Um Estudo De Caso De Segurança Da Informação Baseada No Aperfeiçoamento Do Usuário Em Seu Ambiente Corporativo, Projetando Para Auxílio, Uma Ferramenta Extensível De Treinamento

Luiz Antônio Ferreira do Nascimento Júnior[1], Frederico Coelho[1]

[1]Departamento de Ciência da Computação – Universidade Presidente Antônio Carlos (UNIPAC)
Campus Magnus – Barbacena – MG – Brasil

lafnjr@yahoo.com.br, fredericocoelho@unipac.br

Resumo: *Este artigo realiza um estudo de caso de segurança da informação focando como ponto forte dessa, o usuário do sistema, pois, este se torna um dos maiores pontos críticos de um sistema informatizado devido em grande parte sua falta de preparo. Aborda também o projeto de uma ferramenta para auxiliar o administrador do sistema no treinamento e adequação do usuário, visando desenvolvê-lo como mais um eficiente elemento na sua estrutura de segurança.*

Palavras-chave: Segurança; usuário; informação.

1. INTRODUÇÃO

Desde que o homem tornou-se consciente de suas atitudes, sempre procurou guardar e assegurar o que era importante.

Ao longo da história, essa preocupação continuou a mesma, alternando apenas entre os objetos que eram alvos de desejos e preocupações, chegando até ao atual momento em que o homem tem como bem mais precioso a informação.

Anterior à preocupação com a segurança, surge então o desejo de obter maliciosamente a informação. Porém para não perder essa atual valiosidade, que se tornou um bem das empresas e das pessoas, a forma de protegê-la é acompanhar a evolução tecnológica e os métodos com que os Crackers[1] a roubam. Hoje em dia com a tecnologia em hardware e software de segurança cada vez mais eficiente, a prática do rapto da informação procura meios alternativos e com certeza encontrou uma grande

oportunidade de sucesso em suas investidas, focando-se para isso, o operador desse sistema.

Este artigo tem como objetivo demonstrar como a partir do usuário, pode-se desenvolver um grande ponto de auxílio a uma estrutura de segurança de informação podendo-se enxergar um novo horizonte com relação à utilização do usuário como mais um método de garantir a segurança da informação e de que maneira educar este, a fim de garantir sucesso nesse método.

1- Pessoas que utilizam o conhecimento tecnológico, para obter algo de seu interesse, de maneira ilícita.

A seguir são apresentadas algumas definições que serão de grande importância para entendimento de termos expostos posteriormente nesse artigo.

2.1. A SEGURANÇA

Uma boa definição de segurança é relacionado a aquilo que está protegido, seja de perda ou roubo e\ou que se possa confiar.

"*Qualquer evento diferente do normal, confirmado ou sob suspeita, relacionado à segurança de sistemas informatizados ou de redes de computadores, é considerado um evento de segurança.*
Alguns eventos que devem ser remetidos como incidentes:
→ Tentativas de ganhar acesso não autorizado, seja a sistemas ou aos dados diretamente.
→ Ataques DOS (Denial Of Services – negação de serviços).
→ Uso não autorizado ao sistema informatizado.
→ Desrespeito à política de segurança de uma empresa ou provedor de serviços" (CERT.br, 2007)

2.2. POLÍTICA DE SEGURANÇA

Os incidentes de segurança, como por exemplo, tentativas de ganhar acesso não autorizado, ataques DOS e uso não autorizado ao sistema, são difíceis de serem executados com sucesso caso se adote uma política de segurança coesa e sem brechas, focando tanto na parte de hardware e software como também na parte do usuário.

"Será essa política que irá atribuir direitos e responsabilidades aos usuários que lidam com os recursos computacionais de uma instituição e com as informações neles armazenados. Ela também delibera atribuições a cada um em relação à segurança dos recursos com os quais trabalham. É nessa política de segurança que se está previsto o que pode ou não ser feito dentro desse ambiente; è nela também que são definidas as penalidades que estão sujeitos aqueles que não a cumprem.

