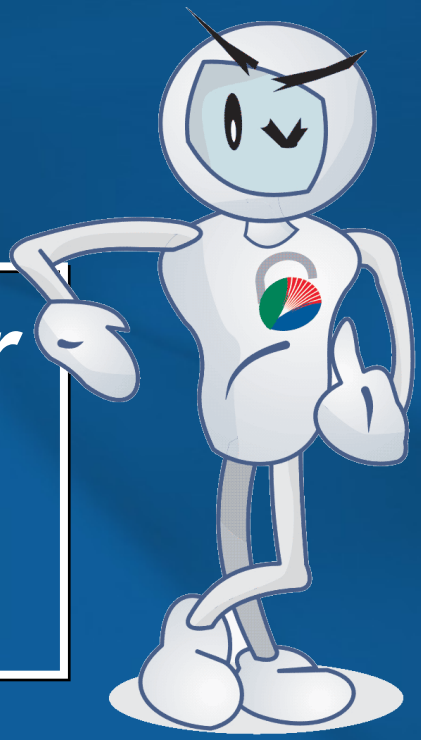
Ambiente de Segurança Corporativa

Francisco José Barreto Nunes - MSc., CISM, CSSLP

Banco do Nordeste

Institucionalizar Segurança no RUP-BNB



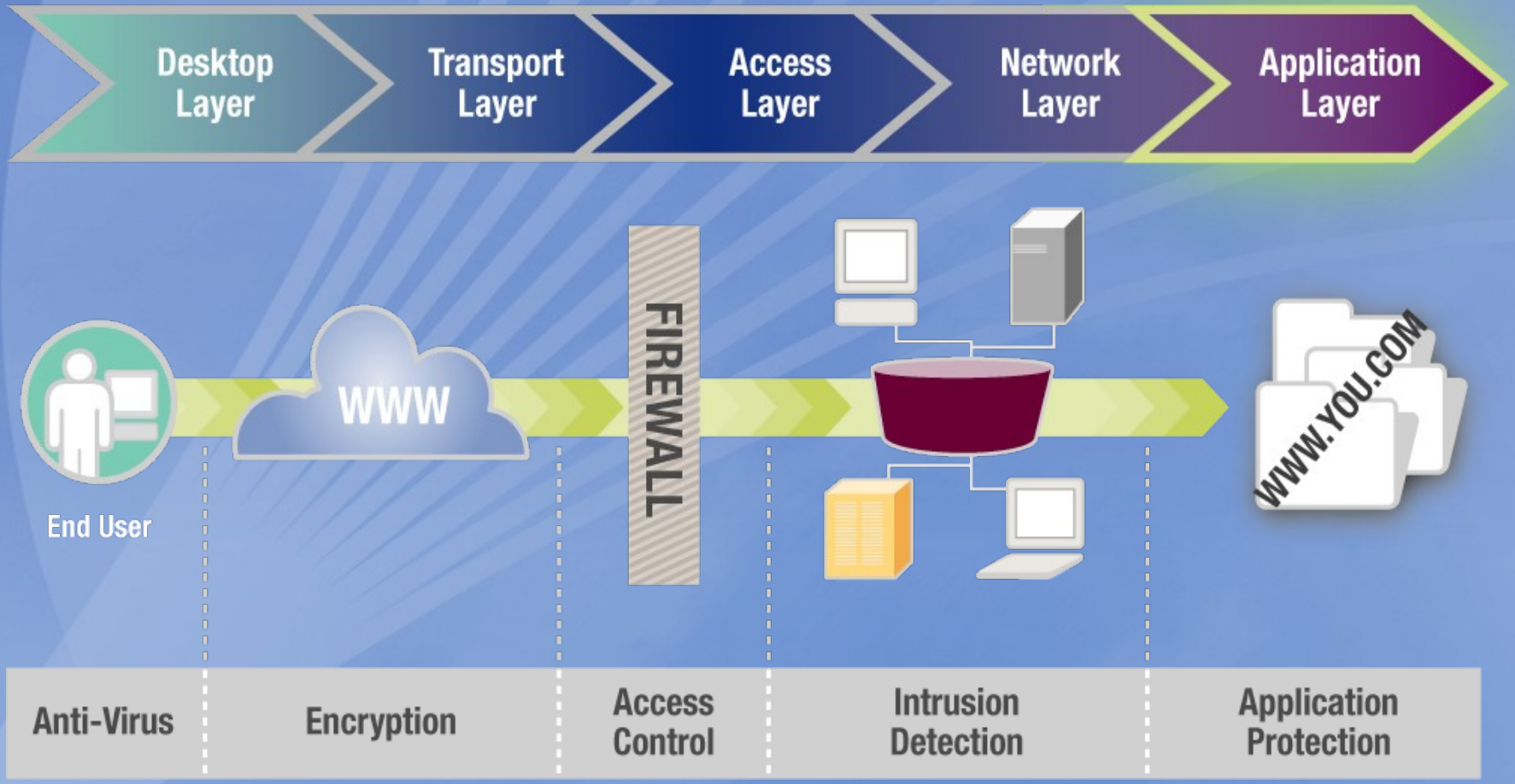
Agenda

- Desafio;
- Objetivos;
- Benefícios;
- Cronograma;
- Resultados atuais;
- Ações planejadas; e
- Lições aprendidas.

