

UNIVERSIDADE LUTERANA DO BRASIL

ULBRA – *CAMPUS* GUAÍBA

CURSO DE SISTEMAS DE INFORMAÇÃO



**PROPOSTA DE TCC - TRABALHO DE
CONCLUSÃO DE CURSO**

**MITIGAÇÃO DO RISCO OPERACIONAL
ATRAVÉS DA CIFRAGEM DO SISTEMA DE
ARQUIVOS EM SERVIDORES DE
APLICAÇÕES**

MIGUEL ÂNGELO CHAGAS NEUMANN

ANDRÉ PERES
Professor Orientador

Guaíba, março de 2009.

DADOS DE IDENTIFICAÇÃO

1. DADOS DO ALUNO

Nome: Miguel Ângelo Chagas Neumann

Endereço: R. São José, 455, AP 202

E-mail: Miguel@rwx.com.br , Miguel_neumann@banrisul.com.br

Fones: (res) 3055-1156 , (com) 3215-1877 , (cel) 9712-6799

2. DADOS DO PROFESSOR ORIENTADOR

Nome: André Peres

E-mail: peres@guaiba.ulbra.tche.br

SUMÁRIO

1	DEFINIÇÃO DO TEMA	4
1.1	Título do TCC	4
1.2	Tema	4
1.3	Delimitação do Tema	4
2	MOTIVAÇÃO	4
3	OBJETIVOS	6
4	HIPÓTESES DE SOLUÇÃO	7
5	FUNDAMENTAÇÃO TEÓRICA	7
6	SOLUÇÃO PROPOSTA	8
7	CRONOGRAMA	8
8	REFERÊNCIAS BIBLIOGRÁFICAS	8

1 DEFINIÇÃO DO TEMA

1.1 Título do TCC

Mitigação do risco operacional através da cifragem do sistema de arquivos em servidores de aplicações.

1.2 Tema

Avaliação da possibilidade de atenuar os riscos à segurança da informação em servidores de aplicações de entidades financeiras, conforme estipula o Acordo de Basiléia e as normas BACEN 2554, ISO IEC/NBR 27002 e ISO IEC/NBR 27005, através da criptografia do sistema de arquivos e análise de performance da implementação visando viabilidade da proposta.

1.3 Delimitação do Tema

O presente trabalho visa identificar pontos relevantes nas normas e melhores práticas de confidencialidade da informação que incidam em empresas do setor financeiro.

Com base nessa identificação, prover processos tecnológicos que assegurem o adequado tratamento das informações contidas nos dispositivos de armazenamento magnético de servidores de aplicações corporativos.

Ao final do trabalho pretende-se implementar a cifragem do file system de um servidor de aplicações Linux e obter um comparativo de desempenho entre um sistema criptografado e outro não-criptografado.

O tratamento das informações proposto refere-se à proteção contra acesso não autorizado, contra roubo ou perda e adequado descarte das mídias, bem como, a garantia da confidencialidade na execução de serviços por terceirizados.

2 MOTIVAÇÃO

Um dos setores mais estratégicos da economia é o setor financeiro. Através das transações executadas no mercado financeiro, outras áreas da economia são beneficiadas, modernizando-se e gerando riquezas para a sociedade.

Porém, a possibilidade de gerir grandes quantias de capitais pode propiciar a ocorrência de fraudes, a potencialização de erros e em consequência, a responsabilização perante clientes e órgãos reguladores. Além disso, ao tomarmos como exemplo a atual crise dos derivativos do mercado imobiliário americano, temos noção da importância do setor financeiro, inclusive em relação à cadeia produtiva.

Para viabilizar suas operações, os bancos realizam pesados investimentos em tecnologia da informação. Associado aos investimentos em performance, ferramentas e serviços, também está inclusa a segurança da informação corporativa e de clientes. Tal situação ocorre, pois a confidencialidade dos dados é um dos ativos corporativos mais importantes.

Ao acompanharmos a imprensa, encontramos vários exemplos de roubo ou vazamento de informações que ocasionaram prejuízos às corporações.

