O Fator Humano na Segurança da Informação [1]

Heleno Menezes, Leonardo, Moises Jacobino de Morais e Wladys [2]

Resumo

Com a adoção de ferramentas cada vez mais sofisticadas para a implementação de autenticação, autorização e manutenção da privacidade/sigilo na transmissão e armazenamento de informações, os sistemas em rede ampliaram o grau de dificuldade para a obtenção de informações de forma não autorizada, tornando as redes de computadores mais difíceis de serem invadidas. Porém, todo sistema é tão forte quanto seu elo mais fraco. Assim, se o aparato de segurança relacionado ao hardware e ao software da rede de computadores torna-se sofisticado e eficiente, os procedimentos adotados para quebra de segurança voltam-se para o fator humano. As técnicas adotadas pela Engenharia Social buscam obter informações que possibilitem atuar sobre os aspectos características e princípios básicos de segurança nos sistemas de informação.

Palavras-chave

Engenharia social, segurança da informação, política de segurança, riscos, fator humano.

The Human factor in the Security of the Information [1]

Summary

The utilization of very sophisticated hardware and software tools for implementation of a security information policy, including authentication, guarantee of privacy, integrity and confidentiality of user's information, are very common nowadays. The network systems have improved the security level in order to avoid having non-authorized computer based information. Therefore, the main vulnerability is the human being. Techniques adopted by social engineering are used in order to get details about characteristics and principles of information security system.

Keywords

Social Engineer, Information Security, Safety Policy, Risks , Human Factor.

---

1 Trabalho desenvolvido no MBA – Gestão de Sistemas de Informação da UCB (julho/2004)

2 Alunos do curso MBA-GSI (heleno.menezes@unimedbrasilia.com.br, Leonardo@, moisesj@prdf.mpf.gov.br, wladys@)

1. Introdução

De acordo com algumas pesquisas feitas em ambientes computacionais, as causas mais freqüentes de acesso não autorizado, perda de dados ou pane nos sistemas informatizados são erros, omissões, sabotagem, extorsão, invasões criminosas provocadas por pessoas contratadas pela própria organização. Os acidentes ambientais (incêndios, enchentes, sobrecarga elétrica, corte de energia), as falhas de *hardware* e *software* e os invasores externos aparecem em segundo plano. Eis porque o fator humano é tão importante.

Os funcionários mal intencionados têm tempo disponível e liberdade de vasculhar as mesas de outros funcionários, ler e copiar documentos e informações internas ou confidenciais. Sabem como a organização funciona e que tipo de informação seria valiosa para a concorrência. A espionagem industrial, por exemplo, costuma utilizar funcionários insatisfeitos como mão de obra.

Os ex-funcionários são igualmente interessantes para a concorrência. Muitas vezes essas pessoas prejudicam sua antiga instituição de maneira não intencional, simplesmente pelo fato de saberem o que sabem. Apesar de não terem mais acesso direto às informações internas, eles conhecem os procedimentos de segurança, a forma de atuação da empresa, seus hábitos e vulnerabilidades.

Para reduzir os riscos de erros humanos ou atos criminosos por parte dos usuários internos, é aconselhável que a organização estabeleça políticas, controles e procedimentos enfocando a área de pessoal. As atividades dos funcionários devem ser controladas por meio de procedimentos de operação e supervisão documentados, e políticas adequadas de seleção, treinamento, avaliação de desempenho, segregação de funções e interrupção de contratos de trabalho.

2. Engenharia Social

"Eu tinha tanto sucesso nessa linha de ataque que raramente tinha que lançar mão de um ataque técnico"

Kevin Mitnick, ex-hacker especialista em Engenharia Social

A engenharia social evita a criptografia, segurança de computador, segurança de rede e tudo o mais que for tecnológico. Ela vai diretamente para o elo mais fraco de qualquer sistema de segurança: O ser humano.

Os ataques desta natureza podem ser realizados através de telefonemas, envio de mensagens por correio eletrônico, salas de bate-papo e pasmem, até mesmo pessoalmente. Já foram identificados casos em que alguém, se passando por um funcionário do suporte técnico de um provedor de acesso Internet, telefonou para um usuário informando que a conexão estava com algum tipo de problema e que para consertar necessitava da sua senha. O usuário, na sua ingenuidade, fornece a senha e depois vai ver no extrato mensal do provedor que utilizou muito mais recursos do que realmente o tinha feito.

Um lado que deve ser muito bem observado por todos, é o fator emocional. Os ataques de engenharia social por correio eletrônico têm sido realizados com maior freqüência através de mensagens de mulheres para homens e vice-versa.Este ataque motivado pelo fator emocional é também muito utilizado nas salas de chat. Meninas

que se dizem jovens, atraentes e de bom papo, podem ser na verdade um verdadeiro farsante, que manipula os sentimentos das pessoas para fisgar uma informação preciosa.

Há de se ter muito cuidado também com os documentos impressos dentro da empresa. Papéis amassados e jogados no lixo são um convite para fraudadores. É preciso estar atentos também com as informações a respeito da empresa. A divulgação de nomes, funções, ramais, endereço eletrônico e outros dados a respeito da estrutura organizacional da empresa, podem ser utilizadas por pessoas maliciosas. Em muitas organizações é comum encontrar uma lista na entrada dos corredores de acesso, ou na mesa das secretárias, contendo o nome, identificação eletrônica do usuário e função exercida pelo mesmo na empresa.

Outro exemplo de ataque de engenharia social diz respeito às entrevistas para emprego, onde muitas vezes o candidato à vaga passa várias informações da empresa em que trabalha. Pode não haver vaga alguma para o cargo. Apenas a empresa, que supostamente abriu a vaga, está tentando levantar informações dos seus concorrentes.