Os usos abusivos da rede devem estar previstos dentro dessa política. Não existe uma definição exata, mas, algumas práticas são consideradas abusivas por grande parte das empresas. Algumas práticas consideradas abusivas são:
→ envio de SPAM;
→ envio de correntes que não são de acordo com os interesses da empresa;
→ cópia e distribuição não autorizada de material protegido por direitos autorais;
→ utilização da internet para fazer difamação, calúnia e ameaças;
→ tentativas de ataques a outros computadores;
→ comprometimento de computadores ou redes; " (CERT.br, 2007)

São apenas alguns exemplos, mas não são universais, sendo cada empresa responsável por personalização de sua política, para ambos se adequarem com as necessidades da outra.

2.3. ELEMENTOS DE REDE

Elementos de software são tão importantes quanto de hardware para criar uma rede segura, porém podem ser decisivos no sucesso ou não dessa segurança. Dois desses elementos são as *VPN´s (Virtual Private Network)* e os *Firewalls.*

2.3.1. VPN

..A idéia de utilizar uma rede pública como a Internet em vez de linhas privadas para implementar redes corporativas é denominada de *Virtual Private Network* (VPN) ou Rede Privada Virtual. As VPN´s são túneis criptografados entre pontos distintos autorizados, criados através de uma rede comum entre esses para transferência de informações, de modo seguro, entre redes corporativas e\ou usuários remotos...(Tanenbaum, 2003). Hoje em dia com softwares simples e acessíveis a todos, como o freeware Teamviewer, é possível montar uma VPN entre quaisquer dois computadores, em qualquer lugar do mundo.

2.3.2. FIREWALL

..Um firewall é basicamente algum tipo de software ou hardware que controla a transferência de dados entre redes. Ele é instalado na entrada de uma rede tornando-se assim um filtro, onde só são permitidas trocas de dados autorizados por ele, dando mais segurança às informações trafegadas dentro daquela rede... (Tanenbaum, 2003). Hoje em dia os Firewalls´s deixaram de ser exclusivos para empresas e começaram a ser utilizados por usuários domésticos; dois deles largamente utilizados são o **Comodo** (plataforma Windows) e o **IpTables** (plataforma Unix).

3. ESTUDO DE CASO

Para avaliação de um sistema de segurança, necessitava-se de uma empresa com uma infra-estrutura já instalada de uma rede de computadores, sendo que essa seria controlada por um CPD (Centro de Processamento de Dados). Essa rede ainda teria que se conectar a outras externamente para uma avaliação da segurança entre essas.

A empresa XCAR foi escolhida por atender as necessidades possuindo toda a infra-estrutura já instalada, configurada e funcionando.

Serão apresentados nesse estudo de caso, o contexto da empresa, a situação atual da empresa em termos de segurança e infra-estrutura e as possíveis falhas e soluções.

3.1. ÂMBITO

A empresa XCAR, concessionária de veículos, tem três unidades em Minas Gerais, sendo a matriz em Barbacena e as filiais funcionando independentes. Além disso, possui mais dois postos de combustíveis como suas filiais na cidade de Barbacena, chamados aqui, respectivamente de 'P1' e 'P2'.

A conexão a internet é realizada através de um link de 1 Mb Oi-Velox empresarial, sendo esta a primária e uma secundaria através de um link de 600 Kb fornecido pela operadora local de internet via rádio.

Na matriz os negócios funcionam sobre o software chamado Sercon. Cada usuário tem seu nível de visão baseado na sua função na empresa. Nos postos filiais funciona um sistema chamado LBC, que conecta ao servidor instalado na matriz, utilizando Windows 2003 Server (win2003). Em grande parte das máquinas a aplicação é executada diretamente no servidor através da conexão de área de trabalho remota oferecida pelo Windows 2003. A exceção são as Workstations que funcionam à pista de abastecimento em que a aplicação roda localmente e os dados são posteriormente enviados ao servidor.

Os dois softwares são de vital importância para sobrevivência da empresa.

3.2. SITUAÇÃO ATUAL DA EMPRESA

A empresa XCAR concessionária de veículos não possui hoje nenhuma política de segurança implantada ou em processo de implantação. Possui um servidor de internet, o qual está instalado o sistema operacional Opensuse, e esse configurado como firewall, o *iptables. E*sse servidor é um computador de marca Dell®, com 256 MB de memória RAM e um Processador Intel-Celeron® de 1.3 GHz. Ele possui um ip-fixo fornecido pela operadora de internet via rádio e um ip-dinâmico oferecido pela empresa Oi. Esse computador funciona como *gateway* e utiliza como link primário a conexão Oi-Velox e em caso de algum problema deste, a conexão secundária via radio deve ser acionada manualmente e, todos na matriz utilizam a banda de internet primária ativa.

