FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE - FANESE
NÚCLEO DE PÓS-GRADUAÇÃO E EXTENSÃO – NPGE
CURSO DE PÓS-GRADUAÇÃO "LATO SENSU"
EM REDES DE COMPUTADORES

RODRIGUS OLIVEIRA FEITOSA

O ELO FRACO DA SEGURANÇA NAS REDES DE COMPUTADORES

Aracaju – SE
2010

RODRIGUS OLIVEIRA FEITOSA

O ELO FRACO DA SEGURANÇA NAS REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão da FANESE, como requisito para obtenção do título de Especialista em Redes de Computadores

Orientador: Prof. Sérgio Andrade Galvão

Aracaju – SE
2010

RODRIGUS OLIVEIRA FEITOSA

O ELO FRACO DA SEGURANÇA NAS REDES DE COMPUTADORES

Trabalho de Conclusão de Curso apresentado ao Núcleo de Pós-Graduação e Extensão – NPGE, da Faculdade de Administração de Negócios de Sergipe – FANESE, como requisito para a obtenção do título de Especialista em Redes de Computadores

_____

Sérgio Andrade Galvão

_____

Professor M.Sc. Mário Vasconcelos Andrade

_____

Rodrigus Oliveira Feitosa

Aprovado (a) com média: _____

Aracaju (SE), 29 de janeiro de 2010.

RESUMO

As reflexões deste artigo centram-se na análise da importância da educação e conscientização do usuário das redes de computadores na elaboração das políticas de segurança das organizações e no fortalecimento da segurança dos dados que trafegam nessas redes, ressaltando o elemento humano como o elo mais importante e frágil no ciclo de proteção das informações, inserindo-o como uma das camadas dos modelos de referência de redes de computadores. Destacamos também a engenharia social como um dos maiores problemas de segurança atualmente.

Palavras-chave: camada 8; política de segurança; redes de computadores.

ABSTRACT

The reflections of this article focus on the analysis of the importance of education and awareness of the computer networks users on elaboration of the organization's security policies and strengthening of the security of data that traveling over those networks, emphasizing the human element as the most important and fragile link in the protection cycle of information, placing it as one of the layers of reference models of computer networks. We also highlight the social engineering as one of the biggest security problems today.

Keywords: layer 8; security policy; social engineering.

LISTA DE FIGURAS

Figura 1 - As oito camadas do modelo OSI 06

SUMÁRIO

RESUMO IV

ABSTRACT V

LISTA DE FIGURAS VI

1 INTRODUÇÃO 01

2 SEGURANÇA NAS REDES DE COMPUTADORES 03
2.1 A importância das Redes de Computadores 03
2.2 Segurança na Internet 04
2.3 Fragilidade na Segurança 05
2.4 A Necessidade da Segurança 05

3 O USUÁRIO COMO VULNERABILIDADE 06
3.1 A Camada 8 06
3.2 O Usuário Comum 07
3.3 Perigos que os Usuário Estão Expostos 07
3.3.1 *Spams* 08
3.3.2 E-mails falsos 08
3.3.3 *Hoaxes* 08
3.3.4 Golpe do *pendrive* 09
3.3.5 Senhas 09
3.3.6 Redes sem fio 10
3.4 Educação do Usuário Como Item da Política de Segurança 11

4 ENGENHARIA SOCIAL 12
4.1 O Que é o Engenharia Social? 12
4.2 Existe Segurança na Rede? 13
4.3 Como se Proteger 13
4.3.1 Defesa contra engenharia social 14

5 CONSIDERAÇÕES FINAIS 15

REFERÊNCIAS 16

1 INTRODUÇÃO

Fazendo uma analogia da segurança da informação com uma corrente, podemos afirmar que o elo mais importante da corrente, porém o mais frágil, é o usuário comum, que já é considerado por alguns profissionais como a camada oito do modelo de referência OSI[1]. Diante deste quadro, vemos que não bastam apenas precauções de segurança sobre a infra-estrutura, acesso e proteção da informação, sem levar em consideração possíveis falhas humanas.

Para se atingir a última camada de segurança, há uma série de cuidados a serem tomados, como capacitação e uso das ferramentas de segurança disponibilizadas, além do conhecimento sobre os riscos associados a cada aplicação. Além disso, devem ser implementados níveis de acesso às informações de acordo com as necessidades funcionais de cada um. E por fim, os usuários devem ter conhecimento de todas as responsabilidades perante o uso dos recursos tecnológicos, através de normas e regulamentos, com vistas à manutenção da confidencialidade e segurança dos dados a que tem acesso. A preparação do usuário serve, portanto, para fortalecer o elo mais fraco da corrente.

