PROJETO SOLIVRE SOFTWARE LIVRE
WILLIAM SHINITI YAMAMOTO

Clique aqui para para ver este resumo

QUESTÕES SOBRE SEGURANÇA E EFICIÊNCIA DOS SISTEMAS DE INFORMAÇÃO NAS EMPRESAS
Márcio Geovani Tavares de Assunção

Clique aqui para para ver este resumo

UM ESTUDO SOBRE OS MÉTODOS DE VARREDURA UTILIZADOS EM PORTSCANS
Clayton Kendy Nakahara Passos

Clique aqui para para ver este resumo

PROJETO SOLIVRE SOFTWARE LIVRE

WILLIAM SHINITI YAMAMOTO
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

ROBINSON PATRONI (Orientador)
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

Projeto SoLivre Software Livre. Robinson Patroni, William Shiniti Yamamoto. Departamento de Informática – Centro Universitário de Maringá (CESUMAR). Av. Guedner, 1610 – Jd. Aclimação – 87050-390 – Maringá – PR – Brazil. patroni@cesumar.br, william@wsy.com.br. O Projeto SoLivre Software Livre, assim como o Sistema Operacional Linux, surgiu a partir de uma idéia do aluno (William Shiniti Yamamoto) e seu Professor (Robinson Patroni), juntos, inspirados em capacitar profissionalmente a comunidade e empresas de Maringá utilizando o Software Livre. Inicialmente foram desenvolvidas pesquisas sobre o Sistema Operacional Linux, Distribuições e Aplicativos. Dentro dessa visão e do interesse da comunidade vários órgãos e empresas, de diversos segmentos, políticos, privados, educacionais, foram contatados demonstrando interesse e apoio ao projeto. OBJETIVOS O Projeto SoLivre tem como objetivos o Ensino a Pesquisa e a Implantação do Software Livre voltados para a Inclusão Social e Digital através da democratização do acesso da População a Tecnologias da Informação em todas as camadas sociais utilizando o Software Livre tendo como objetivo final à capacitação de mão de obra especializada para geração de riquezas e criação de novas tecnologias em Software Livre consolidando a criação de um pólo regional de Desenvolvimento de Soluções em Software Livre no Estado do Paraná. METODOLOGIA Foram avaliadas e disponibilizadas no site www.solivre.wsy.com.br diversos links de distribuições do Sistema Operacional Linux, aplicativos e manuais a serem utilizados no projeto, que servirão como manual para a instalação, aprendizado e uso desses sistemas. RESULTADOS Iniciamos nossos trabalhos por um dos gabinetes da Câmara Municipal de Maringá de forma gratuita, a Implantação e o Treinamento dos Sistemas com o objetivo do levantamento de informações relativas a custos de implantação e treinamento. Após a implantação e o treinamento constatou-se uma interação completa dos usuários com os sistemas e sua plena utilização demonstrando a qualidade dos softwares livres escolhidos.Graças aos excelentes resultados obtidos, iniciamos a implantação do Projeto SoLivre Software Livre em todos os Gabinetes dos Vereadores da Câmara Municipal da cidade de Maringá de forma custeada sendo analisados os itens hardware, software, sistemas operacionais, aplicativos, sistemas especialistas e recursos humanos assim como no Projeto Piloto . CONCLUSÃO O Projeto SoLivre Software Livre vem atender a grande necessidade do setor público na redução de custos em informática e na legalização dos softwares proprietários utilizados apoiando o Programa de Incentivo do Software Livre Paraná do Governo Estadual e do Programa Software Livre do Governo Federal do Brasil.

william@wsy.com.br; patroni@cesumar.br

QUESTÕES SOBRE SEGURANÇA E EFICIÊNCIA DOS SISTEMAS DE INFORMAÇÃO NAS EMPRESAS

Márcio Geovani Tavares de Assunção
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

Aline Maria Malachini Miotto (Orientador)
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

