SEGURANÇA DA INFORMAÇÃO: AMEAÇAS E VULNERABILIDADES DE UMA OM DO EB

AILTON XAVIER DE SÁ[19] , MARCOS NALIN[20]

Resumo. A informação está presente em todas as áreas e atividades da organização. A confidencialidade, a integridade e a disponibilidade da informação, no entanto, podem ser alvo de agentes agressores e fazer com que a marcha normal dos processos da organização seja prejudicada, trazendo prejuízos dos mais variados e inesperados. Assim, é necessário proteger todos os recursos físicos, humanos e tecnológicos que tratam com informações. Mas o primeiro passo não é a proteção em si, mas a conscientização do contra o quê a informação precisa ser protegida (ameaças) e em que pontos os recursos são sensíveis e podem ser atacados (vulnerabilidades). Dada a grandiosidade do tema, foi realizada uma pesquisa bibliográfica envolvendo artigos, livros, legislação e a Internet, de modo que se reuniu aqui uma mostra sucinta da interpretação do que há de publicado sobre o tema e relacionou-se à uma realidade mais próxima de uma organização militar, dando-se uma maior ênfase às ameaças e às vulnerabilidades da segurança da informação relativas aos recursos tecnológicos. A maioria dos itens apresentados é de fácil entendimento, muitos já são conhecidos e quase todos podem ser encontrados dispersos na literatura que trata da segurança da informação.

Abstract. Information is present in all the areas and activities of the organization. Confidentiality, integrity and availability of information, however, can be aim of aggressive agents and make the normal processes of the organization harmed, bringing varied and unexpected damage. Thus, it is necessary to protect all the physical, human and technological resources that deal with information. But the first step is not protection in itself, but the awareness about against what necessary information has to be protected (threats) and where the resources are sensible and can be attacked (vulnerabilities). For the relevance of the subject, a bibliographical research was carried through involving articles, books, legislation and the Internet, so that a succinct presentation of the interpretation of what was published on the subject, relating it to a reality next to a military organization, emphasizing threats and vulnerabilities of the security of the information related to the technological resources. The majority of itens presented is easy to understand, many of then are already known and almost all can be found dispersed in the literature that deals with the security of information.

Palavras chave. Ameaças, vulnerabilidades, segurança, informação.

1. Introdução

A informação é essencial à vida de qualquer organização. Todos os seus integrantes, de todos os níveis, decidem suas ações e elaboram seus planos baseados em informações. Elas circulam por todos os lugares e participam de todos os processos, por isso estão amplamente sujeitas às mais variadas ameaças e vulnerabilidades que transcendem aos aspectos tecnológicos, sendo alvo também de interferências provocadas por aspectos físicos e humanos,

[19] Tenente-Aluno do Curso de Formação de Oficiais do Quadro Complementar de 2003. Graduado em Informática. ailtonxavier@hotmail.com.
[20] Major de Arma de Artilharia. Mestre em Aplicações Militares. majnalin@esaex.mil.br.

gerando impactos mais ou menos graves (SÊMOLA, 2003, p. 1-4).

No final de 2002 a Módulo Security Solutions, empresa brasileira líder na América Latina em segurança da informação, divulgou a 8ª Pesquisa Nacional de Segurança da Informação, que incluiu o governo como 19% do universo entrevistado. Nessa pesquisa 77% dos entrevistados disseram pretender aumentar seus investimentos na área de segurança da informação e 78% das empresas no Brasil reconhecem que tiveram perdas financeiras em decorrência da quebra da segurança da informação. O motivo desses números elevados é claro; trata-se do reconhecimento do fato de que as ameaças e as vulnerabilidades à segurança da informação precisam ser tratadas com atenção e cuidado, dada a importância do assunto.

A segurança da informação é uma problemática difícil de se lidar, pois o perímetro de segurança tende a ser mais lógico do que físico. Redes de computadores têm sido usadas na maioria das OM (organizações militares) do EB (Exército Brasileiro), inclusive aquelas tipicamente operacionais. Tais redes facilitam o trabalho ao permitirem a troca quase ilimitada de informações ou dados eficientemente. Afora isso, ainda há relatórios, mapas, pesquisas, informativos, registros, legislação, manuais, arquivos e uma infinidade de materiais que constituem uma legítima fonte de preocupação.

Nenhuma OM é igual a uma outra; cada uma possui suas particularidades que as tornam únicas, com características singulares. No entanto, há um conjunto vasto de ameaças e vulnerabilidades que são comuns à maioria delas. Levantou-se para este artigo uma grande quantidade de vulnerabilidades relevantes que poderiam ser exploradas por diversas ameaças, também levantadas.

Indubitavelmente, aqui foi privilegiada a segurança no ambiente de tecnologia. No entanto, as seguranças física e humana das organizações são tão importantes quanto aquela e não podem ser deixadas de lado. A razão do enfoque aqui apresentado não se deveu à importância mas à criticidade dos segmentos. A segurança relacionada aos recursos tecnológicos tem si mostrado mais crítica, dada a difusão desses em todas as áreas e atividades de todas as organizações, bem como por ser muito mais nova e menos estudada que a dos demais recursos, já tratada a milênios.

Foram pesquisados vários artigos disponibilizados na Internet, livros que tratam de sistemas de segurança da informação e a legislação atual do Governo Federal e do EB, que foram publicados em cascata, sobre o assunto. Inicialmente são apresentados alguns conceitos básicos relacionados ao tema que serão especialmente úteis àqueles que ainda não travaram um combate mais aproximado com o assunto. Em seguida são apresentados alguns métodos mais comumente usados para análise de risco.

O propósito é provocar a conscientização da necessidade de proteção adequada da informação. Espera-se que ao final do estudo deste trabalho o leitor possa ser capaz de reconhecer a grandiosidade da problemática e ainda, aqueles responsáveis pela implementação da Política de Segurança da Informação (PSI) possam aprofundar seus conhecimentos, inclusive escolhendo alguma das metodologias para análise de risco aqui citadas para que possam fazer uma avaliação mais realista dos riscos a que sua organização está exposta, enquanto a Secretaria de Tecnologia da Informação (STI) não disponibiliza o previsto no inciso VI, do Art. 31, da IG 20-19: uma metodologia básica, para avaliação de riscos, na área de Tecnologia da Informação, a ser aplicada em todas as OM.

