Modalidade do trabalho: Relatório técnico-científico
Evento: XX Seminário de Iniciação Científica

ANÁLISE, MONITORAMENTO E AUDITORIA DA REDE DE COMPUTADORES DE UMA PREFEITURA MUNICIPAL[1]

Marcelo Freitas Do Prado[2], Bruno Otávio Brun Neto[3].

[1] Trabalho Interdisciplinar do quinto semestre do Curso Superior de Tecnologia em Redes de Computadores da SETREM

[2] Formando do Curso Superior de Tecnologia em Redes de Computadores da SETREM, mfprado8@gmail.com

[3] Formando do Curso Superior de Tecnologia em Redes de Computadores da SETREM, bbrunootavio@gmail.com.

Resumo: O presente trabalho teve por objetivos o uso de ferramenta para monitorar o desempenho de servidores e aparelhos de comunicação entre links via rádio (wireless) através de serviços como ping, dns, http entre outros. O trabalho que é do tipo interdisciplinar foi realizado no segundo semestre de 2010 envolvendo as disciplinas de Auditoria em Redes de Computadores, Direito e Ética e Monitoramento e Desempenho em Redes de Computadores. Cita-se ainda de forma mais específica o objetivo de propor melhorias na rede com os resultados obtidos neste trabalho. Foi efetuado processo de auditoria com três pontos de Controle que englobavam parâmetros de controle interno como Eficácia, Eficiência e Segurança.

Palavras-Chave: Nagios; Alertas; Serviços; Interface;

Introdução

Inicialmente foi buscado realizar-se um levantamento da estrutura da rede no que diz respeito à existência de políticas internas de uso da rede englobando assim a disciplina de direito e ética. Além disso, foi realizado estudo sobre a necessidade de monitoramento dos serviços que rodam em três dos quatro servidores, além de onze aparelhos de comunicação wireless. Também houve foco sobre a necessidade de trazer a verificação de pontos de auditoria para controle da rede de computadores da Prefeitura Municipal de Três de Maio.

Após o processo de análise da rede, foi feita pesquisa voltada ao desenvolvimento teórico dos aspectos abordados neste trabalho respeitando-se o devido referencial embasado nas obras de autores da área de redes de computadores.

Metodologia

Na abordagem, o método utilizado foi o quali-quantitativo, que conforme GÜLLICH, LOVATO e EVANGELISTA (2007), esse método visa expressar subjetivamente os resultados da pesquisa.

Fazendo uma análise do estudo realizado, procurou-se representar como uma rede de computadores realmente funciona, seus aspectos na operabilidade e otimizações.

Segundo GÜLLICH, LOVATO e EVANGELISTA (2007), o procedimento é uma análise mais concreta, onde é feito teste e pesquisas mais avançadas para referente estudo.

MÉTODO HISTORICO: De acordo com Lakatos e Marconi (1986), método histórico é um levantamento de dados já existentes para comparar ao estudo feito ou análises utilizadas em determinado estudo.

MÉTODO DE COMPARATIVO: Segundo Lakatos e Marconi (1986), método comparativo permite uma análise referente a estudos feitos de algum determinado assunto.

E a técnica usada foi questionário, a qual, conforme GÜLLICH, LOVATO e EVANGELISTA (2007), é organizada por uma série de perguntas que foram respondidas por escrito sem a presença do pesquisador.

Resultados e Discussão

A rede de computadores da Prefeitura Municipal de Três de Maio possuía cerca de 210 computadores (sendo que a grande maioria roda sistema operacional da plataforma Windows) incluindo laboratórios (Linux), secretarias e departamentos em geral. O link de comunicação é do tipo empresarial com capacidade de 2Mb dedicado.

Foram monitorados os servidores (que segundo Torres (2001), é um micro capaz de disponibilizar serviços à rede) de internet, de banco de dados e de AD. O primeiro deles rodava o sistema operacional Linux de distribuição open Suse 2.6.13-15.13, o segundo servidor tinha igualmente sistema operacional Linux, mas, no entanto, com a distribuição RedHat Enterprise 2.6.9.5. Existe ainda o servidor de AD que rodava o sistema operacional Windows Server 2003 SP3.