Banco do Nordeste

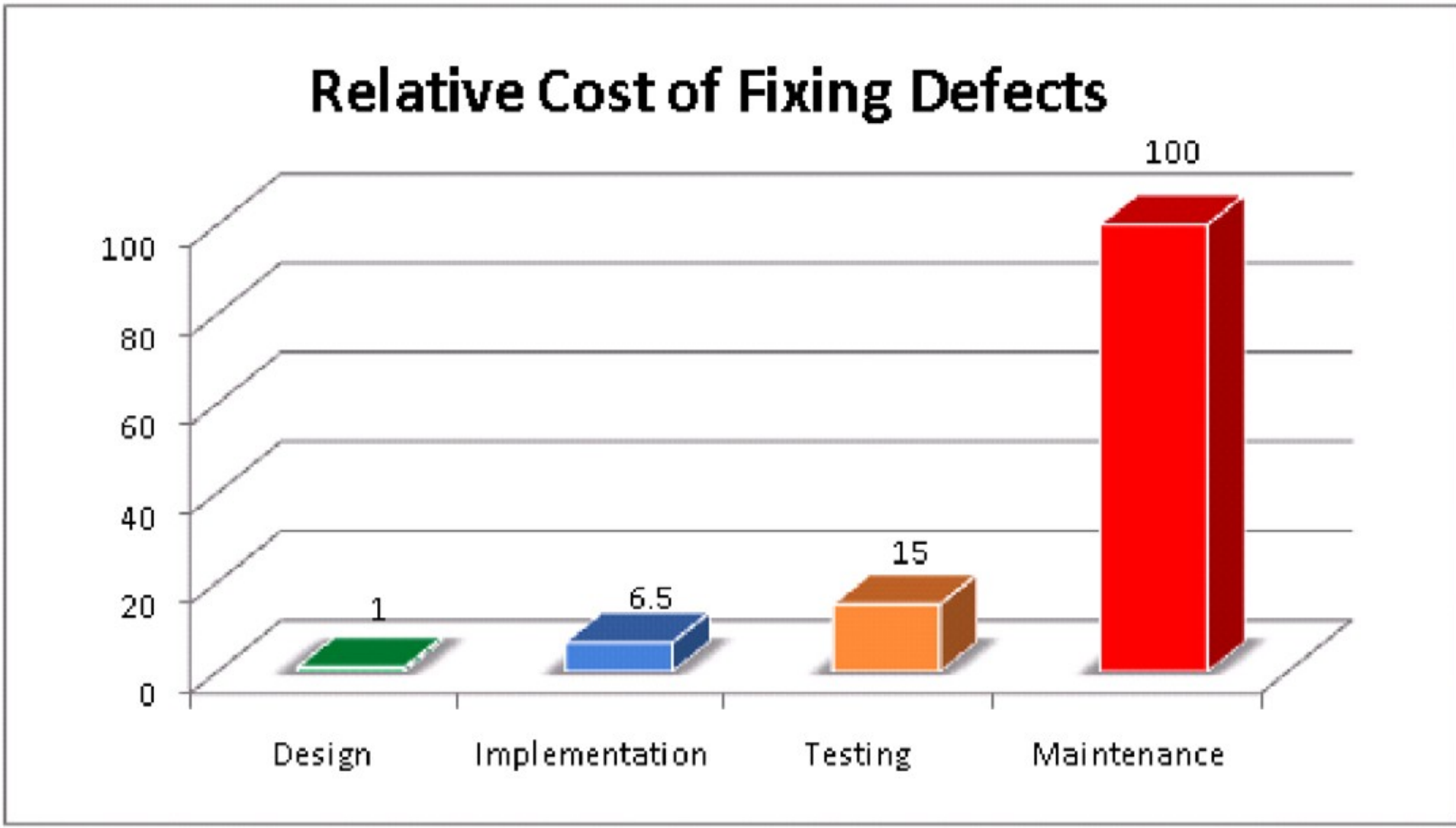
Desafio

70% dos ataques



Fonte: GARTNER

Desafio



Fonte: Implementing Software Inspections, IBM Systems Sciences Institute

Objetivos

- Otimizar o uso de recursos de acordo com as necessidades de segurança (análise de riscos);
- Melhorar a segurança dos aplicativos; e
- Reorganizar práticas de desenvolvimento visando atender requisitos de segurança.

Benefícios

- Melhoria na produtividade dos colaboradores;
- Elevar satisfação dos clientes; e
- Mitigar possíveis perdas financeiras e danos à imagem, decorrentes de incidentes de indisponibilidade, perda de confidencialidade, e perda de integridade das informações.

Cronograma

- Etapa 1: (Concluída)
  - Conscientização e educação.
- Etapa 2: (Em fase de implantação)
  - Organizar atividades de segurança de software no RUP-BNB; (Em fase final)
  - Realizar projeto piloto; e
  - Avaliar resultado, aperfeiçoar atividades.

Resultados atuais

- Lançamento de curso on-line “Introdução à segurança de software”;
- Preparação de material para palestra de conscientização aos funcionários;
- Homologação de diretriz no processo com conjunto de requisitos de segurança, baseado na ISO/IEC 15408 (Parte 2);

Resultados atuais

- Lançamento do guia de orientação de segurança de aplicativo: “Falhas de Autenticação e de Controle de Sessão”; e

- Inclusão de seções sobre segurança nos artefatos: Visão e Especificação Suplementar.

Resultados atuais

- Atividades de segurança propostas:
  - Identificar necessidades de segurança;