2. Situação Geral

2.1. Situação Atual da Segurança da Informação

O pionerismo mundial em termos de regulamentação da segurança da informação é de uma norma inglesa, publicada em 1995,

a BS7799:1995, ampliada em 1999 para a BS7799:1999. Em 2000 a ISO - Organização Internacional para Normalização - homologou uma parte daquela Norma como sendo a ISO/IEC 17799:2000 (CASANAS, 2002), o que foi suficiente para que passasse a ser amplamente referenciada no mundo inteiro.

No Brasil, a ABNT traduziu na íntegra a Norma como NBR ISO/IEC 17799. Essa Norma faz uma série de recomendações com vista a preservar a segurança da informação e apresenta uma infinidade de controles físicos, humanos e ambientais, que, se atendidos, dão direito a um selo de certificação de conformidade, ou seja, um atestado de que a organização certificada tem alto grau de segurança das suas informações.

Por esses dados pode-se constatar como ainda é principiante a segurança da informação, não só no Brasil, mas no mundo. Até julho de 2003, o Brasil possuía somente duas empresas certificadas pela Norma BS7799 parte 2 e NBR ISO/IEC 17799, a SERASA, empresa de análises e informações econômico-financeiras e cadastrais, e a Módulo Security Solutions, empresa especializada em segurança da informação, (Certificate register, 2003).

2.2. Situação atual da segurança da informação no Governo Federal

Numa escalada incessante, todas as organizações têm se tornado dependente dos recursos tecnológicos. A esfera pública já não vive sem sistemas de informações e redes de computadores; desde a declaração do imposto de renda aos julgamentos nos tribunais *on line;* tudo tem encontrado aplicações computacionais. No entanto, as facilidades não vieram gratuitas, trouxeram consigo inumeráveis vulnerabilidades às ameaças.

Atento à urgência do assunto, o Governo Federal tem tomado medidas decisivas no sentido de assegurar, em todos os seus escalões, a proteção da informação sob sua guarda ou a de qualquer cidadão, conforme impõe a Constituição Federal ao garantir o direito à inviolabilidade da correspondência e das comunicações.

Com o Decreto nº 3.505, de 13 de junho de 2000, o Presidente da República instituiu a Política de Segurança da Informação (PSI) nos Órgãos e entidades da Administração Pública Federal. Entre outras medidas, o Decreto apresentou um conjunto de recomendações mínimas para a implementação da PSI de cada órgão federal e criou o Comitê Gestor da Segurança da Informação, do qual faz parte um membro do Ministério da Defesa. Tal Comitê assessora a Secretaria-Executiva do Conselho de Defesa Nacional (SECDN), que por sua vez propôs as diretrizes para a implementação da Política de Segurança da Informação nos órgãos do Poder Executivo Federal (PSIPE).

2.3. Situação atual da segurança da informação no EB

Acatando as disposições do Governo Federal, o EB vem estabelecendo uma base legal necessária às medidas de segurança da informação a ser tomadas no âmbito das OM. Assim é que, só em 2001, foram publicadas diversas normas relativas à segurança da informação:

a) a Portaria nº 011-Gab Cmt Ex, de 10 de janeiro de 2001, aprovou as Instruções Gerais para Salvaguarda de Assuntos Sigilosos (IG 10-51), que estabeleceu diversas instruções relativas à segurança de *hardware, software*, Internet, correio eletrônico, sistemas corporativos, Intranet e redes locais;

b) a Portaria nº 459-Gab Cmt Ex, de 13 de setembro de 2001, aprovou a Política de Informação do Exército, que enumera entre os seus objetivos "possibilitar o sigilo, a integridade, a disponibilidade e a autenticidade da informação", ou seja a segurança da informação;

c) a Portaria nº 460-Gab Cmt Ex, de 13 de setembro de 2001, aprovou a Diretriz Estratégica de Informações Organizacionais, em que o Comandante do Exército estabelece como norma de execução daquela Portaria "que cada Órgão designe um

Assessor de Informações Organizacionais, a fim de gerenciar, orientar e acompanhar o fluxo das informações necessárias", incluindo-se nesse fluxo a segurança;

d) a Portaria nº 462-Gab Cmt Ex, de 13 de setembro de 2001, aprovou a Diretriz Estratégica de Comunicações e Informática, atribuindo à Secretaria de Tecnologia da Informação (STI) a incumbência de "propor os padrões e soluções técnicas para a segurança da informação no âmbito dos sistemas" de informação;

e) a Portaria nº 121-EME, de 12 de novembro de 2001, aprovou as Instruções Reguladoras para Utilização da Rede Mundial de Computadores (Internet) por Organizações Militares e Militares do Exército (IR 20-26), em que emanou várias normas de segurança para a utilização da Internet.

Mas, de toda a Legislação, provavelmente a mais importante no âmbito das OM é a Portaria nº 483-Gab Cmt Ex, de 20 de setembro de 2001, que aprovou as Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19); conforme reza o Art. 1º:

> "Estas Instruções Gerais têm por finalidade orientar o planejamento e a execução das ações relacionadas à Segurança da Informação no âmbito do Exército Brasileiro" e o Inciso II, do Art. 3º: "dotar o Exército de uma referência básica para a elaboração de documentos normativos sobre Segurança da Informação e complementares a estas Instruções".

Essa IG também incumbe os comandantes, chefes e diretores de "assegurar o cumprimento das medidas, normas e procedimentos preconizados nestas IG e nos documentos que lhe são complementares". Mas é muito provável que pouquíssimas OM estejam em condições de atender às disposições da IG 20-19, dado a novidade da matéria. Porém, seja qual for o caminho adotado pelas OM, todas terão que, em algum momento, fazer um levantamento das ameaças e vulnerabilidades que lhes são peculiares.