Modalidade do trabalho: Relatório técnico-científico
Evento: XX Seminário de Iniciação Científica

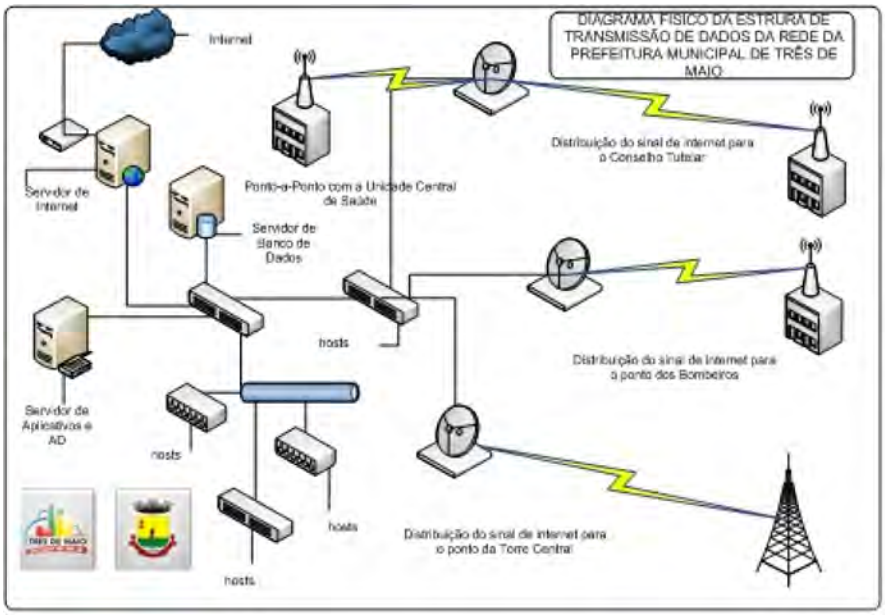

Diagrama Físico da Estrutura de Transmissão de Dados da rede.

O parágrafo abaixo mostra os resultados da auditoria dos três pontos de controle. Consideram-se os números dos votos baseados nos questionários, monitoramento e vivência na rede de forma diária, gerando assim o cálculo para obtenção dos votos médios. Considera-se ainda as técnicas: A= Visita in Loco, B=Questionário e C=Mapeamento Estatístico dos Programas de Computador e Monitoramento.
No Ponto de Controle Satisfação dos Usuários em Relação aos Serviços da Rede tiveram três parâmetros de Controle Interno: Eficácia, Segurança Ambiental e Eficiência. O voto apurado na primeira foi quatro (4), sendo a natureza da fraqueza a Insatisfação dos Usuários em Relação aos Sistemas Computacionais. O voto risco foi um (1). A técnica usada foi a B. O voto esforço foi quatro (4), sendo ainda o voto de média: três (3). Na Evidência foi utilizado um Questionário realizado com vinte e sete funcionários da prefeitura que utilizam os recursos de sistema e rede de computadores. No parâmetro de Controle Interno Segurança Ambiental, o voto apurado foi quatro (4), a natureza da fraqueza foi a Falta de Condições de operacionalidade por parte dos usuários dos sistemas tecnológicos, sendo o voto risco dois (2), a técnica usada foi a B. O voto esforço foi quatro (4), o voto de média foi três vírgula três (3,3) e a evidência foi comprovada com questionário realizado com os usuários da rede. O terceiro Parâmetro de Controle Interno (Eficiência) teve voto apurado cinco (5), a natureza da fraqueza analisada foi a ótima combinação entre recursos humanos, tecnológicos e materiais gerando bom desempenho, o voto risco foi quatro (4), a técnica usada foi B e C, sendo o voto esforço cinco (5) e o voto de média quatro vírgula seis (4,6). Esse último parâmetro de controle interno (Eficiência) foi comprovado por meio do monitoramento com o Nagios dos serviços da rede, bem como dos servidores.
Já no Ponto de Controle Respeito às Normas Internas da Rede ocorreram dois parâmetros de controle interno (Obediência às Políticas da Alta Administração e Conhecimento da Legislação em Vigor). O primeiro parâmetro de controle interno teve voto apurado quatro (4), sendo a natureza da fraqueza o

Comportamento Perante os Recursos Disponíveis, sendo que o voto risco foi quatro (4) e a técnica usada foi a B. Salienta-se ainda que o voto esforço foi quatro (4) e as evidências deste parâmetro de controle interno foram obtidas por meio do questionário aplicado aos vinte e sete usuários da rede da Prefeitura. O Segundo parâmetro de controle interno foi o Conhecimento da Legislação em Vigor que teve um voto apurado quatro (4), a natureza da Fraqueza foi o Conhecimento das Leis em Vigor perante a Prefeitura, teve ainda o voto risco que foi três (3), a técnica usada foi a B. O voto esforço foi quatro (4). O voto médio foi três vírgula seis (3,6) e as evidências foram obtidas por meio do questionário.

