Algumas Leis da Segurança

Marcos Aurelio Pchek Laureano
laureano@ppgia.pucpr.br

Roteiro

- Leis Fundamentais
- Leis Imutáveis
- Seus significados
- Sua Importância

Algumas Leis da Segurança

- As leis
  - Fundamentais
  - As 10 Leis Imutáveis da Segurança
- Servem como guia e não como verdades absolutas

Leis Fundamentais

- São 10 as leis fundamentais
- Deve-se observar estas leis sempre que:
  - iniciar um novo projeto de software
  - iniciar um novo projeto de infra-estrutura
- Estas leis estão relacionadas com tecnologia e processos

Lei Fundamental 01

- Segurança do lado do Cliente não funciona
  - Segurança do lado do cliente é segurança implementada unicamente no cliente;
  - O usuário sempre tem a oportunidade de quebrar a segurança, pois ele está no controle da máquina;
  - A segurança no lado do cliente não fornecerá segurança se tempo e recursos estiverem disponíveis ao atacante.

Lei Fundamental 02

- Você não pode trocar chaves de criptografia com segurança sem uma informação compartilhada.
  - As informações compartilhadas são usadas para validar máquinas antes da criação da sessão;
  - Você pode trocar chaves privadas compartilhadas ou usar SSL (*Secure Socket Layer*) através do seu navegador;
  - As trocas de chaves são vulneráveis a ataques do tipo *man-in-the-middle* (homem no meio).

Lei Fundamental 03

- Não existe proteção total contra código malicioso.
  - Os produtos de software não são perfeitos;
  - Os programas de detecção de vírus e cavalo de tróia se baseiam em arquivos de assinatura;
  - Pequenas mudanças na assinatura de código podem produzir uma variação não detectável (até que a nova assinatura seja publicada).

Lei Fundamental 04

- Qualquer código malicioso pode ser completamente modificado para evitar detecção de assinatura.
  - Os atacantes podem mudar a identidade ou assinatura de um arquivo rapidamente;
  - Os atacantes podem usar compactação, criptografia e senhas para mudar a aparência do código;
  - Você não tem como se proteger contra cada modificação possível.

Lei Fundamental 05

- Os firewalls não podem protegê-lo cem por cento contra ataques.
  - Os firewalls podem ser software ou hardware, ou ambos;
  - A principal função de um firewall é filtrar pacotes que chegam e saem;
  - Ataques sucessivos são possíveis como resultado de regras e políticas incorretas, e de problemas de manutenção.

Lei Fundamental 06

- Qualquer IDS pode ser burlado.
  - Os sistemas de detecção de intrusão (IDS) freqüentemente são projetos passivos;
  - É difícil para um atacante detectar a presença de um IDS quando está sondando;
  - Um IDS está sujeito à configuração incorreta e falta de manutenção. Essas condições podem criar oportunidades de ataque.

Lei Fundamental 07

- Algoritmos criptográficos secretos não são seguros.
  - Criptografia é difícil;
  - A maioria da criptografia não é revisada e testada o bastante antes de ser lançada;
  - Algoritmos comuns estão em uso em diversas áreas. Eles são difíceis, mas não impossíveis de atacar.

Lei Fundamental 08

- Se uma chave não for necessária, você não tem criptografia – você tem codificação.
  - As chaves precisam ser mantidas em segredo ou não existe segurança;
  - As senhas não podem ser armazenadas com segurança no cliente a menos que haja outra senha para protegê-las (requer um segundo mecanismo para fornece segurança);
  - Se uma senha não é criptografada ou não está protegida quando armazenada, ele não é segura;

Lei Fundamental 09

- Para que um sistema comece a ser considerado seguro, ele precisa submeter-se a uma auditoria de segurança independente.
  - A auditoria é o começo de uma boa análise de sistemas de segurança;
  - Os sistemas de segurança, muitas vezes, não são revisados correta ou completamente, permitindo furos;
  - Verificação externa é vital para a defesa; a falta dela é um convite a ataques.

Lei Fundamental 10

- Segurança através de obscuridade não funciona.
  - Ocultar não é proteger;
  - É necessária proteção ativa;
  - O uso da obscuridade por si só convida ao comprometimento.

