

LIGA DE ENSINO DO RIO GRANDE DO NORTE
CENTRO UNIVERSITÁRIO DO RIO GRANDE DO NORTE
GRADUAÇÃO EM SISTEMA DE INFORMAÇÃO

ANÁLISE DA SEGURANÇA DIGITAL
EM UM AMBIENTE MILITAR

ANTÔNIO YURI LULINI DE ASSIS

ANÁLISE DA SEGURANÇA DIGITAL
EM UM AMBIENTE MILITAR

Orientador:
Prof. Aluizio Ferreira da Rocha Neto, MSc

ANTÔNIO YURI LULINI DE ASSIS

ANÁLISE DA SEGURANÇA DIGITAL
EM UM AMBIENTE MILITAR

ANÁLISE DA SEGURANÇA DIGITAL
EM UM AMBIENTE MILITAR

Monografia apresentada ao Curso de Bacharelado em Sistema de Informação do Centro Universitário do Rio Grande do Norte como requisito parcial para obtenção do grau de Bacharel em Sistema de Informação.

Orientador:

Prof. Aluizio Ferreira da Rocha Neto, M.Sc.

NATAL/RN
2012

Catálogo na Publicação – Biblioteca do UNI-RN
Setor de Processos Técnicos

Assis, Antônio Yuri Lulini de.

Análise da segurança digital em um ambiente militar / Antônio Yuri Lulini de Assis. – Natal, 2012.

49 f.

Orientador: Prof. Ms. Aluizio Ferreira da Rocha Neto.

Monografia (Graduação em Sistemas de Informação) – Centro Universitário do Rio Grande do Norte.

1. Segurança da Informação - Monografia. 2. Falhas na segurança - Monografia. 3. Internet - Monografia I. Rocha Neto, Aluizio Ferreira da, Romulo Fagundes. II. Título.

RN/UNI-RN/BC

CDU 004.7

BIBLIOTECA UNI-RN

004.7 A848a - RB: 37267 (M002081)

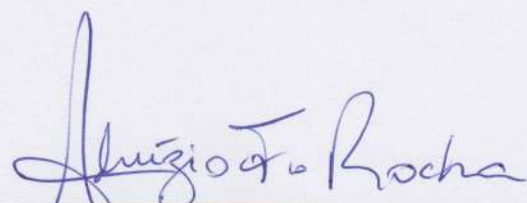
Título: Análise da segurança digital em um

Autoria: Assis, Antônio Yuri Lulini de
2012, ex. 1

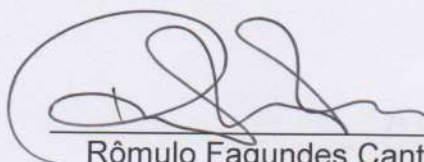
ANTÔNIO YURI LULINI DE ASSIS

ANÁLISE DA SEGURANÇA DIGITAL
EM UM AMBIENTE MILITAR

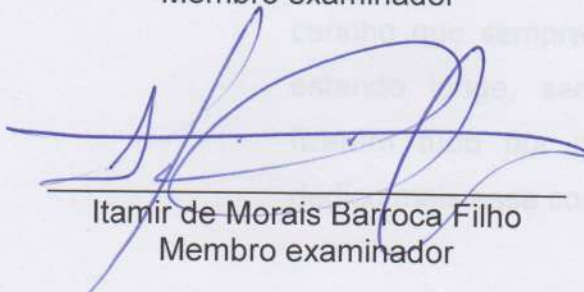
Monografia apresentada e aprovada em ____ de ____ de ____, pela banca
examinadora composta pelos seguintes membros:



Aluizio Ferreira da Rocha Neto, M.Sc.
Orientador



Rômulo Fagundes Cantanhede
Membro examinador



Itamir de Moraes Barroca Filho
Membro examinador

NATAL/RN
2012

AGRADECIMENTOS

Primeiramente a Deus, pois é ele que me sustenta, ele é meu refúgio, a minha fortaleza e meu conforto. A meus pais Antônio Sérgio e Clarinda Lima, que me ensinaram os primeiros passos, as primeiras palavras, que me mostraram o caminho certo e me guiam na caminhada por ele porque sem eles nada disso seria possível. A meus amigos Jure Bezerra Lopes Junior e Vanessa Andrade da Silva, que me ajudaram imensamente na edição deste trabalho. A meu orientador, Antônio Ferreira da Rocha Neto que me inspirou na construção deste trabalho.

A meus pais, Sérgio e Clarinda, pelo grande amor, dedicação, educação e carinho que sempre me deram. E mesmo estando longe, sempre me apoiaram e fizeram tudo por mim, é a vocês, que dedico mais essa conquista.

AGRADECIMENTOS

Primeiramente a Deus, pois é ele que me sustenta, ele é meu refúgio, a minha fortaleza e nele confio. A meus pais Antonio Sergio e Clarinda Lulini, que me ensinaram os primeiros passos, as primeiras palavras, que me mostraram o caminho correto e me guiam na caminhada por ele porque sem eles nada disso seria possível. A meus amigos Jone Bezerra Lopes Junior e Vanessa Andrade da Silva os quais me ajudaram imensamente na edição deste trabalho. A meu orientador Aluizio Ferreira da Rocha Neto que me instruiu na construção deste trabalho.

*"Se o mar se enfurecer, eu não temo o que
venha, porque eu sei que me aguarde o fidei-
jucor não falha"*

(Chris McClarnay)

RESUMO

Este trabalho tem como propósito principal, identificar as ameaças e as consequências da falta de segurança da informação em âmbito militar, bem como propor medidas de segurança da informação para a defesa do Brasil. Para isso, foram realizadas pesquisas bibliográficas e entrevistas com especialistas em segurança da informação. Os resultados da pesquisa indicam que a falta de segurança da informação pode causar danos significativos à defesa do Brasil, especialmente em termos de perda de informações estratégicas e comprometimento da capacidade de defesa. Como conclusão, recomenda-se a adoção de medidas de segurança da informação, como a implementação de políticas de segurança, a realização de treinamentos e a adoção de tecnologias de segurança.

Palavras-chave: Defesa militar, Segurança da informação, Defesa nacional, Internet

*"Se o mar se enfurecer, eu não tenho o que
temer, porque eu sei que me amas e o teu
amor não falha"*

(Chris McClarney)

RESUMO

Este trabalho tem como propósito principal, identificar os causadores e as consequências das falhas de segurança da informação no âmbito militar, tendo como ponto de partida o meio o qual esses riscos transitam, a Internet, comentando sobre seu surgimento e benefícios. Além disso, investigar os diversos riscos e vulnerabilidades encontrados nesse meio, tendo como foco os usuários, o elo mais fraco do sistema de segurança. Por fim, como estudo de caso, tem-se uma organização militar, onde foi avaliado o nível de segurança da informação, por meio de observações, entrevistas e testes, que foram realizadas no decorrer de um ano, com o objetivo de destacar a importância das pessoas na defesa de um sistema computacional e a necessidade de atenção sobre elas.

Keywords: Scope military. Security flaws. Information Security. Users. Internet.

Palavras-chaves: Âmbito militar. Falhas de segurança. Segurança da informação. Usuários. Internet.

LISTA DE ABREVIATURAS E SIGLAS ABSTRACT

This work has as main purpose to identify the causes and consequences of information security failures in the military, taking as a starting point through which the transiting these risks, the Internet, commenting on his appearance and benefits. Also, investigate the many risks and vulnerabilities found in that environment, focusing on the users, the weakest link in the security system. Finally, as a case study, there is a military organization which assessed the level of information security, through observations, interviews and tests, which were conducted in the course of a year, aiming to highlight the importance people in protecting a computer system and the need to focus on them.

MILNET – Military Network

MIT – Massachusetts Institute of Technology

Keywords: Scope military. Security flaws. Information Security. Users. Internet.

NSF – National Science Foundation

NSFNET – National Science Foundation Network

OM – Organização Militar

SPD – Seção de Processamento de Dados

TI – Tecnologia da Informação

LISTA DE ABREVEATURAS E SIGLAS

ARPA – Advanced Research Project Agency
ARPAnet – Advanced Research Project Agency Network
BITNET – Because It's Time
CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil
CPD – Central de Processamento de Dados
CSNET – Computer Science Network
GSI – Gabinete de Segurança Constitucional
ITU – International Telecommunication Union
MILNET – Military Network
MIT – Massachusetts Institute of Technology
MMS – Multimedia Message Service
NSF – National Science Foundation
NSFNET – National Science Foundation Network
OM – Organização Militar
SPD – Seção de Processamento de Dados
TI – Tecnologia da informação

LISTA DE FIGURAS

Figura 1: O crescimento mundial da Internet.....	12
Figura 2: Incidentes na internet reportados de julho à 12 de setembro/12.....	13
Figura 3: Os pilares da Segurança da Informação.....	18
Figura 4: Atual modelo da Segurança da Informação.....	20
Figura 5: Proposta de novo modelo para Segurança da Informação.....	21
Figura 6: Falhas mais comuns na Segurança da Informação.....	39
Figura 7: Motivos que contribuem para as falhas de segurança.....	41
Figura 8: Resultados da Engenharia Social empregada.....	43

2.2.1 Pilares da Segurança da Informação.....	17
2.2.2 Tipos de Vulnerabilidades.....	17
2.2.3 Fator Humano.....	19
2.2.4 Vulnerabilidades Humanas.....	21
2.3 ENGENHARIA SOCIAL.....	22
2.4 TIPOS DE AMEAÇA.....	23
2.4.1 Voluntária Aleatória.....	24
2.4.1.1 Social Engineer.....	24
2.4.1.2 Impulse.....	24
2.4.1.3 Whistle-blow.....	25
2.4.1.4 Black hat.....	25
2.4.1.5 Cyberterroristas.....	26
2.4.2 Voluntária Maliciosa.....	27
2.4.2.1 Virus.....	28
2.4.2.2 Worm.....	29
2.4.2.3 Soft e Hardwar.....	30
2.4.2.4 Backdoor.....	31
2.4.2.5 Trojan Horse.....	32
2.4.2.6 Spyware.....	33
ESTUDO DE CASO.....	35
3.1 O AMBIENTE ANALISADO.....	35
3.1.1 Estrutura de Rede.....	35
3.1.2 Segurança.....	35
3.1.3 Políticas de segurança.....	36
3.2 METODOLOGIA.....	36
3.3 RESULTADOS.....	37
3.3.1 Resultados da observação.....	37
3.3.2 Resultados das entrevistas.....	38
3.3.3 Resultados de teste.....	42
4 CONCLUSÃO.....	44
REFERÊNCIAS BIBLIOGRÁFICAS.....	46
ANEXO A - MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO.....	48
ANEXO B - MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL.....	49
ANEXO C - ROTEIRO DE PERGUNTAS PARA AS ENTREVISTAS.....	51