Não há nenhum controle automático via *proxy* de limitação de banda ou conteúdo, fazendo com que muitas das vezes a internet fique fora do ar, pois o link está ocupado com *downloads*; e tal acesso só é monitorado após reclamações de alguns funcionários, o qual através de uma ferramenta implementada no *gateway*, pode-se visualizar qual link está consumindo tais recursos e este ser desconectado manualmente e temporariamente.

O acesso externo a esse *gateway* é realizado através de uma conexão SSH (*Secure SHell*) pela porta 22. Utilizam-se também outras portas para acesso externo aos servidores dos postos. O gateway tem o serviço DHCP (*Dynamic Host Configuration Protocol* - Protocolo de configuração de *host* dinâmico) ativo, que é utilizado em toda a rede inclusive no roteador wireless. Para um melhor entendimento, o posicionamento físico encontra-se conforme Figura 1:

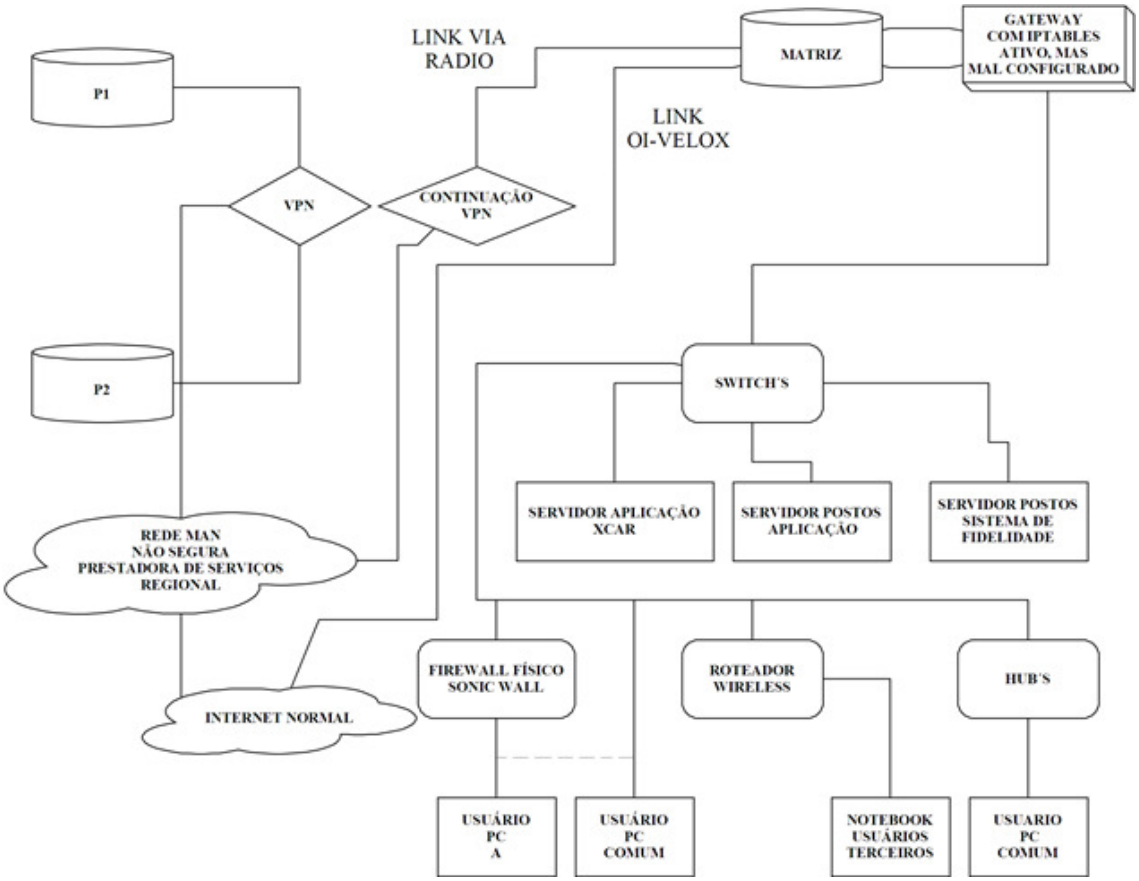

Figura 1. Funcionamento Atual da Rede da Concessionária

Para acesso externo a todos os servidores é necessário passar pelo gateway, mas uma possível invasão pode-se ocorrer a partir dos notebooks de terceiros conectados a rede diariamente e sem controle de acesso e conteúdo algum.