Podemos citar o possível vazamento do balanço financeiro de 2008 da Petrobrás, que permitiu uma queda de 4% no valor de suas ações.

O Ponemon Institute realizou estudo em 43 empresas que tiveram dados perdidos dos Estados Unidos e avaliou que para cada registro perdido houve um prejuízo médio de US\$ 202,00. Sendo que US\$ 139,00 representaram o custo da perda de novas oportunidades de negócio (IDGNow!).

Em janeiro/09, o Identity Theft Resource Center (ITRC) identificou que mais de 35 milhões de registros foram violados em 2008, nos quais a maioria não estava criptografada ou protegida por senha.

Segundo a McAfee, as empresas de tecnologia perderam 1 trilhão de dólares com roubo de dados em 2008. Com relação à propriedade intelectual as perdas somam 4,6 bilhões de dólares (IDGNow!).

Conforme estudo da Symantec, 59% de mil profissionais que deixaram seus empregos em 2008 nos Estados Unidos admitiram ter roubado informações confidenciais de suas antigas empresas (www.noticiasdigitais.com.br).

O roubo de informações como cadastro de clientes, de transações financeiras e de ações estratégicas está cada vez mais inserida nas corporações.

Paralelo a isso, temos a realização de terceirizações de manutenção de hardware, de instalação de aplicativos que mesmo com dispositivos legais e contratuais bem elaborados, pode permitir o vazamento de informações.

Nesse contexto, apresento o presente projeto que visa possibilitar uma camada adicional de proteção aos dados corporativos.

Tendo em vista que a normatização define padrões mínimos de segurança e estipula ressarcimento aos prejudicados quando da ocorrência de perda de dados, entendemos que a cifragem do file system de servidores corporativos permite o acesso somente mediante as credenciais devidamente autorizadas.

A cifragem do sistema de arquivos de servidores apesar de propiciar a segurança das informações, pode possibilitar um decréscimo no desempenho do equipamento.

Pretendemos realizar testes de performance em sistemas operacionais instalados fisicamente no hardware e também em máquinas virtuais. Para isso, necessitaremos analisar ferramentas de análise de desempenho e métricas para elaborar a conclusão do levantamento.

Acreditamos que o presente trabalho auxiliará muitas empresas na escolha de ferramentas para cifragem de file system. Também servirá de apoio a decisão para administradores de sistemas que queiram analisar a viabilidade da criptografia em seus servidores.

Saliente-se que todas as ferramentas utilizadas serão softwares livres, de códigos aberto ou de domínio público.

3 OBJETIVOS

Como objetivo geral, pretendemos fornecer a administradores de servidores de aplicações financeiras, em plataforma Linux, a possibilidade de adequar seus sistemas à normatização e melhores práticas de segurança da informação. Com o projeto também visamos demonstrar a viabilidade da proposta em uma máquina de produção.

Como objetivo específico, propomos a documentação do processo de criptografia de file system e a realização de análises de desempenho entre um sistema cifrado e outro não-cifrado.

4 HIPÓTESES DE SOLUÇÃO

- Hipótese 1: Utilizar um host com o disco rígido particionado, no qual instalaremos um servidor Linux em cada partição. A primeira partição será implementada com sistema de arquivos sem criptografia. A segunda partição utilizará sistema de arquivos criptografado. Havendo a possibilidade, pretendemos testar o projeto em um servidor de produção de empresa do setor financeiro.
- Hipótese 2: Não sendo possível testar o projeto em servidor de produção de empresa do setor financeiro, utilizaremos host em condições que permitam simular o processamento de um servidor em produção.
- Hipótese 3: Não havendo disponibilidade para simular o processamento de um servidor de produção, realizaremos os testes com o processamento o mais adequado possível.
- Hipótese 4: Não sendo possível utilizar um host próprio para o trabalho, realizaremos a pesquisa utilizando somente máquinas virtuais com plataforma Xen.
- Hipótese 5: Não sendo possível utilizar máquinas virtuais com plataforma Xen utilizaremos outra plataforma de virtualização com licença de software que permita a realização das análises.