3. Conceitos Básicos

No âmbito do Exército Brasileiro são reconhecidos seis princípios de segurança da informação, todos definidos na IG 20-19 (2001, Art 5º):

INTEGRIDADE: é a garantia de que o conteúdo original da informação não foi modificado indevidamente, de modo intencional ou acidental;

DISPONIBILIDADE: é a garantia de que o conteúdo da informação estará disponível para os usuários autorizados, sempre que houver necessidade de acesso;

CONFIDENCIALIDADE: é a garantia de que o conteúdo da informação só é acessível e/ou compreensível a quem possui autorização para tanto;

AUTENTICIDADE: é a garantia de que o conteúdo da informação seja verdadeiro, e que a fonte geradora da informação e o seu destinatário sejam realmente quem alegam ser;

IRRETRATABILIDADE: é a garantia de que, num processo de envio e recebimento de informações, o remetente e o destinatário da informação não possam, posteriormente, negar o respectivo envio e recebimento; e

ATUALIDADE: é a garantia de que um documento a ser usado seja realmente o que estiver em vigor.

A SEGURANÇA DA INFORMAÇÃO é o conjunto das medidas, normas e procedimentos destinados a preservar os seis princípios de segurança, durante todo o ciclo de vida da informação (IG 20-19, 2001, Art 6º); o que é conseguido através de medidas que protejam os ativos da informação.

ATIVOS da informação são todos os elementos, físicos, humanos ou tecnológicos, que contêm, manipulam e processam informação (SÊMOLA, 2003, p. 45), ou ainda, a própria informação em si.

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) é um documento que estabelece, de um modo amplo, os padrões

de segurança a serem seguidos por aqueles que lidam com os ativos de informação. A partir da PSI são elaborados outros documentos que estabelecem mais especificamente quais as medidas de segurança a serem usadas.

AMEAÇAS são agentes ou condições capazes de explorar falhas de segurança, vindo a comprometer a um ou mais dos princípios de segurança da informação.

As ameaças são elementos ativos, porém somente causarão impactos se puderem ser combinados com vulnerabilidades específicas.

VULNERABILIDADES são falhas de segurança que ao serem exploradas por ameaças, afetam negativamente a um ou mais princípios da segurança da informação.

As vulnerabilidades são elementos passivos, portanto, podem existir sem causar danos, desde que não sejam exploradas por uma ameaça.

O CICLO DE VIDA DA INFORMAÇÃO é o período de existência da informação, caracterizado por cinco momentos peculiares (produção, manuseio, transporte, armazenamento e descarte), em que pelo menos um dos princípios de segurança é colocado em risco.

4. Classificação

4.1. Das Ameaças

As ameaças podem ser classificadas quanto à sua intencionalidade como:

NATURAIS: são as ameaças que decorrem de fenômenos da natureza e são, quase sempre, imponderáveis. Nesse tipo se classificam os incêndios naturais, as inundações, os terremotos e outras.

INVOLUNTÁRIAS: são ameaças que decorrem de intervenção humana ou não, porém não intencionais, quase sempre relacionadas à ignorância. Nesse tipo se classificam os erros de programação, os erros do usuário, os acidentes, a falta de energia, os incêndios não-naturais e outras.

VOLUNTÁRIAS: são ameaças que decorrem da ação proposital de agentes humanos. Nesse tipo se classificam a sabotagem, a espionagem, a fraude, a invasão, o furto, a ação de *hackers*, a disseminação (consciente) de vírus e outras.

As ameaças ainda podem ser classificadas quanto à sua ação como:

PASSIVAS: são aquelas que ainda que sejam bem sucedidas não alterem o conteúdo da informação (integridade).

ATIVAS: são aquelas que uma vez explorando uma vulnerabilidade alteram o conteúdo da informação (violação da integridade).

4.2. Das Vulnerabilidades

As vulnerabilidades podem ser classificadas quanto à sua localização como:

FÍSICAS: são vulnerabilidades relacionadas aos ativos físicos. Nesse tipo se classificam a falta de dispositivos para o combate a incêndios, em lugares em que haja risco de sua ocorrência, a falta de dispositivos alternativos de energia elétrica em caso de interrupção do fornecimento regular, instalações prediais que não atendam às conformidades de segurança e outras.

HUMANAS: são vulnerabilidades relacionadas aos ativos humanos. Nesse tipo se classificam a falta de treinamento, a não conscientização dos elementos humanos a respeito da segurança da informação e outras.

TECNOLÓGICAS: são vulnerabilidades relacionadas aos ativos tecnológicos. Nesse tipo se classificam a obsolescência de equipamentos, a desatualização de aplicativos, os erros de configuração e outras.

DE PROCESSOS: são vulnerabilidades relacionadas aos processos, ao modo como as tarefas são executadas. Nesse tipo se classificam a inexistência de uma rotina de destruição completa de mídia (*CD-Rom*, disquete, *hard disc*, papel), a permissão de acesso de estranhos às repartições internas sem acompanhamento e outras.

5. Análise de Risco

Em termos práticos e econômicos, nem toda ameaça ou toda vulnerabilidade deve receber a mesma atenção ou grau de preocupação. Elas podem ser eliminadas, amenizadas, administradas ou nem mesmo tratadas.

O que deve determinar o posicionamento a adotar é o risco a que a informação fica sujeita e o impacto que atingiria a organização no caso de violação da informação. Isso significa que uma mera lista de ameaças ou vulnerabilidades serviria apenas de alerta sobre os perigos a que a organização está exposta. Porém, não serve para que sejam tomadas decisões de prevenção.

A análise de risco é um processo pelo qual são identificados os riscos a que estão sujeitos os dados, sistemas de informação e redes de comunicação que lhes dão suporte.