Os servidores dos postos, tanto o de aplicação quanto o de sistema fidelidade, não possuem nenhum controle de acesso além do oferecido pelo Windows 2003 na área de conexão remota. O servidor de aplicações da concessionária também armazena seu banco de dados. O servidor de aplicações da concessionária aceita comunicação via telnet.

80% dos computadores possuem acesso a web, sem nenhuma restrição, e em nenhuma workstation tem-se o e-mail monitorado, e nem há padrões nem com navegadores, nem com clientes de e-mail. Todas os computadores possuem antivírus gratuito atualizado, trinta por cento possuem anti-spyware (proteção contra programas espiões) e em nenhuma foi encontrado um firewall instalado\habilitado.

Pessoas externas aos funcionários, como funcionários bancários, por exemplo, tem acesso direto e irrestrito as máquinas dos usuários da empresa.

Todos os documentos, pastas e impressoras que são compartilhadas, permanecem nesse estado, com todas as permissões liberadas.

A situação atual da empresa merece atenção, pois além de infecções de vírus e *trojans*, os spywares têm preocupado. Recentemente houve um incidente em que o computador utilizado para transações do banco Caixa Econômica Federal foi infectado com um "*keylogger*" (tipo de spyware) proveniente de um site malicioso, encaminhado através de um spam. O(s) cracker(s) responsável por tal ato, transferiu cinco mil reais

para as contas de seus interesses. A sorte segundo a responsável foi que o banco estranhou uma transferência de um valor mais alto do que o habitual e ligou para esta para confirmação, que na mesma hora cancelou tal transferência. Para visualizar algumas questões de segurança, pendentes na empresa XCAR, ver **Tabela 1**.

Encontrou-se também uma grande falha na estrutura não só da XCAR, mas também da multinacional, com relação ao usuário ligado diretamente ao firewall Sonic Wall®. Este é utilizado com o intuito de torna-se inviolável a rede interna mundial da multinacional, porem, devido às necessidades de hardware exigidas pela própria, a XCAR instalou por questões econômicas neste computador outra placa de rede, que é ligada diretamente a rede tradicional de acesso XCAR, permitindo que a rede interna da multinacional fique com a segurança da estrutura comprometida.

Uma falha gravíssima que se encontrou recentemente está relacionada à infra-estrutura, onde dentro da rede local MAN do município de Barbacena da prestadora de serviços, existe a possibilidade de conectar-se à rede interna da empresa, já que com qualquer dispositivo com placa wireless como um notebook, pode-se com uma faixa de IP interno comumente utilizada, na faixa 10.0.x.x, e gateway 10.0.x.1, ter acesso a todos dispositivos conectados na rede, inclusive, de outras empresas.

Tabela 1. Alguns problemas de segurança encontrados

Algumas Questões de Segurança	
Problemas	**Causas**
Portas do servidor de internet abertas	Servidor configurado inadequadamente
Nenhuma Workstation com um firewall ativo	Falta de padronização no hardware nas Workstations, impossibilitando a padronização de um firewall adequado.
Serviço DHCP ativo	Distribuição de IP dinamicamente
Falta de controle de acesso de terceiros aos computadores	Falta de conhecimento e\ou negligência dos riscos ao sistema
Falta de controle de conteúdo de acesso a internet	A não existência de um servidor *proxy* ou política de segurança
Uso das Workstations para fins pessoais	A falta de uma política de segurança
Falha na infra-estrutura	Falta de planejamento tanto da empresa prestadora de serviços, quanto da XCAR