SUMÁRIO

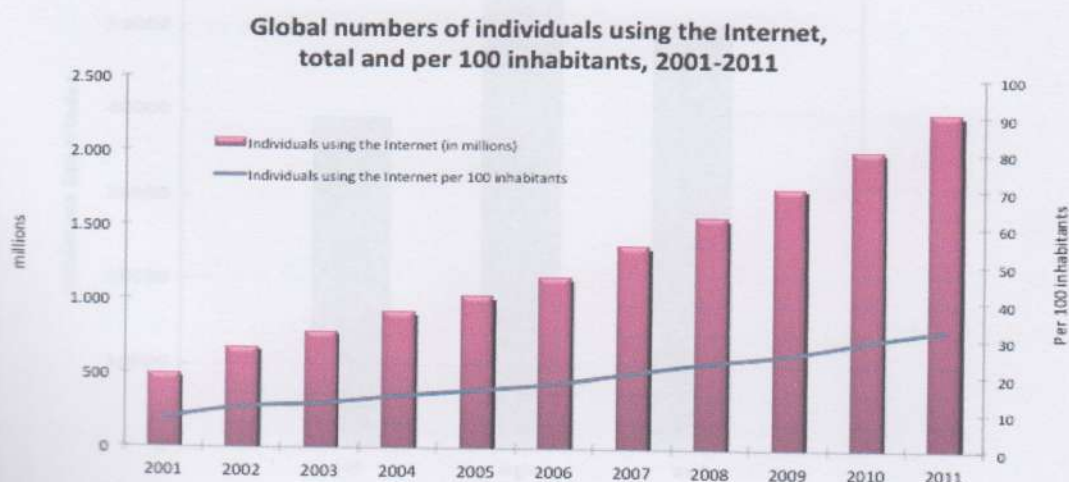
1	INTRODUÇÃO	12
1.1	DEPENDÊNCIA E RISCOS DA INTERNET	13
1.2	OBJETIVOS.....	14
1.2.1	Objetivos Específicos	14
1.3	JUSTIFICATIVA	14
2	REFERENCIAL TEÓRICO.....	16
2.1	INTERNET	16
2.2	SEGURANÇA DA INFORMAÇÃO	17
2.2.1	Pilares da Segurança da Informação.....	17
2.2.2	Tipos de Vulnerabilidades	18
2.2.3	Fator Humano	19
2.2.4	Vulnerabilidades Humanas.....	21
2.3	ENGENHARIA SOCIAL	22
2.4	TIPOS DE AMEAÇA	23
2.4.1	Voluntária: Atacantes.....	24
2.4.1.1	Script Kiddies	24
2.4.1.2	Insiders	24
2.4.1.3	White hat.....	25
2.4.1.4	Black hat	25
2.4.1.5	Cyberterroristas	25
2.4.2	Voluntária: Malware.....	27
2.4.2.1	Vírus.....	28
2.4.2.2	Worm	29
2.4.2.3	Bot e Botnet	30
2.4.2.4	Backdoor.....	31
2.4.2.5	Trojan Horse	32
2.4.2.6	Spyware	33
3	ESTUDO DE CASO	35
3.1	O AMBIENTE ANALISADO	35
3.1.1	Estrutura da Rede	35
3.1.2	Segurança.....	35
3.1.3	Políticas de segurança	36
3.2	METODOLOGIA	36
3.3	RESULTADOS	37
3.3.1	Resultados da observação	37
3.3.2	Resultados das entrevistas	39
3.3.3	Resultados do teste.....	42
4	CONCLUSÃO.....	44
	REFERÊNCIAS BIBLIOGRÁFICAS.....	45
	ANEXO A – MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO	48
	ANEXO B – MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL.....	49
	ANEXO C – ROTEIRO DE PERGUNTAS PARA AS ENTREVISTAS.....	51

1 INTRODUÇÃO

Com a popularização crescente da rede mundial de informação, a Internet, que é "uma gigantesca rede de computadores (ela é na realidade uma rede de computadores em rede)" (HONEYCUTT, 1998, p. 12), muitos desconhecem sua íntima ligação com o meio militar, ao qual ela surgiu. Pode-se afirmar que a Internet é uma das filhas da guerra, desenvolvida na corrida tecnológica durante a Guerra Fria, pela ARPA (Agência de Pesquisa em Projetos Avançados), um órgão científico e militar do departamento de defesa dos Estados Unidos da América, onde inicialmente foi nomeada de ARPAnet (Rede da Agência de Pesquisa em Projetos Avançados).

Atualmente a Internet vem se tornando mais presente a cada dia, chegando a ser indispensável tanto no cotidiano, como também nos setores empresariais, industriais e governamentais. Ela vem crescendo continuamente. Segundo Luiz (2012), o *site* Internet Archive, responsável por armazenar todo o conteúdo da Internet, revelou que o arquivo de *backup* ultrapassou a marca de 10 *petabytes* equivalente a 10 milhões de *gigabytes*. A tecnologia que pôs o mundo na era digital, a mesma que surgiu com o propósito de servi aos militares, vem mudando a forma de interação entre as pessoas e o mundo, facilitando e melhorando muitas coisas em nossas vidas, como a: comunicação, educação, entretenimento, serviços e mercado. A figura 1 demonstra o crescimento contínuo da Internet.

Figura 1: O crescimento mundial da Internet de 2001 a 2011

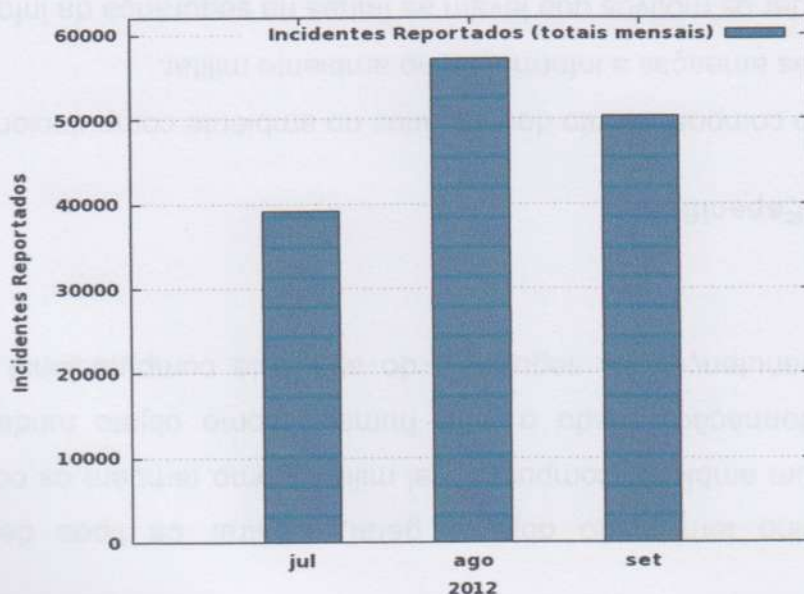


Fonte: ITU, 2012

1.1 DEPENDÊNCIA E RISCOS DA INTERNET

A internet deixou de ser apenas uma fonte de informação e entretenimento e agora está afetando diretamente nossas vidas, até mesmo as pessoas que não a usam, pelo fato de está presente em muitos serviços fundamentais e chegando a ser essencial, como por exemplo: em bancos, aeroportos, em hospitais, na segurança pública e privada, em estações de abastecimento elétrico e até mesmo em usinas nucleares, os quais dependem diretamente da conexão da internet para executar de forma plena suas atividades. Mesmo com tantos benefícios proporcionados pela Internet, a quantidade de riscos defrontados ao longo de uma conexão é imensa. Alguns bem perigosos podendo causar grandes prejuízos, tanto financeiros como físicos e até mesmo psicológicos, chegando a por em risco a própria vida humana. O perigo aumenta à medida que nos convencemos que não corremos riscos e que supostamente ninguém a de ter interesse em nossos computadores para chegar ao ponto de invadi-lo ou contamina-lo com *malwares*, é a partir desse pensamento que surge inúmeras falhas de segurança em uma rede corporativa. A Figura 2 mostra a quantidade de incidentes envolvendo malwares, invasões, golpes, etc. na internet no Brasil, reportados pela CERT.br (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil), no período de apenas 2 meses e meio.

Figura 2: Incidentes na internet reportados de julho a 12 de setembro/12



Fonte: CERT.br, 2012b

1.2 OBJETIVOS

Este trabalho tem como objetivo geral, mostrar os tipos de ameaças encontrados em um ambiente computacional militar, como também os conceitos de segurança da informação, pondo o fator humano como objeto fundamental na estruturação e manutenção da segurança do ambiente computacional no âmbito militar.

1.2.1 Objetivos Específicos

- Conhecer o comportamento dos usuários no ambiente computacional militar.
- Identificar às ameaças a informação no ambiente militar.
- Compreender os motivos que levam as falhas na segurança da informação.

1.3 JUSTIFICATIVA

As organizações militares, que são o foco desta análise, não estão imunes aos riscos defrontados ao se conectar a Internet. O antigo ministro-chefe do Gabinete de Segurança Institucional da Presidência da República, general Jorge Armando Félix, durante o ciclo de palestras da Secretaria de Assuntos Estratégicos da Presidência da República em 2010, afirmou que *“por hora são feitas 2,1 mil tentativas de invasão às redes do governo”* (SITES..., 2010), são dados preocupantes que vem aumentando a cada ano.

Sites, bancos de dados e sistemas *online* sejam eles de correio eletrônico, de controle financeiro, de material ou de pessoal, todos estão sujeitos aos perigos da Internet, e se tratando de uma Organização Militar (OM), onde além de dados pessoais, informações estratégicas do país, mensagens sigilosas e secretas como, por exemplo, uma mensagem informando a data e local de um transporte de armamento, pode existir até mesmo armas controladas remotamente, que se violadas por pessoas mal intencionadas, poderá acarretar consequências graves, como conflitos internos no país ou até mesmo em situações extremas entre nações.

Eugene Kaspersky, fundador da Kaspersky Lab, uma das maiores empresas desenvolvedores do software de proteção de computadores, prevê um *“armagedon cibernético”*, uma guerra no espaço cibernético capaz de por abaixo a maioria dos serviços essenciais, como: elétrico, hospitalar e aéreo. Em entrevista ao *site Folha*

UOL em 2012, Kaspersky disse:

[...] a evolução do “armagedon cibernético” vem seguindo a trajetória prevista. A internet mudou para se tornar mais que um ponto de encontro onde é possível conhecer pessoas. Agora afeta diretamente as nossas vidas por ser usada em todos os serviços vitais, como aeroportos, hospitais, bancos, polícia, etc.

A infraestrutura crítica de todo o planeta depende da internet. Não é mais uma brincadeira de criança. Alguém pode pregar uma peça inofensiva, mas ela pode ter consequências desastrosas. No futuro poderemos ter falta de eletricidade ou paralisações em hospitais por conta de algum malware aleatório ou, pior, em função de um ato deliberado de guerra cibernético.

A questão não é determinar se isso vai acontecer, mas quando. Pense no blecaute na região nordeste dos EUA, em 2003, ou na queda do voo 5022 da Spanair, em 2008, nas aeronaves militares de pilotagem remota que perderam o controle, ou ainda na escassez de banda da internet sul-coreana – todos esses incidentes foram causados por surtos de vírus.

Estamos sentados sobre um barril de pólvora, e estamos serrando o galho que sustenta toda a internet, e junto toda a infraestrutura do planeta. Os militares, aos poucos, estão transformando a internet em um grande campo minado. Quanto mais se observa, mais assustadora a situação parece [...]. (JERUSALÉM, M. N., 2012).

E o componente fundamental na segurança, muitas vezes ignorado pelos analistas das OM's, são os próprios usuários do ambiente computacional, que são “o fator determinante para o sucesso ou fracasso do processo de segurança da informação de uma organização. Cada usuário precisa ser treinado e conscientizado. Precisa saber suas responsabilidades, o que não pode fazer” (FONTES, 2009).

2 REFERENCIAL TEÓRICO

2.1 INTERNET

A Internet é o maior conglomerado de redes de comunicações em escala mundial e dispõe milhões de computadores interligados, que permite o acesso a informações e todo tipo de transferência de dados, ela é “uma gigantesca rede de computadores, ela é na realidade uma rede de computadores em rede” (HONEYCUTT, 1998). Para Honeycutt (1998), a Internet é dividida em duas partes, uma são os computadores e a outra as pessoas, que são definidas respectivamente como: uma vasta rede de computadores à qual qualquer pessoa pode conectar seu computador e como uma vasta comunidade de pessoas que se conecta a rede.