3. Segurança da informação

As pessoas não entendem riscos. Elas podem entender, em um sentido geral, quando o risco é imediato. As pessoas trancam suas portas e suas janelas. Elas verificam se ninguém as está seguindo quando entram em uma rua escura. As pessoas não entendem ameaças sutis. Elas não acreditam que um pacote poderia ser uma bomba, ou que o gentil rapaz da loja de conveniência poderia estar vendendo número de cartão de crédito para o pessoal ao lado. E por que deveriam acreditar? Isso quase nunca acontece.

É importante uma análise dos valores das informações no caso destas serem roubadas ou perdidas para que seja então elaborado o projeto de segurança. Importante também é fazer uma análise das ameaças e vulnerabilidades do ambiente de informática levando em consideração todos os eventos adversos que podem explorar fragilidades de segurança desse ambiente e acarretar danos. É claro que o custo de se proteger contra uma ameaça pode ser mais alto do que o dano que essa ameaça pode provocar, isto é, nem todas as ameaças merecem ser combatidas. É necessário fazer uma análise de custo-benefício antes de tomar qualquer medida. O ambiente deve, além de prevenir os problemas, também ser capaz de efetuar alertas quando sofrer danos ou ser invadido. As soluções devem ser concebidas globalmente: desde a conscientização dos funcionários sobre os riscos até o aumento efetivo do controle de segurança.

3.1. Princípios de segurança:

3.1.1. **Autenticidade:** O controle de autenticidade está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo.

3.1.2. **Confidencialidade:** Significa proteger informações contra revelação para alguém não autorizado. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado

por seu proprietário.

3.1.3. **Integridade:** Consiste em proteger a informação contra modificações sem a permissão explicita do proprietário. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e inclusão de novas informações.

3.1.4. **Disponibilidade:** Consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis, assegurando ao usuário o acesso aos dados sempre que necessário.

3.2. Política de segurança

Uma política de segurança é um instrumento importante para proteger a sua organização contra ameaças à segurança da informação que a ela pertence ou que está sob sua responsabilidade. Uma ameaça à segurança é compreendida neste contexto como a quebra de uma ou mais de suas três propriedades fundamentais (confidencialidade, integridade e disponibilidade).

A política de segurança não define procedimentos específicos de manipulação e proteção da informação, mas atribui direitos e responsabilidades às pessoas (usuários, administradores de redes e sistemas, funcionários, gerentes, etc.) que lidam com essa informação. Desta forma, elas sabem quais as expectativas que podem ter e quais são as suas atribuições em relação à segurança dos recursos computacionais com os quais trabalham. Além disso, a política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

Uma tarefa extremamente importante e que deve fazer parte do cotidiano de administradores de redes é a constante educação dos usuários. Sabe-se que grande parte dos problemas de segurança são originados na rede interna da organização e, muitas vezes, são causados pelo desconhecimento de conceitos e procedimentos básicos de segurança por parte dos usuários.

Um exemplo clássico deste problema é a má configuração do programa de leitura de *emails* de um usuário, que faz com que qualquer arquivo anexado a uma mensagem seja automaticamente aberto ou executado, permitindo a instalação de *backdoors*, cavalos de tróia, disseminação de vírus, etc.

O primeiro fator que contribui diretamente para o processo de educação é o estabelecimento de políticas de segurança e de uso aceitável claras, sem ambigüidades, conhecidas e completamente entendidas pelos usuários da rede.

Outro fator importante é o estabelecimento de um canal de comunicação, por exemplo, através de listas de *emails*, onde informações sobre questões relevantes de segurança são freqüentemente passadas para os usuários da rede. A descoberta de uma vulnerabilidade de segurança que afeta o servidor Web da organização pode não ser relevante para os usuários, mas a notificação da descoberta de um novo vírus, sua forma de infecção e métodos de prevenção são informações que devem ser conhecidas e aplicadas por todos os usuários.

Muitas vezes e, principalmente, em grandes organizações, tarefas como a instalação e configuração do sistema operacional e *softwares* de um computador são realizadas pelo próprio usuário. Daí vem um dos fatores de grande importância neste processo de educação, pois a execução de tais tarefas tem impacto direto na segurança das redes e sistemas de uma organização.

Recomenda-se fortemente que os administradores tenham cuidado ao buscar ajuda em listas de discussão e outros fóruns na Internet. Estes recursos podem ser valiosos na resolução de problemas, mas também podem ser usados por terceiros para coleta de informações.

Procure reduzir a exposição da sua rede em fóruns públicos -- por exemplo, use endereços IP, nomes de *hosts* e usuários hipotéticos, e tente não revelar mais sobre a topologia da rede do que o estritamente necessário para resolver um dado problema. Tome cuidado com orientações passadas por pessoas desconhecidas, e evite executar programas de origem obscura ou não confiável -- eles podem ser uma armadilha.

4. Conclusão

Pelo fato de os recursos humanos serem o elo mais fraco das organizações em questões relacionadas à segurança da informação, uma vez que não correspondem diretamente a área essencialmente técnica, faz-se necessária, dentro de uma política de segurança da informação, a adoção de medidas voltadas para o treinamento, capacitação de RH, apresentação de seminários, palestras que foquem à importância com que deve ser tratado o fator humano na SI. Levando-se em consideração que dificilmente a engenharia social será erradicada, essas medidas, certamente, farão com que vulnerabilidades relacionadas à engenharia social sejam minimizadas no âmbito das organizações.
No fim, a engenharia social provavelmente sempre funcionará.

Referências

MÓDULO Security Solutions. Disponível em: http://www.modulo.com.br. Acesso em: 02/07/2004

NIC Br Security Office. Disponível em: http://www.nbso.nic.br. Acesso em: consulta em 2004