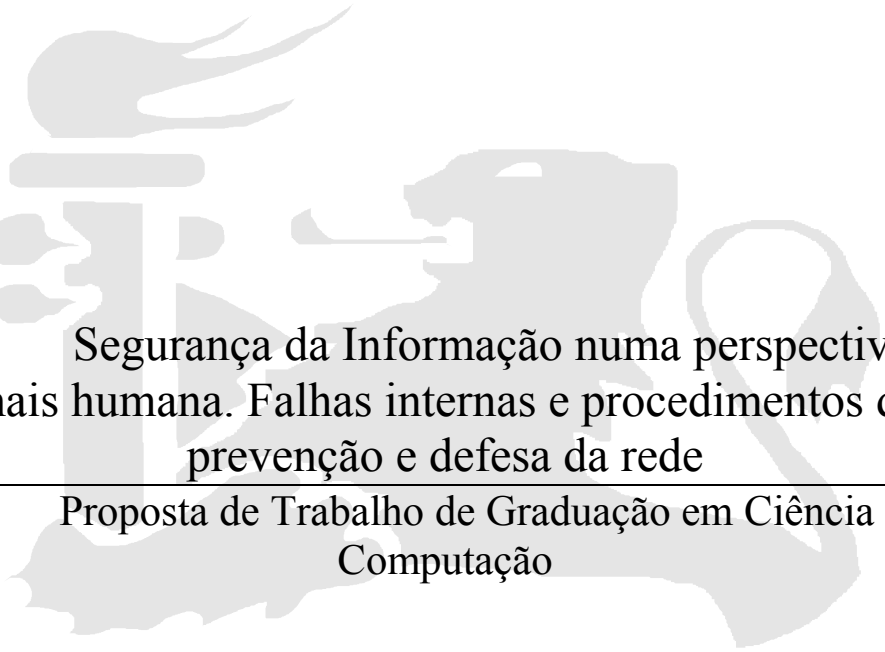
UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE INFORMÁTICA



Segurança da Informação numa perspectiva mais humana. Falhas internas e procedimentos de prevenção e defesa da rede

Proposta de Trabalho de Graduação em Ciência da Computação

Aluno: Felipe Ribeiro Machado (frm@cin.ufpe.br).
Orientador: Ruy José Guerra Barretto de Queiroz (ruy@cin.ufpe.br).

Recife, 17/03/2009

Contexto

Quando ocorrem ataques a redes privadas, são percebidas ações provindas desse ataque que alteram o funcionamento normal do sistema e logo se vêm a tona as complicações causadas por este ataque a rede. A percepção por ações preventivas são percebidas e então concluídas de fato as consequências sérias e a capacidade de prejudicar o funcionamento dos procedimentos comuns de uma instituição. Estas consequências são percebidas não apenas quando por exemplo serviços essenciais param ou dados críticos são perdidos, mas até simplesmente quando serviços simples, porém que seriam a produção diária, deixam a equipe de produção com rendimento abaixo do esperado ou até sem quaisquer aproveitamentos. Alguns exemplos podem ser percebidos. O DETRAN-PE, Departamento Estadual de Transportes de Pernambuco, no início de Fevereiro de 2009, teve seus procedimentos parados por lentidão e falhas durante requisições de serviços internos. O resultado disto foi que seus serviços e atendimentos permaneceram parados por aproximadamente 3 dias – tempo suficiente para a imprensa estampar as "Matérias de capa" dos jornais. Em 31 de Janeiro de 2008, um dos servidores Unix da Fannie Mae parou de responder as requisições a ele realizadas. Milhões de dólares foram perdidos juntos aos dados tendo em vista que o problema detectado em um único servidor, que já seria uma perda considerável, em pouco tempo já se espalhara por todos 4.000 servidores que nesta instituição se encontravam. Os trabalhos dela então foram parados.

Ambas questões foram resultados de ataques maliciosos provocados por vírus e, como percebido, ocorreram sérias consequências visando o negócio das empresas. Algumas questões entretanto valem ser destacadas e debatidas. Qual seria o motivo destes ataques? Será que ações preventivas poderiam ser tomadas a fim de evitar tais ataques ou simplesmente amenizar tais consequencias? Haveriam programas capazes de combater tais investidas por softwares maliciosos?

O vírus que infectou a rede do DETRAN-PE foi o Conficker, responsável pela infecção até 26 de janeiro de 2009 a mais de 15 milhões de máquinas pelo mundo. Não foi constatado de fato o motivo, a causa, desta infecção. Sabe-se porém que a forma mais comum de se pôr o vírus Conficker numa rede interna é através de pen drives infectados. Isto realmente é a idéia mais aceita no caso do DETRAN-PE. A prevenção contra ele seria uma atualização de segurança, que por um considerável

tempo já está disponível na rede mundial de computadores, fornecida gratuitamente pela Microsoft a quem adquire seus produtos. Esta atualização evitaria quaisquer ações deste vírus.

Já em relação ao problema percebido nos servidores Unix da Fannie Mae, o que causou tamanhos estragos e prejuízos foi um script malicioso criado intencionalmente por um ex-funcionário da empresa após sua demissão. Como citado anteriormente, milhões de dólares foram os prejuízos contabilizados pela empresa que viu seus mais de 4.000 servidores serem infectados à partir do primeiro caso. Todo o sistema de proteção foi desativado pelo vírus. Este apenas foi desativado uma semana depois por outro funcionário que descobriu o script o desabilitando.

São vários os casos de empresas vítimas de infecções capazes de causar prejuízos imensuráveis. As razões destas infecções são as mais variadas: má-intenção de funcionários com acessos a informações sensíveis da empresa, ignorância no tratamento de certas “armadilhas” pelos funcionários - “armadilhas” estas já comuns em crimes cibernéticos - ou simplesmente falta de treinamento interno aos funcionários sobre a utilização do sistema e boas práticas. No combate a estas causas de invasões citadas, percebe-se uma predominância de falha humana interna ao sistema.

Objetivo

Esta monografia buscará explanar tais falhas básicas de segurança citando procedimentos que fragilizarão os dados da empresa e tentando citar as consequências sérias capazes de serem provocadas por essas falhas. Tudo isto será demonstrado através de exemplos práticos ocorridos ou de montagens de cenários possíveis e tentadas análises sobre as falhas ocorridas. Será dado um foco especial a falhas internas caracterizadas pela não massificação de procedimentos básicos de prevenção ou simplesmente falta de aplicação desses procedimentos pelos funcionários ou usuários do sistema interno da empresa. Como destacado também, haverá um foco para as pessoas internas da empresa e buscada uma forma de orientação a estas sobre procedimentos de segurança assim como controle destes sistemas sobre suas ações no sistema de informação – isto seria uma prevenção a ataques maliciosos.

Cronograma

A tabela abaixo apresenta o cronograma de atividades a serem realizadas para a produção desse trabalho. O seu desenvolvimento terá início em Agosto de 2008 e será finalizado em Novembro de 2008.

Atividades	Março	Abril	Maio	Junho
Criação da proposta, cronograma e resumo da monografia				
Pesquisas iniciais mais aprofundadas				
Estruturação de tópicos				
Escrita geral da monografia				
Ajustes finais do trabalho				
Elaboração da apresentação				
Apresentação				

Assinaturas

_____

Professor Ruy José Guerra Barretto de Queiroz

Orientador

_____

Felipe Ribeiro Machado

Aluno