Segundo Honeycutt (1998, p. 12), a Internet teve início em 1969, na ARPA (Agência de Projetos de Pesquisa Avançada) criada pelo Departamento de Defesa dos EUA, com o objetivo de projetar uma rede de comunicação de maneira a qual, se parte dela fosse destruída por um ataque nuclear, mesmo assim seria possível o envio de uma mensagem até seu destino desejado, tendo como resultado a ARPAnet. Onde em 1983, principalmente por razões pragmáticas, a ARPAnet se dividiu em dois diferentes sistemas nomeados, ARPAnet e MILNET. A ARPAnet foi reservada para uso civil, tal como pesquisa, e a MILNET foi reservada para uso militar. As redes foram conectadas de modo que seus usuários pudessem trocar informações; isso se tornou conhecido como Internet. Por fim, outras redes surgiram como a BITNET (Because It's Time – “Porque é hora”) e CSNET (Computer Science Network – Rede de Ciência de Computador, inicialmente, elas eram redes totalmente separadas, usadas para propósitos educacionais e de pesquisa, mas com o tempo elas se conectaram a Internet para facilitar o compartilhamento de informações entre organizações. Um dos mais importantes avanços para a Internet veio em 1986, quando o *National Science Foundation* (NSF – Fundação Nacional de Ciência) criou a NSFNET para conectar diversos supercomputadores de alta velocidade ao longo do país – principalmente para propósitos de pesquisa. A ARPAnet foi desativada, e a NSFNET tornou-se o principal *pipeline* (ou backbone) para a Internet.

Nos últimos anos, a Internet vem se tornando mais presente a cada dia, chegando a ser muitas vezes fundamental, tanto no cotidiano de cada um, como também nos setores empresariais, industriais e governamentais. Ela vem crescendo

continuamente a cada instante e segundo Luiz (2012), o *site* Internet Archive responsável por armazenar todo o conteúdo da Internet, revelou que o arquivo de *backup* ultrapassou a marca de 10 *petabytes* equivalente a 10 milhões de *gigabytes*, e a fabricante de equipamentos de rede computacional, segundo Leske (2012), pesquisa da Cisco Systems revela que o tráfego da Internet crescerá 29% até 2016, atingindo 1,3 *zettabytes*, onde o tráfego esperado para 2016, será maior do que todos os anos anteriores somados

2.2 SEGURANÇA DA INFORMAÇÃO

A informação deve ser considerada um ativo da empresa e seu correto gerenciamento é fundamental para o sucesso de qualquer organização. Devido tamanha sua importância nos negócios, a informação precisa ser protegida, de forma que acessos não autorizados, alterações indevidas e indisponibilidades sejam evitados, com o fim de proteger essas informações se emprega a segurança da informação que é definida como “uma área do conhecimento que salvaguarda os chamados ativos da informação, contra acessos indevidos, modificações não autorizadas ou até mesmo sua não disponibilidade” (PEIXOTO, 2006, p. 37).

2.2.1 Pilares da Segurança da Informação

Peixoto (2006), afirma que a segurança da informação é formada pelos seguintes pilares básicos, que podem ser definidos da seguinte maneira:

- **Confidencialidade:** É a garantia de que as informações transmitidas chegarão ao seu destino sem que se dissipem para outro lugar onde não deveria passar. Várias tecnologias como, por exemplo, criptografia e autenticações podem ser usadas, desde que mantenham a integridade das informações;
- **Integridade:** É a garantia de que as informações não sofreram nenhuma modificação durante o trajeto entre a pessoa que enviou e a pessoa que recebeu a informação, garantindo assim a sua real veracidade após chegarem ao destino;

- **Disponibilidade:** De nada adianta possuir integridade e confidencialidade, se a informação nunca está disponível. Então, o grande desafio é manter essa estrutura de passagem de informações de forma confiável e íntegra sem que haja impossibilidade de captar as informações;
- **Não repúdio e autenticidade:** Conhecido como responsabilidade final, tem como objetivo verificar a identidade e autenticidade de alguém ou até mesmo de um agente exterior a fim de garantir a integridade de origem.

Dessa maneira o modelo seria representado como na Figura 3.

Figura 3: Os pilares da Segurança da Informação



Fonte: SKYLAN, 2012

2.2.2 Tipos de Vulnerabilidades

Para Peixoto (2006), os principais tipos de vulnerabilidades existentes podem ser do tipo:

- **Físicas:** Salas de CPD mal planejadas, estrutura de segurança fora dos padrões exigidos;
- **Naturais:** computadores são propensos a sofrerem danos naturais, como tempestades, incêndio, além, por exemplo, de falta de energia, acúmulo de poeira, aumento da umidade e temperatura;

- **Hardware:** Desgaste do equipamento, obsolescência ou má utilização;
- **Software:** Má instalação, erros de configuração, vazamento de informações e dependendo do caso, perda de dados ou indisponibilidade de recursos;
- **Mídias:** Disquetes e CDs podem ser perdidos ou danificados, e a radiação eletromagnética pode causar danos às vezes irreparáveis nas mídias;
- **Comunicação:** Acessos não autorizados ou perda de comunicação;
- **Humana:** Tratadas anteriormente, como por exemplo, as técnicas de engenharia social, as vulnerabilidades referindo-se ao fator humano, como falta de treinamentos, conscientização, o não seguimento das políticas de segurança.

2.2.3 Fator Humano

Sistemas de segurança da informação são como uma corrente com muitos elos, figurativamente representam os componentes envolvidos como, por exemplo, *hardware*, *software*, etc., incluindo o usuário humano, onde o usuário é frequentemente referenciado como o elo mais fraco, também por estar sujeito a enorme variabilidade de fatores e comportamentos potencialmente inseguros.

Uma empresa pode ter adquirido as melhores tecnologias de segurança que o dinheiro pode comprar, pode ter treinado seu pessoal tão bem que eles trancam todos os segredos antes de ir embora e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa empresa ainda estará vulnerável. Os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis. (MITNICK; SIMON, 2003, p. 3).

Marcelo e Pereira (2005), afirmaram que qualquer organização por maior que seja a sua segurança, sempre haverá um fator de desequilíbrio chamado "fator humano". O velho ditado que diz que *"um segredo deixa de ser um segredo quando*

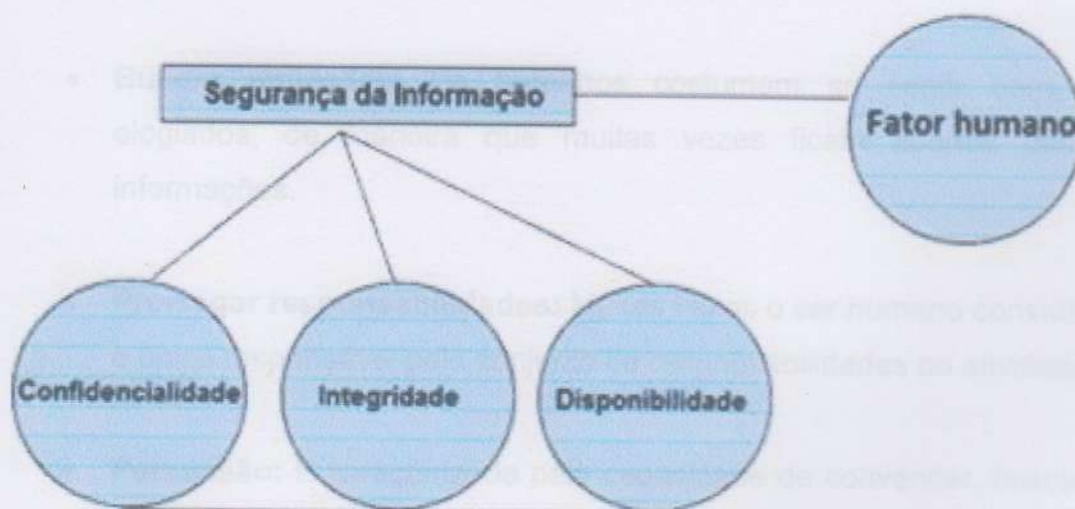
mais alguém sabe” é uma das máximas existentes dentro da segurança da informação. Os maiores engenheiros sociais tiram proveito das fraquezas ou gostos pessoais de seus alvos para assim aproximar e conseguir alcançar seus objetivos.

Segundo Silva e Costa (2009), um dos maiores problemas hoje em dia na segurança da informação está relacionado ao ser humano e sua ignorância. Práticas que permitem o acesso não autorizado a dados, lugares, objetos e entre outros, fragiliza qualquer esquema de segurança da informação, uma vez que as pessoas acabam tendo acesso a informações indevidas, colocando em risco a segurança da informação. A questão comportamental pode afetar significativamente as demais medidas de segurança, por mais modernas que elas sejam.

Um dos grandes assuntos discutidos atualmente é a questão da inclusão do fator humano como um dos elementos base da segurança da informação. Existem propostas de modelos para inclusão desse fator primordial como um dos pilares fundamentais da segurança da informação, pois o modelo atual considera o fator humano em um nível não base. (ALVES, C. B, 2010, p. 23).

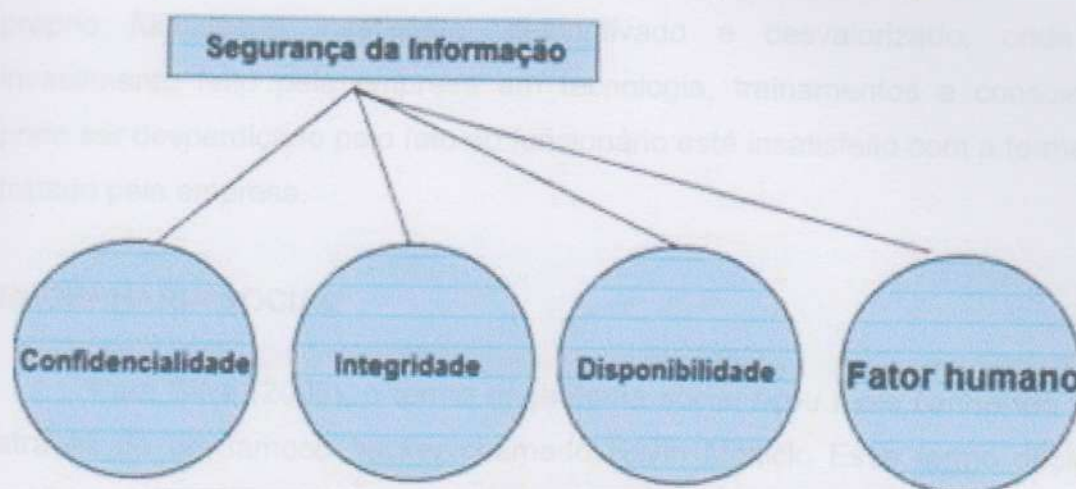
A figura 4 demonstra o modelo atual de segurança atual onde o fator humano não é considerado como um dos elementos base da segurança da informação, mesmo diante de tamanha importância na estrutura da segurança, já na figura 5 mostra a nova proposta para o modelo de segurança da informação onde traz o fator humano como elemento base juntamente com a confidencialidade, integridade e disponibilidade.

Figura 4: Atual modelo da Segurança da Informação



Fonte: SILVA, M.; COSTA, 2009

Figura 5: Proposta de novo modelo para Segurança da Informação



Fonte: SILVA, M.; COSTA, 2009

Serão apresentados no próximo tópico os motivos os quais fundamentam a tamanha importância do fator humano, na estrutura da segurança de qualquer rede seja ela privada ou corporativa.

2.2.4 Vulnerabilidades Humanas

Podem-se destacar as seguintes características do ser humano que o torna vulnerável e suscetível a ataques de engenharia social:

- **Vontade de se tornar útil:** O ser humano procura ser Cortez ou ajudar os outros quando necessário.
- **Buscar amizades:** Os humanos costumam se sentir bem ao serem elogiados, de maneira que muitas vezes ficam abertos para fornecer informações.
- **Prorrogar responsabilidades:** Muitas vezes o ser humano considera não ser o único responsável pelo conjunto de responsabilidades ou atividades.
- **Persuasão:** É caracterizada pela capacidade de convencer, buscando assim a respostas desejadas para alcançar o objetivo. Isso acontece porque o ser humano possui características que o tornam vulneráveis a manipulação.