Os conceitos básicos de segurança da informação envolvem diversas definições. Termos oriundos da língua inglesa, o idioma padrão da computação, dificultam a assimilação por parte dos usuários comuns. Isso talvez seja uma primeira barreira. Exemplos comuns são os termos "*spam*" e "*phishing*", tão largamente usados hoje em dia, mas que muitas vezes não fazem sentido algum ao usuário comum.

Em geral, a primeira pergunta que os usuários podem fazer quando se menciona segurança é: "Por que alguém iria querer invadir meu computador?" Para respondê-la, é necessário que sejam entendidos os fundamentos mínimos da segurança de computadores e o porquê de se preocupar com este aspecto, mostrando ao usuário o quão importante são as informações que lhe podem ser roubadas.

Um sistema computacional é considerado seguro quando atende aos requisitos de confidencialidade, integridade e disponibilidade (CERT.br, 2006). Com base nessa tríade, devemos então ter em mente que os computadores, querem

[1] CARGILE, Antony. http://thecoffeedesk.com/news/index.php/2009/04/11/osi-model-layer-8. KRAUS, Christoffer. http://c2kraus.wordpress.com/2008/11/29/oitava-camada-osi-o-usuario.

sejam domésticos ou corporativos, armazenam informações que poderão ser valiosas para quem não deveria ter acesso. Esses equipamentos são diariamente utilizados para transações financeiras, elaboração de documentos, leitura e envio de e-mails, navegação em páginas web, entre outras coisas. Para evitar riscos, a melhor maneira é definir uma boa política de segurança voltada ao usuário comum, buscando sua educação e compromisso com a segurança.

Para a elaboração deste trabalho, usamos a metodologia da pesquisa bibliográfica em obras de referências internacionais e autores com experiência na área de segurança, e referências a casos reais relacionados ao tema tratado. Com esse trabalho temos o objetivo de evidenciar, principalmente aos profissionais da área de segurança da informação, que o ponto mais fraco das políticas de segurança das organizações e da Internet, deixou de serem os computadores e sistemas de proteção, e passou a ser as pessoas que utilizam desta tecnologia, devendo o elemento humano tornar-se o foco das atenções. Diante de tantos relatos ao redor do planeta de violações de segurança de informações, achamos de extrema relevância levantar esse tema, pois com o barateamento de equipamentos e do acesso à Internet, mais e mais casos de violações de segurança nas redes de computadores ocorrerão, principalmente devido à falta de conhecimento dos usuários, e cabe aos profissionais contornar essa falha e levar o conhecimento onde seja necessário.

2 SEGURANÇA NAS REDES DE COMPUTADORES

Para posicionarmos o nosso usuário no contexto da segurança da informação, precisamos primeiramente analisar o porquê devemos dar tanta atenção à questão da segurança na informação nas redes de computadores, para então entendermos por que o usuário comum deve estar no foco das políticas de segurança.

2.1 A Importância das Redes de Computadores

Hoje em dia podemos falar em rede de pessoas no lugar de rede de computadores, pois com a velocidade com que evoluem as comunicações entre as pessoas devido à convergência digital, não sabemos onde começa ou termina os caminhos que nos ligam uns aos outros. Os nós finais das redes estão onde as pessoas estão, nos *smartphones*, nos PDAs (*Personal Digital Assistant*, ou Assistente Pessoal Digital), nos celulares, nos televisores e também nos computadores. Com as redes sem fio de longo alcance, as redes de computadores não estão mais limitadas aos seus roteadores de borda, os sinais das redes estão no ar para quem quiser utilizar.

É interessante imaginar como as pessoas trabalhavam antes do advento das redes de computadores, pois quem trabalha na administração de redes corporativas, sempre recebe ligações de funcionários reclamando que estão sem poder trabalhar por que estão sem acesso à rede ou à Internet. Será que nos tornamos assim tão dependentes das redes de computadores? A resposta é sim. Temos que admitir que esse é um caminho sem volta, da mesma forma que ocorreu com a energia elétrica.

Claro que as redes de computadores não são somente importantes para a comunicação entre pessoas pura e simplesmente. O maior benefício das redes de computadores é a troca de dados de maneira rápida e confiável. Dados extremamente importantes que podem estar armazenados em computadores ultra seguros, atrás de imensas portas de aço e a metros de profundidade no subsolo, mas que muitas vezes são manipulados por usuários que não têm a mínima noção de segurança da informação.