A análise de risco tem como objetivo identificar as ameaças, vulnerabilidades e impactos que precisam ser administrados (entre os vários a que se está exposto), e o grau de investimento justificado para se alcançar um nível de proteção adequado e facilidade de uso. A forma mais fácil de se efetuar a análise de risco é elaborar uma lista das ameaças significativas e então considerar para cada sistema as oportunidades que essas ameaças teriam de causar um impacto para o serviço. (VYDIA, 2002)

O risco pode ser melhor visualizado se apresentado como uma expressão matemática:

$$R = \frac{V \times A \times I}{M}$$

R = risco. É a probabilidade de que uma ameaça explore uma ou mais vulnerabilidades, provocando a violação de qualquer um dos princípios de segurança da informação e causando impactos para a organização.

V = vulnerabilidade.

A = ameaça.

I = impacto. É a conseqüência do ataque de uma ameaça bem sucedida.

M = medidas de segurança. São as ações preventivas tomadas para que as vulnerabilidades não sejam exploradas pelas ameaças (**SÊMOLA, 2003, p. 55**).

O risco será tanto maior quanto maiores forem V e A e menor for M.

Se o risco é alto, porém o impacto é reduzido talvez não seja o caso de se elevar as medidas de segurança, que normalmente implicam em elevação de custos, dado que o que de fato importa são as conseqüências (impactos) da quebra de segurança, que nem sempre são relevantes. Às vezes é mais vantajoso sofrer o impacto do que dispender uma grande quantidade de recursos para diminuir o risco de sua ocorrência. Os gastos com controles precisam ser balanceados de acordo com os danos causados pelas potenciais falhas na segurança (**NBR ISO/IEC 17799, 2001**).

As metodologias para análise de risco exigem alguns conhecimentos avançados para que possam apresentar resultados satisfatórios. Porém, não é difícil entender como funcionam, em linhas gerais. Há duas espécies principais: qualitativas e quantitativas.

Os métodos quantitativos baseiam-se no ROI - Retorno Sobre o Investimento, ou sejam, visam a equilibrar os custos de implementação de segurança com o possível custo da sua não implementação. O roteiro seria:

- estimar a incidência de cada ameaça, baseando-se em históricos;

- estimar o valor dos prejuízos que as ameaças podem causar;

- estimar o custo de combater essas ameaças;

O investimento em medidas de proteção deverá ser menor que a expectativa de perda anual com as ameaças levantadas.

Os métodos qualitativos (subjetivos) baseiam-se em questionários ou *brainstorming* projetados para avaliar os níveis de risco prováveis de uma variedade de ameaças e vulnerabilidades associadas. Baseados na experiência daqueles que lidam

com os ativos, na inspeção física dos ambientes e na análise de documentação, consiste em atribuir-se notas à probabilidade de ocorrência do ataque e ao nível de severidade dos impactos; o produto da multiplicação dessas duas notas indica o nível de risco; de modo que se pode listar as ameaças e vulnerabilidades por ordem de risco.

Vê-se que é bastante difícil avaliar precisamente a probabilidade de ocorrência de uma ameaça, ou de que essa venha efetivamente a causar danos. Mas, finalmente, há a análise simplificada. Embora seja sumário, esse método é bastante útil para a definição de prioridades de investimentos de segurança. Consiste em atribuir uma pontuação de 0 (baixo risco) a 4 (alto risco) a cada uma das ameaças constantes da lista geral a que a organização está sujeita. Com base nos resultados dessa pontuação a organização terá à disposição uma relação ordenada das prioridades em segurança da informação (**VYDIA, 2002**).

Seja qual for o método utilizado, a organização estará mais preparada para estabelecer prioridades em relação a investimentos em segurança após conhecer quais ameaças apresentam maior possibilidade de inviabilizar o negócio, e que por isso deveriam merecer maior atenção nos planos de ação de curto, médio e longo prazos.

6. Considerações Gerais

Um diagnóstico customizado e completo somente poderia ser obtido com uma análise de risco que leve em consideração as peculiaridades da OM. Uma ameaça pode ter criticidade alta para uma OM e média ou baixa para outra, o que é considerado bastante normal, pois uma vulnerabilidade em um componente pode ser compensada por características positivas de outro componente. Pode ser perfeitamente aceitável, por exemplo, existir um arquivo de metal com gavetas sem fechaduras, mas que esteja situado em uma sala interna com a porta fechada e acesso limitado a usuários possuidores de sua chave. Somente uma análise da situação poderá indicar a relevância da ameaça.

Sêmola (2003, p. 20) descreve diversos erros que são cometidos na hora de pensar em segurança da informação, provocados pela visão míope do problema e a percepção distorcida da questão. Dentre esses erros, pode-se destacar:

a) atribuir exclusivamente à área tecnológica a segurança da informação. Seria o mesmo que afirmar que só há informação associada aos meios informáticos. Os demais elementos humanos não se comprometem e nem são conscientizados que suas ações podem deixar portas abertas (vulnerabilidades) a ameaças;

b) definir investimentos subestimados. As medidas de segurança devem ser adequadas ao que se quer proteger. Porém, as dificuldades orçamentárias, sempre presentes e que já fazem parte da rotina do OD (Ordenador de Despesas), podem obrigá-lo a realizar cortes tais que inviabilizem a adoção das medidas que requeiram maiores somas de dinheiro;

c) adoção de medidas pontuais. Decorrente do entendimento parcial da necessidade de proteção sistêmica. Uma área pode receber menos atenção que uma outra, de acordo com seu risco, mas jamais ser desprezada. O uso de anti-vírus e *firewall*, por exemplo, só beneficia as informações da rede;

d) mentalidade de segurança cultivada apenas por/para um grupo (geralmente de oficiais). Todos os elementos humanos são vulneráveis, mas, igualmente, todos podem ser sustentadores de medidas de segurança da informação.

7. Ameaças

O propósito aqui é de ser abrangente, porém não totalizante, dado que, em qualquer universo considerado, novas tecnologias, mudanças organizacionais e novos processos fazem surgir agentes agressores

que até então não existiam ou que não haviam sido levados em consideração.

