SEGURANÇA EM REDES DE COMPUTADORES: UMA ABORDAGEM SOBRE O COMPROMETIMENTO INDIVIDUAL EM BENEFICIO DA CORPORAÇÃO

Janilson Pereira do Nascimento

Resumo: A constante evolução tecnológica além de alterar o cenário das redes de computadores altera, também, o perfil dos malfeitores. Portanto torna-se necessário investir em software, hardware e treinamento para prover segurança das informações. Contudo, nenhuma dessas medidas é suficiente para prover efetiva segurança se o elo mais frágil do sistema for deixado em segundo plano. O usuário é o ponto mais vulnerável e também o mais importante no quesito segurança. Ele é alvo da engenharia social, que demonstra ser eficiente na obtenção de informações relevantes para desencadear uma sabotagem. Investir no treinamento do usuário para enfrentar as adversidades do mundo digital, revela-se uma estratégia forte no auxilio à manutenção de segurança das informações.

Palavra-chaves: Engenharia social; Tecnologia da informação; Segurança da informação; Vulnerabilidade.

Abstract: *The constant technologic evolution that besides change computer network scene do it either the perfil of the criminals. Therefore it is necessary to invest in software, hardware and training to provide information security. However, none of these measures is sufficient to provide effective security is the weakest link in the system is left in the background. The user is the most vulnerable and the most important in terms of security. He is the target of social engineering, which proves to be efficient in obtaining information relevant to trigger a sabotage. Investing in user training to face adversity in the digital world, reveals a strong strategy to aid in maintaining information security.*

Keyword: *Social engineering; Information technology; Information safety; Vulnerability.*

Introdução

Diante de um contexto tecnológico evolutivo e dinâmico onde a tecnologia avança a uma velocidade tão extraordinária que os equipamentos e as técnicas tornam-se obsoletos rapidamente e onde os vírus e outras ferramentas de sabotagens digitais estão sempre alguns passos à frente das medidas de defesa, burlando as regras de *firewall* e os mecanismos de detecção dos antivírus e dessa forma tornando-se cada vez mais frequentes as invasões sejam em computadores isoladas ou redes corporativas, com notada ênfase em *sites* do governo federal.

Segundo Caruso e Staffen (1991) a segurança em sistemas de informação não é um produto acabado ou algo que possa ser implementado e pronto, pelo contrário, os autores relatam que a segurança é um processo dinâmico e estará em constante evolução para acompanhar o ritmo galopante em que os sistemas de informação são atualizados. O desafio atual consiste em desenvolver ou adotar políticas de segurança em redes que sejam dinâmicas e que possam empregar mecanismos de proteção que sejam ágeis o bastante

para perceberem a mudanças no ambiente computacional e desencadearem medidas de defesa adequadas a cada situação no menor intervalo de tempo possível.

A vulnerabilidade de uma rede está inversamente relacionada ao grau de comprometimento de cada um de seus usuários. Quanto mais este o usuário estiver integrado aos processos de defesa, mais segura será a navegação na rede interna e na rede mundial. Neste sentido, o presente estudo visa estimular o debate sobre questões relacionadas à segurança das informações e redes de computadores, de modo a permitir a construção de uma base de conhecimento capaz de orientar o treinamento dos usuários, e dessa forma fornecer-lhes embasamento teórico suficiente para cada usuário manter seu equipamento livre dos comportamentos de risco. Agindo assim o usuário deixa de ser uma porta de entrada para intrusos e passa a ser uma sentinela a mais, guardando a integridade da rede.

A rotina das instituições assim como as dos usuários domésticos, tem sido alterada frequentemente pela ação de forças malignas[1] do ambiente computacional. Em geral as perturbações advêm da ação de vírus e ou de outras formas de sabotagem eletrônica. As instituições são obrigadas a investir uma soma considerável de seu capital na aquisição de ferramentas como antivírus, contratação e treinamento de pessoal especializado para prover o mínimo de segurança dos dados armazenados e até mesmo das informações publicadas no ambiente externo (internet). Embora não seja objeto deste estudo, os usuários domésticos também se veem obrigados a se protegeram das sabotagens sob pena de terem dados pessoais como número de cartão de créditos, cartão de banco e senhas furtados pela ação de criminosos. Diante de tantas ameaças não resta outra alternativa que não seja a realização de estudos em busca de incentivar os usuário a adotarem uma postura preventiva que seja adequada ao suporte de uma organização que zela pelos princípios da contra-inteligência. Visando dessa forma, prevenir-se contra ações de sabotagem e de espionagem e buscando a manutenção do sigilo e a garantia da integridade das informações armazenadas.

