, em casos graves, a demissão

CISCO: senha de "enable"

- Problema de segurança em roteadores CISCO: pessoal não se preocupa em criptografar as senhas armazenadas nas configurações do roteador
- Logando em um roteador e digitado a senha de "enable", eu dou o comando "show running-config" (mostra as configurações)
  - line con 0
  - password gamkCiSC0rout3r
  - login
  - transport input none
  - stopbits 1
  - line vty 0 4
  - password telnetRtC1sco
  - login
- Senha de telnet = telnetRtC1sco; senha do console = gamkCiSC0rout3r

Exemplo: SANS Institute Diretrizes para anti-vírus

- Sempre usar o anti-vírus padrão da organização
- **NUNCA** abrir arquivos ou macros anexados a um email de alguém desconhecido ou suspeito
- Remover spam, correntes, etc, sem encaminhar
- Nunca transferir arquivos de fontes desconhecidas ou suspeitas
- Evitar compartilhamento de disco com permissão de leitura/escrita a não ser que haja um requisito explícito do negócio para fazer isso
- Sempre escanear pen-drives de fontes desconhecidas (ou conhecidas) antes de usá-los
- Fazer cópias de segurança das configurações do sistema regularmente e armazenar em local seguro
- Se algum teste entrar em conflito com o anti-vírus, desabilitar momentaneamente e depois retornar
- Atualizar constantemente a base de dados do programa anti-vírus corporativo

Política de Segurança da UFABC

- POSIC UFABC 2018
  - https://nti.ufabc.edu.br/seguranca-da-informacao

Ferramentas de Políticas de SI

- SANS
  - Projeto de Políticas de Segurança
    - www.sans.org/resources/policies
    - Templates para políticas de segurança