8º FÓRUM ENSINO · PESQUISA EXTENSÃO · GESTÃO FEPEG
UNIVERSIDADE: SABERES E PRÁTICAS INOVADORAS
Trabalhos científicos · Apresentações artísticas e culturais · Debates · Minicursos e Palestras
REALIZAÇÃO: Unimontes
APOIO: FAPEMIG FADENOR
24 a 27 setembro
Campus Universitário Professor Darcy Ribeiro
www.fepeg.unimontes.br

Segurança Digital: Uma Revisão sobre Ataques Perpetrados por *Hackers* e *Crackers*

Ismael Mendes dos Santos Junior, Reginaldo Morais de Macedo, June Marize Castro Silva Martins, Heráclides Veloso Marques

INTRODUÇÃO

O surgimento da *World Wide Web* no início dos anos de 1990, com a capacidade inédita de exibição de imagens, sons e textos em forma hipertextual propiciou o desenvolvimento de ferramentas de negócios eletrônicos (*e-business*), tanto em sua forma privada (*e-commerce*) quanto pública (*e-government*) (LAUDON; LAUDON, 2010; TANENBAUM, 2011). O fortalecimento dos negócios no ambiente virtual trouxe para as organizações, além, de maior agilidade para realização de suas operações, também, maiores responsabilidades no gerenciamento de seus dados disponibilizados, assim como de seus clientes (SCHNEIER, 2001).

Garantir a segurança de tais dados, então, passou a constituir-se de atividade prioritária para as organizações que desejam atuar no ambiente virtual, buscando, simultaneamente, maximizar a segurança de dados e informações sem, contudo, maximizar a complexidade dos sistemas a serem utilizados por todas as categorias de indivíduos envolvidos em suas transações e, para isto, em última instância, tornou-se necessário compreender os processos pelos quais *hackers* e *crackers* buscam ter acesso ao ambiente organizacional digital que costumeiramente são conhecidos como ataques (SCHNEIER, 2001; FONTES, 2006; LAUDON; LAUDON, 2010; GORDON; GORDON, 2011).

"Hacker é um indivíduo que pretende obter acesso não autorizado a um sistema de computador [...] Cracker normalmente é usado para designar o hacker com intenções criminosas", embora os termos sejam utilizados de forma indiferente fora das comunidades específicas (LAUDON; LAUDON, 2010, p. 221).

Em termos metodológicos, o presente trabalho caracteriza-se pela abordagem qualitativa, de base bibliográfica, constituindo-se de revisão da literatura baseada em livros internacionais e nacionais de autores reconhecidos pela experiência em gestão da segurança organizacional digital.

DESENVOLVIMENTO

CATEGORIAS DE ATAQUES

Ataques Genéricos

Para Cheswick, Bellovin e Rubin (2003), violar o arquivo de **senhas** é uma das primeiras ações que os invasores tentam realizar. Historicamente, a segurança dos arquivos de armazenamento de senhas estava baseada na ocultação destes arquivos; em seguida, os arquivos de senha passaram a ser criptografados e os ataques aos arquivos de senhas passaram a ser, então, sobre a criptografia que os protegia. Fontes (2006, p. 33) é categórico ao afirmar que "[...] ao utilizar senhas, escolha uma sequência de caracteres fácil de ser lembrada por você e difícil de ser adivinhada por outra pessoa", visto que romper sólidos algoritmos de criptografia é substancialmente mais complexo que buscar determinar senhas consideradas fracas definidas pelos usuários.

A **Engenharia Social**, por sua vez, conforme Schneier (2001, p. 266), "[...] vai diretamente para o elo mais fraco de qualquer sistema de segurança: o pobre ser humano sendo forçado a realizar seu trabalho, e precisando de toda a ajuda que puder obter". Schneier (2001), Cheswick, Bellovin e Rubin (2003) e Fontes (2006) demonstram que a engenharia social pode ocorrer de forma pessoal, principalmente, por telefone, em que o invasor contata a vítima e faz-se passar por algum conhecido a fim de obter informações como senhas, características dos sistemas de segurança ou mesmo conhecimento de como evitá-las, ou ainda, de forma impessoal e automatizada, como, por exemplo, através de e-mails enviados a grandes grupos de usuários que atendem a um determinado requisito ou parâmetro; certamente, nem todos responderão, mas alguém responderá positivamente municiando o invasor com aquilo que deseja.