Segundo Prescott (2007), outra grande vulnerabilidade dentro da empresa é o próprio funcionário insatisfeito, desmotivado e desvalorizado, onde todo o investimento feito pela empresa em tecnologia, treinamentos e conscientização, pode ser desperdiçado pelo fato do funcionário estar insatisfeito com a forma o qual é tratado pela empresa.

2.3 ENGENHARIA SOCIAL

Para Silva (2008), o termo engenharia social ficou mais conhecido em 1990, através de um famoso *hacker* chamado Kevin Mitnick. Esse termo designa para práticas utilizadas a fim de se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informação, explorando a confiança das pessoas para enganá-las. Pode-se também definir engenharia social como a arte de manipular pessoas a fim de contornar dispositivos de segurança ou construir métodos e estratégias para ludibriar pessoas, utilizando informações cedidas por elas de maneira a ganhar a confiança delas para obter informações. Muitos são os significados e interpretações dadas ao termo “Engenharia Social”. Uma das melhores encontradas é a seguinte:

Engenharia Social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de Engenharia Social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo tipo de fraudes, inclusive invasão de sistemas eletrônicos. (KONSULTEX, 2004 apud PEIXOTO, 2006, p. 4).

O termo “engenharia” foi atribuído a essa prática segundo Santos (2004), porque é construída sobre informações e táticas de acesso a informações sigilosas de forma indevida. Já o termo “social” foi atribuído porque utiliza pessoas que vivem e trabalham em grupos organizados. Essas práticas simplesmente ganharam esse novo termo, pois são bem antigas sendo bastante utilizadas por detetives a fim de obterem informações e também por magistrados com o objetivo de comprovar se um declarante fala a verdade. “A engenharia social, propriamente dita, está inserida como um dos desafios (se não o maior deles) mais complexos no âmbito das vulnerabilidades encontradas na gestão da segurança da informação” (PEIXOTO, 2006, p. 36).

Os ataques de engenharia social podem ser divididos em dois grupos:

- **Ataques diretos:** Como o próprio nome já diz, são aqueles caracterizados pelo contato direto entre o engenheiro social e a vítima através de telefonemas, fax e até mesmo pessoalmente. Este exige do engenheiro social, um planejamento antecipado e bem detalhado, além de um segundo plano para caso o primeiro não dê certo, além de muita criatividade e articulação para que o plano seja bem sucedido.
- **Ataques indiretos:** Caracterizam-se pela utilização de *softwares* ou ferramentas para invadir como, por exemplo, vírus, *Cavalos de Troia* ou através de sites e *e-mails* falsos para assim obter informações desejadas.

2.4 TIPOS DE AMEAÇA

Muitas vezes nos sentimos ameaçados em determinadas situações, mas isso não quer dizer necessariamente que você se sente vulnerável. Já na situação oposta, quando alguém se considera vulnerável, certamente essa pessoa se vê ameaçada. Não é uma regra, mas é válida se comparada com o que diz respeito às informações. Para Peixoto (2006), as ameaças são o resultado das vulnerabilidades existentes, o que prova a perda dos elementos básicos para existir segurança da informação que são eles a confidencialidade, integridade e disponibilidade. Essas ameaças podem ser divididas em:

- **Naturais:** Fenômenos da natureza. Como por exemplo, raios que danificam equipamentos, chuvas, umidade, terremotos e etc.
- **Involuntárias:** Aquelas que ocorrem por causa do desconhecimento, erros ou acidentes e entre outros.
- **Voluntárias:** São aquelas propositais, resultantes de ações como, por exemplo, ações de *Crackers*, espiões, disseminadores de vírus de computador.

2.4.1 Voluntária: Atacantes

Todo indivíduo que ataca um sistema computacional é genericamente intitulado pela mídia como *Hacker*, porém “os *hackers*, por sua definição original são aqueles que utilizam seus conhecimentos para invadir sistemas, não com o intuito de causar danos às vítimas, mas sim como desafio às suas habilidades” (NAKAMURA; GEUS, 2010, p. 66). Surgindo então diversas classificações de tipos de *hackers*, que serão mostradas a seguir.

2.4.1.1 Script Kiddies

Segundo Nakamura e Geus (2010), *script kiddies* também conhecidos como *newbies*, trazem muitos problemas às organizações, porque geralmente eles são novatos e inexperientes, que conseguem ferramentas de invasão que podem ser na internet, e depois as utilizam sem entender o que estão fazendo. Devido à grande facilidade em se obter essas ferramentas, os *script kiddies* são bem numerosos e considerados perigosos para um grande número de organizações, as quais não possuem uma boa política de segurança. Em consequência de uma fraca política de segurança ou inadequada, essas organizações sempre apresentam alguma abertura na segurança pronta para serem exploradas, principalmente as que são geradas pela falta de atualizações de um *patch* do servidor. Isso é o suficiente para que os *script kiddies* executem as ferramentas encontradas na internet contra seus servidores e causem estragos consideráveis.

2.4.1.2 Insiders

Os *insiders* são os maiores responsáveis pelos incidentes de segurança mais graves nas organizações. A “espionagem industrial é atribuída, geralmente a eles, e são considerados uma nova modalidade de crime organizado, assim como as máfias e os cartéis de droga” (NAKAMURA; GEUS, 2010, p. 70). Em um nível mais alto, o que se vê é o surgimento de organizações especializadas em espionagem industrial, pois o próprio governo de alguns países, como Japão, França e Israel, financiam esses trabalhos, institucionalizando essa prática.

A identificação dos *insider* pode ser difícil, mas geralmente são funcionários descontentes com seu trabalho, que sentem que suas funções são subestimadas pelos seus chefes. Frequentemente, eles são maltratados e querem mostrar seu real valor realizando alguma

coisa para se sentirem importantes. Esse tipo de funcionário pode ser facilmente manipulado por concorrentes, que sabem como persuadir as pessoas que se encontram em uma posição não muito confortável dentro da organização. (NAKAMURA; GEUS, 2010, p. 71).

2.4.1.3 *White hat*

Segundo Nakamura e Geus (2010), também conhecidos como *hacker* do bem ou *hacker* éticos os quais utilizam seus conhecimentos para descobrir vulnerabilidades nos sistemas e aplicar as correções necessárias, trabalhando de maneira profissional e legal dentro das organizações. Eles veem a si próprio como guerreiros que protegem os sistemas das organizações que os contratam contra os *black hat*. Eles são os responsáveis pelos testes de invasão, em que simulam ataques para medir o nível de segurança da rede, e também pelas diversas análises de segurança necessárias para a proteção da informação em uma organização.

2.4.1.4 *Black hat*

São também conhecidos como *crackers*, diferentemente dos *White hat* apesar de serem especialistas em computação, com um conhecimento tão vasto quanto eles, os *black hat* “utiliza seus conhecimentos para invadir sistemas e roubar informações secretas das organizações” (NAKAMURA; GEUS, 2010, p. 75). Geralmente, buscam vender as informações roubadas de novo à sua própria vítima, ameaçando a organização de divulgação das informações roubadas, caso o valor desejado não seja pago. Esse tipo de prática é conhecido como chantagem ou *blackmail* e a exposição pública das informações roubadas pode trazer consequências indesejadas à vítima. Além do *blackmail*, qualquer ação que venha a prejudicar afetando de forma negativa e causando prejuízos às suas vítimas pode ser considerada de autoria de *black hats*.

2.4.1.5 Cyberterroristas

Segundo Nakamura e Geus (2010), cyberterrorista é o termo utilizado para definir os *hackers* que realizam seus ataques contra alvos selecionados cuidadosamente, com o objetivo de transmitir uma mensagem política ou religiosa (*hacktivism*) para derrubar a infraestrutura de comunicação ou para obter

informações que podem comprometer a segurança nacional de alguma nação. Os meios para que isso seja alcançado são:

- Um ataque semântico, que é consequência de uma 'pichação' de *sites*, quando a modificação de uma página do *site* pode disseminar informações falsas, além de mensagens políticas ou religiosas;
- Ataques sofisticados de negação de serviços distribuídos (*Distributed Denial-of-Service* – DDoS);
- Invasões a sistemas com o objetivo de obter informações confidenciais.

Esses tipos de ataques cibernéticos devem ser considerados com extrema importância, ainda mais em uma época de guerras, como a dos Estados Unidos contra o Afeganistão e o Iraque. É interessante notar que as estatísticas mostram que existe uma relação muito grande entre conflitos político-religiosos e ataques de *hackes*. Um exemplo é o grande aumento de *sites* modificados na Índia, que estava em conflito com o Paquistão, no Kashmir: em 1999, foram registrados 45 ataques contra *sites* indianos, em comparação com 133 ataques ocorridos em 2000 e 275 ataques realizados até agosto de 2001. Os *hackers* paquistaneses são notórios em casos de ataques semânticos, além de realizarem ataques sofisticados, como o que foi feito contra o Bhabha Atomic Research Center, quando foram roubados cinco megabytes de informações possivelmente confidenciais sobre pesquisa nuclear e outras áreas.

Segundo Nakamura e Geus (2010), outro exemplo que mostra a conexão entre ataques físicos e cibernéticos pode ser visto no conflito entre israelenses e palestinos. Chamada até mesmo de *cyberjihad*, a conexão pode ser vista pelo aumento do número de incidentes de segurança em *sites* israelenses, quando um conflito físico acontece. Já ocorreu aumento de até 1000% no número de ataques de *hackers*; por exemplo, quando bombas mataram quatro e feriram 69 israelenses, ou quando duas semanas de violência culminaram no ataque de um homem-bomba em um ponto de ônibus na periferia de TelAviv, refletindo sempre no aumento dos ataques cibernéticos.

As invasões não autorizadas que resultam no 'vazamento' de informações têm confidenciais podem resultar em grandes consequências, principalmente quando essas informações envolvem a segurança nacional. No caso conhecido como *Moonlight maze*, a Rússia executou contra sistemas do governo norte-americano uma série de invasões que tiveram início em março de 1998 e duraram

alguns anos. Apesar de autoridades negarem o fato, centenas de redes privadas do Pentágono, do Departamento de Energia, da NASA e de órgãos de defesa foram invadidos e há suspeita de que grande quantidade de pesquisas técnicas e documentos confidenciais foram obtidos pelos *hackers*. (NAKAMURA; GEUS, 2010, p. 78).

Até mesmo a infraestrutura de um país pode ser vítima de *hackers*. Além dos ataques de DDoS, que podem ser executados contra a infraestrutura de comunicação, uma simulação realizada pelo Pentágono, conhecida como *Elegible Receiver*, mostrou as vulnerabilidades da infraestrutura de distribuição de energia dos Estados Unidos. O fator crítico é que essas vulnerabilidades foram exploradas realmente em junho de 2001, quando *hackers* chegaram até a rede do *California Indeopendent Systems Operator* por meio de redes operadas pela *China Telecom*. Os *hackers* permaneceram nessa rede durante 17 dias. (NAKAMURA; GEUS, 2010).

2.4.2 Voluntária: Malware

Muitos se equivocam ao pensar, que todos os programas que causam algum dano ou altere alguma configuração no sistema operacional se trata de um vírus, eles fazem parte da família dos *malwares*, que é a combinação das palavras inglesas *malicious* e *software*, ou seja, programas maliciosos, “códigos maliciosos (*malware*) são programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador”. (CERT.br, 2012). Algumas das formas que esses *malwares* podem afetar um computador são as seguintes:

- Pela exploração de vulnerabilidades existentes nos programas instalados;
- Pela auto-execução de mídias removíveis infectadas, como *pen drives*;
- Pelo acesso a páginas *Web* maliciosas, utilizando navegadores vulneráveis;
- Pela ação direta de atacantes que, após invadirem o computador, incluem arquivos contendo códigos maliciosos;
- Pela execução de arquivos previamente infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *Web* ou diretamente de outros computadores (através do compartilhamento de recursos).

