Ambiente de Segurança Corporativa

Banco do Nordeste

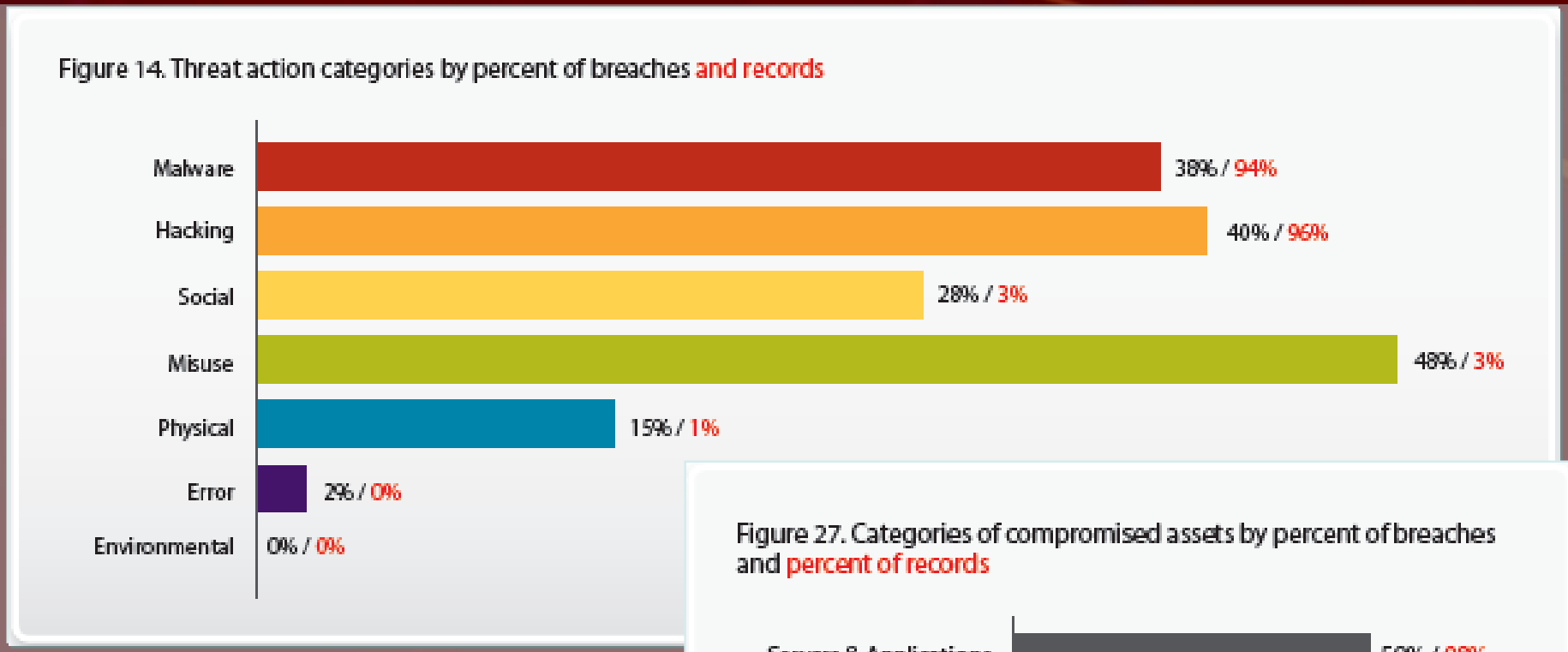
Institucionalizar Segurança no RUP-BNB

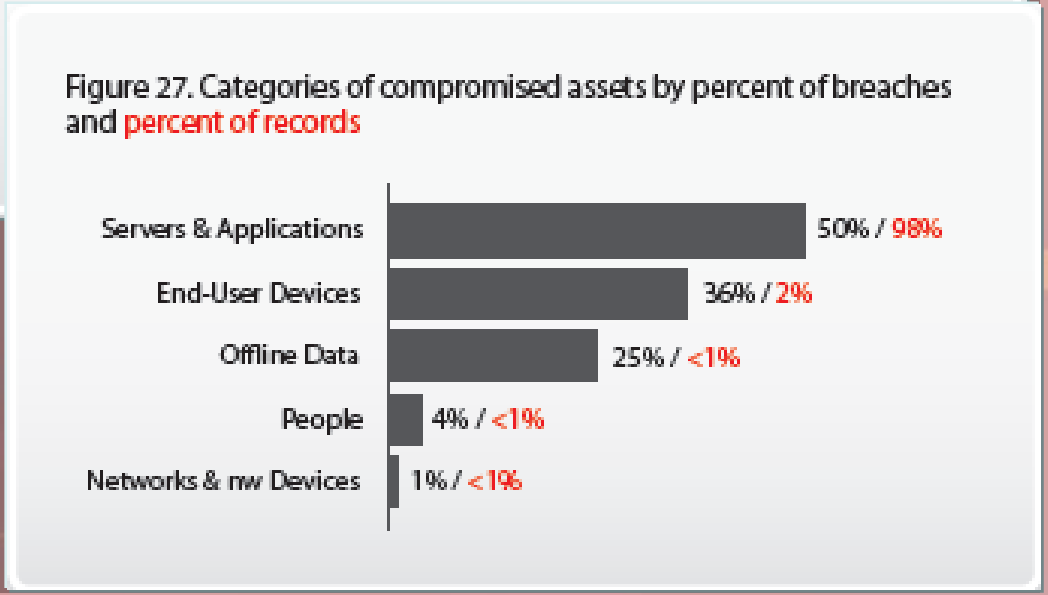
Francisco José Barreto Nunes - MSc., CISM, CSSLP

Agenda

- Desafio;
- Objetivos;
- Cronograma;
- Projeto Piloto;
- Resultados do Piloto;
- Resultados do Projeto;
- Dificuldades;
- Lições Aprendidas.