3.3 - GARANTINDO A SEGURANÇA

Apesar de muitas falhas na configuração do hardware a rede em si mostra-se com um bom rendimento, porém vulnerável. Rendimento avaliado com o aplicativo "***Wireshark***" (ver Figura 2) que é um analisador de pacotes, executado em modo promíscuo, que coloca uma escuta na rede permitindo a captura de pacotes endereçados a outras máquinas. Disponível em "http://www.wireshark.org" na sessão de downloads do site. Demonstrou uma rede estável, onde a atividade de rede permaneceu normal. Em caso de contaminada, a rede poderia se comportar de várias formas, sendo que alguns sintomas como instabilidade, fluxo de dados direcionado a um único endereço IP, ou ainda, alteração de fluxo de dados fora do padrão em algum dos protocolos, poderiam levar o administrador a essa conclusão. Com relação ao conteúdo da Figura 2,

a rede mostra-se normal, pois, há transações comuns de pacotes do gênero de requisição de nomes, trafego na internet e etc. Não há sobrecarga de pacotes de mesmo tipo, gênero e quantidade a um determinado IP.

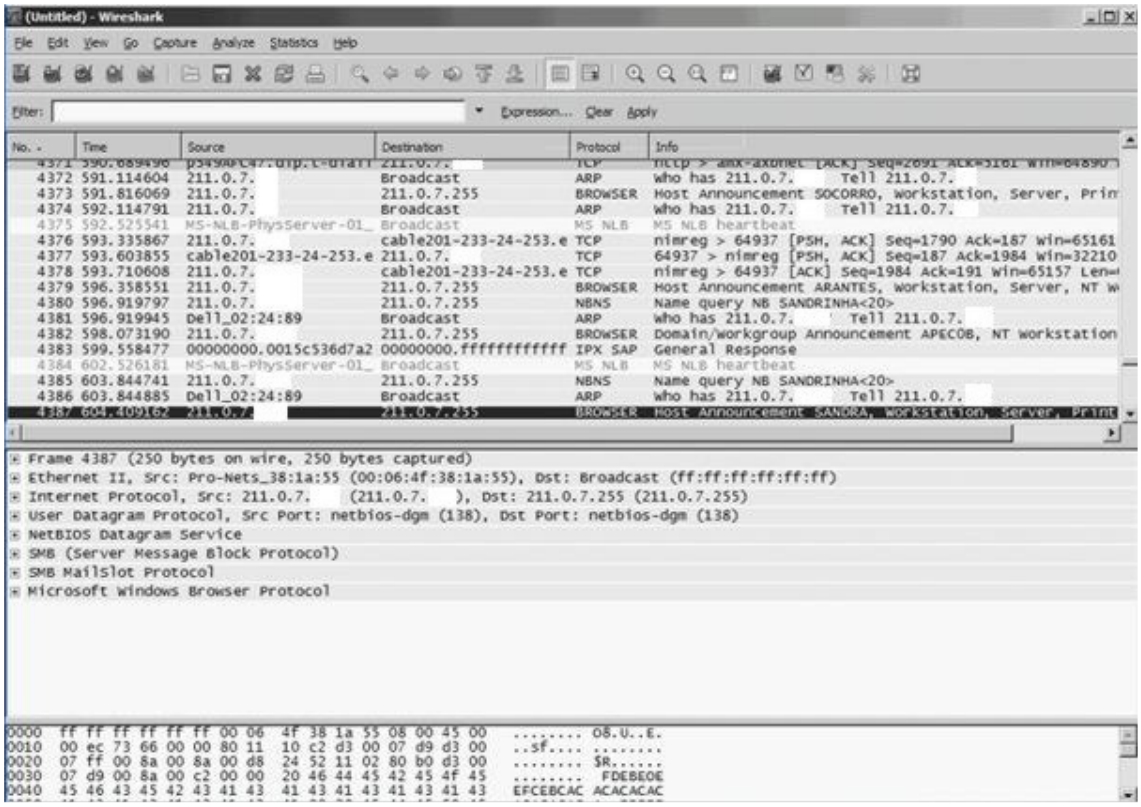

Figura 2. Funcionamento do aplicativo "*wireshark*" dentro da rede da concessionária. Os IP´s foram removidos da figura por garantia de sigilo