Os principais tipos de *malware* serão apresentados nas seções seguintes.

2.4.2.1 Vírus

De acordo com CERT.br (2012), vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos, funcionando de certa forma igual a um vírus biológico, por esse motivo herdou o nome vírus.

Para que possa se tornar ativo e dar continuidade ao processo de infecção, o vírus depende da execução do programa ou arquivo hospedeiro, ou seja, para que o seu computador seja infectado é preciso que um programa já infectado seja executado.

O principal meio de propagação de vírus costumava ser os disquetes. Com o tempo, porém, estas mídias caíram em desuso e começaram a surgir novas maneiras, como o envio de *e-mail*. Atualmente, as mídias removíveis tornaram-se novamente o principal meio de propagação, não mais por disquetes, mas, principalmente, pelo uso de *pen drives*.

Há diferentes tipos de vírus. Alguns procuram permanecer ocultos, infectando arquivos do disco e executando uma série de atividades sem o conhecimento do usuário. Há outros que permanecem inativos durante certos períodos, entrando em atividade apenas em datas específicas. (CERT.br, 2012).

Alguns dos tipos de vírus mais comuns são:

- **Vírus propagado por e-mail:** recebido como um arquivo anexo a um *e-mail* cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os *e-mails* encontrados nas listas de contatos gravadas no computador;
- **Vírus de script:** escrito em linguagem de *script*, como VBScript e JavaScript, e recebido ao acessar uma página Web ou por *e-mail*, como arquivo anexo ou como parte do próprio *e-mail* escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de *e-mail* do usuário;
- **Vírus de macro:** tipo específico de vírus de *script*, escrito em linguagem de macro, que tenta infectar arquivos manipulados por aplicativos que utilizam esta linguagem como, por exemplo, os que compõem a Microsoft Office (Excel, Word e PowerPoint, entre outros);

- **Vírus de telefone celular:** vírus que se propaga de celular para celular por meio da tecnologia *bluetooth* ou de mensagens MMS. A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa. Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas e drenar a carga da bateria, além de tentar se propagar para outros celulares.

2.4.2.2 Worm

De acordo com CERT.br (2012), worm é um programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não se propaga por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, mas sim pela execução direta de suas cópias ou pela exploração automática de vulnerabilidades existentes em programas instalados em computadores. *Worms* são notadamente responsáveis por consumir muitos recursos, devido à grande quantidade de cópias de si mesmo que costumam propagar e, como consequência, podem afetar o desempenho de redes e a utilização de computadores. O processo de propagação e infecção dos *worms* ocorre da seguinte maneira:

a. **Identificação dos computadores alvos:** após infectar um computador, o *worm* tenta se propagar e continuar o processo de infecção. Para isto, necessita identificar os computadores alvos para os quais tentará se copiar, o que pode ser feito de uma ou mais das seguintes maneiras:

- Efetuar varredura na rede e identificar computadores ativos;
- Aguardar que outros computadores contatem o computador infectado;
- Utilizar listas, predefinidas ou obtidas na Internet, contendo a identificação dos alvos;
- Utilizar informações contidas no computador infectado, como arquivos de configuração e listas de endereços de *e-mail*.

b. **Envio das cópias:** após identificar os alvos, o *worm* efetua cópias de si mesmo e tenta enviá-las para estes computadores, por uma ou mais das seguintes formas:

- Como parte da exploração de vulnerabilidades existentes em programas instalados no computador alvo;
- Anexadas a *e-mails*;
- Via canais de IRC (*Internet Relay Chat*);
- Via programas de troca de mensagens instantâneas;
- Incluídas em pastas compartilhadas em redes locais ou do tipo P2P (*Peer to Peer*).

c. **Ativação das cópias:** depois de realizado o envio da cópia, o *worm* necessita ser executado para que a infecção ocorra, o que pode acontecer de uma ou mais das seguintes maneiras:

- Imediatamente após ter sido transmitido, pela exploração de vulnerabilidades em programas sendo executados no computador alvo no momento do recebimento da cópia;
- Diretamente pelo usuário, pela execução de uma das cópias enviadas ao seu computador;
- Pela realização de uma ação específica do usuário, a qual o *worm* está condicionado como, por exemplo, a inserção de uma mídia removível.

d. **Reinício do processo:** após o alvo ser infectado, o processo de propagação e infecção recomeça, sendo que, a partir de agora, o computador que antes era o alvo passa a ser também o computador originador dos ataques.

2.4.2.3 Bot e Botnet

De acordo com CERT.br (2012), *bot* é um programa com mecanismos de comunicação com o atacante, que permite a ele controlar remotamente o computador infectado. Assim como o *worm*, ele possui a capacidade de se propagar automaticamente, explorando vulnerabilidades existentes em programas instalados no computador. A comunicação entre o invasor e o computador infectado pelo *bot* pode ocorrer via canais de IRC, servidores *Web* e redes do tipo P2P, entre

outros meios. Ao se comunicar, o invasor pode enviar instruções para que ações maliciosas sejam executadas, como desferir ataques, furtar dados do computador infectado e enviar *spam*.

Um computador infectado por um *bot* costuma ser chamado de zumbi (*zombie computer*), pois pode ser controlado remotamente, sem o conhecimento do seu dono. Também pode ser chamado de *spam zombie* quando o *bot* instalado o transforma em um servidor de *e-mails* e o utiliza para o envio de *spam*. *Botnet* é uma rede formada por centenas ou milhares de computadores zumbis e que permite potencializar as ações danosas executadas pelos *bots*. Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

2.4.2.4 Backdoor

De acordo com CERT.br (2012), *backdoor* é um programa que permite o retorno de um invasor a um computador comprometido, por meio da inclusão de serviços criados ou modificados para este fim. Pode ser incluído pela ação de outros códigos maliciosos, que tenham previamente infectado o computador, ou por atacantes, que explorem vulnerabilidades existentes nos programas instalados no computador para invadi-lo. Após incluído, o *backdoor* é usado para assegurar o acesso futuro ao computador comprometido, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado. A forma usual de inclusão de um *backdoor* consiste na disponibilização de um novo serviço ou na substituição de um determinado serviço por uma versão alterada, normalmente possuindo recursos que permitem o acesso remoto. Programas de administração remota, como BackOrifice, NetBus, SubSeven, VNC e

Radmin, se mal configurados ou utilizados sem o consentimento do usuário, também podem ser classificados como *backdoors*.

Há casos de *backdoors* incluídos propositalmente por fabricantes de programas, sob alegação de necessidades administrativas. Esses casos constituem uma séria ameaça à segurança de um computador que contenha um destes programas instalados pois, além de comprometerem a privacidade do usuário, também podem ser usados por invasores para acessarem remotamente o computador.

2.4.2.5 Trojan Horse

De acordo com CERT.br (2012), cavalo de troia, *trojan* ou *trojan-horse*, é um programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário. Exemplos de *trojans* são os programas que você recebe ou obtém de *sites* na Internet e que parecem ser apenas cartões virtuais animados, álbuns de fotos, jogos e protetores de tela, entre outros. Estes programas, geralmente, consistem de um único arquivo e necessitam ser explicitamente executados para que sejam instalados no computador.

Trojans também podem ser instalados por atacantes que, após invadirem um computador, alteram programas já existentes para que, além de continuarem a desempenhar as funções originais, também executem ações maliciosas. Há diferentes tipos de *trojans*, classificados de acordo com as ações maliciosas que costumam executar ao infectar um computador. Alguns destes tipos são:

- **Trojan Downloader:** instala outros códigos maliciosos, obtidos de *sites* na Internet;
- **Trojan Dropper:** instala outros códigos maliciosos, embutidos no próprio código do *trojan*;
- **Trojan Backdoor:** inclui *backdoors*, possibilitando o acesso remoto do atacante ao computador;

- **Trojan DoS:** instala ferramentas de negação de serviço e as utiliza para desferir ataques;
- **Trojan Destrutivo:** altera/apaga arquivos e diretórios, formata o disco rígido e pode deixar o computador fora de operação;
- **Trojan Clicker:** redireciona a navegação do usuário para *sites* específicos, com o objetivo de aumentar a quantidade de acessos a estes *sites* ou apresentar propagandas;
- **Trojan Proxy:** instala um servidor de *proxy*, possibilitando que o computador seja utilizado para navegação anônima e para envio de *spam*;
- **Trojan Spy:** instala programas *spyware* e os utiliza para coletar informações sensíveis, como senhas e números de cartão de crédito, e enviá-las ao atacante;
- **Trojan Banker ou Bancos:** coleta dados bancários do usuário, através da instalação de programas *spyware* que são ativados quando *sites* de *Internet Banking* são acessados. É similar ao *Trojan Spy* porém com objetivos mais específicos.

2.4.2.6 Spyware

De acordo com CERT.br (2012), *spyware* é um programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros. Pode ser usado de duas formas as quais se diferem do modo de instalado, das ações realizadas, do tipo de informação monitorada e do uso que é feito por quem recebe as informações coletadas, que são:

- **Legítimo:** quando instalado em um computador pessoal, pelo próprio dono ou com consentimento deste, com o objetivo de verificar se outras pessoas o estão utilizando de modo abusivo ou não autorizado;

- **Malicioso:** quando executa ações que podem comprometer a privacidade do usuário e a segurança do computador, como monitorar e capturar informações referentes à navegação do usuário ou inseridas em outros programas (por exemplo, conta de usuário e senha).

Alguns tipos específicos de programas *spyware* são:

- **Keylogger:** capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Sua ativação, em muitos casos, é condicionada a uma ação prévia do usuário, como o acesso a um *site* específico de comércio eletrônico ou de *Internet Banking*;

- **Screenlogger:** similar ao *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou a região que circunda a posição onde o *mouse* é clicado. É bastante utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*;

- **Adware:** projetado especificamente para apresentar propagandas. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos. Também pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas, de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito.

3 ESTUDO DE CASO

Neste capítulo será apresentado, o estudo de caso realizado em uma organização militar, onde por questão de segurança sua localização exata e seu nome serão preservados.

3.1 O AMBIENTE ANALISADO

Trata-se de uma organização militar, situada no estado do Rio Grande do Norte na cidade de Natal, composta por 462 militares, onde cerca de 120 trabalham diretamente com os recursos computacionais e o restante possuem acesso indireto.

3.1.1 Estrutura da Rede

A LAN da OM opera a 100Mbps utilizando somente *Switches* em sua composição. As ligações entre prédios mais distantes são feitas por meio de fibra óptica operando a 1Gbps. Existem segmentos utilizando cabo de par trançado categoria seis (CAT) operando a 1Gbps. Os segmentos gigabit abrangem cerca de 90% dos *uplinks/dowlinks* formando um *backbone* com essa capacidade nominal o que ocasiona uma perda considerável na largura de banda, sendo que todas as estações de trabalho operam a 100Mbps.

3.1.2 Segurança

- **Segurança física:** Os servidores possuem uma sala específica mas ainda não contam com a segurança adequada; *Switches* são ligados a *nobreak* em seus respectivos pontos, lacrados dentro de *racks*, sendo que nem todos possuem *rack*;
- **Segurança lógica:** Todas as estações de trabalho contam com as ferramentas de proteção padronizadas, as quais são instaladas e atualizadas via ePO¹. As atualizações automáticas do Sistema Operacional são feitas via WSUS²;

¹ ePolicy Orchestrator (ePO) – software de gerenciamento de segurança da McAfee.

² Windows Server Update Service (WSUS) – gerenciador de atualizações do Windows.

- **Segurança de tráfego de informações digitais:** Há ferramentas de criptografia padronizadas para tráfego de mensagens. Há também software de criptografia padronizado para armazenamento de dados e software de assinatura eletrônica padronizada.