Poderíamos definir o conceito de poder em três tempos distintos. Antes da Revolução Industrial, tinha o poder quem possuía a força bélica. A partir da

Revolução Industrial, o poder estava nas mãos de quem possuía a força financeira, o dinheiro. Mas na Era da Tecnologia Digital, detém o poder quem possui a informação. Portanto, na atualidade as maiores riquezas das corporações estão nos computadores, cadastros de clientes, registros de transações financeiras, registros contábeis, projetos científicos, etc.

2.2 Segurança na Internet

A Internet na maioria dos países ainda é “terra sem lei”, pois não existem legislações fortes e abrangentes o bastante para punir com rigor os criminosos virtuais. Mesmo naqueles países onde existem leis para crimes na Internet, elas não são tão abrangentes quanto a variedade de delitos que podem ser praticados na web. Até por que, ainda não existem formas suficientemente eficazes de se chegar aos verdadeiros culpados.

No Brasil, por exemplo, existe o Projeto Substitutivo do Senador Eduardo Azeredo ao projeto de Lei da Câmara nº 89/2003, e Projetos de Lei do Senado nº 137/2000, e nº 76/2000, que prevê que todos os provedores de Internet do país deverão armazenar os registros de acessos (*logs*) de todos os seus clientes por até três anos, para que possam ser usados para rastrear os usuários que cometerem ilícitos na Internet. Se pararmos para pensar, veremos que isso é impraticável e ridiculamente ineficiente.

O primeiro motivo é que os provedores teriam que possuir vários petabytes (10^{15} bytes) ou mais, para armazenar todos esses *logs*, o que iria encarecer muito este serviço aos clientes. E o segundo motivo, é que esses registros são passíveis de falha, pois se um cliente possui um *malware* instalado em sua máquina que a tornou um *host* zumbi, como ele poderia ser responsabilizado, pois sequer sabe que isso estava ocorrendo e o que é isso. Essa lei poderia até funcionar, há 15 anos.

Cada vez mais pessoas descobrem os benefícios e facilidades do mundo virtual. Transações bancárias, compras pela Internet, troca de mensagens instantâneas. Porém, todos esses benefícios vêm seguidos de implicações de segurança, e essas implicações normalmente são desconhecidas da maioria dos usuários comuns da rede, pois estes não compreendem, muitas vezes por pura falta de orientação, que a segurança também é sua responsabilidade.

2.3 Fragilidade na Segurança

A segurança das redes de computadores atualmente se baseia, em sua maioria, somente em controle de acesso por usuário e senha. E o acesso à Internet se popularizou de uma forma incomensurável. Talvez, o advento das redes sem fio tenha sido a queda da maior barreira para essa popularização do acesso à rede, mas não foi da melhor forma.

Praticamente qualquer pessoa pode comprar um roteador sem fio e usar em casa, é só conectar os cabos e pronto. Desta forma as pessoas não se preocupam em mudar o nome e senha padrão dos equipamentos, só querem que funcione da maneira mais fácil possível. A maioria dos equipamentos de rede sem fio 802.11 em funcionamento não utilizam nem mesmo os mecanismos básicos padrão de segurança, como o uso de senha, por mais simples que seja. (KUROSE, et al. SHIPLEY, 2001).

2.4 A Necessidade de Segurança

Os usuários comuns precisam entender que a necessidade de segurança é um problema de todos, e não somente dos provedores, inclusive por que os mais prejudicados são eles mesmos.

Com o crescimento das mídias sociais como Orkut, Facebook, Twitter, golpes cada vez mais elaborados são desenvolvidos, pois as técnicas usadas para escolher as vítimas se tornam mais inteligentes, além de e-mails e mensagens instantâneas. Isso ocorre porque as pessoas não estão preocupadas em preservar informações pessoais e divulgam dados sobre seu dia-a-dia, seus familiares, etc.

Com a disponibilização de uma série de informações pessoais, gostos e interesses, que por sua vez podem ser cruzados com os interesses e gostos dos seus amigos e amigos dos amigos, no fim do cruzamento pode-se gerar um forte motivo para conseguir um clique deste usuário, ou até para criar uma lista de possíveis senhas dele com o auxílio de ferramentas como o John the Riper[2].

[2] Ferramenta que a partir de sementes (*seeds*) pode gerar várias combinações de caracteres.