As 10 Leis Imutáveis da Segurança

- Proposta por Scott Culp, gerente central de resposta de segurança da Microsoft
- Estas leis estão mais relacionadas com pessoas

1ª Lei Imutável da Segurança

- Se um malfeitor consegue te persuadir a executar um programa no seu computador, este computador deixa de ser seu.
  - O conselho de - jamais executar arquivos de estranhos - merece, justamente, o primeiro lugar nessa lista.Este é o principal problema enfrentado por usuários com excesso de confiança. Pessoas más podem facilmente tomar o controle do seu computador se te convencerem a executar os seus (deles) programas.

2ª Lei Imutável da Segurança

1. Se um malfeitor consegue alterar o sistema operacional do seu computador, este computador deixa de ser seu.
   1. Programas executam comandos que são interpretados pelo sistema operacional do computador.
   2. Se um programa pode prejudicar seu funcionamento, imagine o que uma alteração no próprio sistema operacional pode fazer.

3ª Lei Imutável da Segurança

- Se um malfeitor tiver acesso físico irrestrito ao seu computador, este computador deixa de ser seu.
  - Nenhum sistema lógico de segurança é suficientemente bom para proteger um computador se esse estiver acessível fisicamente.
  - Milhares de ameaças que surgem neste cenário
    - jogar o computador pela janela
    - abrir o equipamento
    - conectar dispositivos

4ª Lei Imutável da Segurança

- Se você permitir que um malfeitor envie programas para seu website, este website deixa de ser seu.
  - Um webserver possui um sistema operacional e programas que respondem pela tarefa de "servir" páginas na internet.
  - Se você permitir que um visitante instrua este computador a executar seus comandos, estará sob a mesma vulnerabilidade da primeira lei.

5ª Lei Imutável da Segurança

- Senhas fracas triunfam sobre a mais forte segurança.
  - Uma senha é, por definição, secreta.
    - Serve para dizer se você é quem diz ser.
    - Deixar alguém usar sua senha é como permitir que assumam sua identidade.
    - Qualquer ação tomada, será de sua responsabilidade.
  - Sem falar nos que nem mesmo “têm” uma senha
    - Senha default (de fábrica),senha igual ao login.
    - Senhas óbvias, nomes, datas de aniversário..

6ª Lei Imutável da Segurança

- Um sistema é tão seguro quanto seu administrador é confiável.
  - Ele possui controle total sobre o sistema.
  - A confiança no responsável pela administração dos sistemas de segurança deve ser apoiada por mecanismos de monitoração de acesso exclusivo dos auditores.

7ª Lei Imutável da Segurança

- Dados criptografados são tão seguros quanto à senha usada para sua decriptação.
  - Um sistema - por mais forte que seja - perde seu valor caso a senha usada esteja disponível para terceiros.
  - Ao invés de gravá-los no próprio computador, procure guardá-los em um disquete (e leve este disquete para um lugar seguro).
  - Jamais as anotem em cadernos, *post-it*, *palms* etc.

8ª Lei Imutável da Segurança

- Um antivírus desatualizado é apenas ligeiramente melhor do que nenhum antivírus.
  - As mais eficientes tecnologias de combate aos vírus são baseadas em assinaturas
  - As assinaturas podem mudar, tornando ineficaz o antivírus a novas pragas

9ª Lei Imutável da Segurança

- O anonimato absoluto não existe, nem dentro, nem fora da Internet.
  - Em uma conversa em um elevador você já deixou disponível, de forma aproximada, seu peso, sua altura, sua idade, seu *status* na sociedade, seu poder aquisitivo, sua origem...
  - Computadores que conversam com outros computadores deixam as informações sobre a comunicação ou seus próprios sistemas armazenadas no interlocutor ou em pontos intermediários.

10ª Lei Imutável da Segurança

- Tecnologia não é um remédio para todos os males. OU Tecnologia não é uma panacéia.
  - Não existe soluções milagrosas, perfeitas, definitivas e de baixo custo.
  - Nenhum software ou hardware é suficientemente bom para proteger eternamente seus sistemas computacionais.
  - Segurança não se consegue só com tecnologia nem só com atitudes.
  - Segurança não é um produto, é um processo (contínuo).

Então....

- Dúvidas ??
- Perguntas ??
- Comentários ??