A Vulnerabilidade física foi comprovada através do aplicativo "***advanced port scanner 1.3"*** (ver Figura 3), que faz uma varredura em qualquer computador remoto em busca de portas abertas. Ele está disponível em "http://www.radmin.com/download/pscan13.exe" para download. Ao realizar a análise do servidor de internet, foram detectadas 6 portas abertas sendo que as portas podem oferecer alguns riscos, como por exemplo a porta 22(SSH), que está aberta, onde caso se a senha do servidor for obtida, será muito fácil o usuário conectar-se remotamente a rede, adquirindo o domínio sobre a mesma, lembrando que o servidor de internet é a única barreira entre a internet e a rede local. Apesar da maioria das portas estarem fechadas, nenhuma porta está oculta, isto pode deixar a maquina identificável na internet facilitando algum possível ataque. As portas abertas estão listadas na Figura 3.

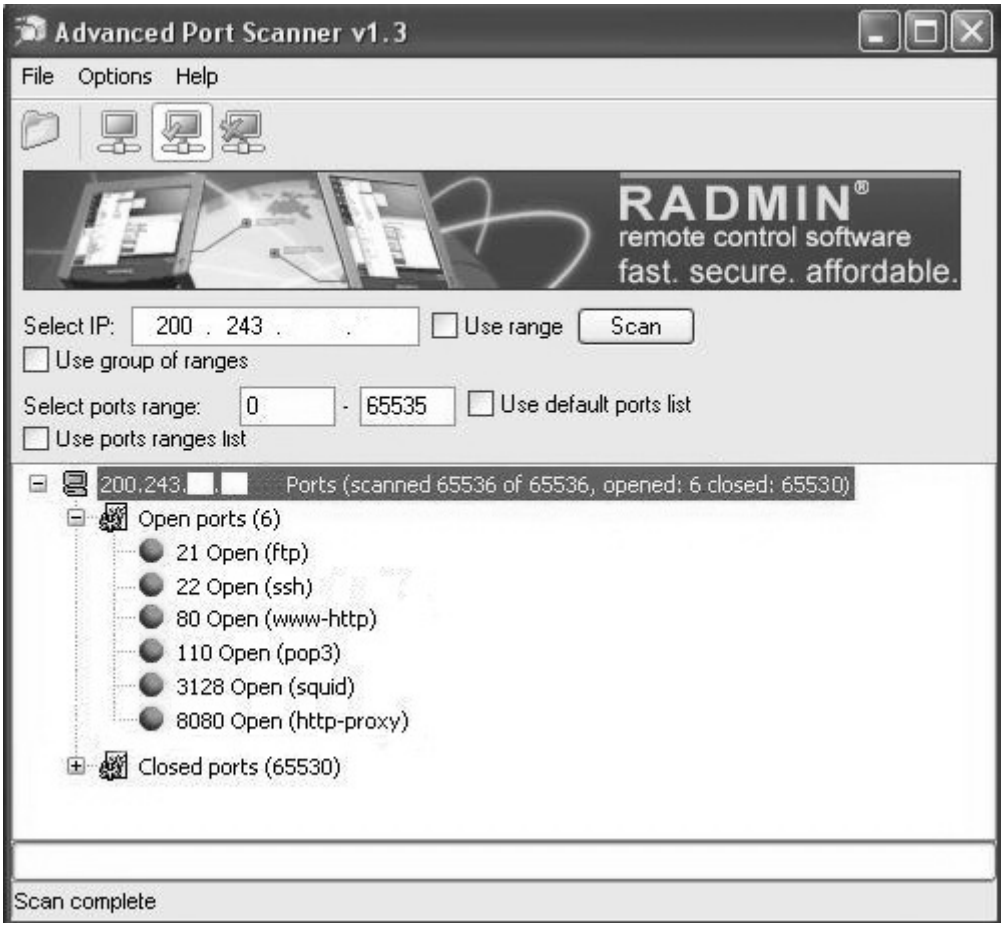

Figura 3. Situação do servidor de internet avaliada pelo *scanner* de portas. O IP foi removido da figura por garantia de sigilo

O hardware em si não é um ponto crítico. Os problemas estão desde configurações erradas até a limitação de software. O mais grave dos problemas vistos até agora é a falta de preparo do usuário que compromete e muito a segurança de toda a rede, utilizando e deixando que terceiros utilizem as máquinas de maneira inadequada. Em entrevista a uma funcionária que não quis se identificar descobriu-se que nunca houve qualquer tipo de treinamento específico aos usuários.