Os **erros** (*bugs*) existentes nos sistemas acarretam vulnerabilidades que podem comprometer a segurança dos mesmos (CHESWICK; BELLOVIN; RUBIN, 2003). Conforme Schneier (2001, p. 206): "[...] erros ocorrem aleatoriamente, e a maioria deles nunca será encontrada sob o uso normal. Mas os atacantes buscarão erros em potencial e os usarão deliberadamente para o seu proveito". Por sua vez, as **portas dos**

fundos (*backdoors*) são fragmentos de código que permitem que alguém acesse o *software* em tempo ou espaço não autorizado (TANENBAUM, 2011). Em relação à utilização de *backdoors* pode-se classificar o software malicioso em vermes que são programas de computador que vagam pela rede, rastreando, analisando e transmitindo informações consideradas importantes para o invasor, e cavalos de tróia que são trechos de algum *software* que passam a realizar tarefas inesperadas a partir de um determinado evento monitorável (SCHNEIER, 2001).

Concordam Cheswick, Bellovin e Rubin (2003), Kaufman, Perlman e Speciner (2005) e Schneier (2001) que, de forma geral, os **ataques aos sistemas de autenticação** baseiam-se na subversão daquilo que identifica e garante o acesso do usuário ao sistema. Desta forma, ataques a sistemas baseados em algo que o usuário sabe, como, por exemplo, senhas, têm por objetivo identificar esta chave e de posse da mesma garantir o acesso ao sistema. Alternativamente, ataques a sistemas baseados em como é o usuário, caso da biometria, tentam replicar as formas, cores, posições, dentre outros atributos que o usuário apresenta em si, como, por exemplo, digitais, formato e cor dos olhos e voz.

Por sua vez, ataques a sistemas cuja autenticação é realizada através de algo que o usuário possui, como, por exemplo, **cartões inteligentes**, são realizados com a intenção de obter acesso aos mesmos, ou ainda, duplicá-los. Schneier (2001) apresenta os principais ataques perpetrados contra os *smart cards* (cartões inteligentes), quais sejam: a) o terminal é modificado e retém informações do cartão e do usuário durante o processo de interação, as quais, oportunamente, são repassadas ao atacante; b) o atacante utiliza cartões roubados, clonados ou modificados para acessar os sistemas do terminal; c) o usuário do cartão deseja ter acesso e modificar determinadas informações contidas no cartão; d) o proprietário do terminal pode monitorar a utilização do cartão, armazenar suas principais informações, bloquear determinadas atividades, falsificar transações e/ou registros, bem como dificultar a auditoria do emissor do cartão; e e) ataques contra a privacidade do usuário do cartão através do monitoramento, armazenamento e análise das operações realizadas com o cartão.

Ataques aos Algoritmos de Criptografia

Para Kaufman, Perlman e Speciner (2005), a **criptoanálise** é a ciência ou arte de ler mensagens encriptadas sem o conhecido da chave, ao passo que a criptoanálise prática refere-se aos processos utilizados para descobrir a chave (ou senha) pelos meios que se fizerem necessários.

Tanenbaum (2011), por sua vez, explica que o **ataque ao texto simples** conhecido ocorre quando o criptoanalista possui partes de um texto claro (não criptografado) e um texto cifrado criptografado com a mesma chave e, passa, segundo, Kaufman, Perlman e Speciner (2005), a estabelecer comparações que minimizam sobremaneira o tempo necessário para desproteger a mensagem completa. Adicionalmente, Kaufman, Perlman e Speciner (2005) e Tanenbaum (2001, 2011), apresentam o **ataque somente ao texto cifrado** que ocorre quando o criptoanalista possui acesso somente ao texto cifrado. Schneier (2001) define o **ataque ao texto simples escolhido** como o processo pelo qual o atacante criptografa uma mensagem utilizando o algoritmo preferido da vítima com o intuito de obter a chave.

De acordo com Kaufman, Perlman e Speciner (2005), a **pesquisa exaustiva**, também conhecida como força bruta, consiste em testar todas as possíveis chaves de um sistema. É interessante notar que, para Tanenbaum (2001), "quanto maior for a chave, mais alto será o fator de trabalho [...] para decodificar o sistema através de uma exaustiva pesquisa no espaço da chave". (TANENBAUM, 2001, p. 662) A opinião, a respeito das 'senhas' acima, é compartilhada por Schneier (2001, p. 110), com uma ressalva, conforme se depreende da seguinte afirmação "[...] Se elas forem longas o suficiente, os ataques pela força bruta estão simplesmente além das capacidades da engenharia humana. Mas existem duas preocupações. A primeira é a qualidade do algoritmo de criptografia, e a segunda é a qualidade das chaves. [...]". (SCHNEIER, 2001, p. 110)