Segurança em redes de computadores

Segundo Houaiss (2007), segurança é o ato ou efeito de tornar algo seguro, dar estabilidade, firmeza, sustentação. Esse é um conceito geral e que abrange todas as formas de segurança, mas quando se fala em segurança de rede de computadores é necessário valer-se de algumas formas de abstrações para restringir o conceito geral ao nível desejado, ou seja, segurança física que envolve desde segurança do local onde a rede está instalada até a maneira de descarte do lixo tecnológico; segurança lógica que envolve a aplicação de conceitos de criptografia, geração e salvaguarda das senhas, rotinas de back-up, sistemas de detecção de intrusos entre outros; e o fator humano que é o elemento mais vulnerável no que se refere à segurança. Simplificando o conceito geral a ser aplicado em uma rede de computadores, a ação de segurança deve ser responsável por garantir que as informações armazenadas e as que trafegam pelas estruturas da rede, incluídos as que saem para a rede mundial e as que regressam dela, estejam livres da ação de pessoas não autorizadas (TANENBAUM, 2003).

Para prover segurança em uma rede de computadores, normalmente, a equipe de suporte utiliza diversas ferramentas e métodos, que em geral são baseadas em hardware e software como, por exemplo: antivírus, backup, firewall. No entanto como pode ser observando todas essas

[1] O termo "força maligna" foi empregado para representar qualquer programa, rotina ou procedimento que represente algum tipo de perigo ou ameaça à integridade dos dados e ou serviços da rede.

medidas estão baseadas em mecanismos de prevenção e detecção de vulnerabilidades. Analisando os conceitos de segurança e os mecanismos de prevenção e detecção, pode-se afirmar que segurança não pode ser considerada uma tecnologia, mas sim um processo em constante desenvolvimento e sabendo-se que os processos de espionagem e sabotagem também estão em larga escala de evolução, torna-se ineficiente qualquer mecanismo de defesa que não possa ser constantemente atualizado para fazer frente às ferramentas de ataque (WADLOW, 2001).

Ainda na mesma linha de pensamento, SCHNEIER(2001) Acrescenta que ao contrário do que o autor imaginava, o uso de criptografia não vai por si só resolver todos os problemas de relacionados à segurança e ao sigilo. O autor conclui que cada ferramenta em separado não pode solucionar nenhuma dessas questões, mas sim o uso coordenado de diversos recursos para a obtenção do êxito almejado. Torna-se, portanto, necessário que esse processo de segurança seja constantemente atualizado e a interface com usuário, que é o elo mais frágil e mais vulnerável desta corrente, deve ser amigável, pois esse deve se sentir confortável para utilizá-la com o máximo de proveito das ferramentas de defesa. Quando um usuário não consegue interagir com a interface do aplicativo, seja por diferença de idioma, seja por não encontrar facilmente o link para atualização do mesmo, seja por não saber pesquisar por vírus nos seus documentos em mídias removíveis entre outras atividades básicas, esse usuário passa a não acreditar no recurso que foi disponibilizado e torna-se um potencial ponto de vulnerabilidade para todo o sistema.

O elo mais frágil

Quando de fala de segurança de rede, infelizmente, os fatores humanos são deixados em segundo plano. E esse é um encaminhamento natural, tendo em vista que, equivocadamente, imagina-se que as ferramentas e artifícios utilizados na tentativa de prover segurança sejam por si só suficientes para garantir a integridade do sistema. No entanto VIDAL (2003), afirma que o ponto mais vulnerável em um sistema computacional é o componente humano, também conhecido pelo termo Humanware[2], conforme relata VIDAL (2000), o usuário fica sempre em segundo plano, sendo considerado apenas como um fator de produção. Ainda de acordo com VIDAL (2003) engenharia social é um artifício largamente empregado por malfeitores com o intuito de adquirir informações relevantes para serem utilizadas em suas ações de sabotagens. O comportamento humano é uma das variáveis mais complexas e por muitas vezes previsível. E qualquer pessoa mal intencionada irá utiliza-se das possibilidades de previsibilidade para aproximar-se de suas vítimas e lentamente adquirir a confiança, a partir desse momento, fazendo-se uma analogia e empregando-se um termo popular, "o peixe foi fisgado". Neste sentido, as redes de relacionamento demonstram-se perigosamente eficientes.