3 O USUÁRIO COMO VULNERABILIDADE

A maioria dos autores e profissionais definem a segurança de uma rede concentrando-se principalmente em proteger a comunicação e os recursos da rede (KUROSE e ROSS, 2006), implementando medidas de proteção, detecção de falhas e ataques à infra-estrutura, e reação aos ataques. Porém, esquece de um elemento fundamental no ciclo de proteção contínua, o usuário comum da rede, que não é um profissional de informática, mas utiliza os recursos da rede para acessar informações da organização.

3.1 A Camada 8

O usuário é tão importante para as redes computacionais que em alguns círculos de profissionais este é considerado como a camada oito do modelo de referência OSI (ou camada cinco no modelo TCP/IP) como observamos na figura abaixo.

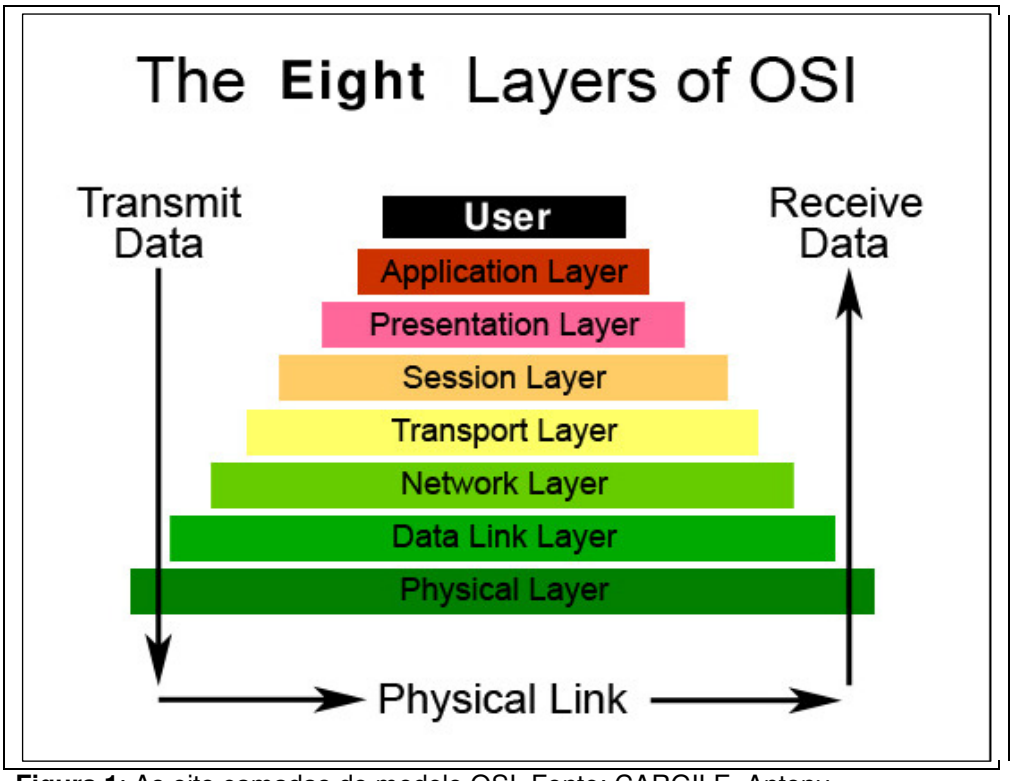

Figura 1: As oito camadas do modelo OSI. Fonte: CARGILE, Antony. http://thecoffeedesk.com /news/index.php/ 2009/04/11/osi-model-layer-8/..

No modelo de referência OSI relacionamos sete camadas, porém concordamos que os dados não podem passar pelas camadas e trafegar pela rede

sem a interferência dos usuários. É claro que para os conceitos de programação e eletrônica o usuário não tem interferência alguma, mas para o conceito de segurança, este é sim um elemento importantíssimo na elaboração de um projeto de segurança forte.

Talvez o usuário seja a camada mais difícil para se tratar a segurança, pois as demais estão sobre controle absoluto do profissional de segurança, mas o usuário não, ele tem vontade própria, e quase sempre não faz o que deveria seja qual for o motivo.

3.2 O Usuário Comum

O usuário comum seria aquele que usa o computador como uma ferramenta para seu trabalho, como o contabilista que usa uma planilha, o arquiteto que usa um programa CAD (*Computer-Aided Design*, ou desenho assistido por computador), ou uma secretária que usa o editor de texto e o leitor de e-mail. E, também podemos enquadrar aí, os usuários domésticos que usam a rede de computadores para realizar pesquisas, atualizar seus perfis nas redes sociais, enviar e receber e-mails e arquivos, trocar mensagens instantâneas, assistir vídeos, etc.