De um modo geral são ameaças à segurança da informação: desastres, explosões, incêndios, água (vazamentos, corrosões e enchentes), tremores e abalos sísmicos, tempestades, furacões, terrorismo, acessos (remotos ou locais) indevidos, espionagem, sabotagem, vandalismo, roubos, furtos, fraudes, erros humanos, usuários insatisfeitos, acidentes, desmoronamento de construções, materiais tóxicos ou corrosivos, lixo informático, interrupção de energia, interrupção das comunicações (links, voz, dados), falhas em equipamentos e outras.

Cada uma dessas ameaças devem ser devidamente analisadas, caso a caso. Algumas devem ser simplesmente descartadas por serem de ocorrência extremamente remota, como furacões no Brasil; já outras precisam ser destrinçadas adequadamente, eliminadas ou administradas.

7.1. Ameaças de vírus e programas hostis

O disquete já foi o principal veículo de transporte de vírus e com isso causou grandes estragos. Com a disseminação do *e-mail* e da Internet em grande escala, os perigos foram potencializados em uma velocidade alarmante.

Vírus são programas feitos para destruir ou prejudicar o funcionamento de um computador. Copiam-se automaticamente para outros arquivos ou computadores.

VÍRUS DE MACRO: são programas que alteram as características do aplicativo contaminado, retirando opções dos menus, salvando arquivos adulterados ou com nomes errados e pode até mesmo apagar documentos e arquivos. Esses vírus se escondem dentro de documentos e precisam ser executados no aplicativo que o criou para que a contaminação aconteça. Após contaminado, o aplicativo reproduz o vírus nos outros documentos abertos em seguida, alastrando o mal. Os vírus de macro contaminam documentos com extensões como .DOC (word), .DOT (word), .PPT (PowerPoint), .PPS (PowerPoint) e .XLS (Excel).

CÓDIGO MALICIOSO: é um tipo genérico de ameaça que consiste, quando executado, em causar danos variados em um sistema, quando somente então são descobertos. Incluem cavalos de Tróia, *worms* e vírus.

WORMS: são códigos maliciosos que não contaminam outros programas e cuja principal característica é a da replicação própria e o envio de si mesmo a outros computadores e sistemas.

CAVALO DE TRÓIA (*Trojan Horse*): é um programa (não é um vírus e nem se reproduz) que o usuário instala em sua máquina e, sem saber, abre uma porta traseira, ou seja, uma brecha no sistema que permite então que o invasor alcance o sistema usando a Internet para roubar senhas, ler e apagar arquivos e realizar outras atividades prejudiciais. Uma fonte explorada é aquilo que a vítima digita no teclado; por isso bancos têm optado por um teclado virtual em que a senha é inserida com cliques do mouse em um teclado mostrado na tela.

APPLETS E SCRIPTS HOSTIS: são rotinas que usam falhas de segurança preexistentes nos aplicativos para provocarem danos ao sistema. Propagam-se por *e-mail* e páginas hospedadas na Internet.

7.2. Ameaças associadas ao uso da Internet

A Internet é uma porta larga de entrada e de saída de informações. As ameaças associadas ao uso da Internet podem ser classificadas da seguinte forma:

SINDICÂNCIA: ocorre quando um violador tenta acessar ou descobrir informações sobre um sistema por meio de tentativa e erro até que dê certo (confidencialidade).

ESQUADRINHAMENTO: é a versão automatizada de uma sindicância, permitindo que o violador faça uma grande quantidade de tentativas rapidamente (confidencialidade).

COMPROMETIMENTO DE CONTA: ocorre quando um violador compromete outra pessoa por usar uma conta de acesso que não lhe pertence, não sendo portanto autorizado. Nesse caso a conta não possui privilégios como de administrador, por exemplo (confidencialidade, integridade).

COMPROMETIMENTO DA RAIZ: é um caso semelhante ao anterior, contudo, o violador usa privilégios ilimitados (superusuário), podendo fazer praticamente tudo no sistema da vítima (confidencialidade, integridade).

SNIFFER DE PACOTES: esse caso é um programa capaz de capturar dados contidos em pacotes enquanto são transmitidos pela rede. Pode-se captar assim senhas ou qualquer outro dado em transmissão (confidencialidade).

NEGAÇÃO DE SERVIÇO: é o ataque que visa a impedir que usuários legítimos tenham acesso a algum sistema. Uma forma de se fazer isso é inundando a rede com elevado volume de dados o que torna lento ou derruba o sistema alvo. Este tipo de ataque não causa perda ou roubo de informações, mas é um ataque preocupante, pois os serviços do sistema atacado ficarão indisponíveis por um tempo até que seja restabelecido (disponibilidade).

EXPLORANDO CONFIANÇA (SPOOFING): ocorre quando um violador falsifica a identidade de seu computador de modo a passar-se por um computador confiável. Isso se dá porque antes de executar um comando o computador verifica um conjunto de arquivos que especificam que outros computadores da rede têm permissão de usar esses comandos. Ao falsificar a identidade o violador obtém esse acesso livre (autenticidade).

SPAMS: citados pelo Gartner Group como sendo 34% das mensagens que circulam pela Internet, são propagandas, correntes ou apelos humanitários, freqüentemente falsos. Ocupam parte do tempo dispensado às mensagens recebidas; perda de tempo em apagá-las; tráfego inútil gerado; consumo de banda; gasto de espaço nos servidores; disseminação de vírus (CONTI, 2003).

7.3. Ameaças diversas

a) Quebra de senhas - muitos violadores tentam quebrar senhas através de técnicas de quebras de senhas, como tentar as senhas padrões de sistemas ou as senhas simples como nomes pessoais, nome da empresa, datas, entre outros. Mas para facilitar a descoberta de senhas podem ser utilizadas diversas ferramentas desenvolvidas especialmente para esse fim, como dicionários de senhas e programas que tentam todas as combinações possíveis de caracteres para descobrir a senha (ver sindicância e esquadrinhamento).

b) Invasão - é a entrada em um local físico, site, servidor, computador ou serviço de alguém não autorizado. As principais formas de invasão são: acesso remoto, sistemas internos, Internet, invasão física e engenharia social.