A manutenção de um estado de segurança em redes de computadores e em sistemas digitais de maneira geral é um ponto dos mais complexos. Segundo SCHNEIER(2001), mesmo se existisse uma rede ideal, protegida por um firewall ideal, um sistema de backup ideal, um aplicativo antivírus também ideal, em algum momento este hipotético e milagroso sistema computacional deveria ser acionado por um usuário. Essa interação é o maior risco á segurança de todo o sistema. As pessoas representam o elemento mais fraco e o fator mais susceptível de ser alterado ou burlado por outras pessoas que geralmente fazem uso da engenharia social para iludirem os

[2] Termo empregado em VIDAL (2000) para definir o componente humano de um sistema computacional,

usuários de um sistema e dessa forma alcançarem seus objetivos de passar pelas barreiras de segurança por mais que elas sejam bem elaboradas. De acordo com Tanenbaum (2003), A maioria dos casos de falhas em sistemas digitais são originados a partir de vulnerabilidades humanas. De modo geral causadas por pessoas que de alguma forma estão ou estiveram envolvidas com a organização afetada. São geralmente pessoas demitidas ou insatisfeitas com alguns aspectos de trabalho ou de relacionamento dentro da instituição[3], alguém que se sentiu subestimado ou que tenha sido preterido em alguma promoção profissional ou que julga lhe faltar o reconhecimento por parte de seus chefes ou de amigos de trabalho.

Além do que já foi exposto, Wadlow(2001) lembra que três fatores são extremamente importantes para que ocorra uma operação maliciosa de sabotagem ou invasão de um sistema, que são: habilidade, motivação e oportunidade. Se alguém que tenha habilidade e oportunidade, a qualquer momento que venha a ser motivado, pode tornar-se um potencial atacante ou abrir as portas para que outros possam realizar as operações indesejadas. No entanto evitar a insatisfação de alguém é uma variável impossível de ser controlada por parte dos profissionais envolvidos diretamente com as questões de segurança das informações. Os profissionais de Tecnologia da Informação (TI) que são os responsáveis por elaborar, propor e manter as políticas de segurança das informações devem também se preocupar com os aspectos sociais que podem comprometer a segurança da rede de dados. Uma equipe de segurança da informação pode carecer do apoio de psicólogos e especialistas em análise do comportamento humano. Tais profissionais poderiam ser de grade aplicabilidade na detecção de alguns aspectos relativos à mudança de comportamento, tais: introspecção, pouca ou excessiva sociabilidade dentre outros, que poderiam ser indícios de um potencial atacante ou uma vítima.

Engenharia social

A engenharia social pode ser definida como uma metodologia empregada para obter informações privilegiadas sem a necessidade do emprego de aparatos tecnológicos. Não necessita do emprego de força bruta para quebrar chaves de criptografias ou descobrir senhas. Conforme afirma SCHNEIER(2001), o pobre ser humano acaba forçado ou convencido a ceder informações ao oponente que sempre se apresenta e aparenta ser amigo. O engenheiro social utiliza todas as artimanhas possíveis para enganar sua vítima e de maneira sutil vai colhendo informações preciosas que na maioria das vezes são reveladas por pura inocência da vítima.

As pessoas dessa natureza aproveitam-se de momentos de fraqueza de algum funcionário. Eles são geralmente hábeis na arte de enganar e detêm grande poder de convencimento, mostrando-se solicito e atencioso e agindo assim acabam evolvendo o funcionário e conquistando-lhe a confiança.(VIDAL, 2007).

MELO(2006), afirma que essa é "uma técnica muito utilizada por *crackers* para adquirir informações importantes para o desenvolvimento de seu ataque." O malfeitor tenta obter informações relevantes para utilizá-las em seu ataque por meio de recursos onde ele se faz passar por outra pessoa ou até mesmo por uma entidade. Por exemplo, pelo telefone o impostor se faz passar por um cliente da instituição, solicitando que o funcionário lhe tire alguma dúvida. Certamente o malfeitor já conhece algum ponto fraco do funcionário ou alguma vulnerabilidade

[3] O termo instituição foi empregado inúmeras vezes para designar a organização com o intuito de preservar em sigilo o nome da organização.

da instituição e aproveita-se da situação para convencer a vítima lhe ceder informações que não deveriam ser divulgadas para qualquer pessoa.