Esses usuários devem ser o foco principal da segurança, pois em sua maioria não conhecem os perigos que se escondem nas redes de computadores. E, como dito anteriormente, possuem vontade própria e nem sempre obedecem às regras de segurança, seja por desconhecimento, negligência ou propositalmente.

Todos os aspectos relacionados à segurança dos usuários e dos sistemas computacionais utilizados por estes indivíduos devem ser previstos nas políticas de segurança de forma a resguardar as corporações e os próprios usuários.

3.3 Perigos que os Usuários estão Expostos

Os usuários das redes de computadores estão expostos a diversos perigos, e não só por parte dos *hackers*, mas também de organizações criminosas que compram ferramentas de *hack* e as utilizam sem precisar de conhecimento algum de informática. Vamos falar um pouco dos golpes mais frequentes contra os usuários comuns.

3.3.1 *Spams*

Os tão indesejados *spams* são nada mais que e-mails com propagandas e correntes de pedidos enviados para inúmeros usuários sem que tenham sido solicitados. Isso não é uma tática nova dos vendedores, pois já existia bem antes da Internet, através dos correios. O que mudou foi a forma de entregar as correspondências e o custo para os vendedores. O incômodo só aumentou para quem as recebe. A medida que o usuário cria um novo e-mail e começa a utilizá-lo,a quantidade de *spams* que chega a sua caixa postal também começa a aumentar, por que o e-mail é mais divulgado na rede mundial, e alimenta as listas dos *spammers* (que são quem enviam os *spams*).

Para esse problema, não existe muito que fazer, além de aplicar filtros em sua conta, e a utilização de sistemas anti-spam por parte dos provedores do serviço.

3.3.2 E-mails falsos

Um e-mail falso tem por objetivo enganar quem o recebe, tentando se passar por verdadeiro, e levando o usuário a acessar uma página para roubo de senhas ou para induzi-lo a instalar um programa espião. Muitos destes e-mails são forjados para se passar por e-mails de bancos, da Receita Federal, da polícia, da empresa de telefonia, etc. As pessoas devem sempre desconfiar, pois esses órgãos e empresas nunca mandam e-mail para seus clientes, e na dúvida é só ligar para a organização e se esclarecer.

Recebendo um e-mail de uma instituição ou pessoa com que nunca teve contato ou cadastro deve-se desconfiar, pois muitas vezes os e-mails são muito bem forjados. O Centro de Atendimento a Incidentes de Segurança da Rede Nacional de Ensino e Pesquisa (CAIS/RNP) possui um catálogo constantemente atualizado de fraudes que pode ser consultado nesses casos, através do link: http://www.rnp.br/cais/fraudes.php.

3.3.3 *Hoaxes*

Hoaxes ou boatos, em português, se enquadram também no quesito de e-mails falsos, mas tem uma abordagem um pouco diferente. Um e-mail *hoaxe* possui

uma mensagem falsa utilizando-se de algum fato de repercussão nacional ou internacional, com a intenção de levar o usuário a instalar um *malware* ou acessar uma página maliciosa. Como exemplos, temos o acidente com o voo 447 da Air France no Oceano Atlântico, e mensagens com promoções de operadoras de telefonia.

O objetivo do atacante é atiçar a curiosidade de quem recebe o e-mail *hoaxe*, o que sabemos que não é difícil, uma vez que a curiosidade humana pode ser incontrolável. Da mesma forma que os e-mails falsos, o CAIS/RNP também lista em seu catálogo de fraudes esse tipo de mensagem.

3.3.4 Golpe do *pendrive*

Esse golpe é facilmente aplicável num país como o nosso, uma vez que o brasileiro sempre tenta tirar vantagem em tudo. O golpe do *pendrive* como ficou conhecido consiste em um *hacker* instalar um programa malicioso no dispositivo e deixá-lo em algum lugar público, esperando que alguém o encontre e resolva utilizá-lo. Assim que o "sortudo" que encontrou o *pendrive* conectá-lo ao computador, se o sistema de reprodução automática estiver ativado (que é o padrão), o programa contido no dispositivo será instalado automaticamente e a partir daí, poderá coletar tudo que for digitado no computador, como senhas e número de contas bancárias, e então enviá-las para o "azarado" que perdeu o *pendrive*.