5 FUNDAMENTAÇÃO TEÓRICA

Conforme a ABNT NBR ISO/IEC 27002, a Segurança da Informação é a preservação da confidencialidade, da integridade e da disponibilidade da informação, adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

A informação é um ativo da empresa e por isso, possui valor e está sujeita a riscos que permitem prejuízos para a organização (ISO 27002).

O 8º Princípio do Acordo de Basiléia preceitua que os sistemas que utilizam dados na forma eletrônica devem ser seguros, independentemente monitorados e resguardados por planos de contingência adequados.

6 SOLUÇÃO PROPOSTA

No trabalho proposto apresentaremos a documentação para escolha da plataforma de virtualização, os procedimentos de instalação dos ambientes, as análises de performance e a conclusão dos levantamentos realizados.

A primeira parte do trabalho abordará a fundamentação teórica, referência bibliográfica. Também serão apresentadas as tecnologias, ferramentas, métodos e métricas escolhidos.

Na segunda parte será implementado o projeto, serão realizados os testes e as análises de performance.

7 CRONOGRAMA

Atividade	Março			Abril			Maio			Junho		
Revisão Bibliográfica												
Análise de Requisitos												
Elaboração dos Diagramas												
Implementação												
Elaboração do artigo para Seminário de Andamento												
Testes												
Homologação												
Elaboração do Relatório Final												
Entrega do Relatório Final												

8 REFERÊNCIAS BIBLIOGRÁFICAS

[SIS04] Rômulo de Oliveira, Alexandre Carissimi, Simão Toscani. Sistemas Operacionais 3 Ed. Porto Alegre: Sagra Luzzatto, 2004.

[TCP05] Luciano Palma, Rubens Prates. TCP/IP Guia de Consulta Rápida. São Paulo: Novatec, 2005.

[RSL05] Morimoto, Carlos. Redes e Servidores Linux. Porto Alegre: Sulina, 2005.

- [LFT05] Morimoto, Carlos. Linux: Ferramentas Técnicas. Porto Alegre: Sul Editores, 2005.
- [JOA03] Lima, João Paulo. Administração de Redes Linux. Goiânia: Gráfica Terra Ltda., 2003.
- [DAN06] Dan Farner, Wietse Venema. Perícia Forense Computacional Teoria e Prática Aplicada. São Paulo: Pearson Prentice Hall, 2006.
- [AND06] Rodrigues de Freitas, Andrey. Perícia Forense Aplicada à Informática – Ambiente Microsoft. São Paulo: Brasport, 2006.
- [RUF01] Rufino, Nelson Murilo de O. Segurança Nacional Técnicas e Ferramentas de Ataque e Defesa de Redes de Computadores. São Paulo: Novatec, 2001.
- [DIA00] Dias, Cláudia. Segurança e Auditoria da Tecnologia da Informação. São Paulo: Axcel Books, 2000.
- [INS93] Instituto dos Auditores Internos do Brasil. Procedimentos de Auditoria Informática. São Paulo: Câmara Brasileira de Auditoria Informática.
- [ISO05] Associação Brasileira de Normas Técnicas. ABNT NBRISO/IEC 17799:2005. Rio de Janeiro: 2005.
- [ISO05] Associação Brasileira de Normas Técnicas. ABNT NBRISO/IEC 27005:2008 Rio de Janeiro: 2009.
- [COM04] FEBRABAN. Compliance e Auditoria de Sistemas nas transações de e-Commerce. São Paulo: 2004.
- [MET04] FEBRABAN. Metodologia de Auditoria Interna com Foco em Riscos. São Paulo: 2004.
- [NOV04] FEBRABAN. Novos Conceitos de Auditoria de Sistemas em Bancos. São Paulo: 2004.
- [BIS06] Bank for International Settlements. Basel Committee on Banking Supervision. Basileia Suíça.2006