Responsabilidade na utilização dos recursos da rede

À medida que ocorre o crescimento das estruturas de rede instaladas, normalmente crescem também os problemas e as vulnerabilidades. Dessa forma faz-se necessário a adoção de todas as medidas possíveis e aplicáveis para se obter melhore rendimento no desempenho das atividades básicas da instituição com o menor impacto na performance da rede. Nesse sentido o usuário deve ser tratado com prioridade, pois quando os administradores de redes podem contar com a colaboração e o apoio do usuário, as tarefas de manter a rede segura se tornam menos penosas. É necessário tê-lo como um aliado na difícil tarefa de prover segurança a uma rede de dados. Para a obtenção de melhores resultados deve-se disponibilizar treinamento adequado por meio de cursos de capacitação profissional, campanha de conscientização e mecanismo de estímulo, visando com isso preparar o usuário para identificar e lidar com situações de vulnerabilidade, reforçando dessa forma o elo mais frágil e reduzindo o espaço de atuação dos sabotadores e em consequência aprimorando os mecanismos de segurança da informação.

Considerações finais

Negar a relevância desse tema é negar a realidade de uma sociedade globalizada e absolutamente sem fronteiras. É necessária uma análise detalhada do caso de cada ambiente computacional dentro do seu contexto local e global, levando-se em consideração os aspectos do ambiente computacional e do contexto social em favor da relevância das informações, sejam estas geradas no interior da instituição, armazenadas em base de dados ou apenas que transitam pela rede interna.

Uma política de segurança das informações voltada a priorizar as necessidades dos usuários sem comprometer os aspectos relevantes das atividades da instituição, e que vise à redução das vulnerabilidades de seu elemento mais frágil e, portanto, o mais importante. Pode representar o ponto de equilíbrio que tornará a rede de computadores tanto mais segura quanto maior for o comprometimento de seu capital humano.

O comprometimento do usuário diante de situações críticas no manuseio dos recursos tecnológicos pode evitar que este usuário venha a ser envolvido pelas ações da engenharia social, ou que ele venha a cair nas ciladas digitais que evoluem mais velozmente que os mecanismos de defesa.

Portanto conclui-se que as ações que tenham como foco orientar o usuário obtêm resultados mais imediatos, mais sólidos e mais duradouros. O usuário bem treinado atinge um nível de comprometimento com a segurança mais elevado no que se refere à prevenção contra os malfeitores do mundo digital. E esse usuário necessitará de menos treinamento para adaptar-se às novas situações do que aquele que nunca teve contato com tais orientações. Portanto o usuário estará constantemente aumentando o seu nível de conhecimento e estará evoluindo constantemente e somando o seu esforço individual aos esforços dos profissionais encarregados pelas políticas e ações de segurança, contribui para a manutenção da segurança das informações. Por essa razão torna-se uma estratégia de defesa orientar, prover treinamento e

encorajar os usuários para que eles possam sair da condição de vítimas dos sabotadores para a condição de sentinelas atentas na defesa dos interesses coletivos e de crescimento da instituição.

Referências

CARUSO, C. A. A., STEFFEN, F. D. ***Segurança em Informática***. 1. ed. Rio de Janeiro: LTC-Livros Técnicos e Científicos Editora, 1991. 274 p.

HOUAISS. ***Dicionário da língua portuguesa***. Referência online HTTP://houaiss.uol.com.br Acessado em maio de 2009.

MELO, Sandro. ***Exploração de Vulnerabilidades em Redes TCP/IP*.** 2ª ed., Rio de Janeiro: Alta Books, 2006.

SCHNEIER, Bruce. ***Segurança.com: Segredos e mentiras sobre a proteção na vida digital***. Rio de Janeiro: Campus, 2001.

TANENBAUM. Andrew S. ***Redes de computadores***. 4. Ed. Rio de Janeiro. Campus. 2003.

VIDAL, Marcos Tadeu 6on Lützow. ***Segurança de Redes 1*** – Rio de Janeiro: UFF / CEP – EB, 2007. 156p. – (Curso de Criptografia e Segurança em Redes). Rio de Janeiro 2007.

VIDAL, Mario César. ***Introdução à ergonomia***. Apostilha do curso de especialização em ergonomia contemporânea - CESERG – COPPE/UFRJ. Rio de Janeiro. 2000.

WADDLOW, Thomas A. ***Segurança de redes***: Projeto e gerenciamento de redes seguras. Rio de Janeiro. Campos. 2001.