3.3.5 Senhas

Uma senha serve para autenticar, ou seja, garantir a identidade do usuário. Por conta disso, deve ser mantida em sigilo, ser de difícil descoberta e trafegar em rede sempre criptografada. Uma pessoa de posse de uma senha alheia poderá assumir tal identidade. Isso a permitirá enviar e-mails, ter acesso a dados que normalmente não teria (quebra de confidencialidade) ou ainda desferir "ataques" a outros computadores escondendo sua real identidade. Por esses motivos, uma senha além de sigilosa, deve ser bem elaborada e ter um prazo de validade.

A elaboração de uma boa senha, ou seja, uma senha "forte", requer uma combinação de uso de letras maiúsculas e minúsculas, números e caracteres

especiais; devem-se evitar palavras que existam no dicionário, datas, ou associações pessoais (time pelo qual o usuário torce, nome de filhos etc.).

A validade da senha permitirá que o usuário use o sistema durante o tempo em que estiver prestando serviço a uma corporação. Há o relato de casos de usuários que mesmo após estarem desligados da uma instituição, têm suas senhas ativas no sistema. Outro fato importante da validade é que a repetição constante da senha, mesmo sendo "forte", poderá ser paciente e repetidamente observada por outra pessoa que tenha interesse em um acesso indevido. Diante de tais situações, a senha deve, portanto, ser um item de especial atenção no trato da segurança da informação.

3.3.6 Redes sem fio

Uma rede sem fio também tem fragilidades que podem ser exploradas, especialmente as instaladas no ambiente doméstico. Em geral, os usuários instalam equipamentos com a configuração de fábrica. As senhas de administração desses equipamentos são largamente conhecidas. Além disso, o acesso é feito sem chave de criptografia. Consequentemente, esses dois pontos devem ser cuidados com atenção. A senha padrão do equipamento deve ser trocada. Se possível, limitar a administração do equipamento a uma porta ethernet, não permitindo tal ação pela rede sem fio ou pela Internet. Outro cuidado que deve ser tomado é o uso de chaves de criptografia. Deve-se, por fim, trocar o nome da rede. O nome padrão indica o tipo de equipamento usado e pode servir para um ataque direcionado. Assim como no acesso através de banda larga, uma rede sem fio com a segurança comprometida poderá permitir que pessoa mal intencionada esconda sua identidade.

Outro ponto importante relacionado às redes sem fio é o fato do usuário desinformado, que tenta aproveitar uma rede sem fio que alguém inadvertidamente deixou sem senha. É fato que um *hacker* pode facilmente forjar uma rede sem fio com o uso de uma placa de rede sem fio, e induzir que as pessoas se conectem à Internet por meio desta rede, e assim roubar seus dados e senhas.

3.4 Educação do Usuário como Item da Política de Segurança

É necessário acompanhar toda a estrutura de TI para melhor orientar o usuário. Os problemas que os usuários enfrentam devem ser monitorados e analisados para uma solução correta. Muitos deles tentam ter acesso a conteúdo não autorizado, geralmente utilizam a técnica de tentativa e erro para descobrir senhas ou falhas de segurança. É preciso que o acompanhamento das ações dos usuários culmine num plano de esclarecimento e orientações para que o mesmo saiba que seus sistemas e dados estão seguros e monitorados inibindo ou descobrindo uma tentativa que possa ocorrer pelo fato dele acreditar que não há uma vigilância eficiente.

Os incidentes devem ser analisados para a formulação de um plano de segurança, este plano deve ser baseado na análise dos incidentes causados pelos usuários e suas necessidades. É necessário mostrar aos usuários os cuidados que devem ter ao trafegar informações por uma rede de dados. Os mais comuns são os vírus, eles necessitam da execução de um arquivo para que entre em funcionamento, assim, é importante informar que CDs, notebooks ou outra mídia portátil que entre na empresa seja verificado por antivírus ou outra ferramenta de remoção de *malware* para que não infecte a rede no qual se quer acessar.

Deve-se informar aos usuários os cuidados com *pendrives*, os riscos de sua utilização e as conseqüências se estiverem infectados. Tais mídias removíveis são de fácil infecção, pois os usuários as utilizam em diversos equipamentos muitos destes sem software de proteção antivírus. Outra precaução é com o vírus de macro. Os arquivos Word, Excel, PowerPoint e Access são os mais comuns a apresentarem esse tipo de vírus. Eles tendem a explorar vulnerabilidades dos aplicativos e interferem nos trabalhos do usuário.