Desafio





Fonte:
Verizon Data Breach Investigations Report

Objetivos

- Melhorar a segurança, e por conseguinte a qualidade, de aplicativos.
- Otimizar o uso de recursos de acordo com as necessidades de segurança.
- Reorganizar práticas de desenvolvimento visando atender requisitos de segurança.
- Realizar projeto piloto para validar conjunto de ações de segurança a serem executadas na disciplina Requisitos.
- Avaliar resultado, aperfeiçoar as ações de segurança e planejar novas necessidades de segurança dentro da metodologia de desenvolvimento RUP-BNB.

Cronograma

- Etapa 1: (Concluída)
  - Conscientização e educação.
- Etapa 2: (Concluída e Aprovada)
  - Adaptar artefatos do RUP-BNB;
  - Organizar ações de segurança na disciplina Requisitos.
- Etapa 3: (Concluída)
  - Realizar projeto piloto;
  - Avaliar resultado, aperfeiçoar ações de segurança;
  - Identificar novas necessidades.

Projeto Piloto

- Processo de cobrança extrajudicial terceirizada:
  - Operações em cobrança, Consolidação de dados, Integração com outros sistemas.
- Principais Atividades:
  - Realizar reunião com principais envolvidos;
  - Definir premissas:
    - Equipe técnica conhece novidades de segurança no RUP-BNB;
    - Identifica o que for mais crítico para funcionamento seguro do aplicativo e prioriza necessidades de segurança.

Projeto Piloto

- Principais Atividades:
  - Definir responsabilidades pelas ações de segurança;
  - Organizar informações sobre o novo sistema;
  - Identificar pontos mais críticos (ação “Identificar Necessidades de Segurança”);
  - Indicar impactos para pontos críticos, como: imagem, confidencialidade, ou resultado financeiro;
  - Formalizar principais necessidades de segurança.

Projeto Piloto

- Principais Atividades:
  - Utilizar “Guia de Orientação” e diretrizes de segurança para subsidiar a descrição de alguns requisitos;
  - Transformar necessidades em requisitos de segurança inseridos no artefato Especificação Suplementar (ação “Capturar Requisitos de Segurança”);
  - Identificar funcionalidades críticas do sistema que precisariam continuar ativas mesmo em cenários de falha.

Resultados do Piloto

- Formalização das necessidades de segurança:
  i. Acompanhamento/gerenciamento das operações em cobrança;
  ii. Assegurar privacidade e conformidade com leis e regulamentações, como lei do sigilo fiscal;
  iii. Assegurar contínua comunicação com empresa terceirizada;
  iv. Assegurar acurácia nos cálculos; e
  v. Controlar a segurança nas interfaces e integrações com outros sistemas.

Resultados do Piloto

- Aprovação de requisitos de segurança, por exemplo:
  i. Controle de acesso ocorre conforme o nível de sigilo das informações manipuladas pelo sistema;
  ii. Controle de entrada de dados por usuários e ou interface utilizará validações para os tipos de dados, ou expressões regulares, entre outras técnicas para evitar a entrada de dados inconsistentes ou scripts com comandos invasores;
  iii. Utiliza canais seguros, a partir de controles nas funcionalidades consideradas críticas e na comunicação de informações confidenciais que mantém sua privacidade e integridade conforme regras do sigilo bancário.

Resultados do Projeto

- Maior percepção dos envolvidos sobre importância de tratar a segurança dentro do ciclo de vida de software;
- Discussão e sugestão de assuntos que, direta ou indiretamente, repercutiam com a confidencialidade, integridade e disponibilidade das informações:
    i. Inserção de matriz de responsabilidades, conhecida como "RACI chart".
- Atualização, no novo "Plano de Testes", das abordagens "Teste de Segurança e de Controle de Acesso" e "Teste de Tolerância a Falhas e de Recuperação";
- Ações de segurança na disciplina Requisitos provaram-se eficazes e institucionalizáveis, uma vez que gerou resultados esperados e atingiu os objetivos iniciais.

Dificuldades

Banco do Nordeste

- Elevar conhecimento sobre segurança da informação e segurança de software entre colaboradores envolvidos com o processo de desenvolvimento;
- Definir as responsabilidades pelas ações de segurança;
- Transcrever requisitos de segurança em casos de uso, cenários arquiteturais, controles (rotinas) programáveis;
- Verificar e validar requisitos de segurança.

Lições Aprendidas

- Apresentar vantagens da integração de segurança no projeto;

- Assegurar frequente participação de usuários nas discussões de segurança:

  i. Alinhamento de percepções, Compreensão de necessidades;

  ii. Maior confiança sobre o projeto e o funcionamento do sistema.

Lições Aprendidas

- Sempre avaliar / conversar sobre novos riscos potenciais;

- Envolver pessoa(s) com conhecimento em segurança de software e em processo de desenvolvimento, com o objetivo de orientar e prestar o apoio necessário, até que as equipes de sistemas estejam capacitadas a conduzirem, de forma autônoma, as ações de segurança.

Dúvidas? Muito obrigado!

Banco do Nordeste

www.bnb.gov.br – cliente consulta | ouvidoria - 0800 728 30 30

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