Os sistemas de informação podem ser definidos como uma combinação de recursos humanos e computacionais que inter-relacionam a coleta, o armazenamento, a recuperação, a distribuição e o uso de dados com o objetivo de melhorar a eficiência gerencial de uma empresa, garantido maior segurança em seus processos.A utilização das tecnologias de informação disponíveis no mercado e a indiscutível importância desse fator para o sucesso das organizações, seja nos mais diversos segmentos de negócios, deixa de ser uma perspectiva de empreendimento bem-sucedido e torna-se dia-a-dia, um componente decisivo, uma vez que as soluções tecnológicas dinamizam os processos organizacionais apoiando e, se não, definindo o processo de tomada de decisão nas organizações. Nesse sentido, os processos de coleta, armazenamento, processamento e transmissão da informação, no momento certo e para destinatário certo, é requisito fundamental para a melhoria continua da qualidade e da competitividade de mercado.Identificar as características gerais dos sistemas de informação presentes nas empresas de médio porte da região de Maringá – PR, bem como as necessidades por sistemas de informação que supram, no que se refere a eficiência gerencial, as necessidades tecnológicas das mesmas e, como processo conseqüente a essa identificação, propor uma arquitetura de informação genérica para empresas do mesmo porte. O desenvolvimento do estudo apresentando, baseou-se em pesquisas bibliográficas e no trabalho de campo, no qual, valeu-se da utilização do questionário de avaliação pré-definido para a realização das entrevistas em empresas previamente selecionadas da região. Ainda como componente importante para uma melhor analise do tema abordado, a possibilidade de um laboratório, recriando de forma fictícia uma empresa hipotética com funcionamento real, também contribuirá para a identificação das necessidades para as quais o trabalho proposto pretende suprir. A análise dos dados obtida até o então, ainda em fase de leitura estatística, impossibilita a sugestão de arquitetura de informação genérica que esteja de acordo com as necessidades especificas das empresas de médio porte da região de Maringá, por se tratarem de resultados parciais de uma realidade finita, mas que exige uma análise sistemática situacional mais elaborada, baseada nos resultados já obtidos: Validação do questionário e coleta de dados a campo.

m.geovani@isbt.com.br; amiotto@cesumar.br

UM ESTUDO SOBRE OS MÉTODOS DE VARREDURA UTILIZADOS EM PORTSCANS

Clayton Kendy Nakahara Passos
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

Fabrício Ricardo Lazilha (Orientador)
CESUMAR - Centro Universitário de Maringá, Maringá - Paraná

A ultima estatística do NBSO (NIC BR Security Office), janeiro a março de 2004, nos mostra que de todos os tipos de ataques existentes 49%% deles são ataques de varreduras de portas, tais ataques nos preocupa, pois se sabe que estes são justamente o tipo de ataque que antecede uma real invasão de sistemas ligados a Internet. Este dado retrata uma situação preocupante, pois à medida que aumenta os sistemas dedicados a Internet aumenta também os sistemas vulneráveis. Diante desta situação torna-se necessário uma ferramenta que possa ludibriar ou até mesmo evitar tais investidas. Uma vez que a grande maioria dos ataques começa com varredor de portas, nós podemos evitar muitos dos ataques bloqueando a ação destes portscans. Para tanto devemos encontrar “assinaturas” de cada método utilizado, a fim de documentar e possibilitar a criação de uma ferramenta que identifique e bloqueie em tempo real, de acordo com as exigências do administrador de segurança. O programa tcpdump foi utilizado para análise dos diversos métodos dos varredores de portas, em conjunto com o varredor de portas NMAP, que nos serviu como gerador de “assinaturas”. Estes programas foram utilizados sob o Sistema Operacional Linux. Foram encontradas reações interessantes e curiosas sobre o comportamento do protocolo TCP, que levou a identificação de diversas assinaturas, ou seja, foram identificados e documentados diversos comportamentos que podem ser utilizados para detectar e bloquear a ação de ferramentas como o Nmap. Foi possível observar, dezenas de “pacotes” não convencionais chegam aos servidores diariamente, sendo ignorados por muitos administradores por serem considerados erros causados pela própria rede. Hoje em dia tais pacotes são reconhecidos como tentativas de varredura de portas ou exploração de vulnerabilidades. Alguns tipos de varreduras de portas não são detectados e podem levantar as informações necessárias para uma futura invasão, sem nem mesmo deixar rastro. Por isto é necessário o desenvolvimento de uma ferramenta que possa detectar e possibilitar ao administrador agir de acordo. Mas não basta apenas detectar uma simples assinatura, pois este método detecta apenas ataques já documentados (conhecidos), deve-se criar uma ferramenta que possa prevenir ataques ainda não existentes, isto será possível com o auxílio da inteligência artificial. As assinaturas encontradas podem ser utilizadas para “alimentar” tal sistema, ensinando o básico sobre varreduras de portas.

netstart@brturbo.com; fabricio@cesumar.br