Além disso, deve-se também ter cautela com os vírus de celular. Muitos usuários que utilizam *smartphones* ou que armazenam dados no celular correm o risco de ser infectados utilizando redes sem fio desconhecidas para acesso a arquivos por e-mail e MMS (mensagem multimídia) desconhecidos. Deve-se, então, informar aos usuários para que mantenham seus dispositivos Bluetooth desativados, habilitando-os apenas quando necessário, e atualizem os softwares do celular. Os celulares possuem uma opção de restaurar as configurações de fábrica, caso exista problema com relação a vírus e segurança.

4 ENGENHARIA SOCIAL

Com o barateamento nos custos de produção de componentes de tecnologia, os computadores e a Internet puderam alcançar ainda mais usuários, porém a educação para utilização deste valioso recurso não costuma contemplar o item segurança. Os *hackers* modernos descobriram que a obtenção de informações que podem ser usadas para invasão de sistemas e roubo de dados é muito mais fácil aplicando a engenharia social que tentando invadir redes de computadores.

4.1 O que é Engenharia Social?

A engenharia social é o método de se obter informações sensíveis de uma pessoa de forma aparentemente legal ou inofensiva. Existem centenas de recomendações que poderiam ser dadas aos usuários quanto à engenharia social, mas ainda assim eles estariam vulneráveis a um novo método de "ataque". Por isso, que se considera o usuário de computador o elo mais fraco na área de segurança da informação.

A partir de uma pesquisa da literatura e entrevistas com "*password crackers*" (literalmente, quebradores de senhas), algumas técnicas básicas foram relacionadas para o aprendizado de senhas por parte dos *hackers* e para implementação de programas de quebra de senhas (STALLINGS, 1995):

- Tentar senhas padrão usadas em contas padrão que são inclusas no sistema operacional e softwares. Muitos administradores não trocam essas senhas.
- Tentar exaustivamente combinações de caracteres (força bruta).
- Tentar palavras de dicionários ou listas de senhas mais usadas (*rainbow lists*).
- Coletar informações sobre os usuários tais como: nome completo, nome de parentes, animais de estimação, fotos e livros que o relacione a suas atividades, número de telefones, documentos ou residencial.
- Usar um cavalo de Tróia para liberação de acesso remoto à máquina.
- Fingir ser um usuário legítimo e solicitar a um operador ou gerente uma nova senha.
- Procurar senhas anotadas no escritório ou mesa do usuário (fato muito

comum de ocorrer).

- Observar o usuário digitando a senha.

As três últimas formas de obter a senha do usuário não são de natureza técnica, e recebe uma designação, Engenharia Social. A resposta para esse tipo de ataque geralmente também não deve ser técnica e envolve principalmente educação e conscientização dos usuários.

4.2 Existe Segurança na Rede?

O que é uma rede segura? Segundo Comer, redes não podem ser classificadas simplesmente como seguras ou não seguras, por que o termo não é absoluto (COMER, 1997). Cada pessoa ou organização deve definir, dentro de sua área de interesse, o nível de acesso que é permitido ou negado.

Devido à relatividade da definição de rede segura, o primeiro passo para uma organização seria elaborar sua política de segurança e definir o que dever ser segurado e até onde o deve ser, limitando desta forma o escopo de sua segurança.

Em seu livro “A Arte de Enganar”, Kevin Mitnick, o *hacker* mais famoso da história, lembra um ditado popular no meio da informática que diz que: Nem mesmo um computador desligado seria a forma mais segura de se guardar informações, pois um engenheiro social pode convencer o usuário a ligá-lo.

4.3 Como se Proteger

Já deixamos claro que para proteger informações e redes de computadores, não bastam ferramentas e trancas de segurança, pois o elemento humano é o ponto mais vulnerável. Portanto, cabe aos profissionais de segurança procurar meios para conscientização e treinamento em segurança da informação para esses usuários, e dentro das regras, lhes cobrar o estrito cumprimento das medidas adotadas para garantir a segurança na organização.

Definir uma política de segurança é algo complexo e requer muita experiência. Comer ensina que, definir uma política para dados que trafegam na rede não garante que os dados estarão seguros (COMER, 1997), por isso a política deve focar nos extremos desta rede, e nesses extremos encontram-se os usuários.

Além disso, uma política de segurança não pode ser definida a menos que a organização entenda o valor de suas informações.

Uma organização deve controlar o acesso à informação da mesma forma que controla o acesso a recursos físicos tais como escritórios, equipamentos e suprimentos. Por exemplo, para uma organização financeira, os dados cadastrais de seus clientes são tão, ou mais, importantes quanto o dinheiro contido nos cofres. Neste exemplo, os dados dos clientes deveriam ser mais bem protegidos, pois se roubados e disseminados na Internet, podem nunca mais terem seu sigilo recuperado, por outro lado, o dinheiro roubado pode ser ressarcido por uma seguradora contratada pelo banco.