Para solução de tal problema é necessária uma implantação de uma política de segurança. Porém um desenvolvimento e implantação dessa, leva mais tempo do que se deseja e não há disponibilidade de alocação dos funcionários para treinamentos. Para auxiliar no processo mais demorado que é a implantação e adequação da política de segurança, propõe-se o desenvolvimento de um projeto de uma ferramenta extensível de treinamento progressivo. Essa ferramenta poderá alem de ser utilizada como auxilio na implantação da política de segurança da informação, poderá também ser configurada para aperfeiçoamento em outras áreas como uma política de qualidade, por exemplo, tornando o funcionário melhor preparado, com custo de treinamento bem reduzido.

3.4 – SOLUÇÕES

Com base na análise realizada dos dados obtidos, chegou-se às seguintes sugestões para solução dos problemas propostos na Tabela1 conforme listados na Tabela2.

Tabela 2. Algumas soluções para as questões de segurança encontrados na Tabela1

Algumas Questões de Segurança	
Problemas	**Soluções**
Portas do servidor de internet abertas	Configurar adequadamente fechando as portas e deixando-as ocultas
Nenhuma Workstation com um firewall ativo	Configurar adequadamente instalando e configurando um firewall, como por exemplo o **Comodo firewall**.
Serviço DHCP ativo	Configurar adequadamente desativando o serviço e utilizando ip´s fixos
Falta de controle de acesso de terceiros aos computadores	Implantação de uma política de segurança e treinamento de todos os funcionários que possuem Workstations
Falta de controle de conteúdo de acesso a internet	Implantação de uma política de segurança e\ou instalação de um servidor *proxy*
Uso das Workstations para fins pessoais	Implantação de uma política de segurança
Falha na infra-estrutura	Análise e Reformulação de todo funcionamento da infra-estrutura

4. A FERRAMENTA EXTENSÍVEL

Hoje em dia, o treinamento e especialização de funcionários demanda tempo livre e dinheiro, as vezes não planejados dentro do orçamento da empresa. Treinamentos desse tipo na maioria das vezes não surtem o efeito necessário graças a exatamente a falta de tempo, onde são entregues muitas informações ao usuário para um curto espaço de tempo. Pensando nisso propõe-se o desenvolvimento de um projeto sobre uma ferramenta extensível de treinamento progressivo.

4.1. FUNCIONAMENTO

A ferramenta será executada no computador cliente em que esse se conectará ao banco de dados que se encontra no computador servidor requisitando para aquele usuário o tipo correspondente de treinamento. Através das respostas dos usuários será possível

focar em uma área específica definida pelo baixo índice de conhecimento sobre o relativo assunto.

Será uma ferramenta extensível, pois, possibilitará adicionar módulos para utilização dessa não só na área de segurança de informação, mas também em áreas cotidianas de uma empresa como segurança do trabalho, meio ambiente, qualidade total, etc. Adicionando em cada módulo, funcionalidades peculiares a tais áreas permitindo obter resultados a partir de informações pré-gravadas no banco de dados.

4.2. PROJETO

O projeto de um software é realizado seguindo os padrões da engenharia de software para garantir um software seguro, de fácil manutenibilidade e estável.

Dentre a área de projetos, uma parte que se deve preocupar é em qual infra-estrutura se vai desenvolver e executar o sistema realizando para isso uma análise, sendo está que poderá acarretar o sucesso ou fracasso de todo o projeto. Para isso, desenvolve-se um estudo no qual são representadas através do diagrama de implantação, as reais necessidades para o sistema.

Nesse sistema que está sendo projetado, o seguinte diagrama de implantação (Figura 4) descreve suas necessidades físicas e lógicas. Tal diagrama demonstra a necessidade fundamental para o sistema, lembrando que por se tratar de uma ferramenta extensível, essas definições podem sofrer alterações, sendo que estas devem ser anexadas ao diagrama identificando-os correspondentemente aos seus Módulos.