Schneier (2001, p. 111), conclui que a melhor forma de empreender uma pesquisa exaustiva é realizar um tipo de ataque conhecido como **ataque de dicionário**, pelo qual um *software* experimentará inicialmente "senhas comuns [...], depois o dicionário inteiro, e depois combinações variadas de maiúsculas e minúsculas, números extras, e assim por diante". Por fim, o **ataque de aniversário**, de acordo com Tanenbaum (2001, 2011) e Kaufman, Perlman e Speciner (2005), ocorre quando o intento é subverter a assinatura digital de uma mensagem. O ataque demonstra que o número de interações necessárias para quebrar a assinatura digital não é 2^n como se seria de se supor, e sim $2^{n/2}$, em função de questões estatísticas, no campo das probabilidades.

Ataques a Protocolos de Comunicação

Conforme Kaufman, Perlman e Speciner (2005) e Schneier (2001), o **ouvinte passivo** é o tipo de ataque em que o invasor apenas monitora o tráfego e a comunicação, ao passo que no **atacante ativo**, o mesmo altera ou exclui mensagens de um ou vários participantes do processo de comunicação.

O **ataque da brigada de incêndio**, também conhecido como *wo(man)-in-the-middle*, ocorre quando o atacante posiciona-se entre os interlocutores, recebendo destes as mensagens, alterando-as, excluindo-as e/ou repassando-as, conforme a sua necessidade ou conveniência. Ocorre também, com frequência, o **ataque copiar-e-colar** no qual duas mensagens, criptografadas com a mesma chave, podem ser mescladas originando uma nova mensagem. O **ataque de repetição** ocorre quando uma mensagem realmente enviada por um dos interlocutores é interceptada pelo atacante e reenviada pelo mesmo ao destinatário algum tempo depois. Uma forma de contornar o ataque acima é utilizar temporizadores únicos para as mensagens. O **ataque de *time-resetting*** consiste em tentar confundir sistema computacional acerca da veracidade, acuidade e/ou integridade da hora a fim de que o mesmo reprocesse a mensagem anterior (KAUFMAN, PERLMAN, SPECINER, 2005; TANENBAUM, 2011).

CONSIDERAÇÕES FINAIS

Por todo o exposto conclui-se que os dados e informações sob guarda das organizações em seus sistemas de informações, tanto seus quanto de parceiros e clientes, encontram-se sob risco nos mais distintos momentos, desde o seu cadastramento, passando pelas etapas de processamento até a recuperação e posterior disponibilização aos legítimos interessados.

Estar em uso de ferramentas e tecnologias que maximizem a segurança de dados e informações, então, é fundamental para organizações que operam direta ou indiretamente no ambiente digital. Contudo, a conscientização dos usuários de tais sistemas ainda se constitui em ação primordial a fim de que se possa estabelecer um sistema de segurança eficaz, eficiente e efetivo, tendo-se em vista, que, em última análise, sua participação nas atividades de planejamento da segurança, organização de dados e informações e monitoramento, controle e intervenção em momentos de crise é considerada especialmente importante.

REFERÊNCIAS

CHESWICK, William R.; BELLOVIN, Steven M.; RUBIN, Aviell D. **Firewalls and Internet Security**: repelling the wily hacker. 2. ed. Englewood Cliffs, NJ: Prentice Hall, 2003.

FONTES, Edison. **Segurança da Informação**: o usuário faz a diferença. São Paulo: Editora Saraiva, 2006.

GORDON, Steven R.; GORDON, Judith R. **Sistemas de Informação**: uma abordagem gerencial. 3. ed. Rio de Janeiro: LTC, 2011.

KAUFMAN, Charlie; PERLMAN, Radhia; SPECINER, Mike. **Network Security**: PRIVATE Communications on a PUBLIC World. 2. ed. Englewood Cliffs, NJ: Prentice Hall, 2005.

LAUDON, Kenneth; LAUDON, Jane. **Sistemas de Informações Gerenciais**. 9. ed. São Paulo: Pearson Prentice Hall, 2010.

SCHNEIER, Bruce. **Segurança.com**. Rio de Janeiro, RJ: Editora Campus, 2001.

TANENBAUM, Andrew S. **Redes de Computadores**. 3. ed. Rio de Janeiro, RJ: Editora Campus, 2001.

_____. **_____**. 5. ed. Rio de Janeiro, RJ: Pearson, 2011.