4.3.1 Defesa contra engenharia social

Determinados ataques de engenharia social são particularmente difíceis de defender, por que a maioria das pessoas não é treinada para manter segredos. Assim, as pessoas não têm o hábito, por exemplo, de destruir anotações e recados em papel onde podem ter escrito senhas, de conversar discretamente sobre assuntos sensíveis, ou até manter um registro permanente de suas senhas próximas ao seu computador pessoal.

Algumas políticas e procedimentos de segurança que as organizações podem prover são:

- Educação e treinamento continuado a todos os empregados sobre segurança, com diretrizes de como lidar com requisições de informações sensíveis. E ensinar sobre as vulnerabilidades dos e-mails e redes sociais.
- Auditoria abrangente e periódica a fim de detectar intrusões.
- Termos de sigilo assinados por todos os empregados, atestando que têm conhecimento de suas responsabilidades sob a política de segurança da organização.

5 CONSIDERAÇÕES FINAIS

O usuário é de fundamental importância na segurança da informação. Ao entender e praticar os conceitos relativos aos temas, o usuário torna-se parte responsável na utilização dos recursos computacionais da organização. Como extensão, as práticas podem ser levadas ao ambiente doméstico, aumentando a segurança como um todo, uma vez que computadores domésticos são, em geral, mais vulneráveis. Os usuários devem, portanto, ser bem orientados para que possam incluir nas suas rotinas diárias as práticas referentes à segurança da informação.

Cada vez mais a segurança nas redes de computadores se tornará uma necessidade ainda mais visível, da mesma forma que as pessoas buscam segurança nos bancos, nas ruas, nas casas, etc. Com a velocidade que as redes sociais se expandem e oferecem mais e mais funcionalidades aos usuários, consequentemente mais vulneráveis se tornaram os meios de comunicação digitais e os dados que neles trafegam.

Assim, concluímos que somente com um conjunto de regras e boas práticas de segurança adotadas nas organizações e nos lares quanto ao correto e seguro uso dos recursos computacionais, poderemos controlar e prevenir os riscos que se escondem nas redes de computadores, em especial na Internet.

REFERÊNCIAS

CAIS - Centro de Atendimento a Incidentes de Segurança. **Fraudes identificadas e divulgadas pelo CAIS**. Disponível em: http://www.rnp.br/cais/fraudes.php. Acesso em: 13 de junho de 2009.

CAIS - Centro de Atendimento a Incidentes de Segurança. Recomendações **de Segurança**. http://www.rnp.br/documentos/arquivo.php?v=recomendacoes. Acesso em: 10 de junho de 2009.

CERT.br. **Cartilha de Segurança para a Internet**. Disponível em http://cartilha.cert. br/download/cartilha-completa.zip. Acesso em: 14 de junho de 2009.

COMER, Douglas E. **Computer Networks and Internets**. New Jersey: Prentice-Hall, 1997.

DOU. Diario Oficial da União, 14 Junho 2000. Decreto Nº 3505, de 13 de junho de 2000. **Institui a Politica de Segurança da Informação Nos Orgãos e Entidades da Administração Publica Federal**.

FONTES, Edison. **Segurança da Informação: O Usuário Faz a Diferença**. São Paulo, Saraiva: 2006.

KUROSE, James F., ROSS, Keith W. **Redes de Computadores e a Internet: uma abordagem top-down**. 3ª ed. São Paulo: Pearson Addison Wesley, 2006.

MITNICK, Kevin D., SIMON, Willian L. **A Arte de Enganar**. São Paulo, Pearson Education: 2003.

SAFERNET. **Projeto de Lei Sobre Crimes Cibernéticos**. Disponível em: http://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo. Acesso em: 29 de dezembro de 2009.

STALLINGS, William. Network **and Internetwork Security: principles and pratice**. New Jersey: Prentice-Hall, 1995.

TANEMBAUM, Andrew S. **Redes de Computadores**. 4ª Ed. Rio de Janeiro: Campus, 2003. 7ª Tiragem.

TEIXEIRA, Eli. **CCJ deve examinar projeto que pune crimes cometidos pela Internet**. Agência Senado. Disponível em: http://www.senado.gov.br/agencia/ver Noticia.aspx ?codNoticia=59325&codAplicativo=2. Acesso em: 29 de dezembro de 2009.