  - Consultar guias de orientação de segurança de aplicativo;
  - Definir requisitos de segurança; e
  - Obter acordo sobre requisitos de segurança.

Ações planejadas

- Realizar projeto piloto;
- Analisar resultado e aperfeiçoar atividades;
- Elaborar novos guias de orientação:
  - Exploração de Privilégio, Injeção de Código, Manipulação de Recurso, Vazamento de Informação, e Criptografia Insegura;

Ações planejadas

- Atualizar conteúdo do curso on-line; e

- Identificar nova necessidade de segurança no RUP-BNB e iniciar novo projeto:
  - Teste de segurança; ou
  - Análise de risco.

Lições aprendidas

- Equipe de desenvolvimento precisa pensar como as funcionalidades poderiam ser comprometidas ou usurpadas;

- "*Abuse Cases*" mostraram-se, inicialmente, ineficazes devido ao desconhecimento e inexperiência em segurança de software (maior volume de trabalho – impacto na produtividade!);

- Guias de orientação são valiosas ferramentas de conscientização e integração;

Lições aprendidas

- Cada guia foi pensando a partir da organização de informações sobre vulnerabilidades e ameaças de segurança de software coletadas em:
  - www.owasp.org
  - www.webappsec.org/projects/threat/
  - http://measurablesecurity.mitre.org

- Os guias contribuem para a integração do projeto, arquitetura e teste com a estruturação dos requisitos de segurança, permitindo identificar o impacto das vulnerabilidades e ameaças de forma a evitar que problemas de segurança passem despercebidos.

Ambiente de Segurança Corporativa

franzenunes@bnb.gov.br
fcojbn@yahoo.com.br

Banco do Nordeste

Obrigado!