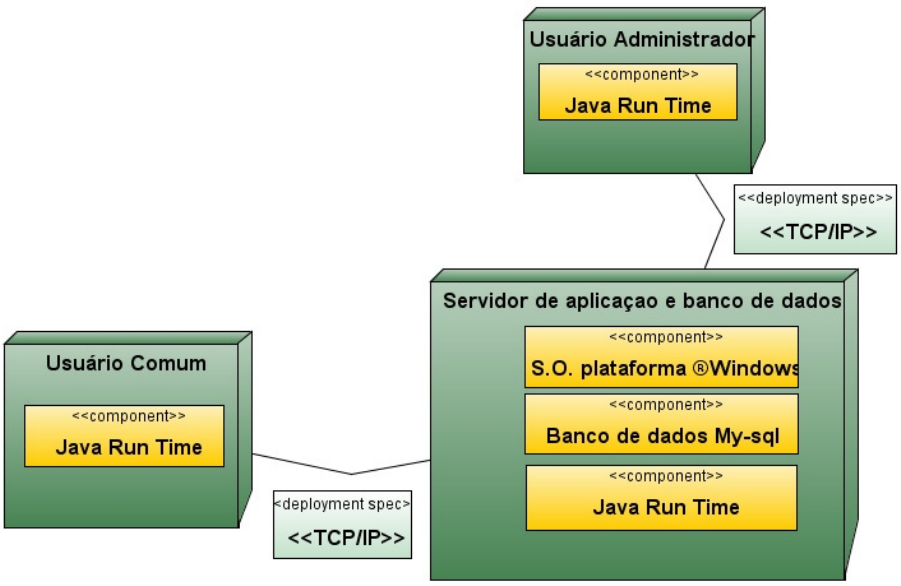

Figura 4. Diagrama de implantação

5. CONCLUSÃO

Cheguei após confeccionar este artigo, à conclusão de que não basta uma boa infra-estrutura física e lógica na rede que se quer proteger, pois, uma coisa que não mudará tão cedo é a necessidade de uma pessoa operar dentro da mesma. Por mais níveis de abstrações que isso leve, no final, sempre há um ser humano por trás operando e em caso de despreparo do mesmo, abrindo uma grande falha na estrutura, seja diretamente ou indiretamente.

Por isso a necessidade de preparação do usuário que se utiliza dessa infra-estrutura, deve ser colocada como uma prioridade após a adequação de todo meio físico e lógico no ambiente de segurança. Para no fim, chegar a um nível de segurança ideal.

Fica como sugestão para trabalhos futuros, uma implementação da aplicação proposta, ou ainda uma otimização do modelo já construído e disponível em : http://sites.google.com/site/usuarioeachave/ a partir do dia 27 de novembro de 2008. Esse modelo foi desenvolvido em Java e utiliza como banco de dados o My-sql. Nele, já se encontra funcional a parte onde o sistema fica rodando na bandeja do sistema, a parte onde se realiza cadastro e exclusão de usuários e textos de treinamento. Já se encontra desenvolvido nele também o timer para configuração da freqüência com que o as mensagens serão visualizadas.

6. BIBLIOGRAFIA

MARCIANO, João Luiz; Marques, Mamede Lima. **O enfoque social da segurança da informação**. Disponível em: < http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000300009&lng=en&nrm=iso>
Acesso em: 26 de Abril de 2008.

PLAMONDON, Scott. **Seu pior risco de segurança pode trabalhar para você**. Disponível em:
< http://www.microsoft.com/brasil/corporativo/securityrisk.mspx>
Acessado em: 4 de março de 2008.

THALENBERG, Marcelo. **Usuário e segurança**. Disponível em: http://www.microsoft.com/brasil/technet/Colunas/marcelothalenberg/usuario_seguranca.mspx. Acesso em: 4 de março de 2008.

CERT.br.**Cartilha de segurança para internet 3.1**. Disponível em : http://cartilha.cert.br/ . Acesso em: 26 de abril de 2008.

BOOCH, Grady; RUMBAUGH, James; JACOBSON, Ivar. **UML – Guia do Usuário.** Rio de Janeiro: Campus, 2006.

TANENBAUM, A., S. **Redes de Computadores**. Rio de Janeiro: Campus, 2003.