3.1.3 Políticas de segurança

As normas de segurança da informação da OM, que constituem a política de segurança, são muitas, impondo um grande controle de acesso às estações de trabalho e a Internet, obrigando ao usuário a concordar com dois termos, que são:

- **Termo de recebimento da estação de trabalho:** o qual discrimina as configurações da estação de trabalho, tanto *software* como *hardware*, o responsabilizando sobre qualquer alteração que venha a ser feita na estação de trabalho, conforme o "ANEXO A";
- **Termo de responsabilidade individual:** torna ciente o usuário das principais normas existente sobre a segurança da informação, conforme o "ANEXO B".

3.2 METODOLOGIA

Com o objetivo de levantar dados, para avaliar o estado da segurança da informação, foi realizada uma pesquisa que é um "procedimento reflexivo sistemático, controlado e crítico, que permite descobrir novos fatos e dados, relações ou leis, em qualquer campo do conhecimento" (ANDER-EGG, 1978, p. 28) de caráter observacional e quantitativo, por meio de observações assistemáticas, entrevistas não estruturadas e testes, os quais foram:

- **Observação assistemática:** pesquisa a qual "consiste em recolher e registrar os fatos da realidade sem que o pesquisador utilize meios técnicos especiais ou precise fazer perguntas diretas" (MARCONE; LAKATOS, 2010, p. 175). Realizada no decorrer do expediente de trabalho, observando como os usuários se comportam no ambiente computacional;

- **Entrevista não estruturada:** a entrevista não estruturada ocorre quando “o entrevistador tem liberdade para desenvolver cada situação em qualquer direção que considere adequada.[...] Em geral, as perguntas são abertas e podem ser respondidas dentro de uma conversa formal” (MARCONE; LAKATOS, 2010, p. 180), fundamentando-se nesse pressuposto foram realizadas entrevistas, durante os atendimentos técnicos com o propósito de conhecer as dificuldades enfrentadas pelos usuários;
- **Teste:** foram testados a resistência dos usuários contra ataques a segurança da informação, se utilizando para isso da engenharia social direta, executada através do contato direto onde 20 voluntários que não possuem acesso as estações de trabalho teriam que de algum modo obter acesso a elas e indireta, onde pelo telefone 10 voluntários instruídos a se passarem por um dos técnicos buscariam obter senhas de acesso as estações de trabalho.

3.3 RESULTADOS

Apurados ao decorrer deste ano pelos meios já citados na seção 3.2, os quais tornaram possível coletar informações para assim chegar aos seguintes resultados.

3.3.1 Resultados da observação

Ao observar o modo ao qual os usuários que possuem acesso direto as estações de trabalho se comportam no ambiente computacional, foi possível notar que 100% dos usuários não cumprem pelo menos uma das regras da política de segurança adotada, descritas nos termos mencionados na seção 3.1.3, confirmando assim o que diz Mitnick (2003), ao afirmar que uma organização pode ter adquirido as melhores tecnologias de segurança disponíveis no mercado e pode ter contratado guardas para o prédio na melhor empresa de segurança que existe. Mesmo assim essa organização ainda estará vulnerável.

As principais vulnerabilidades identificadas a parti da observância dos usuários interagindo com ambiente computacional da OM, foram:

- **Anotações e exposições de senhas:** 16 usuários foram observados com senhas anotadas em pedaços de papel fixados no gabinete, no monitor, em

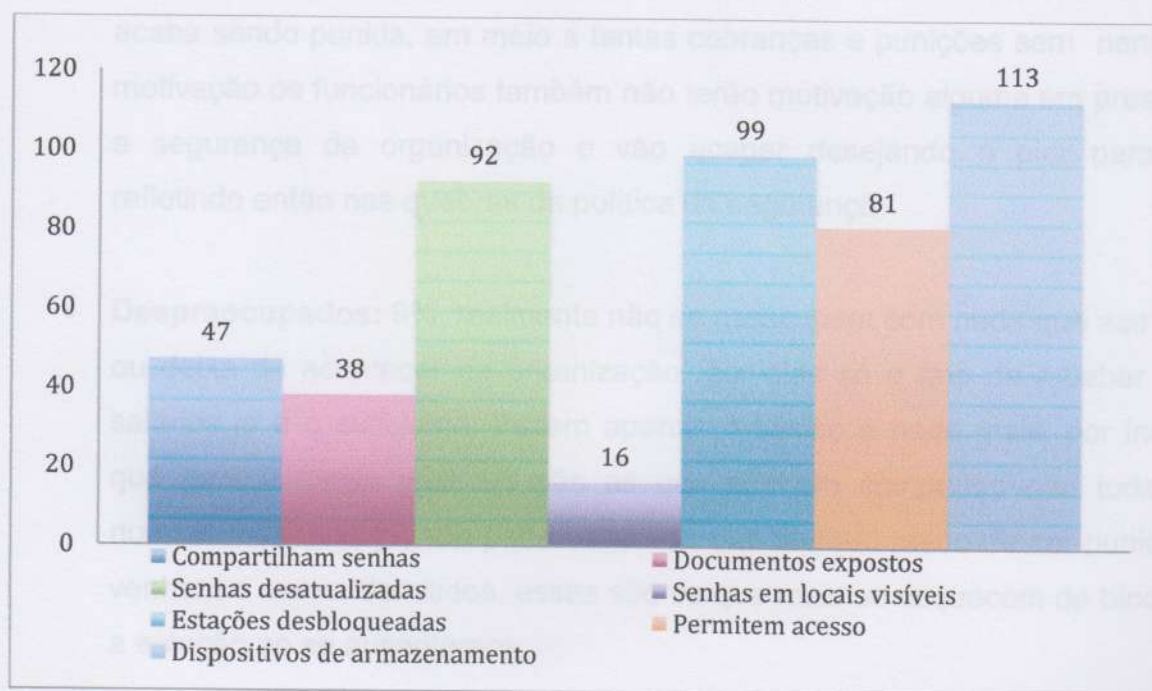
cima da mesa e na tentativa de uma segurança maior chegaram a colocar embaixo do teclado;

- **Compartilhamento de senhas:** 47 usuários foram observados informando suas senhas para terceiros, muitas das vezes com o propósito de repassar tarefas a eles incumbidas ou simplesmente com a finalidade de ajudar militares que não possuem acesso às estações de trabalho e por algum motivo necessitam do à rede;
- **Documentos expostos:** 38 usuários foram observados com documentos em cima da mesa e quando digitais desprotegidos no *desktop* ou em pastas de fácil acesso, mesmo com cada estação de trabalho contar com ferramenta de criptografia ela não era utilizada, onde por muitas vezes os documentos eram sigilosos;
- **Senhas desatualizadas:** 92 usuários foram observados utilizando a senha padrão de configuração inicial comum a todas as estações de trabalho, a qual deve ser mudada imediatamente após o recebimento da estação, onde se não for alterada mesmo com a estação bloqueada ainda estará vulnerável a acessos indevidos por terceiros, por se tratar de uma senha de conhecimento comum;
- **Estações desbloqueadas:** 99 usuários foram observados, que ao se ausentarem das estações de trabalho não as bloqueiam, muitas vezes pela correria do expediente ou por estarem realizando várias tarefas ao mesmo tempo, onde mesmo com a existência do bloqueio automático programado para 10 minutos ainda assim as estações estarão vulneráveis a acessos indevidos por terceiros, que quando mal intencionados podem facilmente infectar a estação com malwares, podendo contaminar toda a rede de computadores ou o roubo de informações valiosas;
- **Permitem acesso:** 81 usuários foram observados permitindo o acesso de outras pessoas as suas estações de trabalho, muitas vezes com o intuito de

ajuda-las ou de serem ajudados no cumprimento de alguma tarefa, mesmo tendo como objetivo apenas ajudar acabam pondo em risco a segurança da informação da mesma maneira decorrente do esquecimento do bloqueio das estações;

- **Dispositivos de armazenamento:** 113 usuários foram observados utilizando algum tipo de dispositivo de armazenamento, sendo sua grande maioria *pen drive* de uso pessoal o mesmo que é utilizado em outros computadores fora do ambiente computacional da OM, segundo Pereira (2010) a AVAST Software, empresa de *software* de segurança afirma em sua pesquisa que a cada oito ataques de *malware* um veio por dispositivo USB, isso equivale a 13,5% do total das infecções por *malware* no mundo.

Figura 6: Falhas mais comuns na Segurança da Informação



Fonte: Pesquisa do estudo de caso, 2012

3.3.2 Resultados das entrevistas

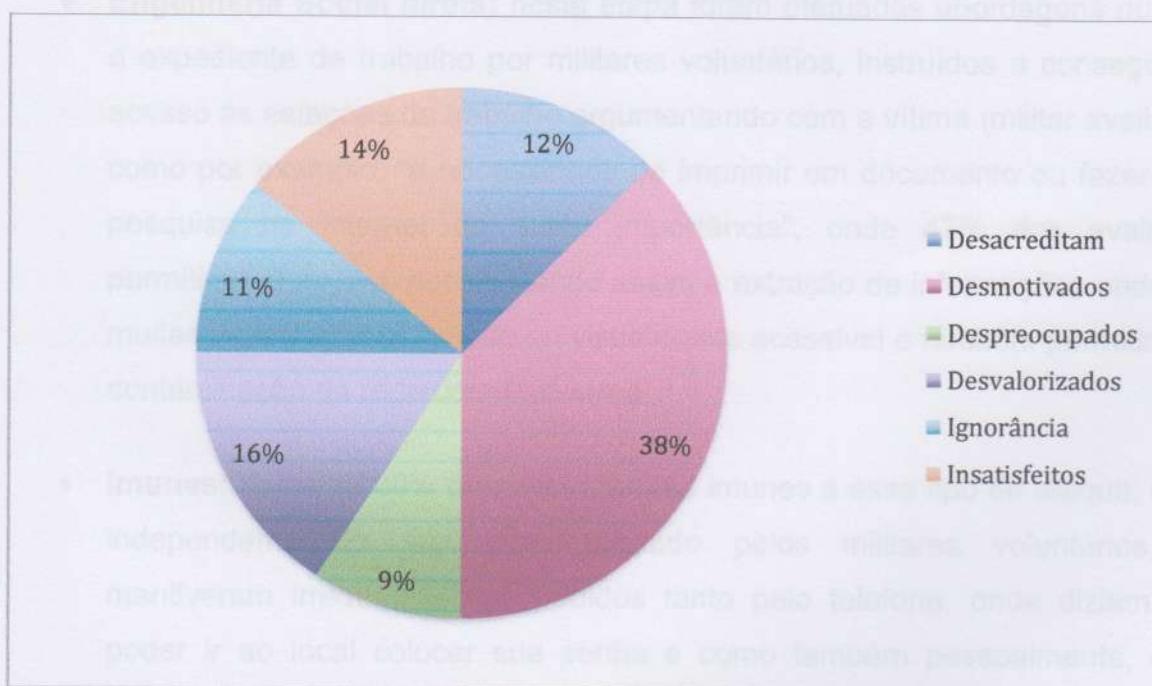
As entrevistas feitas ao longo deste ano foram executadas de acordo com o roteiro de perguntas do "ANEXO C", dissolvidas em meio a conversas casuais para evitar o temor de represaria dos entrevistados e buscar com isso respostas verdadeiras, possibilitando assim identificar os motivos os quais os levam a

descumprirem as normas da organização. Como resultado disso, obtiveram-se as seguintes causas:

- **Desacreditam na engenharia social:** 12%, simplesmente não acreditam que estão sujeitas a ser uma vítima de engenharia social, quando defrontadas com essa ideia durante a entrevistas agiam de forma irônica se referindo a essa possibilidade como uma piada, essas pessoas acabam se tornam as mais suscetíveis a ser uma vítima da engenharia social pelo fato de não se protegerem uma vez que não acreditam que possa acontecer com elas;
- **Desmotivados:** 38%, se sentem desmotivados por só receberem cobranças e punições, exemplificando na realização dos serviços incumbidos a uma certa pessoa, se a mesma o cumpri no prazo muitas vezes acaba sendo cobrada para fazer melhor e mais, se por acaso houver atraso a mesma acaba sendo punida, em meio a tantas cobranças e punições sem nenhuma motivação os funcionários também não terão motivação alguma em preservar a segurança da organização e vão acabar desejando o pior para ela, refletindo então nas quebras da política de segurança;
- **Despreocupados:** 9%, realmente não se preocupam com nada que acontece ou deixa de acontecer na organização, por elas só o fato de receber seus salários já é o suficiente. Fazem apenas o básico e nada mais, por incrível que parece essas pessoas são as que acabam cumprindo não todas as normas mas uma grande parte, uma vez que tenham medo de ser punidas e venham a serem demitidos, esses são os que mais se esquecem de bloquear a estação ao se ausentarem;
- **Desvalorizados:** 16%, se sentem desvalorizados pela falta de reconhecimento durante sua carreira, onde muitos por pouco são beneficiados e poucos por muito não são, causando grandes frustrações para o funcionário e o impedindo de dar o seu melhor pela OM uma vez o qual a OM não reconhece seu esforço, refletindo assim no descumprimento da política de segurança da organização;

- **Ignorância:** 11%, demonstraram pouco conhecimento sobre o ambiente computacional, de maneira a qual os tornam suscetíveis a ataque provido da engenharia social por serem facilmente lubrificados devido ao pouco conhecimento acabam acreditando nas afirmações e pedidos do engenheiro, entregando assim senhas e informações importantes, como será demonstrada na seção 3.3.3;
- **Insatisfeitos:** 14%, declararam estar insatisfeito com a carreira profissional decorrente dos pontos mencionados acima, esses funcionários acabam sendo os maiores riscos para a segurança, como afirma Valle e Ulbrich (2009 p. 127) “explorar a fragilidade de pessoas insatisfeitas com as condições de trabalho é muito mais simples do que podemos imaginar”, dessas pessoas é possível conseguir informações sigilosas e até mesmo o apoio para atacar.

Figura 7: Motivos que contribuem para falhas de segurança



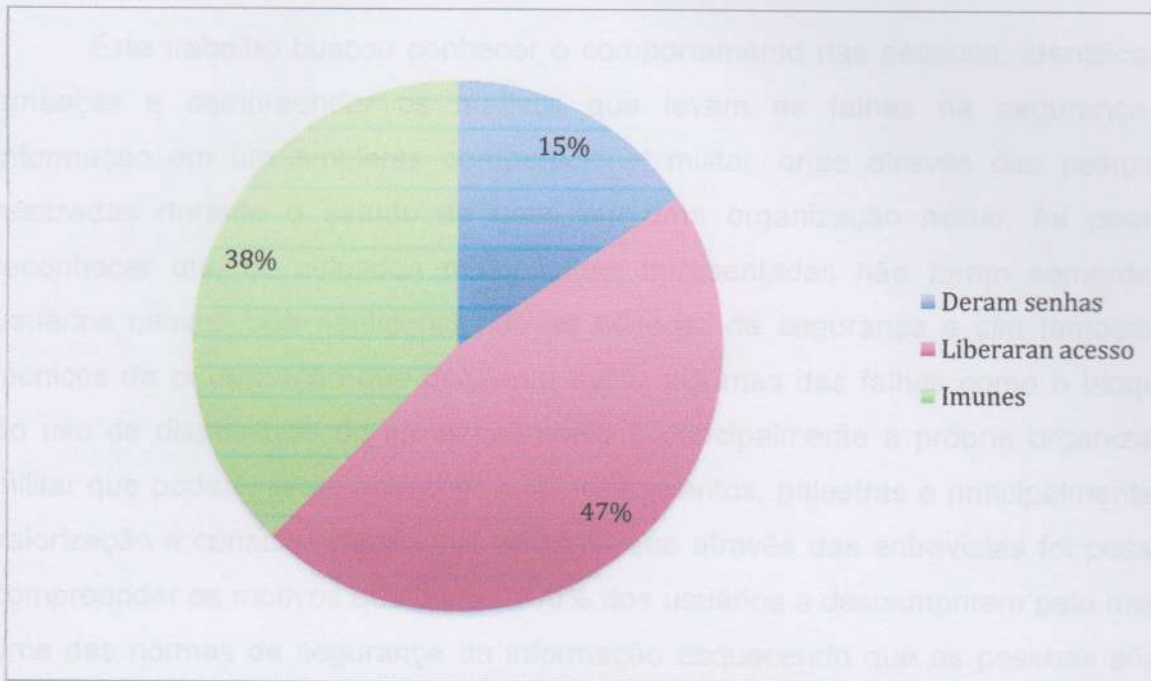
Fonte: Pesquisa do estudo de caso, 2012

3.3.3 Resultados do teste

E por fim, foram testados 90 militares dos 120 que possuem acesso direto as estações de trabalho, utilizando para isso a engenharia social onde não foi possível executar o teste em 100% dos militares por motivos de acessibilidade aos demais. Foram executados os seguintes testes:

- **Engenharia Social indireta:** se utilizando da telefonia foram realizadas ligações por militares voluntários, instruídos a se passarem por um dos técnicos da OM, tendo como argumento a necessidade de saberem a senha de acesso da vítima (militar avaliado), como por exemplo, “a realização do teste de um sistema de manutenção via rede que necessita da senha da vítima”, mesmo que alguns tenham demonstrado algum tipo de resistência 15% dos avaliados acabaram entregando suas senhas.
- **Engenharia Social direta:** nesta etapa foram efetuadas abordagens durante o expediente de trabalho por militares voluntários, instruídos a conseguirem acesso às estações de trabalho argumentando com a vítima (militar avaliado), como por exemplo, “a necessidade de imprimir um documento ou fazer uma pesquisa na internet de suma importância”, onde 47% dos avaliados permitiram o acesso possibilitando assim a extração de informações onde por muitas vezes de fácil acesso ou visualmente acessível e também permitindo a contaminação da rede com *malwares*.
- **Imunes:** somente 38% demonstraram-se imunes a esse tipo de ataque, onde independente do argumento utilizado pelos militares voluntários, se mantiveram irredutíveis aos pedidos tanto pelo telefone, onde diziam que poder ir ao local colocar sua senha e como também pessoalmente, onde alegaram não ser permitido pela política de segurança da OM que não permite o acesso as estações pelo pessoal não autorizado.

Figura 8: Resultados da Engenharia Social empregada



Fonte: Pesquisa do estudo de caso, 2012

É natural para o ser humano confiar em seus colegas, principalmente quando o pedido passa no teste como sendo razoável, os engenheiros sociais usam esse conhecimento para explorar suas vítimas e atingir seus objetivos onde diante a engenharia social segundo Mitnick (2003, p. 3) “os indivíduos podem seguir cada uma das melhores práticas de segurança recomendadas pelos especialistas, podem instalar cada produto de segurança recomendado e vigiar muito bem a configuração adequada do sistema e a aplicação das correções de segurança. Esses indivíduos ainda estarão completamente vulneráveis.”

4 CONCLUSÃO

Este trabalho buscou conhecer o comportamento das pessoas, identificar as ameaças e compreender os motivos que levam as falhas na segurança da informação em um ambiente computacional militar, onde através das pesquisas realizadas durante o estudo de caso em uma organização militar, foi possível reconhecer que os culpados pelas falhas apresentadas não foram somente os usuários mesmo que negligenciando as políticas de segurança e sim também os técnicos da organização que poderiam evitar algumas das falhas como o bloqueio do uso de dispositivos de armazenamento e principalmente a própria organização militar que poderia facilmente promover treinamentos, palestras e principalmente na valorização e conscientização dos militares que através das entrevistas foi possível compreender os motivos que levam 100% dos usuários a descumprirem pelo menos uma das normas de segurança da informação esquecendo que as pessoas são “o fator determinante para o sucesso ou fracasso do processo de segurança da informação em uma organização” (FONTES, 2009).

Diante de um quadro deste, onde 100% dos funcionários quebram pelo menos uma regra da política de segurança de modo a inutilizar todo o investimento em equipamentos empregados na segurança da informação, onde “o esquecimento de um único ponto, faz com que os esforços dispensados na segurança dos outros pontos sejam em vão” (NAKAMURA; GEUS 2010, p. 27).

Com base nos resultados obtidos podemos então concluir que para se atingir uma boa segurança da informação seja no ambiente militar ou civil não basta apenas investir em equipamento caros de segurança deve-se primeiro conhecer as fraquezas das pessoas envolvidas no ambiente computacional para que assim possam ser tratadas da melhor forma possível, pelo fato das pessoas serem o elo mais fraco da segurança da informação.

FONTES, E. Dez falhas em segurança da informação. Disponível em: <http://redesofontes.blogspot.com.br/2009/05/01-2009-05-31-Acesso-em-15-dez-2012>.

GOODCHILD, J. Engenharia Social: porque ainda não é o elo mais fraco. In: *especialista*. - IGGNOW UOL. - São Paulo. 2010. Disponível em: <http://iggnow.uol.com.br/seguranca/2010/05/25/engenharia-social-porque-ainda-nao-e-lo-mais-fraco-especialista-1-Acesso-em-25-dez-2012>.

REFERÊNCIAS BIBLIOGRÁFICAS

ALVES, C. B. **Segurança da Informação VS. Engenharia Social: Como se proteger para não ser mais uma vítima**. 2010. 61 p. Artigo apresentado ao Centro Universitário do Distrito Federal para a obtenção do grau de bacharel em Sistema de Informação Disponível em: http://www.administradores.com.br/_resources/files/_modules/academics/academics_3635_20101207234707794d.pdf. Acessado em: 2 nov. 2012.

AMOROSO, D. **Aprenda as diferenças entre vírus, trojans, spywares e outros: nem todos os arquivos que prejudicam seu PC são vírus**. Disponível em: <http://www.tecmundo.com.br/phishing/853-aprenda-as-diferencas-entre-virus-trojans-spywares-e-outros.htm#ixzz2COJ1jJiW>. Acessado em: 12 out. 2012.

ANDER-EGG, E. **Introducción a las técnicas de investigación social – para trabajadores sociales**. 7. Ed. Buenos Aires: Humanitas, 1978.

BARWINSKIEM, L. **O que é rootkit?**. Tecmundo, junho de 2009. Disponível em: <http://www.tecmundo.com.br/antivirus/2174-o-que-e-rootkit-.htm>. Acessado em: 11 out. 2012.

CERT.br. **Cartilha de Segurança para Internet, versão 4.0**. 2 ed. São Paulo: Comitê Gestor da Internet no Brasil, 2012a. 126 p. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acessado em: 08 out. 2012.

CERT.br. **Incidentes reportados ao CERT.br: Julho a Setembro de 2012**. [S.l.]: Nucleo de Informação e Coordenação do Ponto BR, 2012b. Disponível em: <http://www.cert.br/stats/incidentes/2012-jul-sep/ataques-mensal.html>. Acessado em: 1 out. 2012.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Spam**. Disponível em: <http://www.antispam.br/>. Acessado em: 12 out. 2012.

EINA, N. **A história da Internet: pré-década de 60 até anos 80**. Disponível em: <http://www.tecmundo.com.br/infografico/9847-a-historia-da-internet-pre-decada-de-60-ate-anos-80-infografico-.htm>. Acessado em: 11 out. 2012.

FERREIRA, F. N. F.; ARAÚJO, M. T. **Política de segurança da informação: guia prático para elaboração e implementação**. 2. ed. Rio de Janeiro: Ciência Moderna, 2008.

FONTES, E. **Dez falhas em segurança da informação**. Disponível em: http://edison.fontes.blog.uol.com.br/arch2009-05-01_2009-05-31. Acessado em: 16 out. 2012.