Antes da invasão propriamente dita, o invasor poderá fazer um teste de invasão, que é uma tentativa de invasão em partes, em que o objetivo é avaliar a segurança de uma rede e identificar seus pontos vulneráveis. Conhecidos como *Hackers* ou *Crackers*, conforme seus objetivos, podem ter as seguintes motivações: roubo de informações, protestos, supremacia sobre grupos rivais, por mérito, para promoção pessoal, desafios propostos por empresas de informática, estudo e busca de conhecimento, curiosidade ou simples prazer (SELEGUIM, 2002).

c) Falta de conscientização dos usuários quanto à importância da senha. Em conseqüência são divulgadas abertamente, anotadas em locais de fácil acesso ou emprestadas. Sua utilidade costuma ser subestimada. Os usuários autorizados, apesar de confiáveis, podem não estar convencidos dos impactos que podem advir do uso de senha sem os devidos cuidados de proteção.

d) Usuários autorizados descontentes com a organização e que detêm certas

informações ou o simples acesso a elas podem atingir objetivos prejudiciais à organização com muito mais facilidade que qualquer intruso.

e) Uso de notebooks. Geralmente disponível somente ao comandante, chefe ou diretor e outros elementos em funções singulares, contém informações extremamente vulneráveis. Sua portabilidade, mobilidade e fácil subtração lhe garantem grande exposição a agentes ameaçadores.

f) Forma de descarte da informação. Quando a informação termina seu ciclo de vida, é essencial que o descarte da mídia que a contém seja feito adequadamente, conforme sua característica. O papel pode ser picotado, por exemplo, já um disco rígido, dado seu valor residual insignificante, poderá ser destruído; nesse caso, não no fim do ciclo de vida da informação, mas no da mídia. Agindo-se adequadamente pode-se prevenir o acesso indevido de dados.

8. Vulnerabilidades

Tal qual foi dito para as ameaças, o propósito aqui é de ser abrangente, porém não totalizante, dado que seria impossível listar todas as fragilidades particulares pelos motivos também já explicitados.

8.1. Vulnerabilidades relativas à infração da lei

A pirataria é uma prática ilícita, cujas características principais são a reprodução e o uso indevido de programas de computador legalmente protegidos.

Algumas formas de pirataria são bastante sutis e exigem controles rígidos para que se evite incorrer nas duras sanções legais. Ainda que não haja uma autorização explícita, o responsável pela organização torna-se o responsável pelo crime. A vulnerabilidade consiste em enquadrar-se fora da lei, sendo a OM uma presa fácil à ameaça de fiscalização.

A Lei nº 9.609/98, de 20 de fevereiro de 1998, inclui o *software* no rol dos direitos autorais. Portanto, a reprodução, a cópia, o aluguel e qualquer utilização de cópias de programas de computador feitos sem autorização do detentor dos direitos autorais constituem crime.

Os infratores estão sujeitos a ação criminal e a ação cível de indenização. Pela ação criminal o infrator está sujeito a detenção de seis meses a dois anos ou a multas diárias pelo uso ilegal dos programas. Pela ação cível o infrator está sujeito a ressarcir ao detentor dos direitos as perdas e os danos pelo valor equivalente a 3000 cópias de cada *software* ilegalmente pirateado.

CÓPIA EFETUADA PELO USUÁRIO FINAL: pirataria em que o usuário final cria cópias adicionais do programa dentro de uma organização, para utilização em um número maior de micros do que previsto na licença; é uma das mais difundidas.

CÓPIA EFETUADA PELO REVENDEDOR: pirataria praticada pelo revendedor (mas que não isenta o usuário final) que instala no disco rígido dos computadores que vende cópias de *software*.

FALSIFICAÇÃO: pirataria que consiste na reprodução e venda de *software* com se fosse o original.

PIRATARIA ATRAVÉS DA INTERNET: pirataria que ocorre quando o *software* é transferido para o usuário conectado à Internet, sem autorização do detentor dos direitos autorais.

8.2. Vulnerabilidades diversas

a) As mídias de *backup* podem estar sendo armazenadas em local inadequado. Ameaças: acesso indevido por pessoas não autorizadas; fraudes ou sabotagens; indisponibilidade por perda ou estrago.

b) Testes de restauração de *backup* comumente não são executados regularmente. Ameaças: falsa sensação de segurança; fraudes e sabotagens; erros e acidentes; paralisação dos trabalhos.

c) Utilização de equipamentos obsoletos. Ameaças: perda de performance na utilização e conseqüente perda de produtividade; perda de dados; perda de interoperabilidade com outros equipamentos.

d) Instalação de programas de *chat* (ICQ ou MIRC). Ameaças: recepção de vírus anexados ao *download*; perda de produtividade; diminuição da performance do computador; congestionamento do trânsito de dados.

e) Inexistência de anti-vírus instalado e atualizado. Ameaças: exposição a vírus; perda de dados; paralisação dos trabalhos; retrabalho; invasões.

f) Existência de grande quantidade de arquivos inúteis (piadas, fotos, mensagens-corrente). Ameaças: diminuição da performance do computador; perda de produtividade; aumento do tempo de procura dos arquivos úteis.

g) Existência de arquivos provenientes de *downloads* da Internet. Ameaças: recepção de vírus anexados ao download; diminuição da performance da computador; perda de produtividade.

h) Inexistência de expiração de senha nos computadores. Ameaças: perda progressiva do sigilo da senha e conseqüente uso indevido; invasões ao computador e à rede.

i) Inexistência de restrição quanto à reutilização da mesma senha. Ameaças: acessos indevidos; invasões.

j) Inexistência de padronização de protetor de tela com senha. Ameaças: acessos indevidos; furto de informações.

l) o nome do último usuário que efetuou o *logon* é exibido. Ameaças: facilitação às invasões ao fornecer o domínio e o nome de um usuário.