Já no terceiro ponto de controle que considerava o Controle de Acesso à Rede Física e Lógica da Prefeitura, foram observados três parâmetros de controle interno que são: Segurança Física, Segurança Lógica e Eficiência. O primeiro teve voto apurado cinco (5), a natureza da fraqueza foi a Segurança no Acesso à Sala dos Servidores. O voto risco foi quatro (4) e a técnica usada foi a A. O voto médio foi quatro vírgula seis (4,6) e foi evidenciado com Visita in Loco. O parâmetro de controle interno Segurança Lógica teve voto apurado cinco (5), a natureza da fraqueza que compõe o risco foi o Acesso à Rede Lógica e a Realização de Alterações nos dados de forma ilegal. O voto risco foi dois (2) e a técnica foi a A. O voto esforço foi cinco (5) e o de média foi quatro (4), sendo que as evidências foram comprovadas por meio da vivência diária na rede que comprovaram contínuos problemas de conflito de endereço IP. O terceiro parâmetro de controle interno foi a Eficiência com voto apurado quatro (4), sendo a natureza da fraqueza a Ótima Combinação dos Recursos Humanos, Materiais e Tecnológicos Disponibilizando Segurança aos Dados da Prefeitura. O voto Risco foi dois (2) e a técnica utilizou-se de A e C, o voto esforço foi cinco (5) e o voto médio foi três vírgula seis (3,6) sendo que as evidências foram comprovadas por meio de Visita in Loco e Consulta às Políticas Internas de Uso da Rede.

A ferramenta usada para efetuar o monitoramento dos serviços que rodam tanto nos servidores como nos aparelhos que comportam os links via rádio foi o Nagios, o qual segundo Rebello (2010), é uma aplicação de código aberto, sob licença GPL. O Nagios foi criado no ano de 1999, sendo seu patrocinador principal a Nagios Enterprise e atualmente engloba aplicações de terceiros, tendo a colaboração de desenvolvedores do mundo inteiro. Ele foi desenvolvido para realizar monitoramento, análise e alerta de problemas (eventos) ocorridos nos objetos monitorados. Os principais serviços que o Nagios monitora são: SMTP, POP3, HTTP, NNTP, ICMP. Ele possui uma interface Web que permite realizar toda a configuração, além de gráficos coloridos indicadores e plug-ins que possibilitam ajuste mais afinado da configuração embora necessitem de um conhecimento mais refinado. Outra grande vantagem que o Nagios oferece são os gatilhos que podem ser acionados de forma automática quando acontece um problema, basicamente eles tentam reiniciar um serviço, caso não consigam estes alertas avisam o administrador da rede sobre o problema através de mensagens que podem ser enviadas tanto para o aparelho celular quanto para o e-mail do gerente da rede. Além disso, o Nagios disponibiliza a aplicação que também é web chamada NagiosQL que é próprio para efetuar apenas alterações nos arquivos de configuração do programa sem no entanto, apresentar a tela com os monitoramentos e gráficos como se encontra na interface web principal do Nagios.

O tempo de resposta do serviço FTP foi de 0,0003 segundos na porta 21, a latência de 0,084 segundos, sendo que a checagem durou 0,009 segundos, em um status de OK. Os monitoramentos ocorreram por dez dias num período 24x7.
O serviço DNS, com 0,171 segundos de tempo de resposta para o site www.yahoo.com.br, começou a ser monitorado no dia 28/10.

Conclusões

Na primeira hipótese (a Prefeitura Municipal de Três de Maio submete sua rede de computadores a algum tipo de auditoria baseada em COBIT com pontos de controle delineados e seus respectivos parâmetros de controle interno? Se não, tal implementação traria benefícios?), foi comprovado que não há nem um tipo de auditoria na rede de computadores, seja em software ou hardware, bem como em infraestrutura.
Considerando-se a segunda hipótese (em caso de existência de auditoria na rede da prefeitura ela é voltada a análise (uso de ferramentas), ou a implementação (aquilo que será colocado para monitorar)?) Foi comprovado que como não há nenhum processo de auditoria, consequentemente não há nem um foco, seja para análise ou para implementação.
A terceira hipótese (se a Prefeitura Municipal de Três de Maio possui políticas internas de tratamento de dados e acesso a internet e demais serviços da rede?). Sim, foi comprovado que existe uma Cartilha de Uso dos Recursos da Rede e Internet na Prefeitura Municipal de Três de Maio.
E concluindo com a quarta hipótese (se há satisfação por parte dos usuários com relação aos serviços e aplicativos da rede da prefeitura?). Sim, pois treze (dos vinte e sete) usuários afirmaram (quando perguntados no questionário sobre a satisfação em relação a vários aspectos da rede) que consideravam a mesma boa.

Referências Bibliográficas

GÜLICH, Roque Ismael da Costa; LOVATO, Adalberto; EVANGELISTA, Mário dos Santos. Metodologia da Pesquisa: normas para apresentação de trabalhos: redação, formatação e editoração. Três de Maio: Ed. SETREM, 2007.
REBELLO, Hugo. Instalação do Nagios - O que é Nagios? Disponível em: < http://www.linuxnarede.com.br/artigos/fullnews.php?id=152 > Acessado em: 16/10/2010.
TORRES, Gabriel. Redes de Computadores Curso Completo. Editora Axcel Books. Rio de Janeiro: 2001.