GOODCHILD, J. **Engenharia Social: pessoas ainda são o elo mais fraco, diz especialista**. IDGNOW UOL, São Paulo, 2010 Disponível em: <http://idgnow.uol.com.br/seguranca/2010/05/25/engenharia-social-pessoas-ainda-sao-elo-mais-fraco-diz-especialista/#&panel2-1>. Acessado em: 29 out. 2012.

HONEYCUTT, J. **Usando a Internet**. Tradução de Edson Furmankiewicz, 3. ed. Rio de Janeiro: Campos, 1998.

INTERNATIONAL TELECOMMUNICATION UNION. **Statistics**. Disponível em: <http://www.itu.int/ITU-D/ict/statistics/>. Acessado em: 06 nov. 2012.

JERUSALÉM, M. N. **A internet é um barril de pólvora**. Disponível em: <http://www1.folha.uol.com.br/ilustrissima/1127046-a-internet-e-um-barril-de-polvora.shtml>. Acessado em: 10 out. 2012.

LAURENTINO, A. **Hacker x Cracker: Quem é quem?**. Disponível em: <http://technoguia.info/tecnologia/hacker-x-cracker-quem-e-quem/>. Acessado em: 08 out 2012.

LESKE, N. **Trafego da Internet crescerá 29% até 2016**. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/trafego-de-protocolo-de-internet-crescera-29-ate-2016-cisco>. Acessado em: 10 out. 2012.

LUIZ, A P. **Site revela tamanho atual do arquivo com todo o conteúdo da internet**. Disponível em: <http://www.tecmundo.com.br/internet/31932-site-revela-tamanho-atual-do-arquivo-com-todo-o-conteudo-da-internet.htm>. Acessado em: 11 out. 2012.

MARCELO, A.; PEREIRA, M. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MARCONE, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica**. 7. ed. São Paulo: Atlas, 2010.

MITNICK, K. D.; SIMON, W. L. **A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação**. Pearson Education. São Paulo, 2003.

MITNICK, K. D.; SIMON, W. L. **A arte de invadir: as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos**. Pearson Prentice Hall. São Paulo, 2005.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de redes em ambientes cooperativos**. São Paulo: Novatec, 2007.

PEIXOTO, M. C. P. **Engenharia social e segurança da informação na gestão corporativa**. Rio de Janeiro: Brasport, 2006.

PEREIRA, A. P. **A cada oito ataques de malware, um veio por dispositivo USB**. Disponível em: <http://www.tecmundo.com.br/pendrive/6331-a-cada-oito-ataques-de-malware-um-veio-por-dispositivo-usb.htm>. Acessado em: 10 set. 2012.

PRESCOTT, R. **Fator humano: um dos pilares da segurança da informação**. Disponível em: <http://itweb.com.br/29599/fator-humano-um-dos-pilares-da-seguranca-da-informacao>. Acessado em: 12 out. 2012.

SANTOS, L. A. L. **O impacto da engenharia social na segurança da informação**. 2004. 82 f. Monografia (Especialização)– Universidade Tiradentes, Aracaju, 2004. Disponível em: http://dc357.4shared.com/doc/Ue_esMiB/preview.html. Acesso em: 8 out. 2012.

SILVA, Maicon H. L. F. da; COSTA, V. A. de S. F. **O fator humano como pilar da Segurança da Informação: uma proposta alternativa**. Serra Talhada (PE), 2009. Disponível em: www.eventosufrpe.com.br/jeplex2009/cd/resumos/R0052-3.pdf. Acesso em: 30 out. 2012.

SILVA, Maicon H. L. F.; COSTA, V. A. S. F. O fator humano como pilar da Segurança da Informação: uma proposta alternativa. **IX Jornada de Ensino Pesquisa e Extensão da UFRPE, 2009**. Disponível em: <http://www.eventosufrpe.com.br/jeplex2009/cd/resumos/R0052-3.pdf>. Acesso em: 10 out. 2012.

SITES governamentais são os mais atacados no espaço cibernético, alerta ministro. 2010. Disponível em: <http://www.sae.gov.br/site/?p=3436>. Acessado em: 5 nov. 2012.

ULBRICH, H. C.; VALLE, J. D. **Universidade Hacker: desvende todos os segredos do submundo dos hackers**. 6. ed. São Paulo: Gigerati Books, 2009.

UOL. **O que são vírus de computador?**. Disponível em: <http://antivirus.uol.com.br/quais-sao-os-tipos-de-virus.html>. Acessado em: 11 out 2012.

ANEXO A – ☐ MODELO DO TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

(NOME DA ORGANIZAÇÃO MILITAR)

TERMO DE RECEBIMENTO DE ESTAÇÃO DE TRABALHO

(Local: cidade), _____ de _____ de _____

Pelo presente instrumento, eu, _____ (nome **completo**, **NIP** ou **no da identidade**), perante a Força Armada X, doravante denominada X, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro ter recebido desta OM** uma estação de trabalho com as seguintes configurações:

I – de identificação:

- a) **endereço IP:** (especificar o endereço IP da máquina);
- b) **endereço físico de rede:** (especificar a identificação exclusiva da placa de rede da máquina); e
- c) **identificação da máquina:** (especificar o nome e outros dados de identificação da máquina).

II – de instalação de programas:

- a) (especificar cada um dos programas pré-instalados);
- b) ...

III – de senha de acesso à máquina (“boot”), inicialmente estabelecida pelo Administrador da Rede Local (ADMIN) da OM e por mim alterada, sendo agora de meu conhecimento exclusivo; e

IV – de senha de configuração (“setup”), de conhecimento exclusivo do ADMIN e à qual não devo tomar conhecimento.

Assim, quaisquer alterações ou inclusões nos dados acima são de minha inteira responsabilidade e devem ser previamente autorizadas pelo Oficial de Segurança das Informações Digitais (OSID), conforme previsto nas normas de Segurança das Informações Digitais da OM.

Estou ciente que o ADMIN (executou / **não executou**) a “formatação” prévia dos discos rígidos da referida estação de trabalho e sua correspondente reconfiguração e que, a qualquer momento e sempre que julgar necessário, poderei solicitar ao ADMIN auxílio para a realização dessa “formatação”, de modo a garantir a configuração padronizada da OM e a inexistência de arquivos ou programas irregulares.

Assinatura

Nome Completo, NIP ou no da identidade

ANEXO B – MODELO DO TERMO DE RESPONSABILIDADE INDIVIDUAL**(NOME DA ORGANIZAÇÃO MILITAR)****TERMO DE RESPONSABILIDADE INDIVIDUAL**

(Local: cidade), ____ de ____ de ____

Pelo presente instrumento, eu, (nome **completo, NIP ou no da identidade**), perante a Força Armada X, doravante denominada X, na qualidade de usuário do ambiente computacional de propriedade daquela Instituição, **declaro estar ciente** das normas de segurança das informações digitais da OM, segundo as quais devo:

- a) tratar a informação digital como patrimônio da X e como um recurso que deva ter seu sigilo preservado, em consonância com a legislação vigente;
- b) utilizar as informações disponíveis e os sistemas e produtos computacionais, dos quais a X é proprietária ou possui o direito de uso, exclusivamente para o interesse do serviço;
- c) preservar o conteúdo das informações sigilosas a que tiver acesso, sem divulgá-las para pessoas não autorizadas;
- d) não tentar obter acesso à informação cujo grau de sigilo não seja compatível com a minha Credencial de Segurança (CREDSEG) ou que eu não tenha autorização ou necessidade de conhecer;
- e) não compartilhar o uso de senha com outros usuários;
- f) não me fazer passar por outro usuário usando a sua identificação de acesso e senha;
- g) não alterar o endereço de rede ou qualquer outro dado de identificação do microcomputador de meu uso;
- h) instalar e utilizar em meu microcomputador somente programas homologados para uso na X e que esta possua as respectivas licenças de uso ou, no caso de programas de domínio público, mediante autorização formal do Oficial de Segurança de Informações Digitais (OSID) da OM;
- i) no caso de exoneração, demissão, licenciamento, término de prestação de serviço ou qualquer tipo de afastamento, preservar o conteúdo das informações e documentos sigilosos a que tive acesso e não divulgá-los para pessoas não autorizadas;
- j) guardar segredo das minhas autenticações de acesso (senhas) utilizadas no ambiente computacional da OM, não cedendo, não transferindo, não divulgando e não permitindo o seu conhecimento por terceiros;
- k) não utilizar senha com seqüência fácil ou óbvia de caracteres que facilite a sua descoberta e não escrever a senha em lugares visíveis ou de fácil acesso;
- l) utilizar, ao me afastar momentaneamente da minha estação de trabalho, descanso de tela (“screen saver”) protegido por senha, a fim de evitar que alguém possa ver as informações

que estejam disponíveis na tela do computador;

- m) ao me ausentar do local de trabalho, momentaneamente ou ao término de minhas atividades diárias, certificar-me de que a sessão aberta no ambiente computacional com minha identificação foi fechada e as informações que exigem sigilo foram adequadamente salvaguardadas;
- n) seguir as orientações da área de informática da OM relativas à instalação, à manutenção e ao uso adequado dos equipamentos, dos sistemas e dos programas do ambiente computacional;
- o) comunicar imediatamente ao meu superior hierárquico e ao Oficial de Segurança das Informações Digitais (OSID) da OM a ocorrência de qualquer evento que implique ameaça ou impedimento de cumprir os procedimentos de segurança estabelecidos;
- p) responder, perante a X, as auditorias e o Oficial de Segurança das Informações Digitais (OSID) da OM, por acessos, tentativas de acessos ou uso indevido da informação digital realizados com a minha identificação ou autenticação;
- q) não praticar quaisquer atos que possam afetar o sigilo ou a integridade da informação;
- r) estar ciente de que toda informação digital armazenada e processada no ambiente computacional da OM pode ser auditada, como no caso de páginas informativas ("sites") visitadas por mim;
- s) não transmitir, copiar ou reter arquivos contendo textos, fotos, filmes ou quaisquer outros registros que contrariem a moral, os bons costumes e a legislação vigente;
- t) não transferir qualquer tipo de arquivo que pertença à X para outro local, seja por meio magnético ou não, exceto no interesse do serviço e mediante autorização da autoridade competente;
- u) estar ciente de que o processamento, o trâmite e o armazenamento de arquivos que não sejam de interesse do serviço são expressamente proibidos no ambiente computacional da OM;
- v) estar ciente de que a X poderá auditar os arquivos em trâmite ou armazenados nos equipamentos do ambiente computacional da OM sob meu uso ou responsabilidade;
- w) estar ciente de que o correio eletrônico é de uso exclusivo para o interesse do serviço e qualquer correspondência eletrônica originada ou retransmitida no ambiente computacional da OM deve obedecer a este preceito; e
- x) estar ciente de que a X poderá auditar as correspondências eletrônicas originadas ou retransmitidas por mim no ambiente computacional da OM.

Desta forma, estou ciente da minha responsabilidade pelas conseqüências decorrentes da não observância do acima exposto e da legislação vigente.

Assinatura

Nome Completo, NIP ou no da identidade

ANEXO C – ROTEIRO DE PERGUNTAS PARA AS ENTREVISTAS

1. Já fez algum curso de informática?
2. Tem conhecimento sobre os programas de segurança instalados na estação de trabalho? Sabe usá-los?
3. Já assistiu alguma palestra sobre os programas de segurança existentes?
4. Conhece os riscos da internet?
5. Sabe o que é engenharia social?
6. Já assistiu alguma palestra sobre segurança da informação?
7. Acredita ser possível alguém tentar prejudicar a rede da OM?
8. Existe alguma motivação para trabalhar?
9. Se preocupa com a segurança da informação?
10. Existe reconhecimento pelos serviços prestados?
11. Está satisfeito com esta Força Armada?