m) permissão de acesso à rede mesmo sem introdução de senha (senha em branco), por meio de cancelamento do *logon*. Ameaças: acesso indevido; invasões; perda de rastreabilidade.

n) Inexistência de regras claras para uso e controle da Internet. Ameaças: exposição a vírus; facilitação à pirataria; acessos indevidos; perda de produtividade; diminuição da performance do computador; paralisação do trabalho.

o) Inexistência de procedimentos formais de inclusão, manutenção e exclusão de usuários da rede. Ameaças: perda de rastreabilidade das ações; acessos indevidos; furto de informações; invasões; fraudes e sabotagens.

p) Ambiente de localização da estação servidora inadequado e sem as condições ideais de prevenção e combate a incêndio. Ameaças: paralisação dos trabalhos; incêndios; furtos e sabotagens; acessos indevidos.

q) Carência de treinamento em segurança. Ameaças: erros e acidentes; perda de produtividade; subotimização dos recursos.

r) Quantidade insuficiente de pessoal para manutenção dos sistemas. Ameaças: sobrecarga de trabalho; perda de produtividade; erros e acidentes; paralisação dos trabalhos.

s) Existência de *softwares* piratas em servidores e computares. Ameaças: exposição a vírus; implicações legais; perda de produtividade; diminuição da performance do equipamento.

t) Existência de muitos arquivos temporários e imagens gráficas. Ameaças: perda de produtividade; armazenamento de lixo informático.

8.3. As 20 Vulnerabilidades mais críticas na Internet

O Instituto SANS (System Administration, Networking and Security) e o NIPC/FBI (National Infrastructure Protection Center, FBI) divulgaram em 2002 a "TOP 20 LIST", um documento que resume as vulnerabilidades mais críticas de segurança na Internet. Milhares de organizações têm usado tal lista para priorizar seus esforços de modo que seja possível sanar a priori as vulnerabilidades mais perigosas.

O valor da lista está no fato de que a maioria dos ataques bem sucedidos através

da Internet pode ser atribuída à exploração de falhas de segurança nela incluídas.

Lembrando o enunciado de Vilfredo Pareto, que verificou que numa classificação de causa e efeito, o maior volume de efeitos é atribuível a um pequeno conjunto de causas, enquanto que existe um grande conjunto de causas que contribui apenas com pequeno volume de efeitos, poucas vulnerabilidades de *software* contabilizam a maioria dos ataques bem sucedidos. Isso porque os violadores são oportunistas e usam os caminhos mais fáceis, convenientes, comuns, efetivos e difundidos. Os violadores partem do princípio de que as organizações não corrigem seus sistemas e saem vasculhando sistemas vulneráveis na Internet.

A lista é dinâmica e atualmente contém sete vulnerabilidades gerais, seis do Windows e mais sete do UNIX. Para não fugir ao escopo deste trabalho, será apresentada a seguir apenas uma descrição resumida das vulnerabilidades gerais. Aqueles que considerarem pertinente poderão consultar o documento completo no site da Módulo Security Solutions (www.modulo.com.br) ou no da própria SANS (www.sans.org) de modo a obterem os seguintes tópicos relativos a cada uma das vinte vulnerabilidades: descrição, sistemas afetados, como determinar se se está vulnerável e como se proteger.

a) Instalações *default* de sistemas operacionais e aplicativos - A maioria dos *softwares*, incluindo sistemas operacionais e aplicativos, vêm com *scripts* ou programas que têm por objetivo instalar os sistemas tão rapidamente quanto possível, com a máxima funcionalidade e com o mínimo de esforço por parte do administrador. Para atingir este objetivo, os programas normalmente instalam mais componentes do que a maioria dos usuários necessita. Essa prática origina muitas das mais críticas vulnerabilidades de segurança, pois os usuários não mantêm, nem corrigem componentes de *software* não usados. Além disso, muitos usuários desconhecem o que realmente é instalado, deixando programas perigosos no sistema, simplesmente porque eles não sabem que estão lá.

b) Contas sem senhas ou com senhas fracas - A maioria dos sistemas é configurada para usar senhas como a primeira, e única, linha de defesa. A identidade do usuário (*User ID*) é razoavelmente fácil de obter, e a maioria das companhias oferece acesso *dial-up* que comumente dribla o *firewall*. Consequentemente, se um violador puder determinar um nome e uma senha de cliente, poderá também ter acesso à rede. Senhas fáceis de adivinhar e senhas default constituem um problema grave, pior ainda são as contas sem senha. Na prática, todas devem ser removidas do sistema.

c) *Backups* incompletos ou inexistentes - Quando um incidente ocorre, a recuperação do incidente requer *backups* atualizados e métodos de recuperação dos dados previamente testados. Algumas organizações fazem *backups* diários, mas nunca verificam se eles estão realmente funcionando. Outras criam políticas e procedimentos de *backup*, mas não de restauração. Freqüentemente, tais vulnerabilidades são descobertas somente depois que um *hacker* invade os sistemas ou os dados são destruídos, ou arruinados de alguma outra maneira. Uma segunda vulnerabilidade que envolve *backups* é a falta de proteção física das mídias. Os *backups* contêm a mesma informação sensível que reside no servidor, portanto devem ser protegidos da mesma maneira.

d) Grande número de portas abertas - Tanto os usuários legítimos quanto os violadores, se conectam aos sistemas através de portas abertas. Quanto maior o número de portas abertas, maior a possibilidade de alguém se conectar ao sistema. Consequentemente, é importante manter o menor número de portas abertas necessárias para o correto funcionamento do sistema, o restante deve ser fechado.

e) Ausência de filtro de pacotes de entrada e saída que garantam o uso de endereços válidos - O *Spoofing* de endereços

IP é um método comumente usado por atacantes para esconder evidências. Por o exemplo, o tão popular ataque '*smurf*' faz uso de uma funcionalidade dos roteadores para enviar pacotes a milhares de máquinas. Cada pacote contém o endereço forjado de uma vítima. Os computadores que recebem este tipo de pacote, em resposta, inundam a vítima com outros pacotes, chegando a retirá-la da rede em alguns casos. Filtrar o tráfego que entra na rede (*ingress filtering*) e que sai (*egress filtering*) pode ajudar a elevar o nível de proteção.

f) Sistema de *logs* inexistente ou incompleto – Embora a prevenção seja o ideal, a detecção é imprescindível já que sempre será possível ser violado. Uma vez se tenha sido atacado, sem registros (*logs*), a possibilidade de se descobrir o que foi violado no sistema é mínima. Sem esta informação, a organização tem duas opções: fazer uma restauração completa do sistema operacional a partir da mídia original, torcendo para que os dados armazenados estejam corretos; ou correr o risco de possuir um sistema ainda controlado pelo violador. Os *logs* provêem detalhes sobre o que está acontecendo, os sistemas que estão sendo atacados e os que foram efetivamente invadidos.

g) Programas CGI vulneráveis - A maioria dos servidores, incluindo IIS da Microsoft e Apache, suportam programas CGI *(Comino Gateway Interface)* para proporcionar interatividade em páginas *web*, permitindo algumas funções como o levantamento e a verificação de dados. De fato, a maioria dos servidores *web* são distribuídos com programas CGI de exemplo. Os programas CGI vulneráveis representam para os violadores um alvo particularmente atraente porque são relativamente fáceis de serem localizados e operam com os privilégios do próprio servidor *web*. Os violadores costumam utilizar os programas CGI vulneráveis para desfigurar *websites*, roubar números de cartão de crédito, ou instalar *'backdoors'* para permitir futuras invasões. Como regra geral, os programas de exemplos que acompanham as distribuições dos servidores *web* sempre devem ser retirados dos sistemas de produção. (SANS, 2002)

9. Conclusão

Não sendo totalizante, este trabalho fez uma coletânea sumária das principais ameaças e vulnerabilidades da segurança da informação a que estão sujeitas uma OM típica do EB.

Evidentemente nenhuma lista dessa natureza seria capaz de abranger todo tipo de ameaças e vulnerabilidades e muito menos relativa a todas as OM, por mais que sejam afins. Características intrínsecas como missão, localização, efetivos, orçamento e conjuntura local, tornariam necessário uma listagem única e particular. É por esse motivo que também foram citadas técnicas de análise de ameaças e vulnerabilidades e que junto com análise de impactos decorrentes geram a análise de risco, de modo a incentivar que sejam levantados os casos particulares.

Embora aqui tenha sido seguida uma linha de pesquisa voltada para os recursos tecnológicos, não se pode esquecer da existência de outras inúmeras ameaças e vulnerabilidades da segurança da informação relativas aos recursos físicos e humanos. O fato de não terem sido aqui tratados se deve tão somente à necessidade de restrição do escopo. O que já suscitaria a elaboração de um trabalho mais específico voltado para aqueles recursos.

A mentalidade de todos os que lidam com informações, e poucos são os que não o fazem, deve ser a de que os ativos da informação estão repletos de vulnerabilidades e a todo instante estão sendo rondados por diversas ameaças. O que se quer é que a consciência da existência da grande variedade de ameaças e vulnerabilidades a que está exposta a organização faça com que os gestores chave adotem as medidas de proteção adequadas, pois o primeiro passo é a tomada de consciência da dimensão do problema e o segundo as medidas de solução, como

adoção de uma política de segurança e atribuição clara de responsabilidades.

Agradecimentos
Ao Major Marcos Nalin pela colaboração e revisão do texto em cada etapa de seu desenvolvimento. E ao amigo José Neyardo Alves de Araújo pela elaboração do abstract.

Referências

BRASIL. Lei nº 9.609/98, de 20 de fevereiro de 1998. **Diário Oficial da União**, Poder Executivo, Brasília-DF, 20 fev 1998.

BRASIL. Decreto nº 3.505, de 13 de junho de 2000. **Diário Oficial da União**, Poder Executivo, Brasília-DF, 14 jun 2000.

CASANAS, A. D. G. & MACHADO, C. de S. O impacto da implementação da norma NBR ISO/IEC 17799 - Código de prática para a gestão da segurança da informação - nas empresas. Disponível em <http://www.iso17799.hpg.com.br/downloads/iso17799-1.pdf> e <http://www.alentejodigital.pt/rosadopereira/egov/ Page10549/Seguranca/iso17799-1.pdf> e <http://www.modulo.com.br/pdf/NBR_ISO-IEC_17799_.pdf>. Acesso em: 28 de junho de 2003.

Certificate register. Disponível em <www.xisec.com>. Acesso em 25 de julho de 2003.

CONTI, H. C. de. **SPAM: o que fazer?**. 2003. Disponível em <http://www.modulo.com.br/index.jsp?page=3&catid=17&objid=42&pagecounter=0&idiom=0>. Acesso em: 17 de junho de 2003.

DIAS, C. Segurança e Auditoria da Tecnologia da Informação. Rio de Janeiro: Axcel Books, 2000.

EB-EME. IG 20-19 - **Instruções Gerais de Segurança da Informação para o Exército Brasileiro**. PORTARIA Nº 483, de 20 de setembro de 2001, Comandante do Exército.

NBR ISO/IEC 17799. Tecnologia da Informação – Código de Prática para a Gestão da Segurança da Informação. ABNT, 2001.

SANS Institute. **As 20 Vulnerabilidades Mais Críticas de Segurança na Internet** (Versão em Português).Version 2.501. 30 de Janeiro, 2002. Disponível em <http://www.modulo.com.br>. Acesso em: 17 de junho de 2003.

SELEGUIM, G. C. **Segurança da Informação. Perigos do Mundo Virtual**. 2002. Disponível em <http://suporte.planetarium.com.br/suporte/documentacao/download/perigos-cestarolli.pdf>. Acesso em: 17 de junho de 2003.

SÊMOLA, M. Gestão da Segurança da Informação: Uma Visão Executiva. Rio de Janeiro: Campus, 2003.

VYDIA TECNOLOGIA. **Segurança da Informação**, 2002.